NASCIO

ENTERPRISE ARCHITECTURE DEVELOPMENT TOOL-KIT

October 2004 v3.0

Acknowledgements

NASCIO would like to thank the members of the Architecture Working Group for their contributions to this effort.

Updates of this Tool-Kit and other NASCIO Architecture Program deliverables are funded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, under Grant No. 98-DD-BX-0067.

The opinions, findings, conclusions and recommendations contained in this publication are those of NASCIO, and do not necessarily reflect the official positions or policies of the Bureau of Justice Assistance or the Department of Justice.

For more information contact:
NASCIO
167 W. Main Street, Suite 600
Lexington, Kentucky 40507-1324
Phone: 859.514.9153
Fax: 859.514.9166
Email: nascio@amrinc.net
Website: www.nascio.org

NASCIO
Representing Chief Information Officers of the States

October 4, 2004

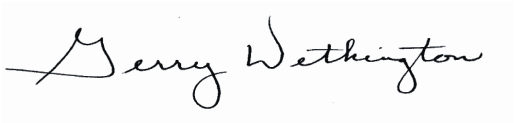
State governments are complex organizations with a host of business processes that need to be supported by the capabilities of information technology. Enterprise architecture can be described as an operating discipline comprised of frameworks, methodologies, and delivery processes that can be leveraged to manage the complexities of government. Enterprise architecture can ultimately guide investments in business and technology solutions insuring these solutions are appropriately aligned with business needs. The Chief Information Officer must demonstrate leadership in the area of enterprise architecture as part of their expanding role.

Enterprise architecture is a blueprint for better government providing a holistic, comprehensive view of the governmental enterprise encompassing strategic business intent and the capabilities that enable that intent. Capabilities include business processes, organizational structure and dynamics, and information technology. This "enterprise" view is necessary in order to effectively manage change and complexity.

Government is continually striving to deliver quality services effectively to its citizens. Government must also maintain the ability to meet the continually rising expectations of taxpayers. Citizens hold state government accountable to meet these expectations. State government can successfully respond through well planned, and well executed processes for delivering effective business and technological solutions.

Version 3.0 of the NASCIO Enterprise Architecture Tool-Kit is part of a portfolio of products and services provided by NASCIO to assist the states in the development of their frameworks, methodologies, programs, and projects for delivering quality business and technology solutions. This Tool-Kit presents approaches to various architectures without being prescriptive. The reader should make adaptations to the material presented based on their specific needs.

On behalf of NASCIO, we extend our thanks to the members of the Architecture Working Group (AWG) for their contributions to this version of the Tool-Kit. Products like this are only possible with the involvement of our members.



Gerry Wethington
Chair NASCIO Architecture Working Group
Chief Information Officer
Office of Information Technology
State of Missouri

Doug Robinson
Executive Director
NASCIO

NASCIO EA Development Tool-Kit

Introduction
&
Architecture Governance

Version 3.0

October 2004

TABLE OF CONTENTS

PREFACE

About NASCIO

The National Association of State Chief Information Officers (NASCIO) represents state chief information officers and information resource executives and managers from the 50 states, six U.S. territories, and the District of Columbia. State members are senior officials from any of the three branches of state government who have executive-level and statewide responsibility for information resource management. Representatives from federal, municipal, and international governments and state officials who are involved in information resource management but do not have chief responsibility for that function participate in the organization as associate members. Private-sector firms and non-profit organizations participate as corporate members.

The mission of the association is foster excellence in government.

MISSION

NASCIO's mission is to foster government excellence through quality business practices, information management, and technology policy.

VISION

NASCIO's vision is government in which the public trust is fully served through the efficient and effective use of technology.

HISTORY OF THE ASSOCIATION

The association was founded as the National Association of State Information Systems or NASIS. In 1989, the membership voted to undertake a major realignment for the association, including a change in name to the National Association of State Information Resource Executives, and an expansion of membership. The association name changed to the National Association of State Chief Information Officers in 2001 as a reflection of the executive-level roles of the state members. All of the changes were aimed at providing NASCIO members with the information they need to meet their growing responsibilities.

ABOUT THE ARCHITECTURE PROGRAM

The Adaptive Enterprise Architecture Development Program is a program funded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, under Grant No. 98-DD-BX-0067, and awarded to NASCIO. In 1998, when the program began, few states considered the importance of enterprise architecture in the provision of services. However, following publication in February 2000 of the NASCIO report, "Toward National Sharing of Governmental Information", a national call for architecture was made. As recommended in 1998 by the Office of Justice Programs and identified as critical in the report findings, NASCIO developed an enterprise architectural framework for government information systems integration.

Adaptive enterprise architecture effectively supports the business of government, enables information sharing across traditional barriers, enhances government's ability to deliver effective and timely services, and supports agencies in their efforts to improve government functions. Enterprise architecture supports the identification and optimization of the entity's interrelated business processes and resulting IT systems. The enterprise architecture promotes a constant re-evaluation of enterprise needs and is the best way to build an adaptive enterprise-wide architecture.
The NASCIO Architecture Program and this Enterprise Architecture Development Tool-Kit guide agencies at all levels of government in the definition, development, utilization, maintenance, and institutionalization of an enterprise architecture program supported by stakeholders of all levels, from the executive to the citizen user.

For more information on the NASCIO Adaptive Enterprise Architecture Development Program please visit the NASCIO website at www.nascio.org.

Acknowledgements

NASCIO Officers and Directors 2004-2005

OFFICERS			
President	Tom Jarrett Chief Information Officer State of Delaware	Department of Technology and Information William Penn Building 801 Silver Lake Blvd Dover, DE 19904-2407	Tel: 302-739-9629 Fax: 302-739-1442 thomas.jarrett@state.de.us
Vice President	Matthew Miszewski Chief Information Officer State of Wisconsin	Division of Enterprise Technology Department of Administration 101 E. Wilson Street, 8th Floor P.O. Box 7844 Madison, WI 53707-7844	Tel: 608-264-9502 Fax: 608-267-0626 matthew.miszewski@doa.state.wi.us
Secretary/Treasurer	W. Val Oveson Chief Information Officer State of Utah	Governor's Office Utah State Capitol Complex East Office Building, Suite E220 P.O. Box 142220 Salt Lake City, UT 84144	Tel: 801-538-1505 Fax: 801-538-1557 valoveson@utah.gov
Past President	Gerry Wethington Chief Information Officer State of Missouri	Truman Building, Room 840 301 West High St Jefferson City, MO 65101	Tel: 573-526-7741 Fax: 573-526-7747 wethig@mail.oit.state.mo.us

DIRECTORS		
James T. Dillon Chief Information Officer State of New York	New York State Office for Technology State Capitol Empire State Plaza P.O. Box 2062 Albany, NY 12220-0062	Telephone: 518-474-3421 James.Dillon@cio.state.ny.us
Otto Doll Chief Information Officer and Commissioner State of South Dakota	Bureau of Information and Telecommunications Kneip Building 700 Governors Drive Pierre, SD 57501	Telephone: 605-773-5110 otto.doll@state.sd.us
John Gillispie Chief Operating Officer State of Iowa	Information Technology Enterprise Department of Administrative Services Hoover Building Level B Des Moines, IA 50319	Telephone: 515-281-3462 john.gillispie@iowa.gov
Greg Jackson Chief Information Officer and Director State of Ohio	Office of Information Technology 30 East Broad Street 40th Floor Columbus, OH 43215-3414	Telephone: 614-644-6446 greg.jackson@ohio.gov
Terry Savage Chief Information Officer and Director State of Nevada	Department of Information Technology 505 E. King Street Suite 403 Carson City, NV 89701	Telephone: 775-684-5800 tsavage@doit.nv.gov
Teresa Takai Chief Information Officer and Director State of Michigan	Department of Information Technology Landmark Building Suite 200 105 West Allegan Street Lansing, MI 48933	Telephone: 517-373-1006 takait@michigan.gov
Dick Thompson Chief Information Officer State of Maine	Department of Administrative and Financial Services 173 State House Station Augusta, ME 04333-0173	Telephone: 207-624-7568 richard.b.thompson@maine.gov
Tom Wade Chief Information Officer and Executive Director State of Georgia	Georgia Technology Authority 100 Peachtree Street. Suite 2300 Atlanta, GA 30303-1913	Telephone: 404-463-2340 twade@gta.gov

CORPORATE LEADERSHIP COUNCIL REPRESENTATIVE		
Pat Cummens	Environmental Systems Research Institute 880 Blue Gentian Road, Suite 200 St. Paul, MN 55121	Telephone: 651-454-0600 pcummens@esri.com

FEDERAL CIO COUNCIL REPRESENTATIVE		
Hord Tipton Chief Information Officer	U.S. Department of the Interior 1849 C Street, NW Washington, DC 20240-0002	Telephone: 202-208-6194 hord_tipton@ios.doi.gov

ARCHITECTURE WORKING GROUP MEMBERS 2004-2005

Gerry Wethington *Chair*	Chief Information Officer	Office of Information Technology State of Missouri
Doug Elkins V*ice Chair*	Executive Chief Information Officer	Department of Information Systems State of Arkansas
John Carey Brown	Information Resource Manager	Division of IS & Communications State of Kansas
Chris Clark	Director, Division of Enterprise Architecture	Commonwealth Office of Technology Commonwealth of Kentucky
Pat Cummens		Environmental Systems Research Institute, Inc. St. Paul, Minnesota
Matthew D'Alessandro	Business Development Manager	Motorola
Dr. Dale Good	Director, Justice Information Technology Services	SEARCH
Alan Grose		Microsoft
Lynn Hadden	Senior Web Architect	Department of Information Technology Fairfax County, Virginia
Nelson Hill	Chief Information Officer	Florida Department of Transportation State of Florida
Stephen Newell	Lead IT Planning and Research Analyst	IBM
Kym Patterson	Manager, Technical Architecture	Office of Information Technology State of Arkansas
Paul Piper	Senior Policy Advisor	Department of Information Services State of Washington
Mike Ryan	Chief Information Architect	Office of Technology State of Minnesota
Chaed Smith	Senior Technology Officer	Governor's Office of Technology State of West Virginia
Alan H. Treiber, Ph.D.		IT Architecture Division State of Connecticut
Barry Van Sant	Vice President, iTEAM Consulting Group	Ciber

Jennifer Witham	IT Business Analyst	Policy and Planning Division State of North Dakota
Nancy Walz	Director, Policy and Planning Division	Policy and Planning Division State of North Dakota

TOOL-KIT REVIEWERS

Jim Bivona	Chief Information Officer	Wyoming Supreme Court State of Wyoming
John Carey Brown	Information Resource Manager	Division of IS & Communications State of Kansas
Chris Clark	Director, Division of Enterprise Architecture	Commonwealth Office of Technology Commonwealth of Kentucky
Pat Cummens	State Government – Special Projects	ESRI
Matt D'Allessandro	Business Development Manager	Motorola
Mark Griffith	Senior Enterprise Architect	Enterprise Technology Strategies Office State of North Carolina
Lynn Hadden	Senior Web Architect	Department of Information Technology Fairfax County, Virginia
Amir Holmes	Justice Information System Specialist	SEARCH
Claude Johnson	Director, Strategic Services Division	Department of Information Technology Services State of Mississippi
Jake Moelk	Systems Consultant	Information Technology Oversight Committee State of Indiana
Steve Newell	Information Technology Architect	IBM
Kym Patterson	Manager, Technical Architecture	Office of Information Technology State of Arkansas
Bill Roth	Chief Architect	Kansas Information Technology Office State of Kansas
Mike Ryan	Chief Information Architect	Office of Technology State of Minnesota
Jennifer Witham	IT Business Analyst	Policy and Planning Division State of North Dakota

ARCHITECTURE WORKING GROUP ASSOCIATE MEMBERS 2004-2005

John Clark	Program Director	General Services Administration Office of Citizens Services
Scott Fairholm	Director of Court Technology	National Center for State Courts Technology Division
Bob Greeves	Policy Advisor	U.S. Department of Justice Office of Justice Programs
Dustin Koonce	Policy Advisor	U.S. Department of Justice Office of Justice Programs
Patrick McCreary	Policy Advisor	U.S. Department of Justice Office of Justice Programs

NASCIO STAFF

Doug Robinson	Executive Director	Telephone: 859-514-9171 drobinson@amrinc.net
Jack Gallt	Assistant Director	Telephone: 859-514-9212 jgallt@amrinc.net
Vince Havens	Program Manager	Telephone: 859-514-9215 vhavens@amrinc.net
Eric Sweden	Chief Enterprise Architect	Telephone: 859-514-9189 esweden@amrinc.net
Beth Roszman	Communications & Programs Coordinator	Telephone: 859-514-9167 broszman@amrinc.net
Chris Dixon	Digital Government Issues Coordinator	Telephone: 859-514-9148 cdixon@amrinc.net
Mary Gay Whitmer	Issues Coordinator	Telephone: 859-514-9209 mwhitmer@amrinc.net
Drew Leatherby	Emerging Issues Coordinator	Telephone: 859-514-9187 dleatherby@amrinc.net
Ashley Sinclair	Membership & Development Coordinator	Telephone: 859-514-9168 asinclair@amrinc.net
Robert Hansel	Project Associate	Telephone: 859-514-9179 rhansel@amrinc.net

NASCIO HEADQUARTERS

National Association of State Chief Information Officers	167 West Main Street, Suite 600 Lexington, KY 40507-1324	Telephone: 859-514-9153 Fax: 859-514-9166 www.nascio.org

ARCHITECTURE WORKING GROUP CONTRACTORS AND CONSULTANTS

John Curley	Project Manager	Ciber, Inc.
Jean Bogue	Senior Architect/Project Lead	Ciber, Inc.
Max Alderson	Senior Architect	Ciber, Inc.
Maria Archuleta	Documentation Specialist	Ciber, Inc.
Dianna Dees	Senior Architect	Ciber, Inc.
Tannia Dobbins	Senior Architect	Ciber, Inc.
Norma Lockner	Architect	Ciber, Inc.
Jeannine Menefee	Architect	Ciber, Inc.
Karla Werkman	Architect	Ciber, Inc.
David J. Roberts	Deputy Executive Director	SEARCH, The National Consortium for Justice Information and Statistics

Audience for Tool-Kit Sections

The Tool-Kit addresses Architecture Governance, Business, Information, Technology and Solution Architectures.

The ***Introduction*** section of the Enterprise Architecture Development Tool-Kit provides information that will be of interest to anyone desiring an overview of the importance of enterprise architecture, an introduction to the enterprise architecture concepts and terms or a general perspective of the topics covered within this Tool-Kit. The remainder of the Tool-Kit is dedicated to the development of the architectures.

The section on ***Architecture Governance*** will be of particular interest to those who currently guide or manage the organization's enterprise architecture or will do so in the future. Organizations with Architecture Governance in place will benefit by using the information on roles and responsibilities contained in this section as an assessment tool. They will also benefit from the sample organizational charts, provided by state, county and city governments.

The ***Business Architecture*** section will interest developers of enterprise architecture and those who participate in the description of the state's business from an enterprise-wide perspective or who wish to gain an understanding of the structure and the type of detail captured about the enterprise from a business perspective. For any Enterprise Architecture effort to be successful, it must be founded on the Business Architecture of the enterprise.

Information Architecture is defined within this tool kit to include data architecture and process architecture. Information Architecture manages the information of the enterprise by clarifying business

relationships and enhancing the understanding of the business rules adopted by the enterprise. Information Architecture aligns the Business Processes to the Information Systems that support these processes, promotes information sharing and facilitates cross-agency information exchanges. Using the set of business processes that provide a view of the functions of the enterprise, the Information Architecture will provide the organization with a high level model of its critical information. Those with interest in business relationships and use of critical information will find this section of interest.

Those who will be guiding, managing or developing the organization's technology architecture will benefit from the ***Technology Architecture*** sections of the Tool-Kit. These sections provide detailed information such as process models, templates for documenting the technology and compliance criteria in use or anticipated within the organization. These sections also include sample tools, data and reports relative to the architectures, compiled from municipal, county and state governments with successful enterprise architecture programs.

Solution Architecture facilitates the development of architectural solutions within the enterprise by guiding the solution architect in formulating solution requirements, design specifications, and logical design models. Individuals interesting in streamlining the design process and leveraging the content of their Business, Information, and Technical architectures to create rapid, reusable enterprise solutions will benefit from this section of the Tool-kit.

The Enterprise Architecture Framework graphic in Figure 1 provides a pictorial view of how the various elements within the Enterprise Architecture interact and influence each other.

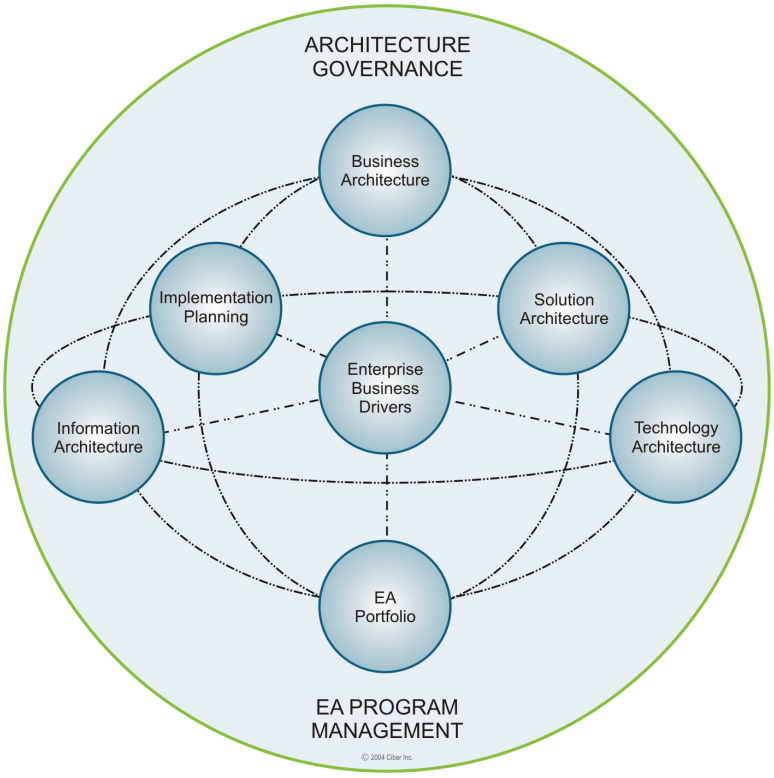


Figure 1. Enterprise Architecture Framework

Executive Summary

An emerging customer-oriented approach to digital-government provides the incentive for this Enterprise Architecture Development Tool-Kit. It is designed to improve information sharing across government boundaries, as well as to position government enterprises for the digital government age and the advantages and opportunities that technology presents.

Enterprise Architecture provides the blueprint for the integration of information and services.

NASCIO's goal is a Tool-Kit that a government enterprise might use as a guide to develop their own Enterprise Architecture. It will support designing, implementing and maintaining the infrastructure for their networks and systems.

The Tool-Kit incorporates the design principles and technical standards necessary to be effective at digital government and to share information nationally.

"Adaptive" is key because the Enterprise Architecture must be able to support a wide variety of applications, and it must evolve as and business and technology drivers changes. The rate of change in the business and administrative process of organizations is accelerating. Consequently, cycle times for implementing new service delivery mechanisms are shrinking. While cycle times of the 1970's and 1980's were typically seven to 10 years in length, in the 1990's, cycle times were averaging one to two years in length. The rate of emerging technology is also increasing, making the need to be adaptive even more critical.

The Enterprise Architecture Framework, which combines structure, processes and templates to document the desired architecture in a systematic and disciplined manner, can be described as a technique for developing the necessary repository for the Enterprise Architecture. Templates describe and organize the relationships among the various components of the Enterprise Architecture. However, over time it is expected that governments will quickly see the value in leveraging visual modeling approaches to Enterprise Architecture. Visual modeling enhances communication and the more sophisticated tools for developing visual models provide the capability to ask questions and conduct sensitivity and impact analyses. In this case, the aforementioned templates may constitute underlying screens for capturing and reporting the details behind visual models. The framework must be constructed before the detail regarding the organization's business, information and technology functions can be documented. Ideally, the creation of systems that work together will be simplified, because Enterprise Architecture ensures that crucial interoperability items are addressed.

Enterprise Architecture is critical because it contains the blueprint for the integration of information and services at the design level across agency boundaries. A well-documented enterprise architecture blueprint will allow data to flow from agency to agency, just as water flows through the pipes and electricity flows through the wiring of a well planned home.

NASCIO's Enterprise Architecture Program Background

NASCIO's goal is to promote national data sharing, the implementation of digital government and the empowerment of municipal, county, and state government to understand, document, control and monitor performance of its IT investments. NASCIO will continue to provide assistance to states in adopting Enterprise Architecture. Specifically, NASCIO continues to develop and expand a Tool-Kit that guides

government enterprises through the development, implementation and evolution of enterprise architecture.

Private industry benefits from the resale of enterprise architecture modeling processes and information technology in general. More and more government enterprises are recognizing the need to share information. Government at every level reaps the highest benefits from sharing common ideas, common approaches and the sharing of information and technology. The Tool-Kit is a product of the government stakeholders it is intended to support. The NASCIO Architecture Work Group, composed of volunteer executive information technology professionals, has worked together to develop the Tool-Kit.

Three government agencies, at varying levels of implementing enterprise architecture (beginning, intermediate and operational), were chosen to participate in a validation program to determine the implications for government enterprises to move toward the national template. The results of this validation effort were incorporated into the final NASCIO Tool-Kit v1.0.

Three regional development workshops were conducted to formalize the presentation of the national template to government representatives and further enhance its applicability. A benchmarking process has been developed and implemented to determine the readiness of municipal, county and state governments to adopt the national enterprise architecture methodology. A number of states participated in a face-to-face benchmarking effort. Additional states and the District of Columbia participated in the benchmarking process through a benchmarking survey instrument.

Additionally, the feasibility of submitting the Enterprise Architecture Development Tool-Kit to nationally recognized standards bodies such as ISO or IEEE for recognition, certification, and publication were explored.

Follow-on efforts to keep the Enterprise Architecture Development Tool-Kit viable are currently being defined. Enterprise architecture viability initiatives include: a continued awareness program, performance measures, technical assistance programs, progress tracking, and an on-going enterprise architecture refresher program to keep the Tool-Kit current, based on emerging government needs.

Integration efforts include mapping the enterprise architecture to the Concept of Operations that has been developed by NASCIO, as well as integration with other national standards initiatives conducted by organizations such as the National Governors Association.

Expanding government participation in this effort includes the development of partnerships with the Federal CIO Council and municipal and county government entities that have been involved in the development and validation activities as appropriate.

INTRODUCTION

Concept - Why Architecture?

...greatly enhance government's ability to deliver effective and timely services.

Adaptive enterprise architecture effectively supports the business of government, enables information sharing across traditional barriers, enhances government's ability to deliver effective and timely services, and supports agencies in their efforts to improve government functions and, thereby, services. NASCIO has developed enterprise architecture processes and templates to guide an organization through enterprise architecture development and adoption, continually providing support that, through standards, narrows the number of products to support and results in reduced complexity. As product numbers and complexity decrease, cost savings emerge. The Tool-Kit is the product of municipal, county and state government input and is applicable to all levels of government with or without existing forms of architecture.

Committing to an ongoing, renewable enterprise architecture process promotes a business-aligned, technology-adaptive enterprise. Enterprise Architecture generates a road map that can provide guidance for future investments and identify and aid in the resolution of gaps in the organization's business and IT functions.

For enterprise architecture to be successful, it must be linked to the business direction of the enterprise. This relationship is confirmed in the Business Architecture, which documents items such as strategies, organization, location, events and information and their existing and future significance.

Information Architecture addresses the informational needs of the enterprise. The information architecture aligns business processes to information systems that support these processes. Using the set of business processes that provides a view of the functions of the enterprise, the Information Architecture will give the organization a high level representation of its critical data. It also promotes information sharing and exchanges across agencies.

Understanding the current application portfolio, future application of technology to new business applications and how future application of technology will be built is presented in the solution architecture of the enterprise architecture. In addition to the applications, it also communicates the supporting technology required to implement the applications,

Technology architecture provides technology commonality that reduces security risks by providing standards for implementing security. It also promotes staff retention by simplifying training and support requirements. It reduces the total cost of ownership by producing technology savings through component commonality, joint purchases and reuse.

Implementing enterprise architecture requires a significant capital investment. It can be compared to moving from an old house to a new one. The old house is a known quantity; we understand what it costs to live there. Moving to a new house, however, potentially requires capital investment for utility deposits, connection fees, appliances, window coverings and landscaping. You would not have been required to make these investments if you had remained in the old house.

Most governments will not have unlimited capital to invest in implementing new enterprise architecture and standards. Implementing enterprise architecture via the big bang theory is not going to work. Migrating to enterprise architecture within available budgets is the only viable method.

Future technology investment and new projects adhere to the adaptive enterprise architecture standards. Over time, the enterprise infrastructure will migrate to the new technology architecture standards. Enterprises with existing in-house architectures and standards can incorporate them into NASCIO's architecture templates. The organization will need only to categorize the existing architecture within the provided templates.

For example, the implementation of technology architecture requires categorizing existing standards and legacy system components into one of the following four technology categories: emerging, current, twilight, or sunset standards.

Many view enterprise architecture standards as constraints that reduce flexibility in system development and deployment, hinder the ability to provide effective service, and increase the cost of service delivery. In fact, enterprise architecture standards create commonality, increasing the enterprise's capability to provide effective information and services and to reduce the cost of delivering those services. Implementation of NASCIO's adaptive Enterprise Architecture model provides this increased capability through familiarity.

Repetitive use of common and adaptive enterprise architecture standards helps to identify and mitigate project risks, increase project success rates, provide the enterprise with interchangeable staff and deliver solutions more quickly. All of these represent opportunities for cost savings. The alternative is to continue to develop and deploy specialized information and business systems with proprietary requirements that may or may not be compatible with other systems.

The debate over whether or not to implement adaptive enterprise architecture standards can be related to a potential homebuyer's decision to buy a tract home or a custom-built home. Both perform effectively in the role for which they were designed. Tract homes typically cost 40% less per square foot than custom homes and rely on proven building plans, defined and readily available building materials, and contractor familiarity with the building process. These advantages are less likely to occur in building a custom home.

Implementing enterprise architecture standards provides a significant benefit in procurement and purchasing. Standards will reduce the variety of items purchased and allow the enterprise to consolidate buying power. The reduced variety also minimizes support and training costs, because it results in a more focused work force.

Additional benefits are realized in providing consistent and common languages in enterprise development of Requests for Proposal (RFPs). Standards may be incorporated as requirements directly into the RFP, leaving no question what the system requirements are from the contractor's perspective. The vendor community must comply with the requirements listed in the RFP and, therefore, can be held accountable for their performance based on requirements that are consistent with the enterprise architecture. In practice, this reduces the procurement cycle significantly. The state of Kansas has reduced its IT project procurement cycle by an average of 41% since its implementation of enterprise architecture. Enterprise architecture compliance also benefits municipal and county government when it is synchronized with state government efforts in the areas of information sharing, integrated services and purchasing through statewide contracts.

A number of potential issues must be effectively addressed when implementing enterprise architecture. These issues include designation of responsible parties for the enterprise architecture effort. Not

everyone will agree with the selection. Data ownership will become a political issue, as enterprise architecture will integrate data from various business units. Identifying the most appropriate and effective owner of the data is key to a successful integration of the data. There will be perceived winners and losers in the process. Traditional system control and responsibility may be handed over to a more appropriate caretaker based on the implementation of enterprise architecture and the integration of data. Simply stated, adopting adaptive enterprise architecture will greatly enhance government's ability to deliver effective and timely services and to support agencies in their efforts to improve the overall functioning of government. Sharing information, maximizing resource investment, increasing technology reuse opportunities, and meeting the public's ever-increasing expectations for electronic access to government information and services are major motivating factors driving the need for implementation of common enterprise architecture and standards.

The necessity to share information electronically in a timely, secure and efficient manner is being driven by the operational requirements of government entities at all levels. A host of state and federal legislative mandates enacted in recent years, such as the Health Insurance Portability and Accountability Act (HIPAA) and other government and private initiatives promoting standards for digital government, communications, e-business and information technology, continue to build on an already strong case for the development of an adaptive enterprise-wide architecture that is widely accepted by government.

Sharing information makes better government. Shared information minimizes clerical errors, information discrepancies and government loopholes. Once information is collected, it is warehoused in a centralized location where it can be upgraded, backed up, archived and easily accessed many times by multiple users.

Public expectation for electronic access to government information and services continues to increase. Citizens expect the same availability of information and efficiencies for government services as they receive from the private sector for information, services and products. Digital government and e-Government initiatives address these expectations. For example, government information and service delivery in many areas have become available electronically on a twenty-four hour, seven day a week basis without expanding office hours or increasing staff.

Common IT standards and technology architecture will provide guidelines for security, information privacy, communications protocols, infrastructure build out, platform and operating system integration, applications development, and user interfaces that will create efficiencies across a multi-disciplined environment that include significant cost and time savings.

The approach to enterprise architecture development is similar to development in construction: Building codes are designed to provide for standardization, safety and longevity in homes and buildings yet can be adapted to specific requirements. For example, residential building codes typically require carpenters to build with 2x4 boards that must be sixteen inches apart. The requirement provides for structural integrity and safety, as well as a number of additional benefits to building material manufacturers, construction companies and occupants. Building material manufacturers make drywall, roofing materials, insulation and ductwork designed to fit this standard. This reduces product line requirements and the need for customized products.

Because of the use of these standards, the construction industry realizes savings in cost and time during construction. Roofing, drywall, plumbing, electrical and heating/ventilation/air conditioning contractors count on the fact that the studs are on sixteen-inch centers to gain efficiencies in installing those products. Occupants benefit from lower building costs.

The following advice comes from the State of Kansas concerning the development of Enterprise Architecture:

"Regardless of the architectural development level with which an organization starts, certain criteria should be considered in order for the end-product to be useful and accepted within the organization:

- *Architectural principles must be derived from agency goals, objectives and written requirements.*
- *An architecture plan should guide individual agency information systems and technology infrastructure decisions.*
- *Senior Managers, legislators, technical project architects, designers, developers, etc. must understand architecture plans.*
- *The architecture should be developed within the enterprise-wide context of IT and technology benefits.*
- *The architecture should enable flexibility and nimbleness in reacting to new changes in IT, systems and data access.*

In general, architecture should:

- *Sell its vision to government leaders and IT management.*
- *Help align the use of technology with strategic goals and objectives.*
- *Facilitate the communication of plans within a decentralized IT community.*
- *Help manage the increasing complexity of IT technologies.*
- *Facilitate "bridging" new and emerging IT to legacy architecture.*
- *Provide guidance in adapting the architecture that packaged solutions bring to the architectural vision.*
- *Be complete and consistent and provide guidance to application developers, IT managers, and end-users that need to plan, budget as well as, implement and use information technology.*
- *Provide for easy access (less paper/fewer binders), be web enabled, easy to view, traverse and query.*
- *Provide a means to analyze how processes, tools, technology and people should interact to produce IT solutions that achieve both individual and combined goals."*

There is a critical need for a common set of IT standards and technology architecture that:

- Ensures a disciplined, independent, adaptive, scalable and portable approach
- Is capable of being implemented in its entirety or in parts
- Will provide government with the guidelines necessary to migrate from their current environment and take advantage of new technologies with appropriate consideration for legacy systems and applications

NASCIO's adaptive enterprise-wide architecture development effort addresses this critical need.

Overview of Enterprise Architecture Concepts & Structure

This Tool-Kit outlines some of the considerations to address as an organization develops or moves through the process to achieve adaptive enterprise architecture. The purpose of the Tool-Kit is to serve as a guide in understanding the enterprise architecture evolution process. As such, it provides process models, templates and samples of completed blueprints, etc. to serve as examples of the elements to consider as a government organization undertakes the development of its Enterprise Architecture.

The Tool-Kit provides guidance and sample structure, process and blueprint detail.

NASCIO working group members, who represent county and state agencies that either have implemented or are in the process of developing enterprise architecture, have compiled the information provided in the samples.

When we plan to build a house, we rely on the knowledge and experience of others who have successfully gone through the building process. We either hire an architect to draw up plans or begin from plans that already exist. In either case, plans are used as a guide to provide detail on the necessary components, considerations and standards.

The original plans are a blueprint and are adapted to include the particular requirements and wishes of the owner. Though there is room to make changes based on needs and wishes, there are still certain standards that must be followed, such as electrical standards, common structure features, etc. Standards such as placing studs and flooring joists on 16" centers; using 3-pronged, grounded electrical outlets; utilizing electric circuits; placing electrical outlets; and using common plumbing fittings make home building less costly. This commonality ensures they are more structurally sound and easier to repair. We also know that, though certain deviations are possible, they may result in more costly construction or difficulty when it comes time to maintain or resell.

In today's world, information sharing is critical, enterprise architecture is essential, and certain building principles must be followed. Standards are required to accommodate the ever-increasing need for interaction among agencies and organizations.

Most people do not think twice when plugging in their appliances at their new home. They can expect the plug will fit and the appliance will work, no matter which room or which house they are in, whether it is next door or in another state. This would not be possible if common building principles and standards had not been developed.

Construction of a new home or any building is very complex. There are many functional areas of concern and many steps to consider. Though drawing up the plan or blueprint may seem time-consuming and laborious, we would not think of building a home without the detailed plan.

Creation of enterprise architecture can also be complex, but having an architecture blueprint or plan is essential for the enterprise, just as starting with the architectural plan is essential to a sound home.

The purpose of this document is to provide a guide for creating government enterprise architecture or a "guide for creating your blueprint". The Tool-Kit can be compared to an initial set of blueprints to use as the starting point when working to create the final plan.

Therefore, the Tool-Kit is not meant to dictate the final product, but to provide principles, standards, best practices, etc. as examples for government agencies creating their own architecture. Certain standards

may not be necessary to a particular organization; however, these standards may be essential to sharing information across organizations and to maintaining viability into the future.

While Enterprise Architecture can be compared to creating a well planned home, in an even broader sense, it can be compared to developing a well-planned community. As a guide, enterprise architecture allows each entity the flexibility to build its enterprise architecture to meet its specific requirements, but it also provides common templates to address the essentials, meet the standards and work through the issues that allow interoperability and information exchange.

Defining, creating and maintaining enterprise architecture is an evolving, long-term process. A strong commitment is required to dedicate the resources and time required to define the enterprise architecture. Likewise, it is also the intention of the NASCIO work group that this Tool-Kit/Template Package be a living document, evolving and being updated on a regular basis. The intent is to include items that are beneficial to agencies developing and actively working on their enterprise architecture development process.

Once the city planners have zoned the various parcels of the land, the individual architects and general contractors can begin to plan the communities and business that will service the city. This allows the management of the city's building plans from a modular perspective.

Just as in the analogy, we need to break the Enterprise Architecture Framework elements into workable modules that can be addressed separately, but in concert with each other. It is important to review these pieces so that, when they are brought out in the details, the reader will understand where they fit and how they interact.

FRAMING THE ENTERPRISE ARCHITECTURE

There are numerous items to consider when undertaking a construction project like a house, a government building or a city plan. So many, in fact, that listing each item to consider would soon become overwhelming. Without some structure for documenting the items to be addressed and a plan for completion, these projects would be impossible.

This section describes concepts for creating and managing the elements of enterprise architecture.

The ***Enterprise Architecture Framework*** refers to the overarching structure that addresses all of the elements of the Enterprise Architecture. Additionally, it defines the interrelationships between these elements in a consistent and organized fashion.

The building of an adaptive Enterprise Architecture begins with the creation of architecture frameworks. In this Tool-Kit the architecture framework refers to the combination of the templates and the structured processes that facilitate the documentation of architecture in a systematic and disciplined manner.

The Enterprise Architecture Framework graphic in Figure 2 provides a pictorial view of how the various elements within the Enterprise Architecture interact and influence each other.

The goals and objectives of the adaptive enterprise architecture are represented conceptually in this graphic. Government organizations should provide a similar conceptual diagram when developing and implementing their Enterprise Architecture Framework.

As can be seen in the pictorial representation of the Enterprise Architecture Framework, Enterprise Architecture is meant to be living program and will consist of numerous elements, all of which influence

and/or have an impact on each other, and will continue to evolve as the EA Program within an enterprise continues to mature.

Each organization will develop their own Enterprise Architecture, based on the definition and circumstances of their enterprise. The descriptions, definitions and processes within this Tool-Kit are provided as examples that organizations can reference as they develop their own Enterprise Architecture.

This version of the Tool-Kit addresses Architecture Governance and four of the allied architectures:

- Business Architecture
- Information Architecture
- Technology Architecture
- Solution Architecture

The frameworks for each of these allied architectures will be discussed in detail within their respective sections of the Toolkit.

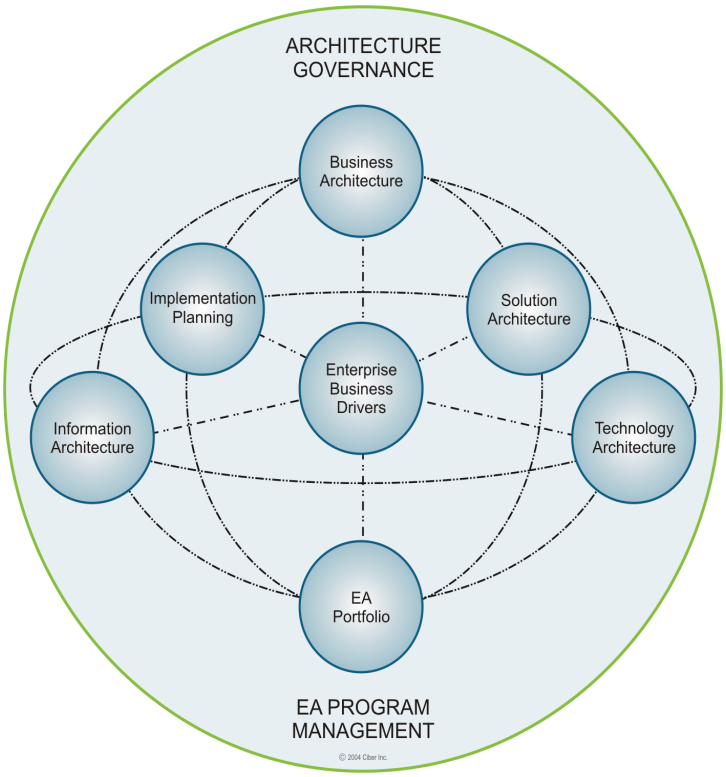


Figure 2. Enterprise Architecture Framework

ARCHITECTURE GOVERNANCE

The Architecture Governance addresses the governance roles and processes required for maintaining Enterprise Architecture.

The Architecture Governance Framework is used to create a sound governance model to support implementation and management of the architecture as necessary to ensure the enterprise achieves its objectives. The architecture governance framework must be resilient enough to allow for those in primary governance roles to learn and adapt, manage the risks, and appropriately recognize opportunities and act upon them. The Architecture Governance section of the Tool-Kit supports NASCIO's architecture program by providing municipal, county and state governments guidance for establishing effective architecture governance.

BUSINESS ARCHITECTURE

Business Architecture provides the high-level representation of the business strategies, intentions, functions, processes, information and assets critical to providing services to citizens, businesses, governments and the like.

The Business Architecture Framework provides the structure for the collection of detail regarding the motivations, organization, location, events, functions and assets that define the direction of the enterprise from the business perspective. The detail captured within the Business Architecture supports business decision-making by providing documentation of where the enterprise is today and where the enterprise wants to be at a specified time in the future.

INFORMATION ARCHITECTURE

Information Architecture is the compilation of the business requirements of the enterprise, the information, process entities and integration that drive the business and rules for selecting, building and maintaining that information.

Information Architecture Framework provides the structure for documenting the detail regarding the information that is critical to the organization, including the baseline and target conceptual (common terms and definitions) and the baseline for the logical and physical. The detail captured within the Information Architecture clarifies business relationships and enhances understanding of the business rules the enterprise has adopted. This understanding forms a baseline for exploring and implementing changes in how business is done, and what business rules the enterprise will adopt.

TECHNOLOGY ARCHITECTURE

Technology Architecture is a disciplined approach to describing the current and future structure and inter-relationships of the enterprise's technologies in order to maximize value in those technologies.

The Technology Architecture Framework provides a sound set of structured processes and templates to support implementation and communication of the Technology Architecture. The mapping of the technology products and standards to the Business Drivers is vital to align the overall enterprise direction. Vendors, employees, and business users can benefit from an understanding what technology standards exist and where these standards can be found.

SOLUTION ARCHITECTURE

Solution Architecture is a process within the Enterprise Architecture that focuses on the development and implementation of a solution or service being created for the enterprise.

The Solution Architecture framework is a combination of structured processes and templates that utilize existing architecture documents (such as business, information, and technology components as well as models and patterns) to design a desired business solution. The Solution Architecture framework, by allowing the development of a Solution Set, facilitates the rapid development and delivery of a solution in a systematic and well-disciplined manner.

ARCHITECTURE BLUEPRINT

The Architecture Blueprint is the dynamic detail for any of the allied architectures that is captured utilizing the structured processes and templates (framework). The blueprint contains detail regarding the Business, Information and Technology that exist currently, and are proposed for the future.

For example, as new technology is brought into the enterprise and older technology is replaced, the Architecture Blueprint needs to be updated to reflect the change in the Business/IT Portfolio. The Technology Architecture Blueprints provides the means to implement technology into the enterprise in a timely and efficient manner. The vitality of the architecture provides for detail concerning the current technology of the enterprise that is "real-time" and accurate.

The benefits of timely decisions based on improved information include cost savings based on better-informed decisions and cost savings due to the advantage of shared buying power. This more than justifies the effort of developing and maintaining the enterprise architecture.

The Enterprise Architecture consists of three types of information:

- Static– Refers to information that changes only when required by business conditions. Architecture Governance and the individual architecture frameworks are a good example of static information
- Semi-Static– Refers to information that changes on an annual or bi-annual basis, or when a major shift in the business or technology occurs. Business Drivers are an example of semi-static information, because they change as new and improved ways of providing services to the stakeholders are found.
- Dynamic– Refers to information that is reviewed and updated frequently, typically every four to six months for content of the Business, Information and Technology Architectures. New information is typically added on a monthly basis as various groups in the organization have business or technology solutions added to the Business/IT Portfolio. The Business, Information, Technology and Solution Architecture blueprints are considered dynamic. The contents of Solution Architecture are typically considered dynamic because new Solution Sets continue to be developed. However, once a solution is implemented, the appropriate Business, Information and/or Technology Architecture blueprints are updated and the content of the specific Solution Set becomes static and is used for historical purposes.

SUMMARY

It is through the discussion of architectural structure, structured processes and templates (Architecture Framework) that the NASCIO Tool-Kit provides guidance for the development of adaptive Enterprise Architecture.

Enterprise Architecture begins with the defining of the architecture frameworks.. The enterprise architecture grows as each of the allied architecture frameworks is completed, and the architecture blueprints, which contain the detail relative to the specific allied architecture, are developed.

The architecture blueprint is not a document that is produced once, stored on the shelf and referenced on occasion. It is a plan and a method; it must be both or it has no value. The blueprint is constantly being renewed and updated to meet the demands on the enterprise. There will be good decisions and bad decisions on the way, but having the information surrounding the decisions captured allows for better analysis for future decisions.

Tool-Kit Map

Figure 3 provides a pictorial overview of the Tool-Kit structure. While the Table of Contents provides directions for the getting to various portions of the Tool-Kit, this graphic provides the map to help the reader determine where they are within the Tool-Kit and to assist with navigation through the Tool-Kit sections.

Figure 3. Tool-Kit Structure

PROGRAM MANAGEMENT – EA

This section of the Tool-Kit begins to introduce the program management aspects of Enterprise Architecture (EA) governance. Many times people initially think of EA as a project, however, as discussed throughout this Tool-Kit, EA must be treated as a program. Projects have defined start and end dates, and are measured on the effectiveness of a specific implementation (e.g. deliverable effectiveness, on-time delivery, delivery within budget, etc.)

EA is an ongoing effort. Once developed, the architecture is kept vital through on-going reviews and updates, allowing the organization to prepare technology plans based on business and technology drivers. The EA program effectiveness must be measured on its ability to provide accurate data for planning and decision-making and translating the impact of those decisions on the organization's operations. As illustrated in Figure 4, leveraging EA for decisions on enterprise projects can lead to better investments and greater customer service.

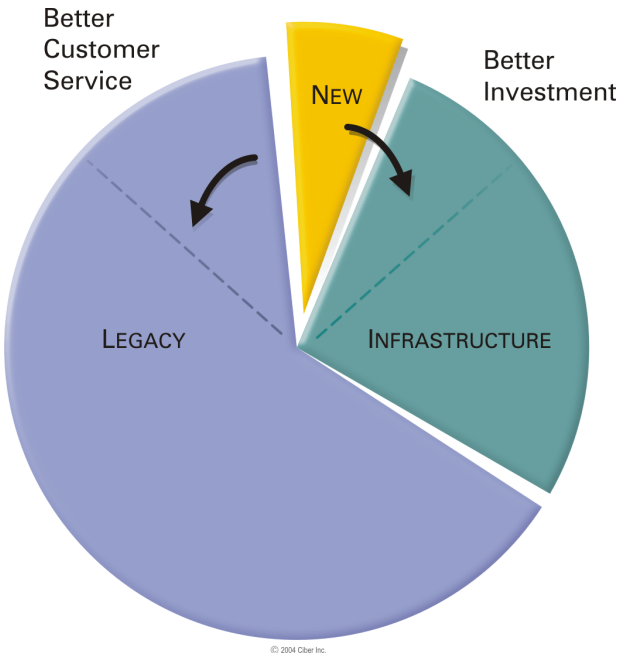


Figure 4. EA Contributes To The Decision-Making Process

An EA program facilitates the alignment between the business strategy and related architecture elements by ensuring the technological responses are well defined and meet the needs of the business. As a program, EA allows for the top-down planning of architectural projects in a balanced and consistent manner. By executing EA program management, these enterprise architectural projects can be accelerated slowed, delayed, stopped, or re-started to suit the available resources and priorities within the organization's strategic plan.

Using program management principles to administer EA assures:

- Creation of a viable EA Framework (structural elements such as Architecture Governance, Lifecycle processes, etc.)
- Documentation of architecture blueprints (content) that provides value to decision-making authorities
- Design of enterprise solutions that leverage existing assets, knowledge, configurations and infrastructure
- Evolution of the program through continuous improvement and refinement of the EA program and content.

Generally, an EA program will provide:

- Management of an EA portfolio
- Alignment of an organization's business strategy with the EA
- The identification of interdependencies between enterprise projects.

- The allocation of resources related to the EA project portfolio.
- The ability to measure progress and the effectiveness of the results of adopting EA practices.

Some of the benefits of managing the EA activities from a program perspective include:

- *Effective Delivery of Change* - Within an EA program, changes are planned and implemented in an integrated manner that ensures current business operations are not adversely affected.
- *Alignment of Enterprise Projects to Business Strategies* - EA provides response to business and technology strategic initiatives by utilizing effective analysis of gaps identified in the architecture.
- *Reduction of Risk* - EA includes the identification of standards, processes and governance that, when followed, will reduce certain risk issues.
- *Coordination and Control* - Having a formal EA program with defined management and governance exercises control over a complex range of business and technical activities.
- *Consistency* - Utilizing policies and standards to guide the EA program will ensure consistency

Program Management for Enterprise Architecture

A critical success factor of any program is the administration of the program. The same is true for EA. The best approach of administering an EA program is by creating an office to manage the program. Some organizations may already have robust program management principles and/or offices in place for other programs. If so, the organization is encouraged to apply those successful models to their EA program. The EA program management office is a resource to help cultivate EA throughout the organization. While EA program management offices may vary by name and/or organizational structure, their charter is promoting and supporting the organization through the application of EA

The EA program management office is an organizational function responsible for support and internal consulting to ensure that enterprise projects (business or technology) are carried out consistently and successfully in alliance with organizational strategy. The creation of an EA program management office enables the following:

- A focal point that provides a repository for architecture standards
- The institutionalizing of a body to enforce the architecture governance
- A means of mapping business strategies into technology solutions
- A forum to help cultivate EA throughout the organization

For example, the EA program management office would:

- Provide primary support to business top and line managers on current and proposed business process opportunities for improvement.
- Provide primary support to Business and line managers due to turn over to help them understand the business and processes and core functional areas they control or are involved in.
- Serve in an advisory capacity on the subject of Business, Information and Technology architectures
- Consult with staff on the design and development of EA components related to specific projects
- Make recommendations and provide advice with respect to policy, procedures, standards, and benefits as they relate to the development, maintenance and evolution of the EA

- Serve as a "working group" for architectural tasks specifically assigned by the Governance committees or other architecture stakeholders
- Promote architectural practices throughout the organization
- Communicate best practices, ideas, and evolutionary architectural elements among stakeholders

An EA program management office may have the following scope of operation:

- Determine the components that define an EA framework and blueprint.
- Create and maintain a set of standards, which can guide future projects while ensuring compliance to the EA and business strategies.
- Create and maintain governance policies that enforce compliance with the current standard EA blueprint.
- Create and maintain an appeals and change process that results in keeping the EA in an up-to-date status.
- Create a communications dialogue that fosters the discussion of, compliance with, and understanding of, current and future EA standards.

The EA program management office responsibilities include:

- Designing, developing, and administering EA
- Application and enforcement of the EA governance
- Developing the overall EA plan and implementation road-map
- Developing, updating, and facilitating the EA review committees
- Assessing technology trends and the impact of these tends on business requirements
- Recommending technology directions to the architecture committees
- Communicating and promoting EA throughout the organization
- Developing educational materials and facilitating the education of EA within the organization
- Developing the transitionary training efforts necessary to evolve traditional development into development using EA as basis and driver.
- Identifying "gaps" in business, information and/or technology, based on business requirements and strategic directions established by the organization
- Overseeing the EA management process
- Ensuring the transfer of the Architecture Help Request between phases
- Assisting with budget and capital planning issues relative to technology improvements
- Participating as architecture consultants on projects
- Assisting in initial reviews of the format, contents, and completeness of submitted architectural documents
- Assuring architecture repositories contain the most current documentation
- Locating appropriate Subject Matter Experts
- Performing reviews on architecture issues
- Distributing the architecture documents, with accompanying unresolved technical and business issues noted for review

An EA program management office, functioning within an organization will have the direct responsibility for the management of the EA program. It is common to find either a Chief Technology Officer or Chief Architect directing the day-to-day operations of an EA program management office. This is a current trend in the management structure of several organizations.

The initial goal of the EA program management office typically includes developing the architecture framework. This includes the development of the architecture processes and structures, establishing the governance processes, and the execution of these framework elements to develop the EA Blueprint.

The Tool-Kit section entitled *Architecture Governance Roles & Responsibilities* covers the roles and responsibilities associated with EA in detail. Figure 5 provides an illustration of the primary roles, and the groups and individuals that serve in supporting roles, as well as their relationship within the architecture. While some of the individuals that serve in these roles may reside in the EA program management office, others may simply interact with the office.

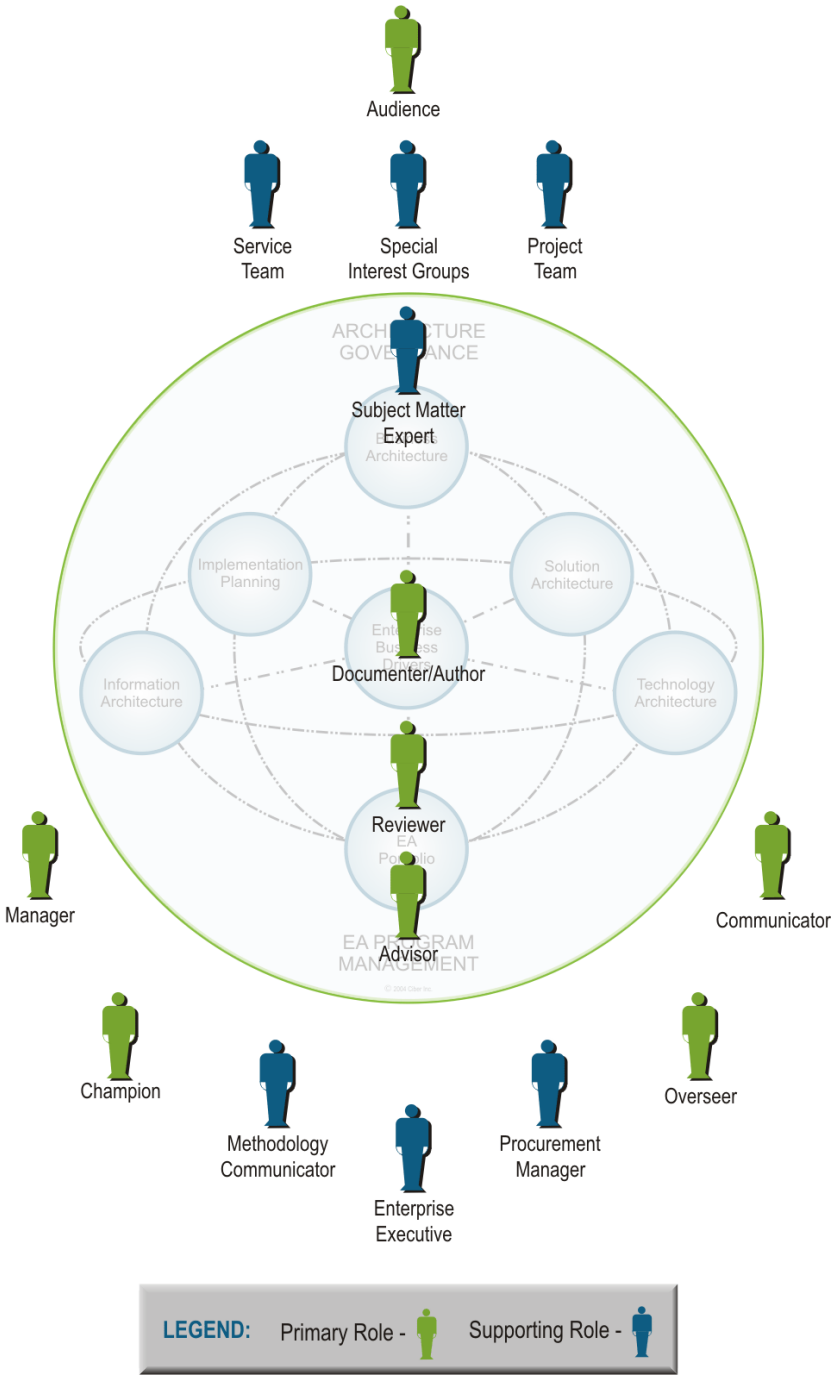


Figure 5. Primary and Supporting Contributors to the Architecture

For example, an architect serves in several roles, such as Documenter/Author, Reviewer, Advisor at various times, and is typically a full time position within the EA program management office. Architects document and update the Architecture Blueprints and Solution Sets as an on-going role, while continuously reviewing the EA Portfolio and emerging technologies to bring about the best, integrated solutions for the enterprise. The architect is also responsible for providing information regarding updates to the various EA Framework elements to the Reviewers and the Communicators.

The role of Business Analyst is a good example of a typically "non-office" role. Though this analyst is not part of the EA program management office, this supporting role of Subject Matter Expert is just as important to the success of the EA program as those reporting directly to the EA program management office. The Business Analyst is responsible for communicating the business processes of their assigned organization and providing an understanding of the links to the technologies that are used to meet those business requirements. Without this knowledge and insight, the EA program management office would be missing valuable information, which would directly impact their ability to deliver the best-architected solutions.

Another key role commonly associated with the EA program management office, but rarely contained within that organization is the Architecture Review Board (ARB). This team is typically a mid- to senior-management-level group responsible for reviewing and recommending approval on the blueprints of the various architectures (Business, Information, and Technology) as well as Solution Sets developed as part of the Solution Architecture.

This group consists of representatives with a basic working knowledge of the organization's key technologies and business processes. The actual membership of this board may vary with each of the allied architectures. The ARB reviews architecture compliance requests and submits recommendations and may act as the approving body for the EA artifacts. Again, while it's not important what title these individuals have or what organization they report to, the role they are filling must be acknowledged and utilized by the architecture program.

Touch-points - EA and Other Management Activities

EA, as described previously, provides many benefits to the organization, especially as it applies to influencing the procurement and retirement of IT related solutions. However, it is also common for the EA governance and management functions to affect, and be influenced by, other common organizational elements including: Project or Program Management programs; processes involved with the identification and reporting of Performance Measures and Metrics; and activities supporting the development of Business Case information.

PROJECT MANAGEMENT

The typical Project Management Office provides the organizational mechanisms to manage and monitor project- or program-related activities for specific projects within the organization, including general project management functions, oversight, risk management, and performance metrics. As EA matures in the organization, it is only natural for the EA program to contribute to, and to utilize the various elements provided by the organizations Project Management Office.

EA should be leveraged to ensure that projects are aligned with architecture goals and objectives, the project deliverables provide an integrated solution and the implementation of these deliverables does not adversely impact standard business operations.

The EA program management office should include in its processes a "checkpoint" with Project Management to assure that the new project conforms to the Enterprise Architecture. By assessing the projects stated goals, objectives, and task deliverables from an architectural perspective, it can be determined if the elements of the project conform to the Enterprise standards. This assessment activity, or architecture compliance review, should be a collaborative effort between the EA program management office and Project Management, and should take place at various points within the project. Activities that typically trigger collaboration between the EA program management office and Project Management include:

- Introduction of new technology
- Changes to computing equipment or infrastructure
- Changes to a purchased package base
- Additions or changes to key interfaces between technologies/solutions
- Changes to the physical data models.
- Additions or changes to external customer or supplier access to the technology/solution
- Migration to a new release of, or alternate vendor for, a key component
- Development of any new solution
- Significant changes in business processes

During these reviews, it is not unusual for the team to uncover issues that may impact the project or the destination environment. The earlier in a project these items are discovered, the more likely the item will be addressed and the management team will have the time to react to and resolve the issue.

As Project Management and EA program management interact, the identification of organizational "best practices" can also occur. The sharing of this information during these "check-point" meetings can therefore, provide benefit to the EA program management office as well as to Project Management. However, the main purpose of the interaction between the EA program management office and Project Management is to ensure compliance with the EA and Project Management standards.

PROJECT RISK MANAGEMENT

Actively managing project risk is an integral part of Project Management. Identification of project risks, along with potential risk intervention and mitigation strategies, is typically done during project definition. Throughout the lifecycle of the project, risk management activities occur to ensure that new risks are identified, risks that come to fruition are managed, and the results of mitigations strategies are monitored for success. EA program management activities assist in managing project risk by defining Business, Information and Technology Architectures in such a way as to allow for the early identification of potential issues before they endanger the success of a project.

In addition to Business, Information, and Technology Architectures, many EA programs include Solution Architecture. Solution Architecture, which addresses the scope, requirements and design specifications for enterprise projects, contributes to project risk identification and mitigation efforts by facilitating the following:

- The leveraging of proven Business Reference Models
- Identification of Capacity Planning needs and impacts
- Reuse of previously identified Solution Set patterns
- Linkage between stated business goals and the solution proposal

- Development of Solution Sets that link to preferred Business, Information, and Technology Architecture components

PROJECT OVERSIGHT

Project Oversight is a typical function of a Program Management Office that provides an independent analysis, review, and report of a project. This information is typically used to provide agency management information on the progress of a project by measuring how well it is doing relative to schedule, cost, and scope. The desired result of an oversight review is to determine if the project is on track to be completed within the time identified, if it will be completed within budget guidelines, and if the project will provide the required functionality when deliverables are implemented.

The EA program management office can contribute to the Project Oversight reviews by ensuring that:

- Projects are prioritized and selected based on linkage to previously identified architecture gaps and migration strategies
- The execution of project reviews occur at the designated times and include architectural reviews as a common practice
- Projects procuring new technologies are referencing existing architecture standards and directions prior to the actual purchase of new solutions
- Any new architectural changes that were introduced when the project deliverables are implemented have been documented appropriately as architecture blueprints and that the architecture repository has been updated to reflect the new environment

Project Oversight also has an impact on the EA program. The development of the framework for each of the program elements (e.g. Architecture Governance and, Business, Information, Technology and Solution Architectures) is typically approached as a project. That is, there are considerations for funding the development, there is a specific timeline identified, and a specific purpose with a defined deliverable. These EA Program development activities can also be analyzed, reviewed, and reported on as a part of the Project Oversight function. This provides information to the management team as to the progress of EA implementation efforts. This progress can then be used as one measure when determining the overall metrics for Enterprise Architecture.

PERFORMANCE MEASURES AND METRICS

As with any major organizational activity, Enterprise Architecture, must demonstrate value to the organization for it to continue, otherwise the organization will realign the supporting resources (e.g., funds, people) to other important tasks. As such, it becomes necessary to define how the effectiveness of EA will be measured. This function typically involves a collaborative effort by the EA program management office and the organization's Project Management Office or entity that is responsible for performance metrics.

Defining a set of business goals and objectives for EA and aligning these with the organization's strategic objectives are critical to the development of strategies for the execution of an adaptive EA program that enables the implementation of the organizational directives. For example, if one of the organizational strategies was to "buy vs. build all Information Technology system applications", the EA Blueprint would reflect the tool/vendor choices and/or standards necessary to implement this strategy. In addition, the EA Governance process would review Solution Set Designs for adherence to this directive.

Achieving strategic objectives is an indicator of effective performance of business functions. Here EA can be linked to the organization's performance measurement system. It is important to keep in mind that EA

is a comprehensive, holistic view of the enterprise, and as such it includes detailed information about an organization's strategic business intent, business operations, organizational units, information, solutions, and the technology used to perform the business operations. If this information is captured in an EA repository, appropriate traceability can be established including traceability to environmental drivers, market/needs analysis, strategic business intent, and business operations.. This relationship to business objectives and the EA elements can be used to determine a measurement for the objective.

The Office of Management and Budget (OMB) defined their Performance Reference Model that incorporates the best parts of several conceptual management measurement models. This model shows the cause-and-effect relationships between enabling technologies, the direct effects of organizational activities, and the results measured from a customer perspective. The focus of this model is on the value-chain that results by analyzing government agency customer relationships or the value that project participants contribute to the organization.

For more information on the Performance Management Model developed by the Federal Enterprise Architecture Program Management (FEAPMO), Office of Management and Budget (OMB) please reference the OMB web site at http://www.feapmo.gov/fea.asp.

BUSINESS CASE DEVELOPMENT

"The creation of a strong Enterprise Business Case is the best hope to get a project approved." [1] This is a common understanding of any project manager or organizational leader as they compete for funds within the organization. All projects proposals must document the business case associated with the project solution being presented. The quality of information within the business case will be used to decide whether the project obtains funding and proceeds to implementation. Therefore, a sound business case is based upon principals that include goals, strategies, initiatives and outcomes, and also addresses short and long-term organization priorities.

EA is integral to the ability to develop accurate business cases. EA, with its documentation of the current and future business models and links to enterprise business drivers, assist in the definition of the project and contributes to its understanding of the touch points within business and technical areas.

In addition, the contents of the architecture (EA Blueprint) will help to identify technology compatibilities, integration opportunities, and the potential for component reuse – all of which contribute to the value of the solution and can be documented as such in the business case.

For more information on business case development see NASCIO's "Business Case Basics and Beyond" available for ordering on NASCIO's website, www.nascio.org.

EA and Technology Planning Processes

As the importance, and cost, of information technology has grown, organizations find that the past traditional methods of making business and technology planning and budget decisions are no longer viable. Today more than ever, organizations depend on successful uses and deployments of technology. One of the challenges is to develop a technology plan and budget that accurately reflects not only the

[1] NASCIO Business Case Basics and Beyond: A Primer on State Government IT Business Cases, By Andris Ozols, Senior Analyst, Department of Information Technology, State of Michigan

initial cost of a solution, but also all the related expenses as the solution matures, i.e. the *total* cost of ownership.

By leveraging the EA blueprints and migration strategies, technology planning processes can enable an organization to take advantage of new opportunities, and substantially re-use existing proven technologies, while minimizing the negative impact of unexpected challenges. In this time of rapid technological change, technology planning and budgeting processes that utilize the EA Implementation Planning processes, EA Governance, and the documented architectural standards, can provide greater opportunities in the use, and re-use, of information technology. Building a technology plan and budget based on the information contained within the EA Blueprint should:

- Clearly identify technology gaps and needs
- Link technology components to proposed business solutions
- Be a formal continuous improvement process
- Be supported by executive management
- Leverage current planning methods
- Result in documented output publicized to the organization
- Be diverse, choosing the best features from a diverse set of resources
- Be broad but bounded in scope, by incorporating economically and technically feasible solutions based on the Implementation Plan and the EA roadmap
- Involve senior administrators, representatives of line-of-businesses, procurement, and information technology staff members
- Present a clear prioritization of possible projects that have articulated a strong business case, defined the solution at the conceptual level, and established a realistic project cost and schedule
- Engage the EA program management office to identify potentially important technological developments and recognize when those developments make the transition from emerging to current, based upon the organizations ability to assimilate technology change as defined by the EA program
- Be driven by organizational issues, opportunities and business needs, rather than technological developments

A technology planning and budgeting process enables management focus and attention on activities and resources necessary to successfully meet technology related needs. EA enables value decisions on the usage and selection of technology prior to the actual start of the dependent project requiring the technology capabilities.

EA Program Management at Work

EA programs can be implemented at various levels within an enterprise. For example, there may be EA efforts and even an EA program management office at the state level, while individual agencies and/or municipalities may also have their own active EA program management offices and initiatives. Each of these efforts provides value. The greatest value for a state is achieved when these offices and initiatives are coordinated and cooperative. Federal and state level architectures should be utilized when determining strategic alignment and strategic direction from the agency and municipality perspective.

The level of the government represented by the organization and the charter given to the architecture development team will determine the amount of detail contained in the architecture blueprints. Where a federal or statewide EA initiative may be at a high level, with focus on the conceptual views and directed toward specific strategic initiatives, individual agencies may choose to develop architectures that detail a specific roadmap for their current organization, as well as including a more tactical approach to accommodate their initiatives.

Every enterprise should evaluate the level of detail and direction to be included in their EA Blueprint, ensuring the level of detail is fitting for the charter of that organization and provides the enterprise the tools necessary to use architecture principles for accomplishing the business initiatives.

There are many public sector EA initiatives across the county. The examples below site the approach to EA program management by several organizations. The inclusion or exclusion of any individual effort is not a reflection on the efforts within that enterprise – the examples provided are simply samples to illustrate the direction and charter these organizations have taken in institutionalizing EA within their organizations.

FEDERAL EA PROGRAM MANAGEMENT OFFICE

In February of 2002, the Associate Director for Information and E-Government, Office of Management and Budget issued a directive establishing the Federal Enterprise Architecture Program Management Office (FEAPMO). This office was established to foster the growth of EA within government agencies. Additionally, the FEAPMO was charged in the development of models to facilitate technology solutions and to develop a complete architecture for each of the 24 Presidential initiatives and to improve government effectiveness and efficiency through new business processes and consolidations.[2]

The Chief Technology Officer for the Office of Management and Budget manages the FEAPMO. The Chief Technology Officer is responsible for the overall success of the program, overseeing completion of program tasks and obtaining approval of program deliverables. There is a Program Manager that is responsible for the day-to-day activities of the FESPMO.[3]

The FEAPMO provides no direct management of the implementation of EA within government agencies. However, it does have the responsibility to develop architectural models and to set standards for the Federal EA Framework.

NORTH CAROLINA – OFFICE OF ENTERPRISE TECHNOLOGY STRATEGIES

The State of North Carolina has an Office of Enterprise Technology Strategies (ETS) that manages the North Carolina Statewide Technical Enterprise Architecture. The mission for the Office of Enterprise Technology Strategies is to provide "leadership in information technology and telecommunications services to accomplish the directives formulated by the State CIO regarding state-level information technology strategies, plans, policies, and procedures. Working with state agencies, federal and local governments, citizens and private sector businesses, ETS helps the implementation of new technologies consistent with the state's enterprise approach."[4]

ETS reviews agency IT projects and offers recommendations on the disposition of the project to governing bodies, provides leadership, guidance, and mentoring to agencies on approaches to IT, IT

[2] http://www.feapmo.gov/about.asp
[3] http://www.feapmo.gov/feapmo_org_structure.asp
[4] http://ets.state.nc.us/about.html

procurement and IT project management, independent verification & validation on key projects, services, and systems and provides enterprise IT planning and strategies for the State CIO and governing bodies.

NORTH DAKOTA – INFORMATION TECHNOLOGY DEPARTMENT

"Through legislative authority, the Information Technology Department (ITD) of the state of North Dakota is mandated to develop policies, standards, and guidelines for technology based on information from state agencies, institutions, and departments with the goal of creating a common statewide architecture. Since 1998, the Standards and Policy Review Group consisting of lead IT coordinators representing every agency have performed this cooperative function. Enterprise Architecture will replace this current process.

Through the Enterprise Architecture (EA) process, state agencies will more effectively partner with ITD in setting future direction of information technology in the state of North Dakota. The success of this highly collaborative process will depend on the strength of its governance structure and the commitment of the participants to its goals and guiding principles." [5]

MISSOURI – OFFICE OF INFORMATION TECHNOLOGY

"Enterprise Architecture is one of the key areas of responsibility for the Office of Information Technology. This is the core business and strategic plan for all technology in Missouri state government. For the purpose of security, service, and efficiency, Missouri must function as one seamless technology enterprise. Architecture will allow Missouri state government to act as a single entity, an enterprise, with respect to information technology.

By implementing a blueprint for standards and methods that are agreed upon by all agencies, the state positions itself to save money, increase service, and gain a competitive advantage for the long term. This is an ongoing process that can swiftly adapt to changes in business and citizen needs.
The goal is always to provide the citizens of the State of Missouri with the most efficient and effective service possible." [6]

NEW MEXICO – INFORMATION TECHNOLOGY COMMISSION (ITC)

New Mexico's Information Technology Commission (ITC) and the Office of the Chief Information Officer (OCIO) are responsible for the statewide information architecture program and plan. "The goal of New Mexico's Enterprise Architecture is to enhance coordination, simplify integration, build a consistent infrastructure, and generally allow greater efficiencies in the development of technology solutions to support our Agencies in the fulfillment of their missions to serve our constituents. Our intent is to provide continuous alignment between the business of state government and technology." [7]

Sample governance models for Kansas and North Carolina, as well as tables to describe the mapping between organizational titles and the primary and supporting roles for relative to EA are included within the Architecture Governance section of this document (See *Architecture Governance – Sample Governance Models*).

[5] http://www.state.nd.us/ea/about/
[6] http://oit.mo.gov/architecture/enterprise%20architecture.html
[7] http://www.cio.state.nm.us/content/architecture/FrameworkForEntArchProg.pdf

Summary

Many of the activities and tools common to program management in general can be applied to EA program management. Numerous resources are available to cover these topics and this Tool-Kit is not intended to recreate what is readily available.

Several topics, related specifically to EA, are covered in detail within this version of the Tool-Kit:

- Architecture Governance
  - Scope
  - Roles & Responsibilities
  - Samples Governance Models
  - Architecture Governance Development
- EA Lifecycle Processes

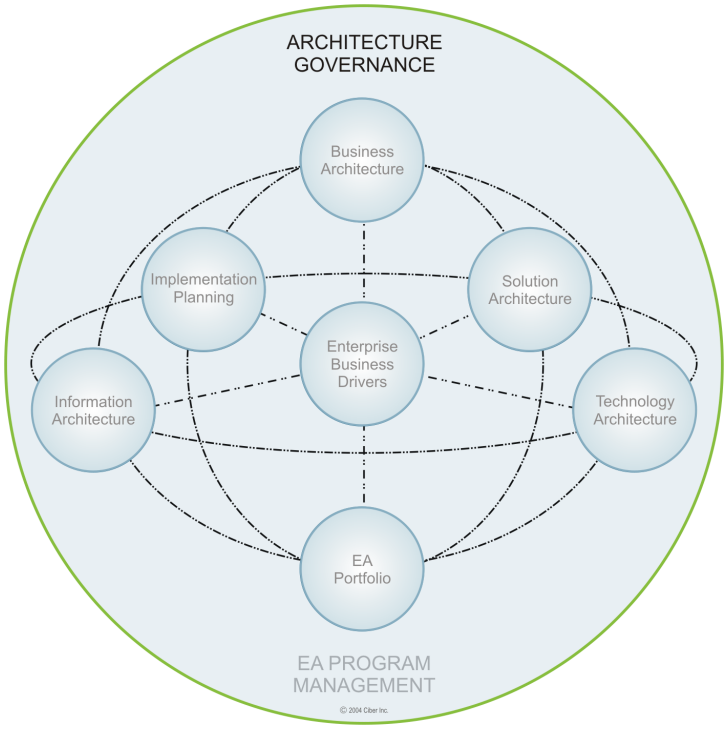
ARCHITECTURE GOVERNANCE

NASCIO has established an Adaptive Enterprise Architecture Program to assist all levels of government with the adoption of adaptive enterprise architecture. As part of the NASCIO's overall Enterprise Architecture Program, this Tool-Kit was created to provide guidance for developing an adaptive enterprise architecture that effectively aligns information technology with the enterprise business direction.

Sound architecture governance, which supports implementation and management of the enterprise architecture, is necessary to ensure the enterprise achieves its objectives. The Architecture Governance must be resilient enough to allow for those in primary governance roles to learn and adapt, manage the risks, and appropriately recognize opportunities to take advantage of technology and act upon them.

This section of the Tool-Kit on governance supports NASCIO's architecture program by providing municipal, county and state governments an understanding of and a method for establishing effective enterprise architecture governance. It effectively supports the analysis of existing governance structures, identifying methods to improve governance performance, as well as the development of a governance structure in its entirety.

The information presented in this section defines the purpose of governance, the concepts of Enterprise Elements and Enterprise Architecture Framework Elements and governance roles and examples of the structured processes for establishing architecture governance. Additionally, samples of effective governance organizational charts from municipal, county and state government are provided for reference.



Architecture Governance is the responsibility of executives, as well as stakeholders, such as citizens, businesses, employees and other organizations, throughout the enterprise. Governance consists of the leadership, organizational structures, direction, and processes that ensure Information Technology (IT) sustains and extends the enterprise's mission, strategies and objectives in a planned manner.

The purpose of Architecture Governance is to direct or guide initiatives, to ensure that performance aligns the enterprise business by taking advantage of the associated benefits, to enable the enterprise business by exploiting opportunities, to ensure IT resources are used responsibly and Technology Architecture-related risks are managed appropriately.

Architecture Governance is typically applied in layers. Strategy and goals are rolled down into the organization. Team leaders report to and receive direction from their managers; managers report to the executive and the executive reports to the mayor, county executive, or governor. Deviations from goals and standards are reported, and recommendations for action requiring endorsement by the governing layer are included.

Scope

The approach to Architecture Governance presented here relies on the development, collection, and utilization of *"Enterprise Elements"*. Enterprise Elements consist of information developed and documented by both the business and IT communities within the enterprise.

Information contained in these Enterprise Elements becomes the foundation for building the Enterprise Architecture Framework Elements. Enterprise Architecture Framework Elements discussed within this version of the Tool-Kit consist of Architecture Governance, the Business, Information, Technology and Solution Architecture Frameworks and the respective Architecture Blueprint for each of these allied architectures. These Enterprise Architecture Framework Elements are the foundation for a comprehensive Enterprise Architecture Framework. These established Enterprise Architecture Framework Elements provide the capability to categorize and identify the details of the enterprise architecture, including the business and information needs, the technological direction, the architecture lifecycle processes and overall enterprise architecture program specifics.

ENTERPRISE ELEMENTS

Enterprise Elements are identified in this section along with a high-level explanation of their relationships to the Architecture Governance Elements. A detailed understanding of these relationships can be gained from the Governance processes identified later in this section. Enterprise Elements aid in communicating information throughout the enterprise and can be classified in three categories: *strategic, procedural* and *tactical*.

"*Strategic*" Enterprise Elements aid in top down communication within the enterprise and ensure enterprise-level strategies are addressed appropriately within the Enterprise Architecture Framework. Some examples of Strategic Enterprise Elements are:

- Enterprise Direction
- Mission Statements
- Organizational Charts
- Operating Budgets
- Goals, Objectives, and Strategies
- Strategic Management Initiatives

"Procedural" Enterprise Elements aid in providing the translation of the top down communication into the bottom up communication and identify the implementation relationships to the Strategic Enterprise Elements. Some examples of Procedural Enterprise Elements are:

- Project Methodologies
- Service Policies and Procedures

- Procurement Policies and Procedures
- Adaptive Enterprise Architecture

"Tactical" Enterprise Elements aid in providing information from the bottom of an enterprise up and provide the actual delivery of the various services, products and initiatives. Tactical elements provide opportunity for measuring the effectiveness of the enterprise architecture efforts. Some examples of Tactical Enterprise Elements are:

- Tactical Initiatives
- Services
- Projects
- Specific Budgets (Project or Unit)

Figure 6 illustrates the flow that the Enterprise Elements follow from the enterprise perspective, along with their relationships.

Enterprise Element Relationships

Strategic elements translate into both the procedural and tactical elements to accomplish the identified goals and objectives of the enterprise. It makes little difference whether an organization utilizes Strategic Planning, Enterprise Direction Statements, or Mission Statements to communicate the various strategic elements. All organizations have, in some form, strategic elements that are then translated into procedural and tactical elements to aid in implementation.

Strategic Elements can be communicated in various ways including, but not limited to:

- Enterprise Direction
- Organizational Charts
- Mission Statements
- Strategic Plans
- Strategic Initiatives
- Enterprise Budget

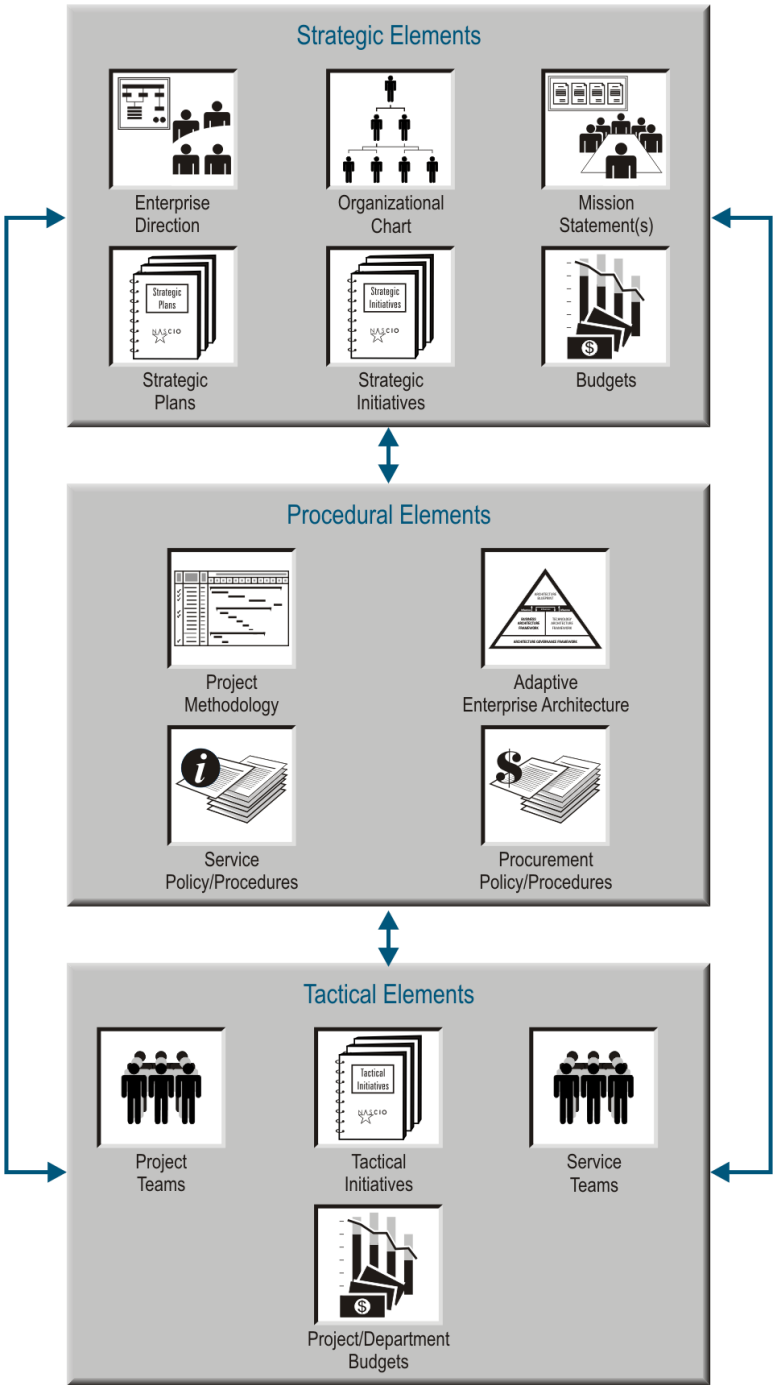


Figure 6. Enterprise Element Relationships

Procedural elements address questions such as what is the best delivery method, which payment options give the best value, and which enterprise architecture best matches the strategic element. Through utilization of the procedural elements, Strategic Initiatives will provide better opportunities to leverage services across the enterprise. This information is provided as feedback into the strategic elements to aid in refining existing strategies and developing new strategies.

There are processes and information available to the service and project teams that are designed to help the business and IT communities consistently and methodically execute projects, purchases, and implement technology solutions. Among these are:

- Procurement Policies and Procedures
- Project Methodologies
- Service Polices and Procedures
- Adaptive Enterprise Architecture

Implementation work begins with the tactical elements, once the delivery method/procedure is determined, the enterprise architecture solution is identified, and the procurement vehicle is established. It is through the tactical elements that the strategic elements are brought to fruition. Tactical elements can include:

- Project Teams
- Service Teams
- Tactical Initiatives
- Project/Departmental Budgets

As the project and service teams work with the various procedural elements, they may see ways to improve the methods, policies, and procedures. These improvement suggestions need to be fed back into the procedural elements to aid in future implementation efforts. All three levels of enterprise elements are required to have an effective and adaptive enterprise:

- Strategic elements provide direction.
- Procedural elements provide consistent, timely, and budget-conscience deliveries.
- Tactical elements provide day-to-day implementation of the services and products.

ENTERPRISE ARCHITECTURE FRAMEWORK ELEMENTS

Now that the overall, top-down flow of Enterprise Elements from Strategic Elements to specific Tactical Elements has been established, their relationship with Enterprise Architecture Framework Elements can be explained (see Figure 7). Enterprise Architecture Framework Elements pertain specifically to the adaptive enterprise architecture, and therefore, fall within the scope of enterprise architecture governance.

The Enterprise Architecture Framework Elements include:

- Architecture Governance Framework (including Lifecycle Processes)
- Business Architecture Framework
- Information Architecture Framework
- Technology Architecture Framework

- Solution Architecture Framework
- Architecture Blueprint

In Figure 7, the Enterprise Architecture Framework Elements are placed between the Strategic Elements and the Tactical Elements. Similar to Project Methodologies/Service Policies/Procedures and Procurement Policies/Procedures, the Enterprise Architecture Framework Elements define the adaptive enterprise architecture structure that supports the project and service teams, which methodically and consistently bring solutions to the enterprise.

Strategic Elements, focused on Business Strategies, provide the information for defining the Business Architecture Framework at the business executive level. The Strategic Elements, focused on Technology Strategies, along with the Technology Architecture Framework, aid in establishing and confirming the Technology Architecture Framework.

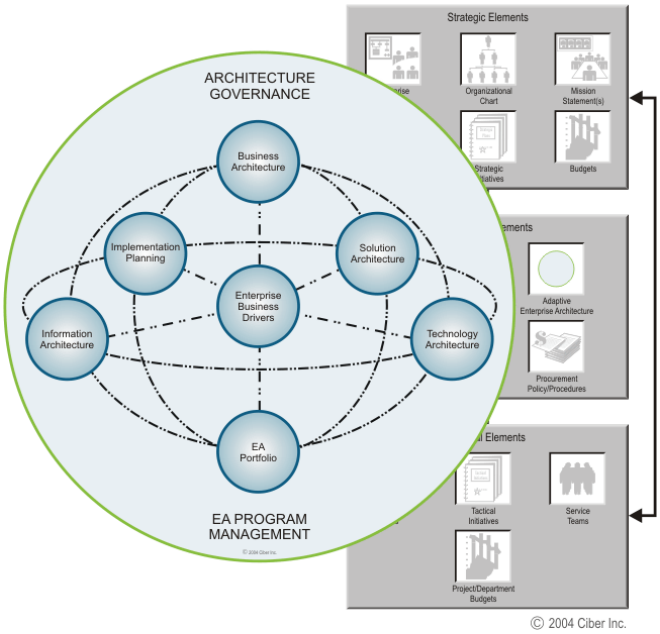


Figure 7. EA Supports Enterprise Elements

The development of, or change to the Technology Architecture Framework or Blueprint can also influence the development of the allied Architectures Frameworks and blueprints. Updates or changes to any of the architecture framework or blueprint should trigger a review of the allied architectures to ensure the enterprise perspective remains intact.

It is through development of structured processes and templates that each of the architecture frameworks is finalized and maintained. Once these foundation pieces of the enterprise architecture are in place, the Architecture Blueprint can be produced. The processes and templates are discussed in detail later in the respective sections of this Tool-Kit.

The EA Portfolio is an additional element to the overall Enterprise Architecture Framework. In the early stages of the development of EA, the Business, Information, and Technology blueprints are primarily focused on the detailed content and uniqueness of the specific architecture components and are often viewed as separate architecture entities. As the organization and architecture practices mature, it becomes more valuable to the organization to view the integration of the specific architecture artifacts holistically – that is, the "the whole is more than the sum of the parts". To provide this value, the architecture artifacts need to be bundled or packaged for documentation and understanding, rapid reuse, adoption, and interoperability.

The EA Portfolio is primarily concerned with developing these views and packages that are the sum of the various components across the Business, Information, and Technical architectures. Often, the packages are referred to as application and infrastructure patterns. In addition, application profiles and technology services are also grouped and presented as a cross view of the specific, individual architecture components.

Roles & Responsibilities

Well-established roles and responsibilities for Architecture Governance are essential to implementing a successful enterprise architecture program. Architecture Governance covers responsibility for such items as:

- Ensuring the Enterprise Elements and Enterprise Architecture Framework Elements effectively represent the needs and wishes of the enterprise
- Defining the Enterprise Architecture Framework and Blueprint
- Maintaining the vitality of the Enterprise Architecture Blueprint
- Maintaining the viability of the Enterprise Architecture Framework

In Architecture Governance, the roles and responsibilities are specific to the function performed. When an organization develops its Architecture Governance structure, these responsibilities will be distributed among individuals, groups, or committees as best meets the needs of the organization.

Governance roles and functions are performed by various groups or individuals. People who consistently work with the architecture processes, framework, and artifacts are considered to be contributing in a primary capacity.

Primary Architecture Roles	
Overseer	Champion
Manager	Documenter/Author
Communicator	Advisor
Reviewer	Approver
Audience	

Other individuals or groups that are identified to support architectural blueprints or elements on an as-needed basis are contributing to the Enterprise Architecture in a secondary or supportive capacity.

Contributors that Play a Supporting Role	
Subject Matter Experts (SME)	Enterprise Executive
Project Teams	Services Teams
Procurement Manager	Special Interest Groups
Project/ Services Methodology Communicator	

Figure 8 shows the primary and supportive roles, groups, and individuals and their close relationships within the Enterprise Architecture Framework.

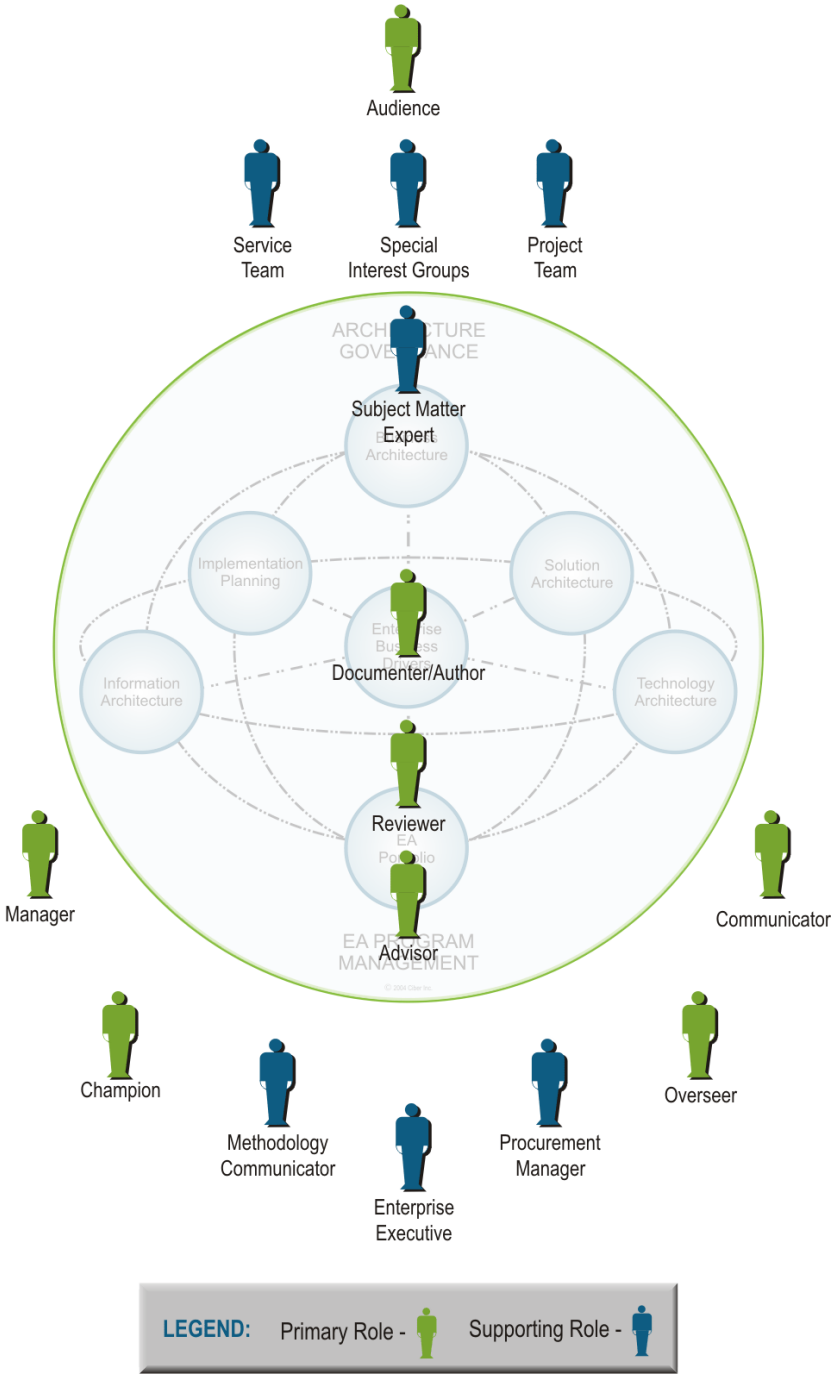


Figure 8. Primary and Supporting Contributors to EA

The contributions provided by the roles, groups, and individuals involved in Architecture Governance are described in detail in this section. For each contributor the following information is provided:

- *Description* – The specific EA role, group, or individual and its relationship to other roles or groups.
- *Implementation recommendations* – Is the function better implemented as a committee or as a single position?
- *Checks and Balances* – Whether this function should be implemented in combination with other roles and what combinations to avoid.
- *Full-time / Part-Time* – Is the contributor typically considered full-time or part-time?
- *Contribution Significance* – Is the function critical, necessary, or helpful? If the function is critical or necessary, a comment addressing the risk of non-implementation is provided under "Missing Contribution Responsibility".
- *Missing Contribution Risk* – An explanation of the risk incurred if no one assumes responsibility for this function from the governance model. This item is included only for critical or necessary contributions.

Appendix B contains a Role & Responsibility Matrix, which provides an "at-a-glance" reference of the responsibilities of each Architecture Governance contributor, the EA Life Cycle aligned with the tasks, and the architecture artifact impacted by the task being performed.

PRIMARY CONTRIBUTORS

Overseer

- *Description:* The Overseer is a role that is established by legislative mandate or similar directive from the Enterprise Executive. Membership on the committee is usually by appointment from the establishing organization or designated representative. A committee, team or group typically fills the role of Overseer. The Overseer is responsible for ensuring that Business and IT plans follow the proper direction for the enterprise and that the associated budgets are well spent.
- *Implementation Recommendation:* The role of Overseer can be implemented as an individual or committee. An informed, consensus opinion must be obtained for effective oversight.
- *Checks and Balance:* The role of Overseer can be combined with the roles of Manager, Advisor, and Communicator. Combining the role of Overseer with the role of Reviewer is not recommended.
- *Full-time / Part-Time:* The role of Overseer is considered part-time.
- Contribution Significance: Helpful
- Missing Contribution Risk: Without the overseer role the architecture participants will need to monitor their program activities without the benefit of a third-party viewpoint.

Champion

- *Description:* While every individual associated with the enterprise architecture effort should be its "champion" by continuously promoting, advertising, marketing, and participating, the role of Champion is typically an executive role. Potentially the role of Champion is held by an executive at the CIO or equivalent level, and is responsible for ensuring the enterprise goals and objectives set out by the enterprise architecture efforts are met. Though the role of Champion is not directly involved in the specific enterprise architecture processes, the Champion provides the cheerleading and public relations that the adaptive enterprise architecture effort requires to be successful. The

Champion is also responsible for promoting the benefits that will be accomplished by creating adaptive enterprise architecture. As with any effort that is conducted at the enterprise level of an organization, a Champion is essential for success throughout the enterprise.

- *Implementation Recommendation:* The role of Champion is best implemented as an individual; however, everyone connected with the enterprise architecture effort should be a champion of the effort. Having an executive-level management Champion for the adaptive enterprise architecture effort is vital to its success, especially in getting started and when seeking compliance.
- *Checks and Balance:* The role of Champion can be combined with the Advisor and/or Manager.
- *Full-time/ Part-Time:* The role of Champion is recommended as part-time.
- *Contribution Significance:* CRITICAL
- *Missing Contribution Risk:* Absence of this role could result in the lack of executive support and enterprise visibility. In addition, the enterprise architecture effort may not be empowered.

Manager

- *Description:* The Manager is responsible for the coordination of the overall enterprise architecture effort. The manager seeks guidance and support from the Champion on enterprise architecture related matters such as selecting contributors to fulfill enterprise architecture functions or enterprise architecture review items that require executive approval. The Manager also receives clarity and support from the Advisor on Strategic Elements from both the business and IT communities within the enterprise.

  The Manager chairs and directs the role of Reviewer. The Manager also receives evaluations and recommendations from the Reviewer. Both the Manager and the Reviewer share in the responsibility of screening enterprise architecture requests and recommendations. The Manager appoints and directs the Documenters. The Manager spells out the responsibilities of the Documenters both in processes and in scope of work.

  The Manager provides information to the Communicator to:

  - Promote the overall enterprise architecture effort.
  - Specify the audience for the information.
  - Identify what information is available during the various enterprise architecture process steps.
- *Implementation Recommendation:* This Manager role is best implemented as an individual, not a committee. The individual should have a solid technical background and, ideally, the Chief Architect or equivalent should fill the role at the enterprise level. Precise decisions and direction are needed.

  The Manager role can be extended into multiple roles at varying levels or in various organizations within the enterprise. Extended Managers act as an extension of the enterprise level Manager and essentially fulfill the same responsibilities, except that they are taking their guidance and direction from the enterprise level Manager.
- *Checks and Balance:* The Manager role can be combined with the Champion and/or Communicator Roles. The Manager can be a Reviewer but should not be the only Reviewer. The combination of role of Manager with the role of Approver is not recommended.
- *Full-time/ Part-Time:* The Manager role is recommended as full-time.
- *Contribution Significance:* CRITICAL
- *Missing Contribution Risk:* Lack of guidance and a single consistent vision.

Documenter/Author

- *Description:* The Documenter/Author can be either senior or junior level IT staff, or business staff depending on what is most appropriate. A Documenter's primary responsibility is to maintain the various Architecture Governance elements. Based on the Documenter's scope, which is directed by the Manager, each Documenter/Author maintains one or more of the following:
  - Architecture Governance Framework
  - Business Architecture Framework
  - Information Architecture Framework
  - Technology Architecture Framework
  - Solution Architecture Framework
  - Business, Information and/or Technology Architecture Blueprint

  The first five Architecture Governance elements are fairly static and change only due to updates to the Strategic Elements or approved enterprise architecture process improvement suggestions. The Architecture Blueprint Documenter is an on-going role that is constantly reviewing the Business/IT Portfolio and emerging technologies to bring about the best, integrated solutions for the enterprise. The Documenter/Author is responsible for providing information regarding updates to the various Enterprise Architecture Framework Elements to the Reviewer and the Communicator. After the Documenter/Author receives the results of the evaluation from the Reviewer, the Documenter/Author is responsible for updating the Enterprise Architecture Framework Elements to include a summary of the results for historical purposes.
- *Implementation Recommendation:* The role of Documenter/Author is best implemented as a committee. A consensus opinion must be put into the documentation. Architecture Documenters often make up Domain Committees responsible for documenting the discipline set that makes up their assigned domain.
- *Checks and Balance:* The role of Documenter/Author can be filled by contributors from the organization's Subject Matter Expert, Support Teams, and/or Project Teams. The combination of the role of Documenter/Author with the role of Reviewer and/or Communicator is not recommended.
- *Full-time/ Part-time:* The role of Documenter/Author is recommended as part-time. At the start of the Architecture documentation period, this may be a full-time role.
- *Contribution Significance:* CRITICAL
- *Missing Contribution Risk:* No documented business, information, technical architecture blueprints, or solution sets available for communication, review or compliance.

Communicator

- *Description:* The Communicator is the conduit for Enterprise Architecture information into the enterprise. An individual with experience in technical writing and/or end user reporting, best fills the Communicator role. This individual can be a junior level IT staff member. Based on parameters established by the Manager, the Communicator both pulls information on behalf of a request and pushes information to the Audience. Information is provided to the Communicator from the following three roles:
  - The Documenter
  - The Reviewer
  - The Manager

Though information can be requested from any of the Architecture roles, the requests will come primarily from the following roles or groups including:

  - Audience
  - Service Teams
  - Project Teams
  - Subject Matter Experts
  - Special Interest Group

- *Implementation Recommendation:* Every individual involved in the enterprise architecture effort has certain inherent communications responsibilities as defined by their designated role. However, the role of Communicator is best implemented as an individual rather than a committee. Precise, formal communication is needed. Differing communication styles can cause for confusion to the Audience.
- *Checks and Balance:* The Communicator role may be combined with the Reviewer and/or Manager. Combining Communicator role with the role of Documenter/Author is not recommended.
- *Full-time/ Part-time:* The Communicator role is recommended as part-time.
- *Contribution Significance:* CRITICAL
- *Missing Contribution Risk:* Lack of visibility, understanding, and accountability in the Architecture Blueprint. Compliance is difficult to ascertain absent an understanding of the previous Audience communication that identified the version of the Architecture Blueprint used for future compliance reviews.

Advisor

- *Description:* An Advisor should be an executive that provides clarity and support to the Manager of the enterprise architecture. This Advisor serves as a representative of the Strategic Elements from both the business and IT communities within the enterprise. This executive will also provide guidance on enterprise architecture variance requests from a business and economic perspective.
- *Implementation Recommendation:* This role can be implemented as an individual, multiple individuals, or a committee. Guidance, decisions, and direction are needed that encompasses all organizations within the enterprise. Advisors should be identified in a manner that effectively represents the enterprise.
- *Checks and Balance:* This role can be combined with the roles of Champion. The Advisor can be a Reviewer but should not be the only Reviewer. The combination of role of Advisor with the role of Manager is not recommended.
- *Full-time/ Part-time:* The Advisor role is recommended as part-time.
- *Contribution Significance:* Necessary
- *Missing Contribution Risk:* A well-rounded perspective of the enterprise needs and requirements will be absent**.**

Reviewer

- D*escription:* The Reviewer should be an executive or senior-level IT person. The Reviewer is responsible for evaluating the suggested Architecture Governance Elements changes for the Manager. The Reviewer may seek advice from the various Subject Matter Experts prior to making a recommendation. The Reviewer may need clarity from the Documenter.

For Architecture Review Items that require executive approval, the Reviewer will ask the Manager for assistance. Reviewer provides recommendation and reviewed information to the Communicator and the Manager.

- *Implementation Recommendation:* The role of Reviewer is best implemented as a committee. More than one opinion must be put into the review.
- *Checks and Balance:* The role of Reviewer can be combined with the roles of Communicator and can be staffed from individuals from the organization's Subject Matter Expert, Support Teams, and/or Project Teams. The combination of role of Reviewer with the role of Documenter/Author is not recommended.
- *Full-time/ Part-time:* The Reviewer role is recommended as part-time.
- *Contribution Significance:* CRITICAL
- *Missing Contribution Risk:* Lacking more than one set of eyes for quality assurance and variety of perspectives.

Approver

- *Description:* An Approver should be a mid-to-executive level member of the management team that provides leadership and direction to the Manager of the enterprise architecture. This approver serves as a business representative with the understanding of the overall organizational strategies, plan, and directions from both the business and IT communities within the enterprise. The Approver also provides leadership and direction to all parties engaged in architecture activities, regardless of their line of business or technical affinities. This individual will also provide final resolution on the approval or rejection of enterprise architecture variance requests from a business and economic perspective.
- *Implementation Recommendation:* The role of the approver is best implemented as a committee. Guidance, decisions, and direction are needed that encompasses all organizations within the enterprise so the committee should be staffed accordingly. Approvers should be identified in a manner that effectively represents the enterprise.
- *Checks and Balance:* This role can be combined with the roles of Champion. The Approver can be a Reviewer but should not be the only Reviewer. The combination of role of Approver with the role of Manager and Advisor is not recommended.
- *Full-time/ Part-time:* The Approver role is recommended as part-time.
- *Contribution Significance:* Necessary
- *Missing Contribution Risk:* Enterprise Architecture accountability, decision authority, and a well-rounded perspective of the enterprise needs and requirements will be absent**.**

Audience

- *Description:* The Audience role is made up of various groups of identified stakeholders in the Architecture Governance Elements, including:
  - Enterprise executives, departmental managers, and enterprise business leaders
  - Internal and external IT Staff that are creating and maintaining IT services for the enterprise.
  - Vendors that provide or wish to provide technology solutions to the enterprise
  - Various enterprise architecture team members
  - Executive IT staff members.

- *Implementation Recommendation:* See the above description for the various implementations of this role.
- *Checks and Balance:* None
- *Full-time/ Part-time:* The role of Audience is considered part-time.
- *Contribution Significance:* Necessary
- *Missing Contribution Risk:* Lack of architecture stakeholders. Must identify those held accountable for compliance and ensure communications are delivered in a timely manner.

SUPPORTING CONTRIBUTORS

Subject Matter Experts

- *Description:* These individuals or groups refer to an internal or external entity that provides expert knowledge on a given subject. Subject Matter Experts contribute information to the following:
  - Documenter
  - Reviewer
  - Service Teams
  - Project Teams
- *Implementation Recommendation:* Subject Matter Experts are most effective when implemented as a committee or a group. More than one opinion must be put into the expert advice.
- *Checks and Balance:* Subject Matter Experts can fill the roles of Documenters, or can participate as members of Support Teams, Project Teams, or architects. Subject Matter Expert should not fill the role of Reviewer as this may lead to the proliferation of self-interest.
- *Full-time/ Part-time:* This Subject Matter Expert is recommended as a part-time function.
- *Contribution Significance:* Necessary
- *Missing Contribution Risk:* Possible inclusion of incorrect product or compliance criteria into the architecture blueprints.

Services Teams

- *Description:* Services Teams support the existing business/IT portfolio for the enterprise. They review Strategic and Tactical Initiatives to determine whether existing service and/or technology can be utilized to solve the initiative. When extending the existing service/technology, the Service Teams communicate new compliances and/or the need for version updates to the Documenter. This allows for continuous improvement to the Architecture Blueprint.
- *Implementation Recommendation:* None
- *Checks and Balance:* None
- *Full-time/ Part-time:* Services Team are utilized in a part-time capacity.
- *Contribution Significance:* Necessary
- *Missing Contribution Risk:* Could not supply day-to-day services to the enterprise. Necessary to enterprise architecture to verify the Architecture Blueprint is providing the plan for achieving services.

Project Teams

- *Description:* Project Teams align Strategic/Tactical initiatives with possible service and/or technology solutions. In determining the best solution the Project Team may:
  - Review the Architecture Blueprint.
  - Seek further technology scans in emerging solutions.
  - Provide information on existing solutions.

  When requesting new service/technology or extending existing service/technology, the Project Team is responsible for reviewing and adhering to Architecture Compliance.
- *Implementation Recommendation:* None
- *Checks and Balance:* None
- *Full-time/ Part-time* Project Teams are a part-time user of the enterprise architecture.
- *Contribution Significance:* Necessary
- *Missing Contribution Risk:* Could not enhance/extend the existing services for the enterprise in large-scale efforts in a consistent and organized fashion without the daily interruptions for existing services. This function is necessary for the vitality of the enterprise architecture in seeking out new services/technology to extend the Architecture Blueprint.

Procurement Manager

- *Description:* The Procurement Manager is responsible for the procurement policies and procedures. These policies and procedures are external to the enterprise architecture; however, the interface with the enterprise architecture processes is essential to assure that purchases have been correctly evaluated and documented in the Architecture Blueprint.
- *Implementation Recommendation:* None.
- *Checks and Balance:* None
- *Full-time/ Part-time:* The Procurement Manager is a part-time advisor to the enterprise architecture groups.
- *Contribution Significance:* CRITICAL
- *Missing Contribution Risk:* This function is critical to the purchasing of new services and technologies for the enterprise. This function is critical to enterprise architecture and ensures that purchase requests adhere to the Architecture Compliance process prior to purchase.

Project/ Services Methodology Communicator

- *Description:* The Project and Services Communicator is responsible for communicating the methodologies and procedural steps to be followed when providing services and project support to the enterprise. The methodology should be adapted to include steps for Architecture Review and Compliance.
- *Implementation Recommendation:* None
- *Checks and Balance:* None
- *Full-time/ Part-time:* The Project/ Services Methodology Communicator is a part-time advisor to the enterprise architecture groups.
- *Contribution Significance:* Necessary

- *Missing Contribution Risk:* Critical to consistent and timely delivery of extensions and services to the enterprise. Necessary to enterprise architecture to verify that Architecture Compliances are done in a timely manner according to the Project and Service methods, policies, and procedures.

Special Interest Groups

- *Description:* Special Interest Groups can vary greatly in make-up as well as interests. They can be both internal and external to the enterprise. An example of internal special interest groups would be a Geographical Information Systems Advisory Group. Examples of external special interest groups would include citizen groups associated with libraries or the state's educational system. Special interest groups provide advisory input into the enterprise architecture by identifying special needs, interests, or considerations, as well as enterprise architecture compliance requirements specific to the group.
- *Implementation Recommendation:* Special Interest Groups are implemented as a committee or group. Generally, the input is the consensus of the groups and is provided to the Manager or Documenter.
- *Checks and Balance:* Special Interest Groups should not be combined with any other role.
- *Full-time/ Part-time:* Part-time as needed.
- *Contribution Significance:* HELPFUL
- *Missing Contribution Risk:* Lacking multiple perspectives on what would benefit the enterprise.

Enterprise Executive

- *Description:* Enterprise Executive provides the Strategic Elements that give direction, goals and objectives to the enterprise. Enterprise Executive is typically an executive role, potentially at the level of governor/mayor or equivalent and is responsible for ensuring the enterprise goals and objectives are set by the state/county/municipality.
- *Implementation Recommendation:* Enterprise Executives are implemented as an individual or group of individuals tasked with strategically aligning the enterprise.
- *Checks and Balance:* The role of Enterprise Executive can be combined with role of Advisor.
- *Full-time/ Part-time:* This Enterprise Executive role is recommended as part-time.
- *Contribution Significance:* CRITICAL
- *Missing Contribution Risk:* Absent the Strategic Elements, implemented technology would not relate to the business of the enterprise.

Each organization will create its Architecture Governance structure based on the previously described roles. The following section provides several examples of how various government organizations implement these roles.

Governance Samples

Successful architecture governance models that have been implemented by municipal, county and state governments are provided as examples of working architecture governance models. The sample governance models in general are not purely representative of governance; they intermingle IT/business organizations and positions not specifically related to architecture governance with the governance roles.

Samples of governance models representing State government include:

- State of Missouri
- Commonwealth of Kentucky
- State of Arkansas
- State of Kansas
- State of Washington
- State of North Carolina

Samples of governance models representing municipal and county government include examples from:

- Philadelphia, Pennsylvania
- San Diego, California
- Virginia Beach, Virginia
- Fairfax County, Virginia

The samples are represented with an organizational chart graphic followed by a description of significant organizational function for each of the governance models. The majority of the samples were developed utilizing a typical organizational chart structure with typical position titles, while the architecture roles previously identified in this Tool-Kit are functional in nature. A cross-reference column is included in the significant organizational function lists that map the governance model components to the architecture roles. Roles identified within the samples are defined by the providing enterprise and interpreted for the purpose of this discussion. In some cases, the rationale for the mapping may not be apparent.

Applicability In The Judicial Environment

The illustrated governance models contained within this document are primarily based on the executive branch of government. The components are equally applicable in the judiciary or legislative branch of government by simply inserting the appropriate Enterprise Executive for the enterprise and applying the other roles and functional relationships as they apply. Established Judicial Branch Governance models, if illustrated, are similar to those identified for the executive branch.

Ideally, an enterprise governance structure in a municipal, county or state government would encompass all applicable entities of the Executive, Legislative and Judicial branches of government.

A good example of this is the illustrated Kansas Governance model, which effectively incorporates all three branches in the governance process. All enterprise decisions at the executive level are by joint decree. All three branches have equal say in the process. It is possible to implement a variation of this model using a structure that allows for independent decision making on issues that are only germane to a specific branch of government.

The requirement to keep the three branches of government separate is more strictly enforced in some enterprise environments. This strict enforcement often prevents in-depth involvement by all members of the government branches. The illustration of Kentucky's governance model is a good example of this situation. Originally, the judicial branch participated as a voting member in Kentucky's governance structure. The Kentucky Supreme Court ruled the participation was unconstitutional, preventing their continued participation. The Judicial Branch, however, is still participating in the process by presenting their business case and having it influence the direction of the enterprise.

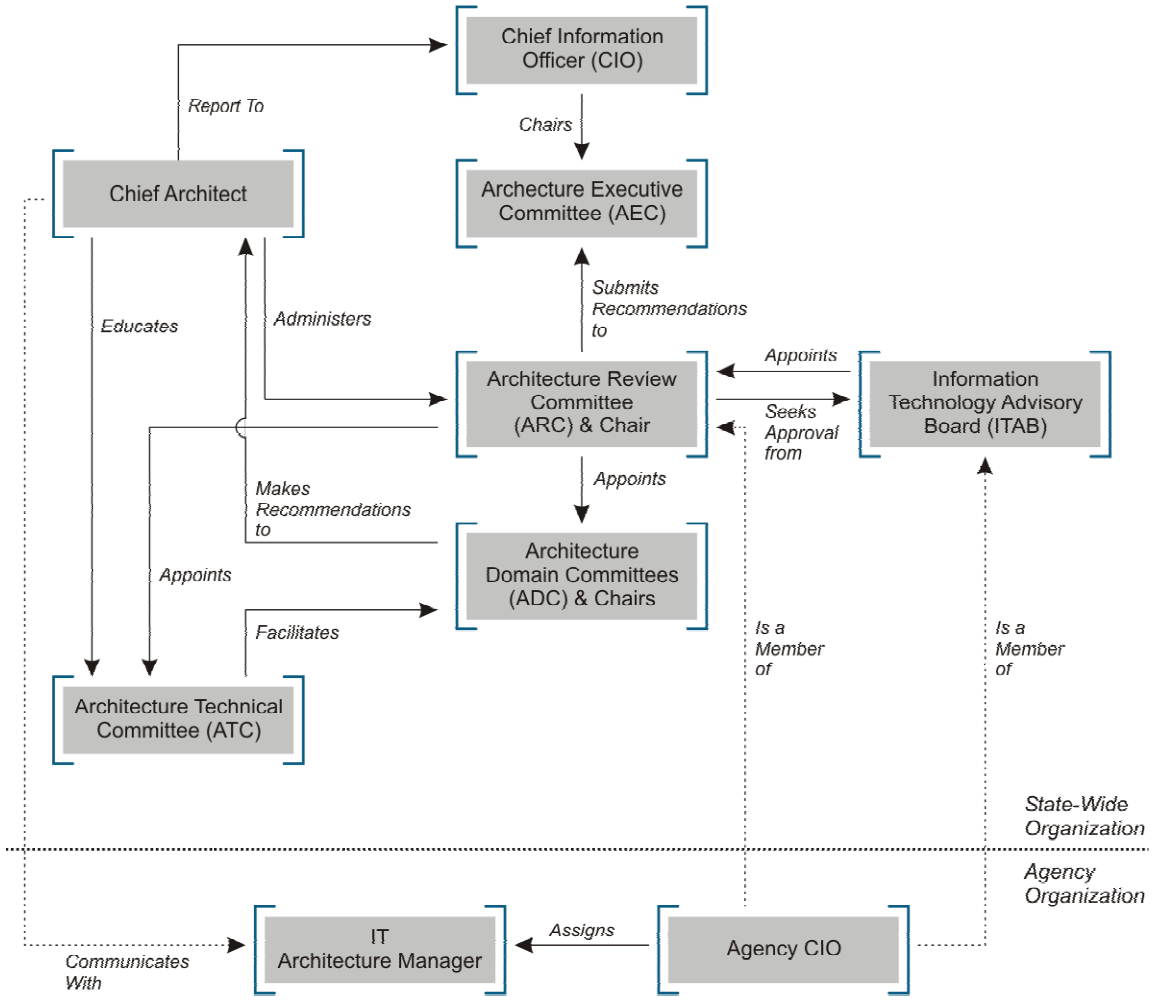
The key is to set up the governance model so that all branches of government can participate. Strong executive leadership is critical in promoting the partnership between the three branches of government and implementing a strong governance model for the enterprise.

GOVERNANCE MODELS

The following examples represent successful Architecture Governance Models implemented in the State of Missouri, the Commonwealth of Kentucky, the State of Arkansas, the State of Kansas, the State of Washington and the State of North Carolina, as well as in the municipal and county government entities for Philadelphia, PA; San Diego, CA; Virginia Beach, VA; and Fairfax County, VA. A description of significant organizational functions of the governance model is provided for each example.

STATE GOVERNMENT – MISSOURI

The following diagram illustrates the Architecture Governance Model for the State of Missouri.



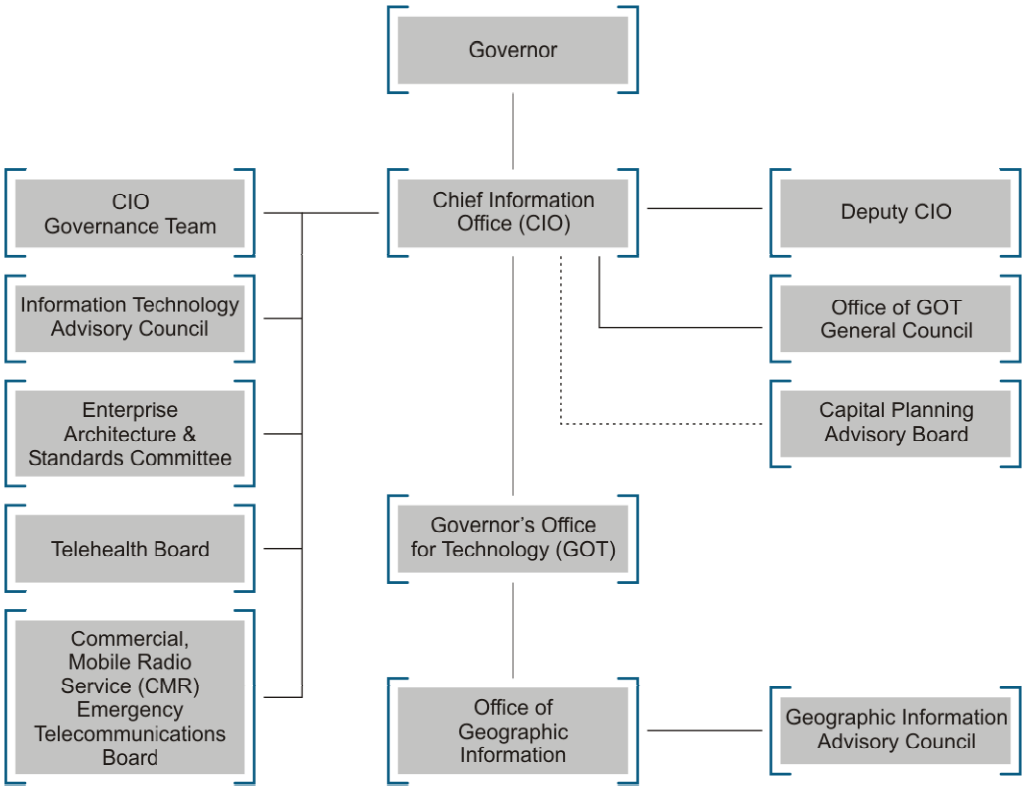
Significant Organizational Functions

The following list identifies the significant organizational functions of the Architecture Governance Model for the State of Missouri.

Functions	*Description*	*Governance Role Mapping*
Chief Information Officer (CIO)	Champions the architecture effort, promotes architecture value, ensures architecture success, assigns appropriate resources, and manages architecture principles. Has IT project approval for large budget projects and supports the budget and appropriation process on behalf of other agencies.	Champion
Architecture Executive Committee (AEC)	Approves architecture variations, reviews project plans, risk strategy for consistency with architecture.	Advisor
Chief Architect	Implements management processes; educates facilitators and users; manages targets and performance measures, manages implementation plan; manages architecture contents; administers compliance reviews; develops domain templates; and administers ARC.	Manager, Communicator
Architecture Review Committee (ARC)	Submits architecture recommendations to AEC, reviews architectural changes, reviews requests for variance, establishes architecture management processes; appoints Facilitators and Architecture domain committees & chairs.	Reviewer
Architecture Domain Committees (ADC)	Recommend architecture standards, provides domain guidance to agencies, and provide technical assistance on architecture domain issues.	Documenters
Architecture Technical Committee (ATC)	Educate domain committees, facilitate domain sessions, assure adherence to methodology, ensure consistent enterprise view, gain consensus of ADC members, serve as methodology experts, and handle special projects.	Subject Matter Experts
Information Technology Advisory Board (ITAB)	This board consists of the department level CIOs and/or IT directors. Implements strategic plan and develops IT strategies. Critical to endorsing CIO initiatives. Functions as the key contact with project stakeholders. Staff many of the committees for policy and standards.	N/A
IT Architecture Manager	Establishes & manages departmental compliance process; communicates to and educates developers, users, & mgrs; establishes architecture targets and measurements; manages departmental architecture database; manages architecture implementation plan; assures adherence to methodology; and acts as a potential members of ATC.	Subject Matter Experts
Agency CIO	Owns department-level architecture.	Audience

STATE GOVERNMENT – KENTUCKY

The following diagram illustrates the Architecture Governance Model for the Commonwealth of Kentucky.



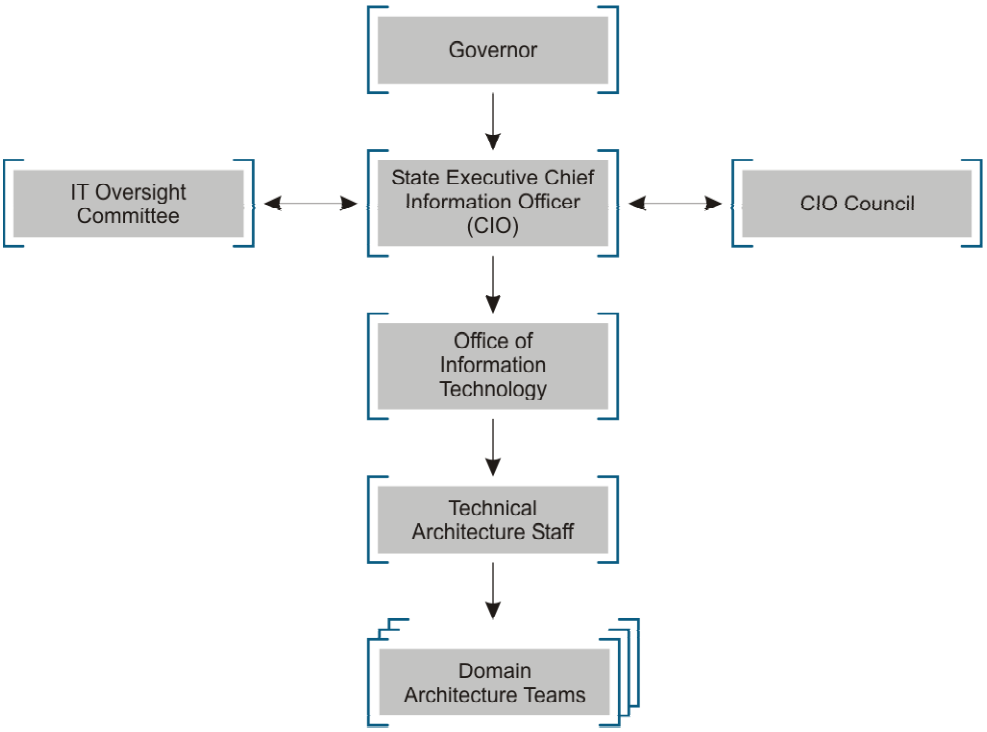
Significant Organizational Functions

The following list identifies the significant organizational functions of the Architecture Governance Model for the Commonwealth of Kentucky.

Functions	*Description*	*Governance Role Mapping*
CIO	Oversees developing, implementing and managing strategic information technology directions, standards and enterprise architecture, including implementing necessary processes to ensure full compliance with those directions, standards and architecture.	Champion, Manager, Advisor
Deputy CIO	Provides support to the CIO for developing, implementing and managing strategic information technology directions, standards and enterprise architecture, including implementing necessary processes to ensure full compliance with those directions, standards and architecture.	Subject Matter Expert
Enterprise Architecture and Standards Committee	Chaired by the CIO. Composed of multiple agency representatives and is administered and supported by the Division of Planning and Architecture, Governor's Office for Technology. Responsible for governing the architecture and standards process.	Documenter
Governor's Office For Technology	This office was established by the legislature to help ensure that the information technology direction of the state adequately supports the needs of the citizens of the commonwealth. Extensive responsibilities including providing support to the CIO for enterprise level initiatives. Manages enterprise level systems and services.	Reviewer, Communicator, Project / Services Methodology Communicator, Overseer
CIO Governance Team	Formed by the CIO (not required by statute). Represents all agency CIOs. Operates as the IT policy and investment board.	Services Team, Project Team,
Information Technology Advisory Council	Advises the CIO on IT issues.	Subject Matter Experts
Telehealth Board	Advises the CIO and IT community on IT issues relating to health.	Special Interest Group
Commercial Mobile Radio Service (CMRS) Emergency Telecommunications Board	Advises CIO and IT community on IT issues relating to mobile radio services and emergency telecommunications issues.	Special Interest Group
Geographic Information Advisory Council	Advises the CIO and IT community on IT issues relating to geographic information.	Special Interest Group

STATE GOVERNMENT - ARKANSAS

The following diagram illustrates the Architecture Governance Model for the State of Arkansas.



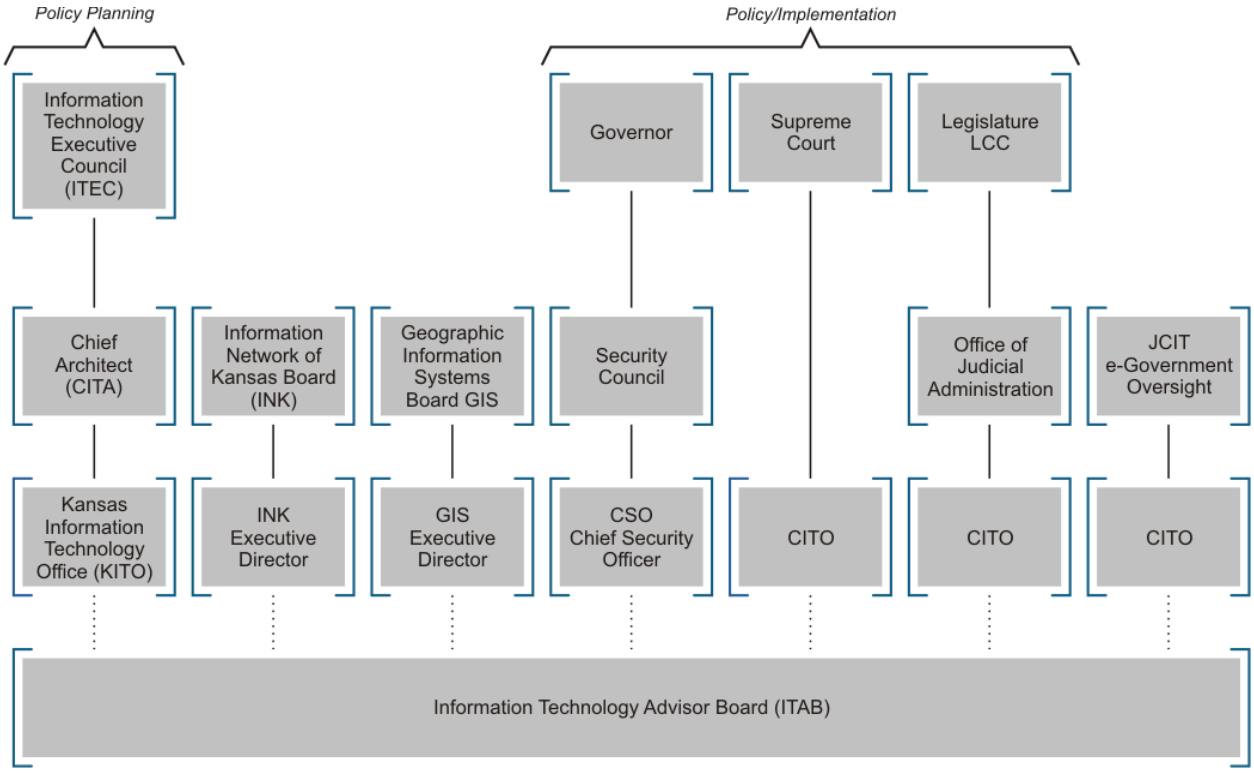
Significant Organizational Functions

The following list identifies the significant organizational functions of the Architecture Governance Model for the State of Arkansas.

Functions	*Description*	*Governance Role Mapping*
State Executive CIO	Directs the formulation of policies, standards and guidelines for IT in the state; reports to the Governor.	Champion, Manager, Advisor
CIO Council	Provides leadership in coordinating information technology in the state; made up of agency CIOs.	Subject Matter Experts
IT Oversight Committee	Committee of private and public entities to advise executive CIO on allocation of information technology resources used by the state.	Overseer, Special Interest Group
Office of Information Technology	Acts as CIO's staff; oversee agency IT planning and review; administer enterprise projects; ensure IT project alignment with state technical architecture; houses technology investigation center; houses state GIS office.	Communicator, Reviewer, Service Teams, Project Teams
Technical Architecture Staff	Work under the direction of the state executive CIO within the Office of Information Technology; facilitate domain architecture teams.	Documenter
Architecture Domain Teams	Business and technical staff from state agencies that research and come to consensus on standards, best practices and policies.	Documenter

STATE GOVERNMENT – KANSAS

The following diagram illustrates the Architecture Governance Model for the State of Kansas.



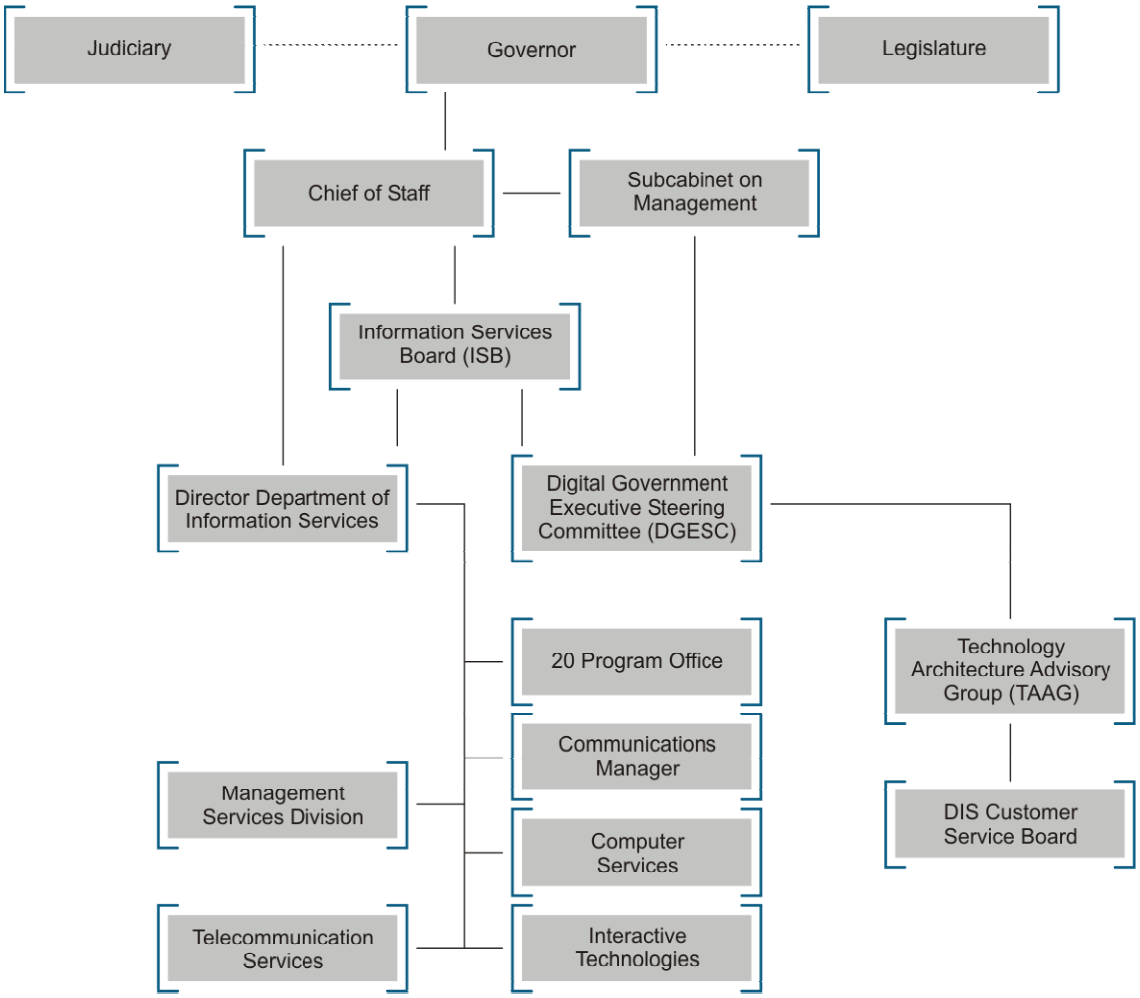
Significant Organizational Functions

The following list identifies the significant organizational functions of the Architecture Governance Model for the State of Kansas.

Functions	*Description*	*Governance Role Mapping*
Information Technology Executive Council (ITEC)	Responsible for adopting information technology resource policies and procedures and project management methodologies for all state agencies/offices; an enterprise information technology architecture, including telecommunications systems, networks and equipment, that covers all state agencies/offices; standards for data management for all state agencies/offices; and a strategic information technology management plan for the state.	Overseer, Champion, Advisor, Reviewer
Chief IT Architect (CITA)	Non-voting member of the ITEC. Develops and recommends information technology resource policies and procedures and project management methodologies for all state agencies/offices; an information technology architecture, including telecommunications systems, networks and equipment, that covers all state agencies/offices; standards for data management for all state agencies/offices; and a strategic information technology management plan for the state.	Manager, Documenter
CHIEF INFORMATION TECHNOLOGY OFFICER (CITO)	Responsible for implementing information technology resource policies and procedures and project management methodologies; an information technology architecture, including telecommunications systems, networks and equipment; standards for data management; and the strategic information technology management plan for the requisite branch of government. CITO also approves all projects and bid specifications over $250,000. Every quarter the CITO reports the status of projects.	Communicator
Information Technology Advisory Board	Functions as a technical resource to the CITO for the executive branch.	Subject Matter Experts

STATE GOVERNMENT – WASHINGTON

The following diagram illustrates the Architecture Governance Model for the State of Washington.



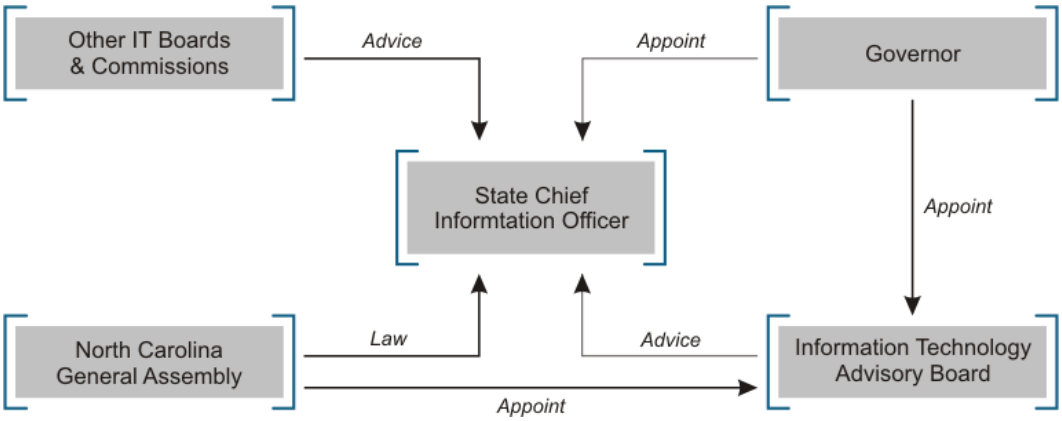
Significant Organizational Functions

The following list identifies the significant organizational functions of the Architecture Governance Model for the State of Washington.

Functions	*Description*	*Governance Role Mapping*
Information Services Board (ISB)	Establishes IT policy, direction, IT plans and technology standards.	Overseer, Champion, Manager
Digital Government Executive Steering Committee (DGESC)	Membership includes the Office of the State Treasurer, Office of the Secretary of State, Office of the State Auditor and Office of Financial Management. Provides enterprise-wide business policy guidance, recommendations, issue resolution and coordination to achieve the goals of the digital government program.	Advisor
Technology Architecture Advisory Group (TAAG)	Makes recommendations to the DGESC regarding technical requirements, tool selection and objectives for e-commerce infrastructure and services, including design of electronic authorization technologies, access control and directory services. The TAAG also participates in the development of digital government policy, standards and guidelines. This group is composed of senior level agency IT managers drawn from the DIS Customer Service Board.	Reviewer, Subject Matter Expert
Department of Information Services (DIS) Customer Advisory Board	Provides technical expertise and guidelines for digital government; coordinates and supports interagency communications; develops and implements new technology infrastructure and services; advises on funding to support agency digital government services; and provides staff support to the ISB.	Communicator, Documenter, Subject Matter Expert, Project / Services Methodology Communicator

STATE GOVERNMENT – NORTH CAROLINA

The following diagram illustrates the Architecture Governance Model for the State of North Carolina.



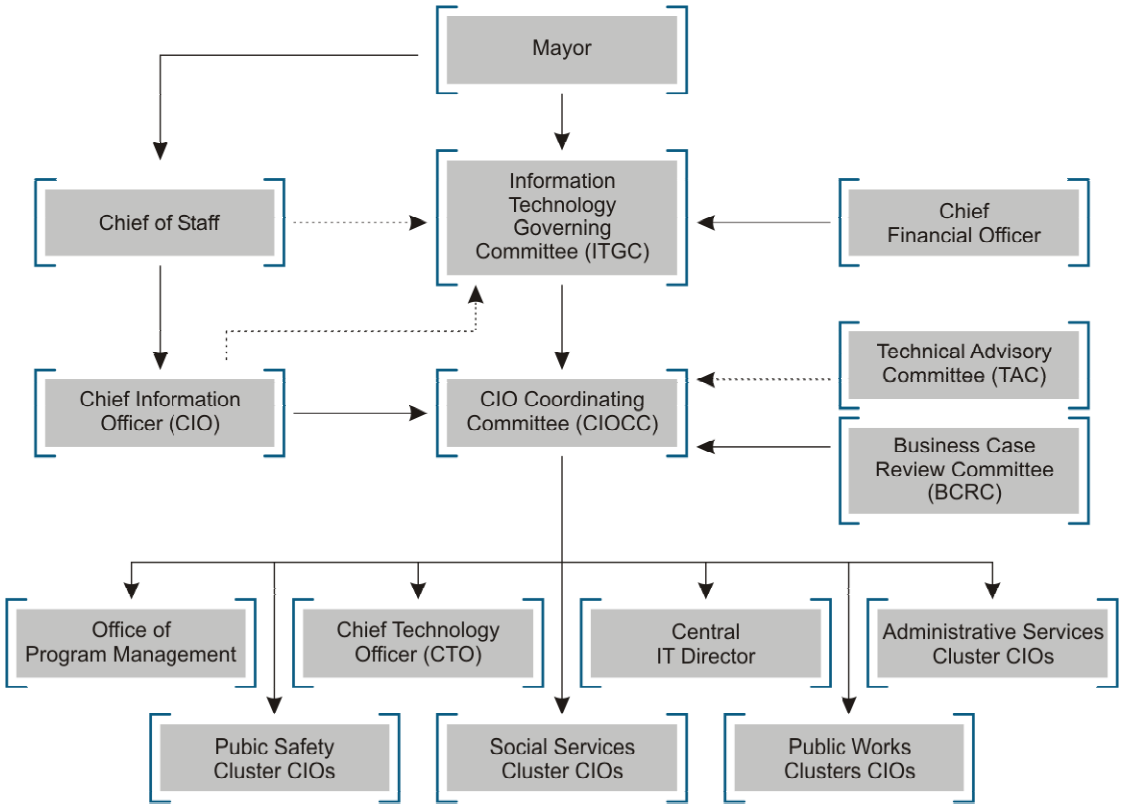
Significant Organizational Functions

The following list identifies the significant organizational functions of the Architecture Governance Model for the State of North Carolina.

Functions	*Description*	*Governance Role Mapping*
CIO	The head of Information Technology Services. State CIO reports directly to the Governor. Identifies IT polices. Develops state IT Plan.	Champion, Manager, Overseer
	Provides statewide common IT services – computing, telecommunications, etc. Responsible for statewide IT strategies and develops state-wide IT initiatives..	
	Through the ETS office, the state CIO provides Technical Architecture, QA and Project Approval, Information Privacy and Protection, and E-Government.	Documenter, Communicator
Information Technology Advisory Board (ITAB)	Board consisting of 12 members: 4 appointed by Governor, 4 appointed by Senate, 4 appointed by House of Representatives.	Advisor, Reviewer
	Reviews and comments on State IT Plan, developed by the state CIO.	
	Reviews and comments on IT plans, developed by executive branch agencies.	
	Reviews and comments on state-wide Technology initiatives, developed by the state CIO.	
CIO Council	A council consisting of representation of the agency CIOs. Provides advice to the state CIO.	Subject Matter Expert

LOCAL GOVERNMENT – PHILADELPHIA, PENNSYLVANIA

The following diagram illustrates the Architecture Governance Model for Philadelphia, Pennsylvania.



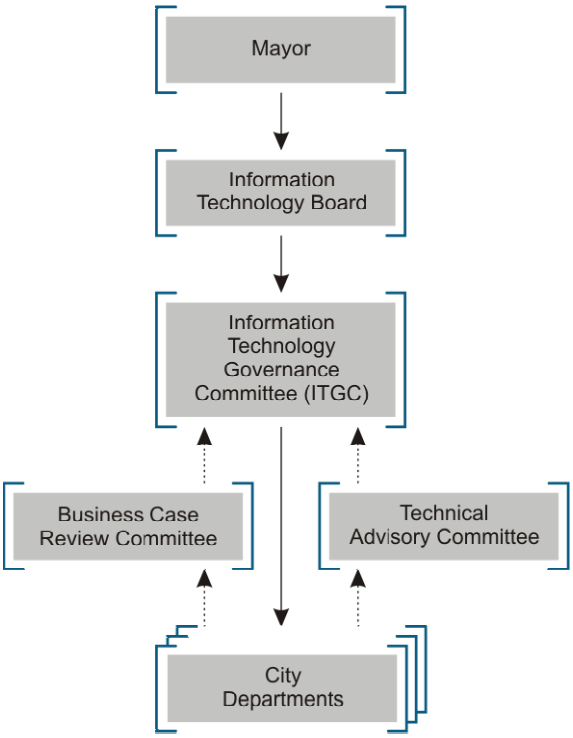
Significant Organizational Functions

The following list identifies the significant organizational functions of the Architecture Governance Model for Philadelphia, Pennsylvania.

Functions	*Description*	*Governance Role Mapping*
Information Technology Governing Committee (ITGC)	Chaired by the Chief of Staff with the CIO, CFO, & MDO making up the remainder of the committee. Responsible for management prioritization approval and resources allocation .	N/A
CIO	The CIO chairs the coordinating committee; is a member of the ITGC; manages the IT infrastructure of the city; and uses the input from the Cluster CIOs and to understand IT needs and priorities across the City.	Champion
Business Case Review Committee (BCRC)	Made up of Department Heads. The BCRC will review all business cases from their specific cluster and recommend sending the proposal to the CIO Coordinating Committee, send the proposal back to the department for additional work, or disapprove the project.	Advisor
Technical Advisory Committee (TAC)	Made up of Department IT Directors. The TAC will assist the CTO and CIO CC on design and architecture for IT systems and implementation of enterprise.	Subject Matter Expert
CIO CC	Responsible for strategic planning for IT: championing the impact of e-government, resource planning and control, systems and technology control, and budgetary control.	Reviewer, Communicator
CTO	In coordination with the CIO CC, responsible for design and architecture for IT systems and implementation of enterprise standards.	Documenter
CLUSTER CIOs	Cluster CIOs work with Department Heads to understand department-specific, cluster-specific and enterprise needs; represents cluster and department in CIO CC and advocates for projects accordingly; supervises department IT directors/managers and project managers.	Project Teams, Service Teams, Project / Services Methodology Communicator

LOCAL GOVERNMENT – SAN DIEGO, CALIFORNIA

The following diagram illustrates the Architecture Governance Model for San Diego, California.



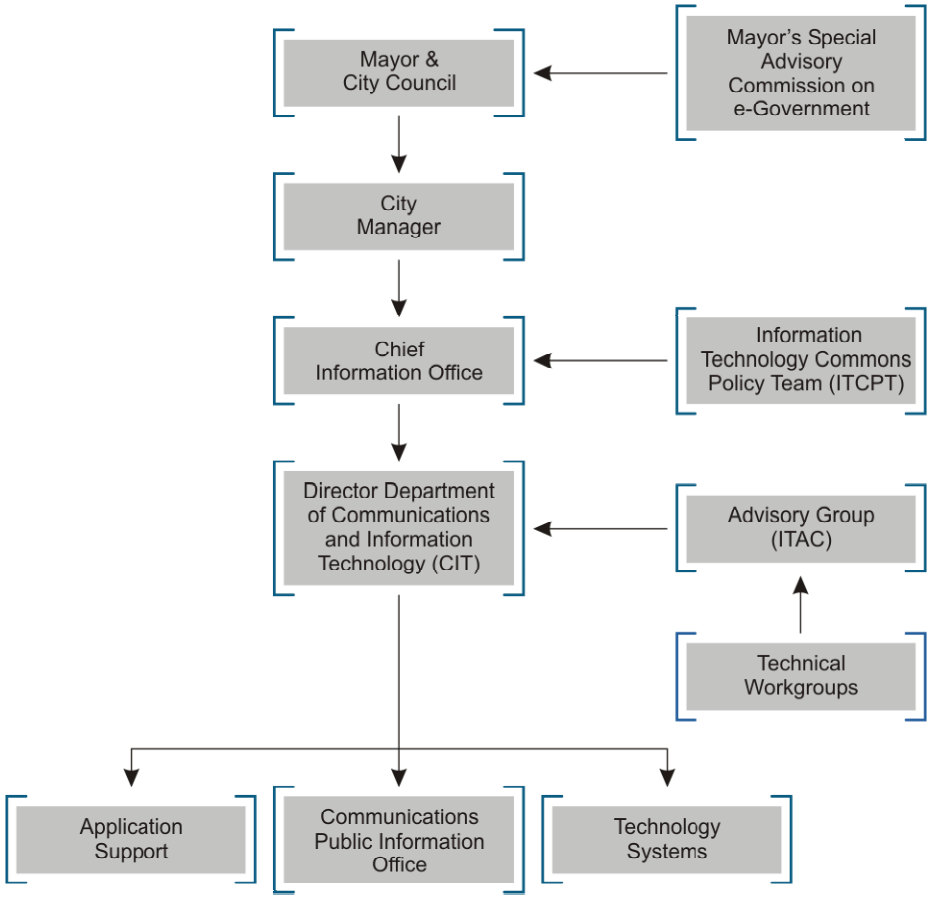
Significant Organizational Functions

The following list identifies the significant organizational functions of the Architecture Governance Model for San Diego, California.

Functions	*Description*	*Governance Role Mapping*
Information Technology Board	Responsible for establishing IT policy; approving IT strategic plans and IT annual budgets; defining and communicating business goals and objectives; and establishing support for high level IT initiatives.	Champion
Information Technology Governance Committee	Responsible for reviewing and prioritizing IT project proposals and annual IT budgets; approving business cases; delineate citywide, multi-dept. and single-dept. initiatives; review major projects; and approving IT standards.	Manager, Reviewer
Technical Advisory Committee	Advises the ITGC on architecture and standards; provides technical review and advice on projects; and ensures departmental IT initiatives are consistent with approved City architecture and standards.	Documenter
Business Case Review Committee	Reviews business cases; provides business case feedback to the (ITGC), provides guidance and assistance to Departments in evaluating significant issues associated with IT projects.	Advisor
City Departments	Advocate and sponsor IT projects; own and manage Department specific IT projects; define and monitor project accountability and success measures.	Project Teams, Service Teams, Project/Services Methodology Communicator

LOCAL GOVERNMENT – VIRGINIA BEACH, VIRGINIA

The following diagram illustrates the Architecture Governance Model for Virginia Beach, Virginia.



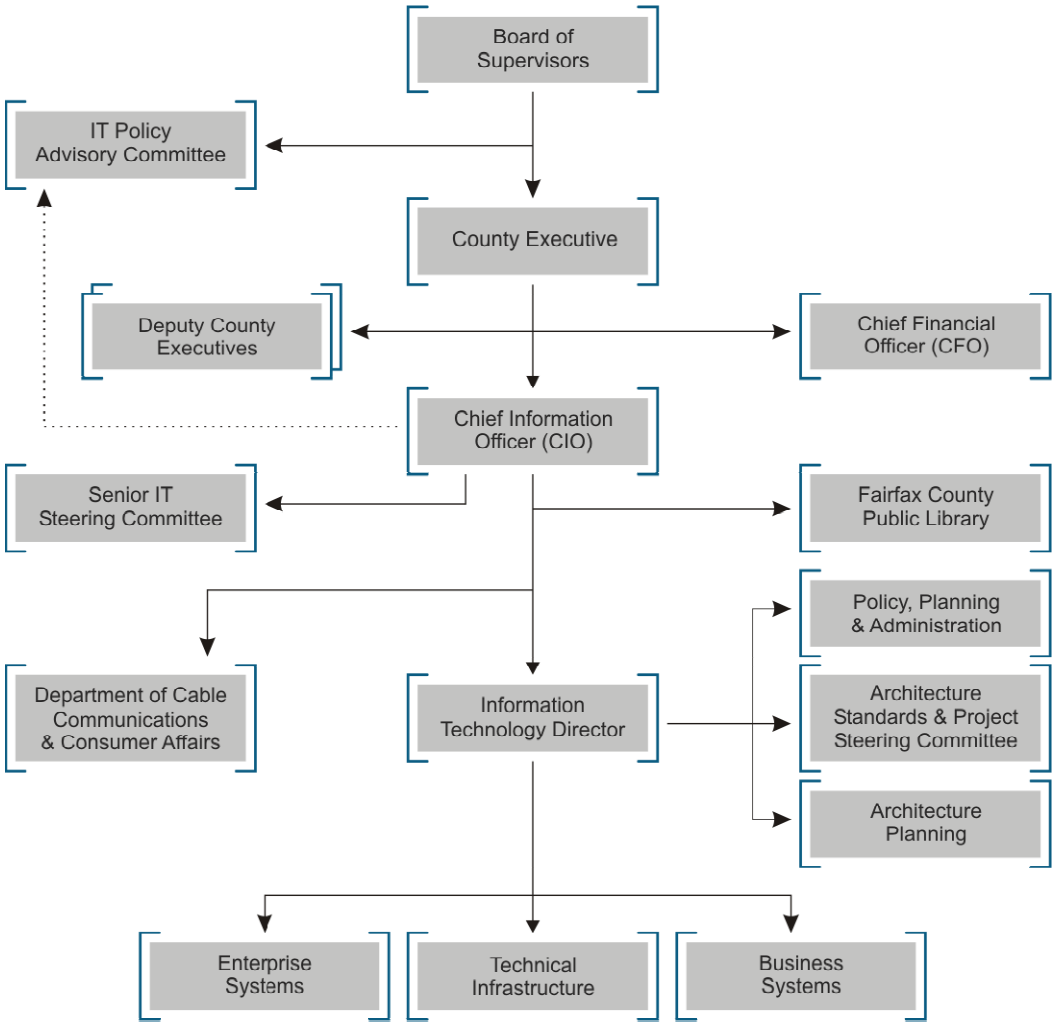
Significant Organizational Functions

The following list identifies the significant organizational functions of the Architecture Governance Model for Virginia Beach, Virginia.

Functions	*Description*	*Governance Role Mapping*
Mayor's Special Advisory Council on E-Government	Made up of citizen appointees. Provide citizen input to the Mayor on IT issues.	Special Interest Group
City Manager	Responsible for coordinating IT vision and city direction with department heads including the CIO.	Champion, Enterprise Executive
Chief Information Officer	The CIO is responsible for establishing Citywide architecture and standards, manages the IT infrastructure of the City and implements City IT policies.	Manager, Documenter
Information Technology Commons Policy Team (ITCPT)	Information Technology Governance Team – Made up of agency directors. Responsible for providing input to the CIO on agency business and IT needs.	Advisor, Reviewer
Director, Department of Communications and Information Technology	Member of the ITCPT. Responsible for operational aspects of implementing IT policies, standards and procedures.	Communicator
Information Technology Advisory Group (ITAC)	Advises the Director of CIT on Information Technology issues.	Subject Matter Expert
Technical Workgroups	Provides technical support to ITAC on IT efforts.	Subject Matter Expert
Applications Support	Responsible for application life-cycle support.	Services Team
Communications Public Information Office	Responsible for maintaining the City's website, providing telecommunications, video and E-911 services and support.	Services Team
Technology Systems	Responsible for supporting technology systems, GIS and printing for the City.	Services Team

LOCAL GOVERNMENT – FAIRFAX COUNTY, VIRGINIA

The following diagram illustrates the Architecture Governance Model for Fairfax County, Virginia.



Significant Organizational Functions

The following list identifies the significant organizational functions of the Architecture Governance Model for Fairfax County, Virginia.

Functions	*Description*	*Governance Role Mapping*
IT Policy Advisory Committee (ITPAC)	Private sector citizen representatives appointed by the Board of Supervisors - Critical to ensuring the Chairman and the Board of Supervisors that IT plans are following the right direction for the County and that IT funding is well spent. This group endorses the IT budget to the Board during budget hearings and are a critical part of the funding process.	Overseer, Special Interest Group
Senior It Steering Committee	Internal advisory group chaired by the CIO. Members include the County Executive, Chief Financial Officer, Deputy County Executives, Director of the Department of Information Technology and major department directors/stake holders. This group sets the overall strategic objectives for the County's IT program and is critical to ensuring that departments are a part of the IT planning process and that proposed IT projects are aligned with the County's overall direction.	Advisor
Chief Information Officer (CIO)	Works with the County Executive, Deputy County Executives, Chief Financial Officer, County departments and IT committees to ensure that that the IT program is meeting its objectives as approved by the Board of Supervisors. The CIO is responsible for the overall management of information and technology countywide and works to establish overall IT architecture, standards, policies and direction.	Champion, Manager
Director Of The Department Of Information Technology	Responsible for the day-to-day operation of the IT Department, infrastructure and projects countywide. The Director is critical to successful collaboration with departments and key IT project stakeholders in the County.	Project / Services Methodology Communicator
Policy, Planning And Administration	This group assists the Director of the Department of Information Technology and the CIO to manage IT enterprise project budgets and funding, produce the annual IT plan, manage the administration for the Department of Information Technology and enterprise IT projects, write IT policy and provide information security.	Advisor
Architecture Planning	Two IT architects, which report to the Director of the Department of Information Technology and focus on architecture from an infrastructure and software development standpoint.	Documenter
Architecture Committees, Standards Committees And Project Steering Committees	Critical to establishing cooperation/collaboration at the working level of the County organization. They are very important in producing the building blocks, architecture, standards, project proposals, statuses etc. for the other groups to review, consider approve etc.	Reviewer
Enterprise Systems	Department of Information Technology Division responsible for Geographic Information Systems, Land Development Systems, Public Safety Systems and E-government.	Services Team
Technical Infrastructure	Department of Information Technology Division responsible for Telecommunications (voice, video and data), Data Center operations, Technical Support Center and user support services.	Services Team

Functions	*Description*	*Governance Role Mapping*
Business Systems	Department of Information Technology Division responsible for Tax Systems, Finance/Procurement/Human Resources Systems, Training, Human Services Systems, Customer Relationship Management Systems and other miscellaneous systems.	Services Team

Architecture Governance Development

This section identifies the process that can be used as a guide by municipal, county or state government to identify a partial or complete architecture governance structure. The presented process is effective for all government levels independent of their maturity in the process of establishing governance. Use the process to identify gaps in existing governance structures and roles that can be added to existing organizations to enhance performance. The Governance Process consists of four sub-processes that will facilitate the documentation of the Governance Elements, Governance Roles, Architecture Lifecycle Processes, and Architecture Governance Organizational Charts. The four sub-processes are:

- Determine Architecture Governance
- Create Architecture Governance Structure
- Document/Update Architecture Lifecycle Processes
- Confirm Architecture Governance Structure

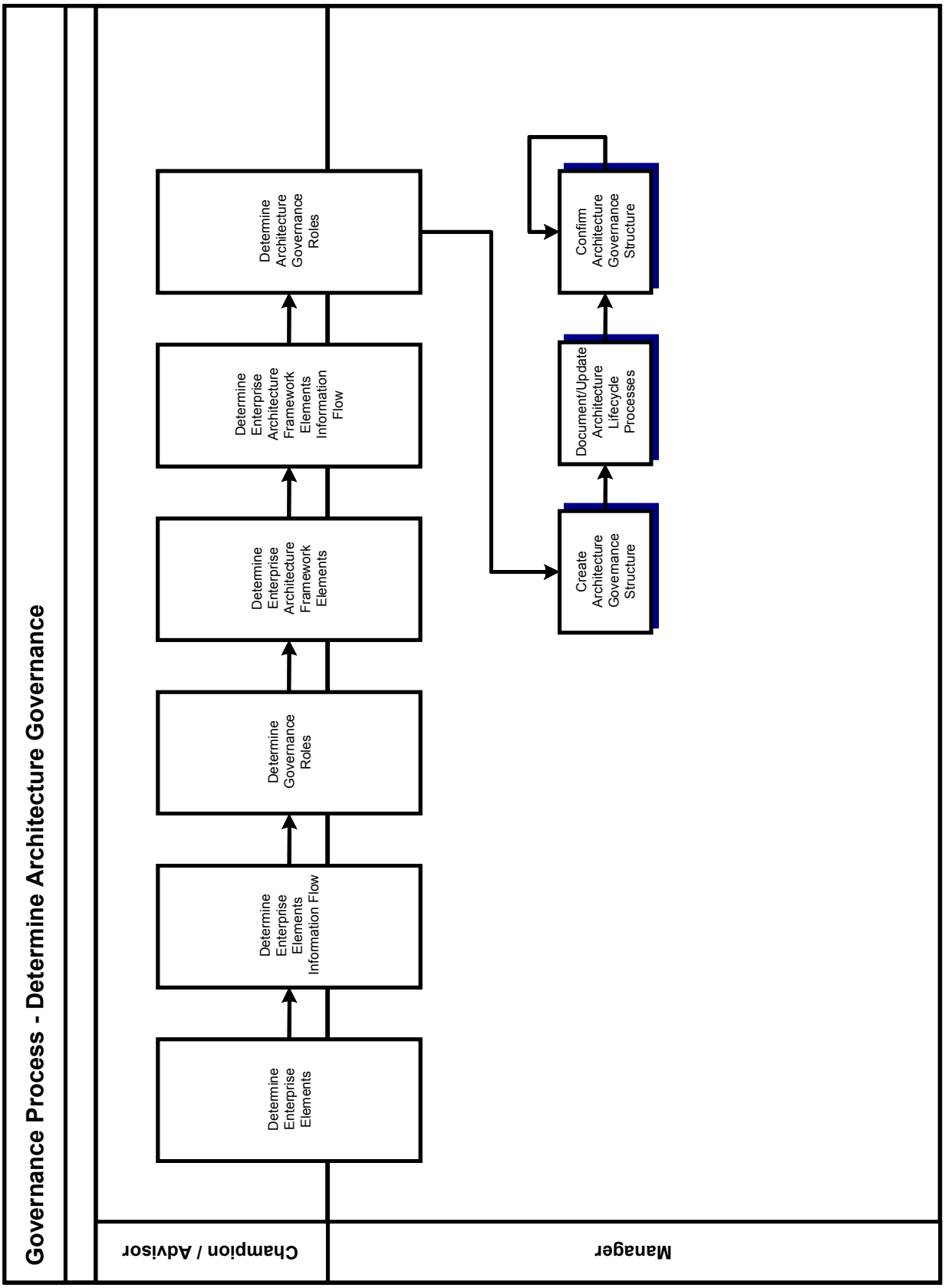
Each of these four sub-processes is presented in detail in this section. A Process Model is presented followed by a narrative of the detail for each of the sub-processes.

The process model for the first of the four sub-processes, "Determine Architecture Governance", is presented on the following page.

DETERMINE ARCHITECTURE GOVERNANCE

PROCESS OVERVIEW

This process entails the defining of the organization's governance based on an understanding of the elements to be governed, the relationship of those elements with each other, and the various governance roles needed to effectively manage the elements. Collaboration between the various roles, when executing these processes, will provide a better overall perspective.


Governance Process - Determine Architecture Governance
Champion / Advisor
Manager
Determine Enterprise Elements
Determine Enterprise Elements Information Flow
Determine Governance Roles
Determine Enterprise Architecture Framework Elements
Determine Enterprise Architecture Framework Elements Information Flow
Determine Architecture Governance Roles
Create Architecture Governance Structure
Document/Update Architecture Lifecycle Processes
Confirm Architecture Governance Structure

PROCESS DETAIL

Determine Enterprise Elements - An understanding of the various Enterprise Elements, objects in the enterprise that are governed by structure and/or process, that go into creating, supporting, and utilizing the Enterprise Architecture Framework Elements need to be determined.

Determine Enterprise Elements Information Flows - Once the Enterprise Elements are determined, document the relationship between the elements. This allows those objects that are specific to enterprise architecture to be scoped and the interdependencies documented.

Determine Governance Roles – Governance roles are determined based on the types of Enterprise Elements defined and the processes that will be executed against those elements. An understanding of these overall roles in the organization aids in setting up the enterprise architecture governance roles.

Determine Enterprise Architecture Framework Elements – Identification and documentation of the Enterprise Architecture Framework Elements should consider what is already provided through the Enterprise Elements. The purpose of enterprise architecture is to document the enterprise architecture elements that do not exist and provide ties to the Architecture Blueprint for previously existing objects.

Determine Enterprise Architecture Framework Elements Information Flow – Once the Enterprise Architecture Framework Elements are determined, document the relationships between the elements. This will identify the order for creation and update of the objects.

Determine Architecture Governance Roles – Architecture Governance roles are determined based on the types of Enterprise Architecture Framework Governance Elements and the processes that will be executed against those elements. Roles include such primary functionality as:

- Advisor
- Manager
- Reviewer
- Documenter
- Communicator
- Audience

The roles can also play supporting positions such as:

- Subject Matter Expert
- Team Member
- Other Managers
- Other Communicators

The remaining three-process steps represent sub-processes that branch off the Determine Architecture Governance Process. They will be presented in the same manner as independent processes in the remainder of this section:

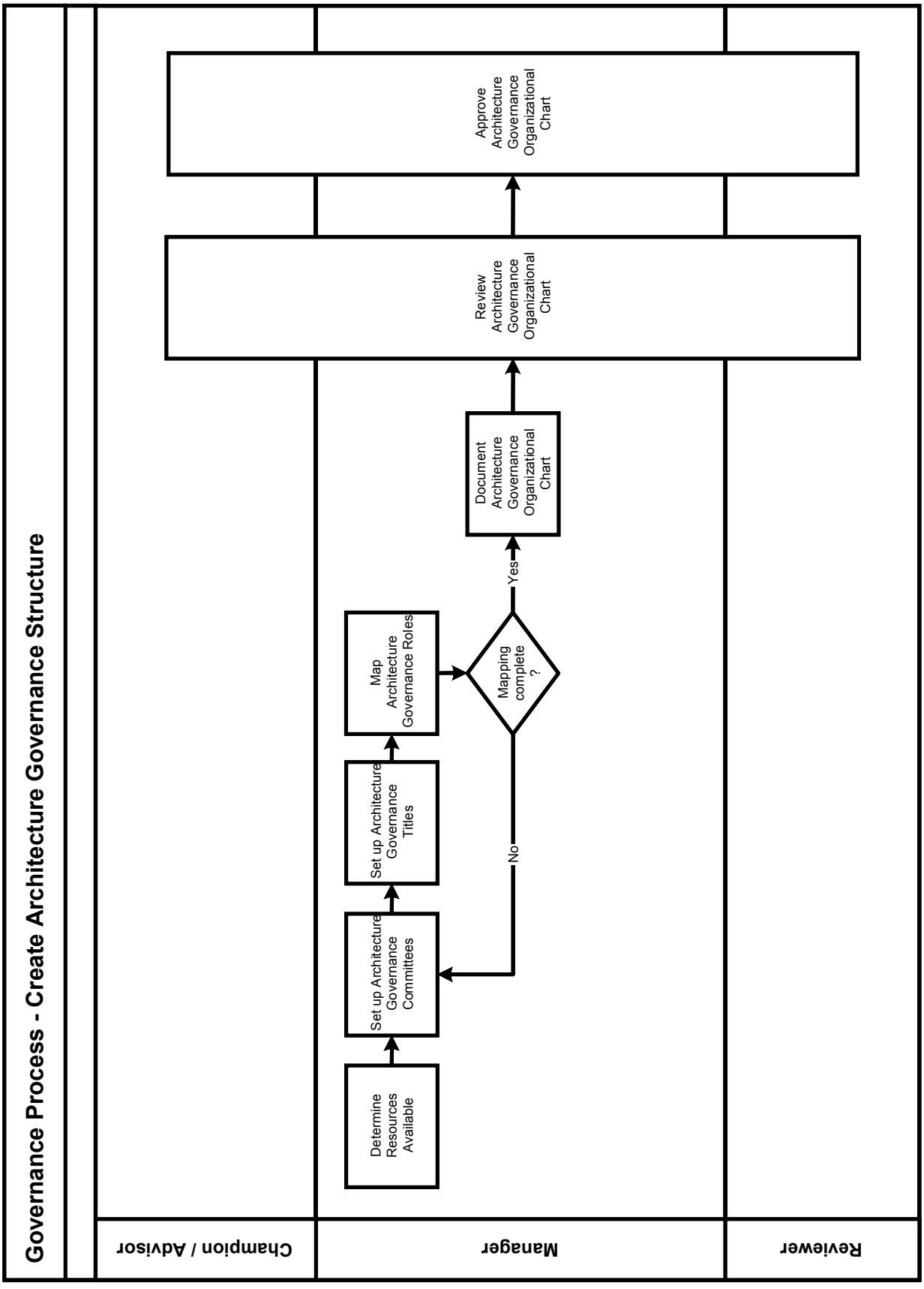
- Create Architecture Governance Structure
- Document/Update Architecture Lifecycle Processes
- Confirm Architecture Governance Structure

The process model for the second of the four sub-processes, "Create Architecture Governance Structure", is presented on the following page.

CREATE ARCHITECTURE GOVERNANCE STRUCTURE

PROCESS OVERVIEW

Create the architecture governance structure based on understanding the various Enterprise Architecture Framework Elements and architecture governance roles. Confirmation of the architecture governance structure occurs after the Architecture Lifecycle processes are finalized.


Governance Process - Create Architecture Governance Structure
Champion / Advisor
Manager
Reviewer
Determine Resources Available
Set up Architecture Governance Committees
Set up Architecture Governance Titles
Map Architecture Governance Roles
Mapping complete ?
No
Yes
Document Architecture Governance Organizational Chart
Review Architecture Governance Organizational Chart
Approve Architecture Governance Organizational Chart

Process Detail

Determine Resources Available – Determine the resources that are available and allocate the roles between committees and individual titles. Many of the resources are only needed on a part-time basis (see Architecture Governance Roles above).

Setup Architecture Governance Committees – Document the Architecture Governance Committee's roles and responsibilities. Also, setup committee charters, periodic meeting times, and the process of introducing the committees to what they will be doing in the Architecture Lifecycle Processes. As the Lifecycle processes are created, these committees should confirm and modify their roles and responsibilities in the processes.

Set up Architecture Governance Titles – Document the Architecture Governance Individual Titles roles and responsibilities. The creation of job descriptions is recommended. The various positions should be involved during the creation of the Architecture Lifecycle processes to confirm and/or modify their roles and responsibilities in the processes.

Map Architecture Governance Roles – Map the Architecture Governance Roles to the committees and titles. Document and map any remaining unmapped roles to existing committees or titles.

Document Architecture Governance Organizational Chart – Based on the committees and titles that have been created, the organizational structure needs to be determined. What are the relationships between the various groups? Who reports to whom? What is the hierarchy followed during escalation?

Review Architecture Governance Organizational Chart – Once the Architecture Organizational Chart is created the various roles in the Architecture Governance need to review the division of labor and the previously identified checks and balances to confirm that the structure will support the various processes to be conducted.

Approve Architecture Governance Organizational Chart – After the review of the Architecture Governance Organizational Chart, the various roles in the Architecture Governance will approve the chart. Like any organizational chart, this is a versioned document. It will change over time as the organization's needs for enterprise architecture are understood and the Architecture Governance aligns itself to meet those needs.

The process model for "Document/Update Architecture Lifecycle Processes," the third of the four sub-processes, is presented on the following page.

Document/Update Architecture Lifecycle Processes

Process Overview

Determine and document the Architecture Lifecycle processes. Figure 9 illustrates the cyclical nature of Architecture program and content development

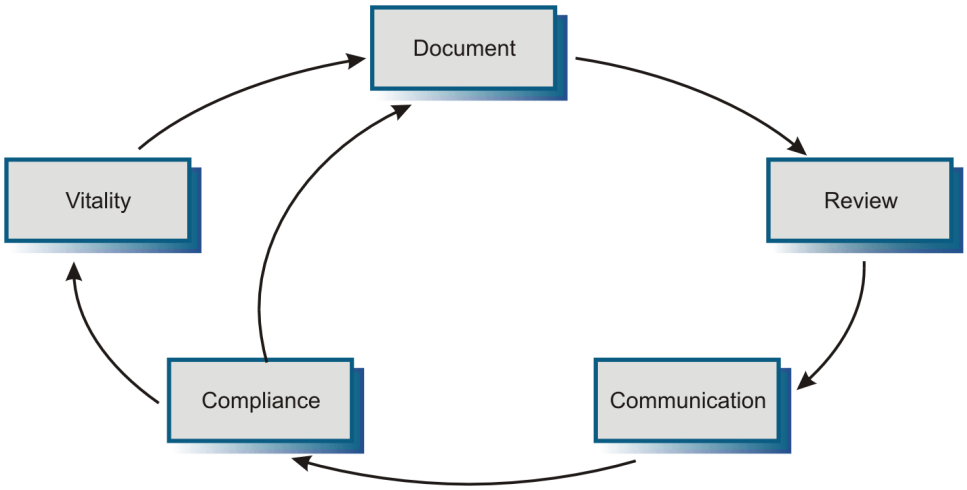
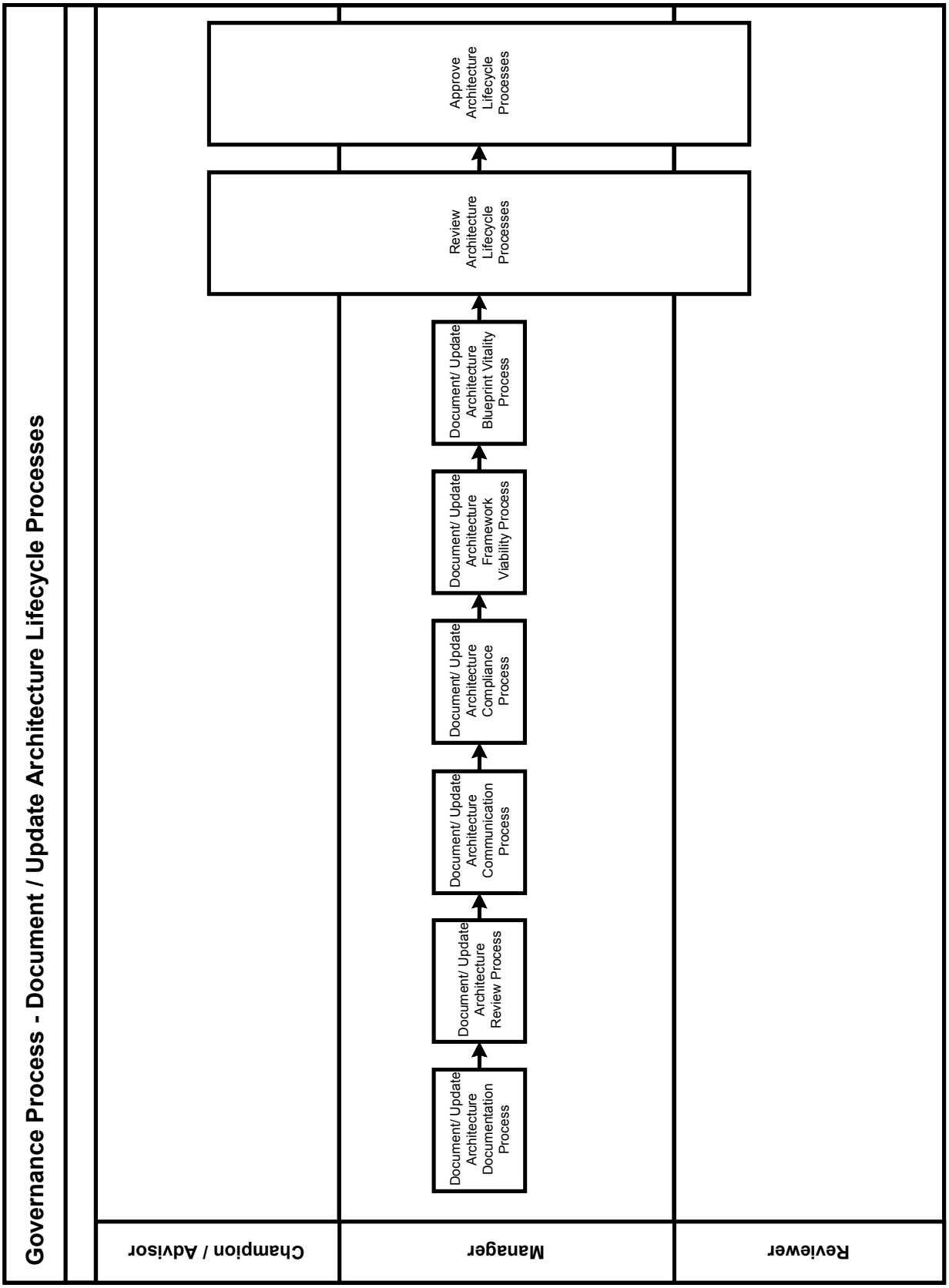


Figure 9. Architecture Lifecycle

The lifecycle processes begin with documenting the various Governance Elements and continue with documenting the Architecture Blueprint. The various Architecture Governance roles should review all created documentation. Once reviewed, the Communicator relays the review results to the Audience. Compliance Process describes the process to request a variance from the approved EA components. Results of the Compliance review typically results in updates to the EA documentation, which would begin the "inner cycle" again.

A critical step in the lifecycle of EA is the continuous refresh (Vitality) of the EA content (EA Blueprint) and the EA program elements (EA Framework). The refresh of the EA Blueprint (Blueprint Vitality Process) is recommended at a minimum of every six months, or on an as needed basis. On a less frequent basis, determined by changes in enterprise direction and technology, the Enterprise Architecture Framework will also undergo a refresh (Framework Viability Process).

All of the processes identified and created are updated during the Confirm Architecture Governance Structure process or the Architecture Governance Elements Vitality Process. The processes described on the following pages must be accomplished in order to set the stage for this lifecycle to begin.


Governance Process - Document / Update Architecture Lifecycle Processes
Champion / Advisor
Manager
Reviewer
Document/ Update Architecture Documentation Process
Document/ Update Architecture Review Process
Document/ Update Architecture Communication Process
Document/ Update Architecture Compliance Process
Document/ Update Architecture Framework Viability Process
Document/ Update Architecture Blueprint Vitality Process
Review Architecture Lifecycle Processes
Approve Architecture Lifecycle Processes

PROCESS DETAIL

Document/Update Architecture Documentation Process – The process steps and information required for creating the Architecture Blueprint will be articulated in the section entitled Architecture Documentation Process. Create and update this process with much consideration. Here are just a few considerations:

- What are the goals and objectives that an adaptive enterprise architecture striving to fulfill for the organization?
- What technology should be controlled from an Enterprise perspective?
- What is the best way to communicate the Architecture Blueprint information?
- What is the immediate need in the organization that the Architecture Blueprint Documenters could aid in researching? (Biggest bang for the buck.)
- How many levels of categories need to go into sorting the products and compliance criteria? (The example presented later in the Tool-Kit has three levels prior to getting to the product and compliance criteria levels.)
- What will be the solution to a product that can be categorized in many of the categories?
  - Will one of the categories be the owner of the product and the others associated categories?

Will a "cross-category" documentation team be set up to document those products that don't fit into a single category?

Document/Update Architecture Review Process – The Architecture Review process articulates the process steps and items for review. Typically, this will include one or more of the Governance Elements. Reviews can be regularly scheduled and/or requested based on a specific need. The Architecture Review Process and the Architecture Compliance Process are where a majority of the architecture governance's primary and supportive roles get involved. Considerations when creating this process would include:

- Availability of Review Committees to meet
- Level of information to be presented
- Governance committees/titles that can provide clarity and expertise
- What criteria determines if IT or business executive perspective is needed.
- How the results will be communicated.
  - To the Audience – Allowing them to know their expected areas of compliance
  - To the Documenters – To capture the history of the decision be it an approval or a rejection

Document/Update Architecture Communication Process – The Architecture Communication Process articulates the information and method of communicating the Enterprise Architecture Framework Elements. Include considerations for the following areas when establishing or updating the Architecture Communication Process.

- Who is the audience?
- At what steps in the Architecture Lifecycle process, should information be provided?
- What are the types of information to be provided? Examples include:
  - Static Information – Architecture Governance Framework
    - Governance (Roles, Elements, and Processes)
    - Architecture Lifecycle Processes

    - Architecture Blueprint Templates
  - Semi- Static Information –
    - Business Architecture Framework
    - Information Architecture Framework
    - Solution Architecture Framework
    - Technology Architecture Framework
  - Dynamic Information –
    - Business Architecture Blueprint
    - Information Architecture Blueprint
    - Technology Architecture Blueprint
    - Solution Architecture Blueprint
- Methods of communication could include:
  - Publishing information in a push fashion
  - Providing ability to search the information based on specific criteria in a pull fashion
- Audience identification:
  - Subscription Audiences
  - Pre-defined Audiences
  - Ad-hoc Audiences

Document/Update Architecture Compliance Process – The Architecture Compliance Process provides the guidelines, process steps, and information required to seek Architecture help and to request deviation from the Architecture Compliance Components. Address the following considerations when establishing or updating this process:

- What Projects and Service enhancements fall under Architecture Compliance's scope?
- How will Architecture Compliance be enforced?
  - Through mandatory step in the Procurement procedures
  - Through mandatory project task in the Project Methodology
  - Through mandatory step in the Change/Release Management process for Services
- Will Architecture Compliance be audited?
- How will the Project and Services Team seek help from the Documenters and Subject Matter Experts?
- What information will be required for requesting a variance from the stated Architecture Product and Compliance Components?

Document/Update Architecture Framework Viability Process – The Framework Viability Process provides the periodic times, normally annually or semi-annually, or triggers that will initiate a change in the various portions of the Adaptive Enterprise Architecture Framework Manual.

Consideration when creating the Architecture Framework Viability Process must include:

- Events that can trigger changes:
  - New Business Strategic Elements, which could generate changes in:
    - Business Architecture Framework

    - Information Architecture Framework
    - Technology Architecture Framework
    - Solution Architecture Framework
  - New IT Strategic Elements, which could generate changes in the Technology Architecture Framework
  - Modification to Enterprise Architecture Framework elements (Governance, Architecture Lifecycle Processes, and/or Architecture Blueprint Templates), which could generate changes in:
    - Business Architecture Framework
    - Architecture Blueprint
  - Modification to Business Architecture Framework, which could generate changes in:
    - Information Architecture Framework
    - Technology Architecture Framework
    - Architecture Blueprint
  - Modifications to Technology Architecture Framework, which could generate changes in the Technology Architecture Blueprint
  - Best time for initiating periodic reviews
  - Feedback methods to improve the processes, templates, and governance in the adaptive enterprise architecture
  - Training on changes to the Adaptive Enterprise Architecture Framework Manual

Document/Update Architecture Blueprint Vitality Process – The Architecture Blueprint Vitality Process provides the periodic times (a minimum of every six months due to short technology cycles is recommended), or triggers that will initiate a review of the Architecture Blueprint. Considerations when creating this process include:

- Who will be responsible for the Architecture Blueprint Vitality Process?
- How to determine the last time something has been examined?
- What are the critical technologies that need to be reviewed?
- What Business Strategic Elements (Initiatives) are coming in the future that may require new technology solutions? Technology scans for products could begin to help clarify possible solutions.

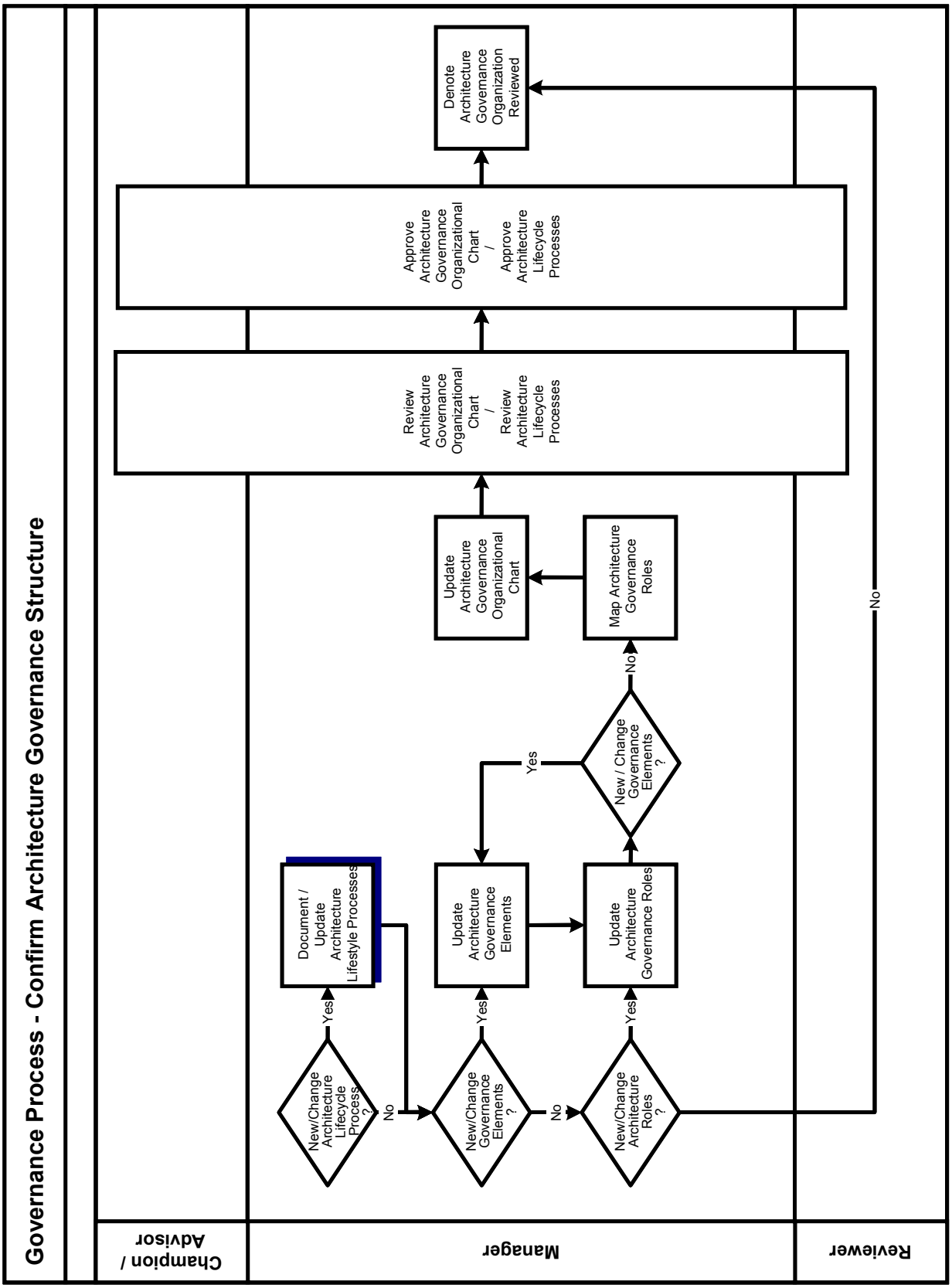
Review Architecture Lifecycle Processes – Once the Architecture Lifecycle processes are documented or updated, each of the governance roles should review the individual processes and their integration. In addition, review any forms or templates used in the execution of the processes.

Approve Architecture Lifecycle Processes – After the review of the Architecture Lifecycle Processes, each of the governance roles should approve the processes. Process models are versioned documents that will change over time as the organization's needs for enterprise architecture are understood and the Architecture Governance aligns its processes to meet them.

CONFIRM ARCHITECTURE GOVERNANCE STRUCTURE

PROCESS OVERVIEW

Confirmation of the Architecture Governance Structure is a continuous process. Initiate this process on a recurring basis, as well as for new and changed governance processes, governance roles, and/or enterprise architecture framework elements. There are relationships between the governance processes, roles and elements; therefore, when one of them changes, review all.


Governance Process - Confirm Architecture Governance Structure
Champion / Advisor
Manager
Reviewer
New/Change Architecture Lifecycle Process ?
Yes
No
Document / Update Architecture Lifestyle Processes
New/Change Governance Elements ?
Yes
No
Update Architecture Governance Elements
New/Change Architecture Roles ?
Yes
No
Update Architecture Governance Roles
New / Change Governance Elements ?
Yes
No
Map Architecture Governance Roles
Update Architecture Governance Organizational Chart
Review Architecture Governance Organizational Chart / Review Architecture Lifecycle Processes
Approve Architecture Governance Organizational Chart / Approve Architecture Lifecycle Processes
Denote Architecture Governance Organization Reviewed
No

PROCESS DETAIL

Document/Update Architecture Lifecycle Processes – If changes to the lifecycle processes are identified, document or update the affected process. Review the remaining lifecycle processes for possible changes.

Examples of process initiating changes include:

- Identification of a new lifecycle process or an update to a process step narrative
- Identification of a new governance role or updates to an existing governance role
- Identification of a new enterprise architecture framework elements or updates to existing architecture framework elements

Update Architecture Governance Roles – This process must be completed for additions or changes in the Architecture Roles. The following information must be created or updated for the additional or changed role:

- Role type - Identifies whether the role is a main role or a supportive role.
- Description - Describes the role and its relationship to other roles.
- Implementation Recommendations – Provides information as to whether the role is better implemented as a committee or as a single position.
- Checks and Balances – Provides information as to whether this role can be implemented in combination with other roles and which roles should not be combined.
- Full time / Part Time – Provides information as to whether the role is typically considered to be full or part-time.
- Role Significance – Provides information on whether the role is critical, necessary, or helpful. If the role is identified as critical or necessary, a comment addressing the risk of non-implementation is also provided under "Missing Role Risk".
- Missing Role Risk – Explains the risk incurred if the role is missing from the governance model.

Update Enterprise Architecture Framework Elements – This process must be completed for additions or changes to the Framework Elements. The following steps, at minimum, should be accomplished for the additional or changed element:

- Review existing Enterprise Architecture Framework Elements for impacts.
- Identify affected areas or new areas to update in the Enterprise Architecture Framework Elements.
- Incorporate changes to the Enterprise Architecture Framework Elements.
- Review Changes to the Enterprise Architecture Framework Elements.
- Approve Changes to the Enterprise Architecture Framework Elements.
- Communicate Changes to the Enterprise Architecture Framework Elements.

Map Architecture Governance Roles – During this process, the new or changed role is mapped to a committee or an individual title. The following questions help determine where to map the role:

- Is the role one that is best accomplished in a committee or as a single position?
- Will mapping this role to a specific committee or position cause a check and balance issue with another role the committee or individual is performing?
- Does the workload of the committee/position have room for one more role?

Update the documentation for the Architecture Governance Committee and Architecture Governance Titles with required changes.

Update Architecture Governance Organizational Chart – Denoted the new/updated committees and positions in the Architecture Governance Organizational Chart. Keeping this information current and available will aid in the working relationships of the Architecture groups. The currency of this information is critical to support an IT community not participating in Enterprise Architecture activities on a daily basis. Keeping the information current will ensure the IT community knows who to contact to help them resolve issues, answer questions, or exchange information in an expedient manner.

Review Architecture Governance Organizational Chart/Review Architecture Lifecycle Processes – Once the Architecture Governance Organizational Chart and Architecture Lifecycle processes are documented or updated, review the various roles in the Architecture Governance.

Approve Architecture Governance Organizational Chart/Approve Architecture Lifecycle Processes – After the review of the Architecture Governance Organization Chart and the Architecture Lifecycle Processes, the appropriate roles in the Architecture Governance will approve the chart and the processes.

ARCHITECTURE LIFECYCLE PROCESSES

The Architecture Lifecycle Processes section of the Enterprise Architecture Development Tool-Kit documents the processes and templates used to manage, initiate, and review the Architecture Blueprints.

The Architecture Lifecycle processes and templates are vital to the success of the adaptive enterprise architecture. Enterprise architecture is made up of a set of dynamic elements. The Architecture Lifecycle Overview (Figure 10) shows the continuous cycle of renewal of these dynamic elements.

The Architecture Lifecycle processes are vital to the success of the adaptive enterprise architecture.

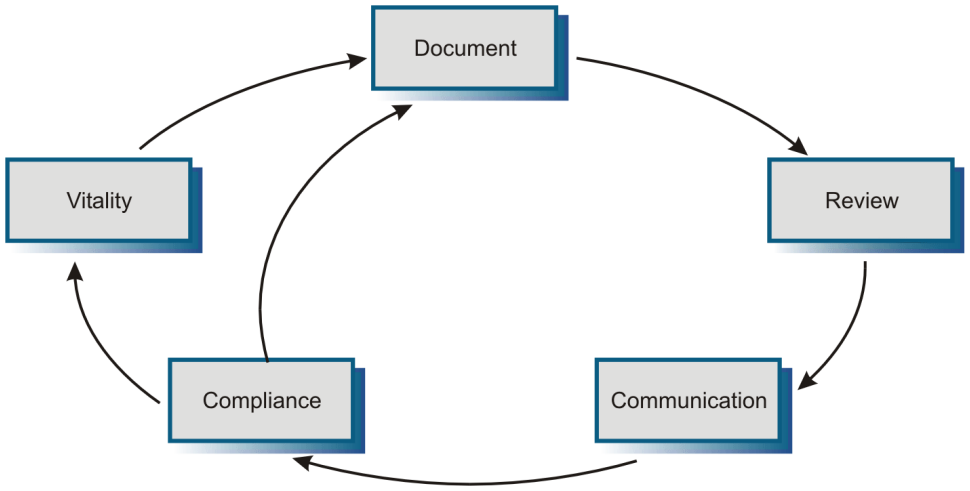


Figure 10. Architecture Lifecycle Overview

The cycle of renewal is achieved with a structure of re-usable processes, discussed in detail in this section The Architecture Lifecycle processes are integral pieces of the overall Architecture Governance Framework used to implement business and technology solutions within government. There are six primary processes:

- Architecture Documentation Process
- Architecture Review Process
- Architecture Compliance Process
- Architecture Communication Process
- Architecture Framework Viability Process (Refresh of the EA Program structural elements)
- Architecture Blueprint Vitality Process (Refresh of the EA content)

Major deliverables from these processes include:

- Updates to the Adaptive Enterprise Architecture Framework Manual (manual developed by governments for their organization, that describes the structure, templates and EA processes in place within their enterprise)
- Architecture Blueprints
- Architecture Communication Document

Documentation utilized by the processes include:

- Adaptive Enterprise Architecture Framework Manual
- IT Strategic Elements
- Business Strategic Elements

Associated management processes include:

- Project Management
- Procurement
- Change and Release Management

See Figure 9 for the data flow of the Architecture Lifecycle processes.

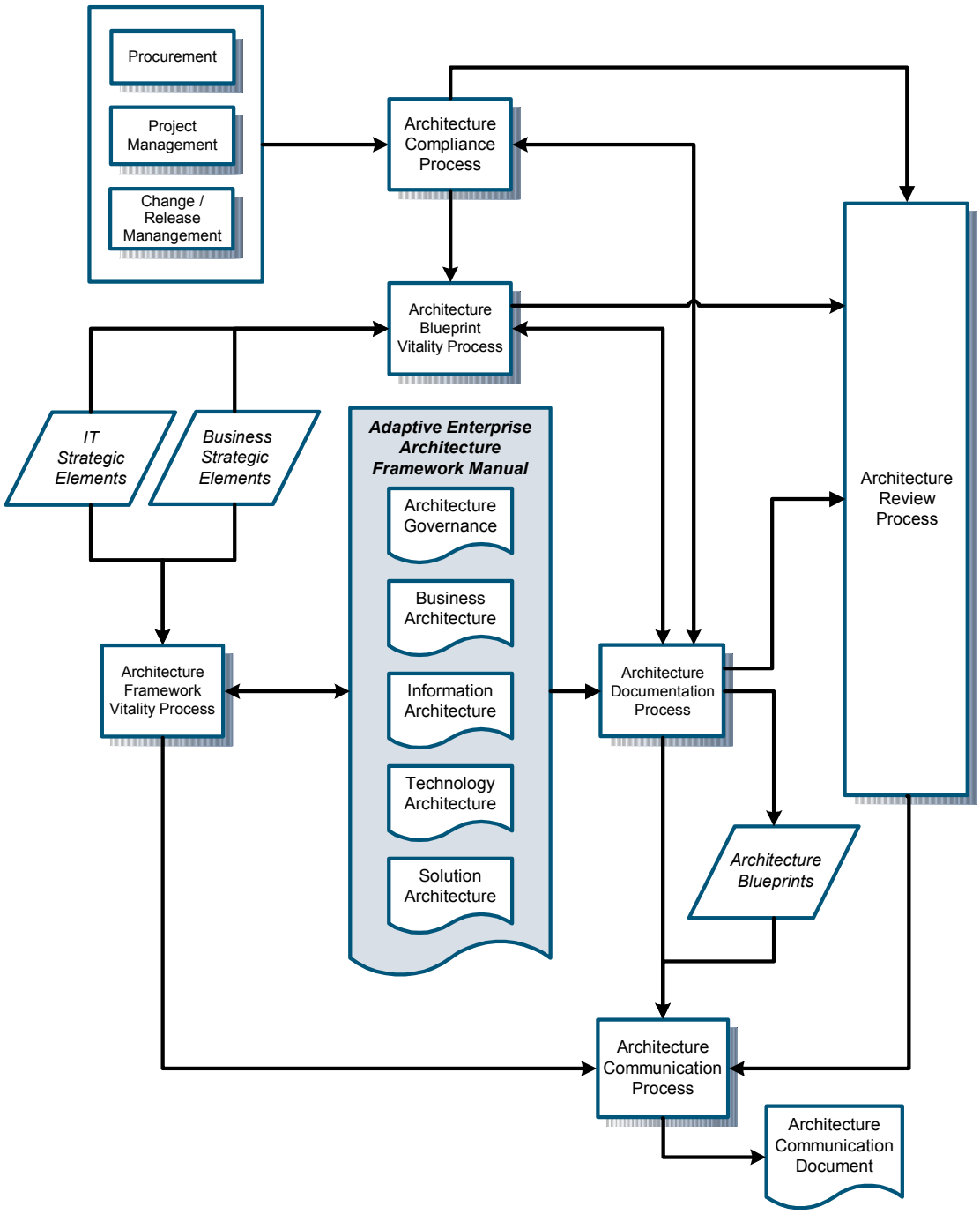


Figure 10 Architecture Lifecycle Processes

Architecture Documentation Process

The Architecture Blueprint articulates the organization's Business, Information, and Technology architecture content. During the Documentation process the components relative to each of the architecture are documented and classified. Acceptance or rejection of the component is also denoted after the review of the Architecture Blueprint items by the appropriate architecture review committees. During the Architecture Documentation Process, a wealth of information will be generated, which can aid agencies in determining business, information and technology solutions.

The Architecture Documentation Process describes the systematic process for developing and maintaining the Architecture Blueprint.

Documenters, identified by the Architecture Manager, are responsible for the development and vitality of the Architecture Blueprint. The committee of Documenters is made up of Subject Matter Experts who are familiar with the organization's IT environment.

The Architecture Documentation Process provides the steps necessary for creating the initial Technical Architecture Blueprint and may be triggered from other Architecture Lifecycle processes including:

- Architecture Framework Viability Process
- Help request generated during the Architecture Compliance Process.
- Architecture Blueprint Vitality Process
- Documenting the results from the Architecture Review Process

The Architecture Documentation Process provides the dynamic information that the Architecture Communication Process uses.

The Architecture Documentation Process applies to both Business and Technology with two sub-processes:

- Outline Domain and train Documenters
- Conduct Documenter work sessions

INITIATE ENTERPRISE DOCUMENTATION PROCESS

PROCESS OVERVIEW

The architecture documentation process may be initiated based on three events:

- The initial development of the adaptive enterprise architecture
- Following the Architecture Blueprint Vitality Process
- Following the Compliance Process (Architecture Help Request)

The starting point depends on the event that triggered the documentation process. The following explains the starting points and rationales:

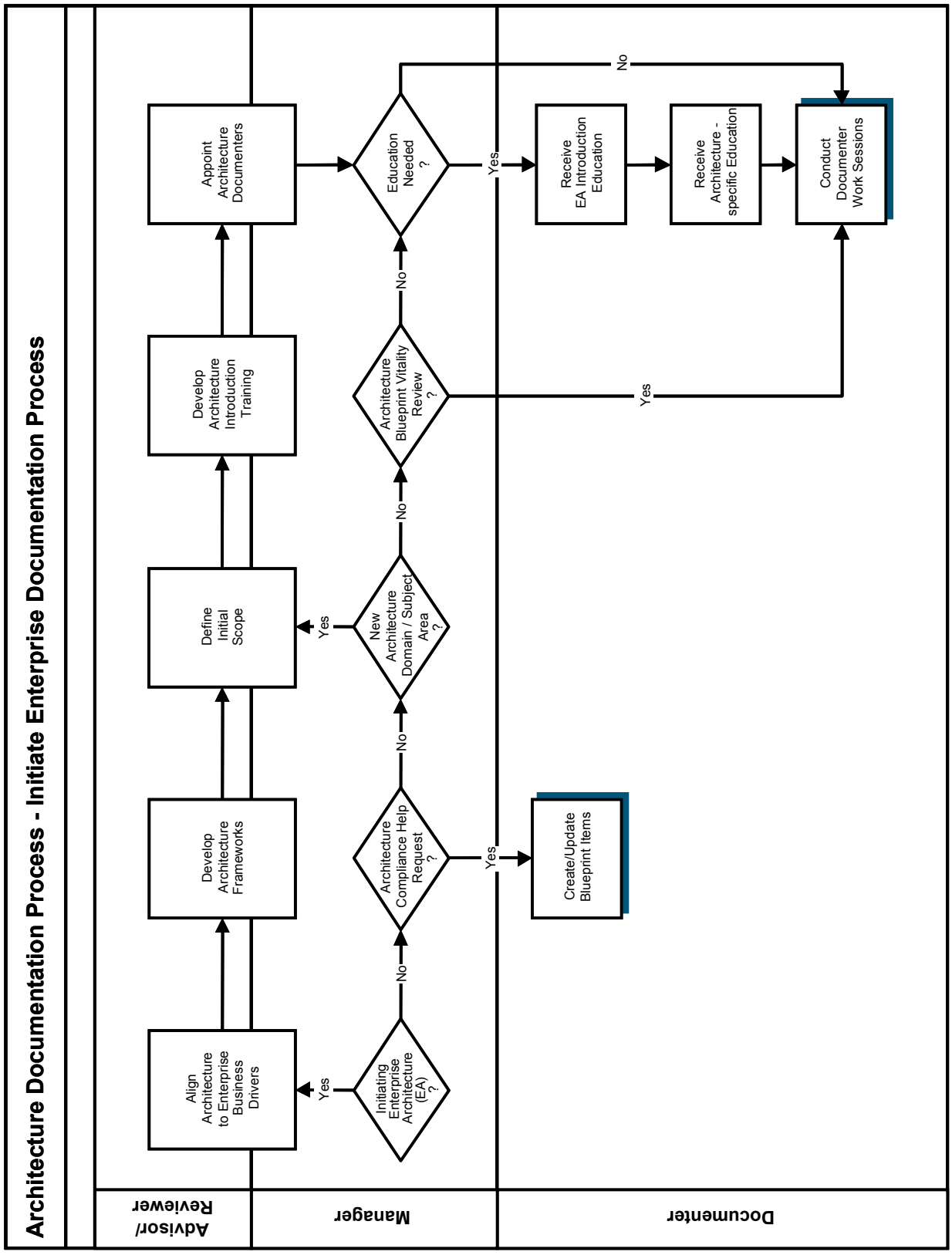
- *Enterprise Architecture Initiation Trigger* – The first time the Architecture Blueprint is documented supply the Documenters with basic information for each of the Domains and Disciplines, such as definition, rationale, benefits, boundary statements and an initial set of subject areas to be covered

within each. Also, train the Documenters on the various enterprise architecture processes and templates.

- *Architecture Blueprint Vitality Process Trigger* – This periodic process verifies that the Architecture Blueprint is staying current with the changes in the business and in the technology world. Vitality can impact the Architecture Blueprint from the Domain level down.
- *Compliance Process Trigger* – The Compliance Process is the point where IT groups outside of the Architecture group interact with the various Architecture processes and blueprints. This process is initiated from an Architecture Help Request. Compliance can impact the Architecture Blueprint from the technology area down.

The process model on the following page provides a generic overview of the documentation process at a high level and applies to each of Business, Information, Technology and Solution Architectures. The details pertaining to the documentation process specific to each of the architectures is provided in the respective section of the Tool-Kit, as follows:

- Business Architecture – *Initiate Business Architecture Documentation Process*
- Information Architecture – *Initiate Information Architecture Documentation Process*
- Technology Architecture – *Initiate Technology Architecture Documentation Process*
- Solution Architecture – *Initiate Solution Architecture Documentation Process*


Architecture Documentation Process - Initiate Enterprise Documentation Process
Advisor/ Reviewer
Manager
Documenter
Align Architecture to Enterprise Business Drivers
Develop Architecture Frameworks
Define Initial Scope
Develop Architecture Introduction Training
Appoint Architecture Documenters
Initiating Enterprise Architecture (EA) ?
Architecture Compliance Help Request ?
New Architecture Domain / Subject Area ?
Architecture Blueprint Vitality Review ?
Education Needed ?
Create/Update Blueprint Items
Receive EA Introduction Education
Receive Architecture - specific Education
Conduct Documenter Work Sessions
Yes
No

PROCESS DETAIL

Align Architecture with Enterprise Business Drivers – The alignment of the architecture with the Enterprise Business Drivers, is an important activity relative to all of Enterprise Architecture. Business Drivers include internal goals and strategies and external trends, such as legislation or regulatory items that influence the business. The Enterprise Business Drivers provide strategic business concepts for Business, Information and Technology Architectures. They also influence Implementation Planning and the enterprise solutions built as part of Solution Architecture.

Three common categories of Business Drivers include Principles, Best Practices and Trends. A detailed discussion of Business Drivers and the process for developing them as Principles, Best Practices, and Trends are under consideration for inclusion in a subsequent version of the NASCIO Tool-Kit.

Business Drivers may be documented in various strategic documents within the organization, such as Strategic Plans and/ or budget documents. It may be necessary to pull the Business Drivers together from these sources so they are readily available to those who will be working with the architecture.

Including a review of the Enterprise Business Drivers prior to developing any of the architecture frameworks will provide an understanding the pulse of the organization in regards to items such as the functional and topical Business Domains, Information Subject Areas, Technology Domains, etc. This information can provide insight into the fields that should be included on templates or specific reviews that should be included in the architecture processes.

Develop Architecture Framework – The information documented within the Architecture Framework will play an important role in the development of the Architecture Blueprints. The NASCIO Architecture Frameworks provide the structure, processes and templates necessary for capturing this information. An enterprise may decide to use the framework described in the NASCIO Tool-Kit or may choose other processes, template and governance structure.

Define Initial Scope – Develop the initial definition of the Business/Technology Domain or Information Subject Area and add any detail that will be helpful in identifying the documentation team members. Also, add any information that will help the team develop the appropriate level of documentation for this domain/subject area.

Develop Architecture Education Sessions– The Architecture Education Sessions provide high-level overviews of the Enterprise Architecture Program and prepare Documenters for their role in the Business Architecture effort. Developers of education materials should consider inclusion of the following materials:

- Purpose
- Presenters
- Intended audience
- Session structure
- Prerequisites
- Syllabus
- Objectives
- Class materials for both instructors and attendees

Appoint Architecture Documenters – At this point, the Documenters are appointed from subject matter experts familiar with the business, information or technology of the enterprise, depending on the architecture to be documented. The team will be responsible for steering, shaping, and developing the Architecture Blueprints.

The educational sessions described below, are progressive in nature. The sessions will be conducted after the architecture team is identified:

Receive EA Introduction Education – Documenters should receive initial training that covers the overview of enterprise architecture and architecture governance.

Receive Architecture-specific Education – After receiving initial enterprise architecture training, the Documenters will receive specialized instruction, addressing the business, information or technology architecture documentation templates and respective architecture documentation processes that they will use to document the Architecture Blueprint.

Conduct Documenter Work Sessions – Applying knowledge gained in first two sessions, Documenters will begin development of the Architecture Blueprint documentation. The detail pertaining to architecture-specific work sessions is presented as a separate process (see *Conduct Documenter Work Sessions*).

CONDUCT DOCUMENTER WORK SESSIONS

PROCESS OVERVIEW

These architecture-specific work sessions are intended to produce the documentation that initially populates the Architecture Blueprint. Ongoing Documenter meetings are required to maintain the vitality of the Architecture Blueprints.

Documenter Work Session: The first session will include:

- Defining roles and responsibilities
- Reviewing architecture blueprint documentation requirements
- Determining expectation of on-going meetings

After the first meeting, on-going working sessions are triggered from Architecture Lifecycle Processes including:

- Architecture Review Process
- Architecture Compliance Process
- Architecture Blueprint Vitality Process

The process model and details pertaining to the work sessions specific to each of the architectures is provided within the respective sections of the Tool-Kit:

- Business Architecture – *Conduct Business Architecture Work Sessions*
- Information Architecture – *Conduct Information Architecture Work Sessions*
- Technology Architecture – *Conduct Technology Architecture Work Sessions*
- Solution Architecture – *Conduct Solution Architecture Work Sessions*

Architecture Review Process

The Architecture Review Process allows the architecture governance groups to review, debate, discuss, and make decisions about the various additions and changes to the Architecture Blueprint and Enterprise Architecture Framework. This process also determines which variances will be accepted into the organization's technology portfolio.

The proposed architecture changes may be triggered from any of the following processes:

- Architecture Compliance Process
- Architecture Blueprint Vitality Process
- Architecture Documentation Process
- Architecture Framework Viability Process

The process of reviewing changes to the Enterprise Architecture Framework, Architecture Blueprint, and/or variance requests is made up of three sub-processes. The sub-processes include:

- Propose Architecture Change
- Determine Architecture Review Decision
- Document Review Decisions

Each of the sub-processes follows the same format, providing a Process Model followed by the process detail.

PROPOSE ARCHITECTURE CHANGE

PROCESS OVERVIEW

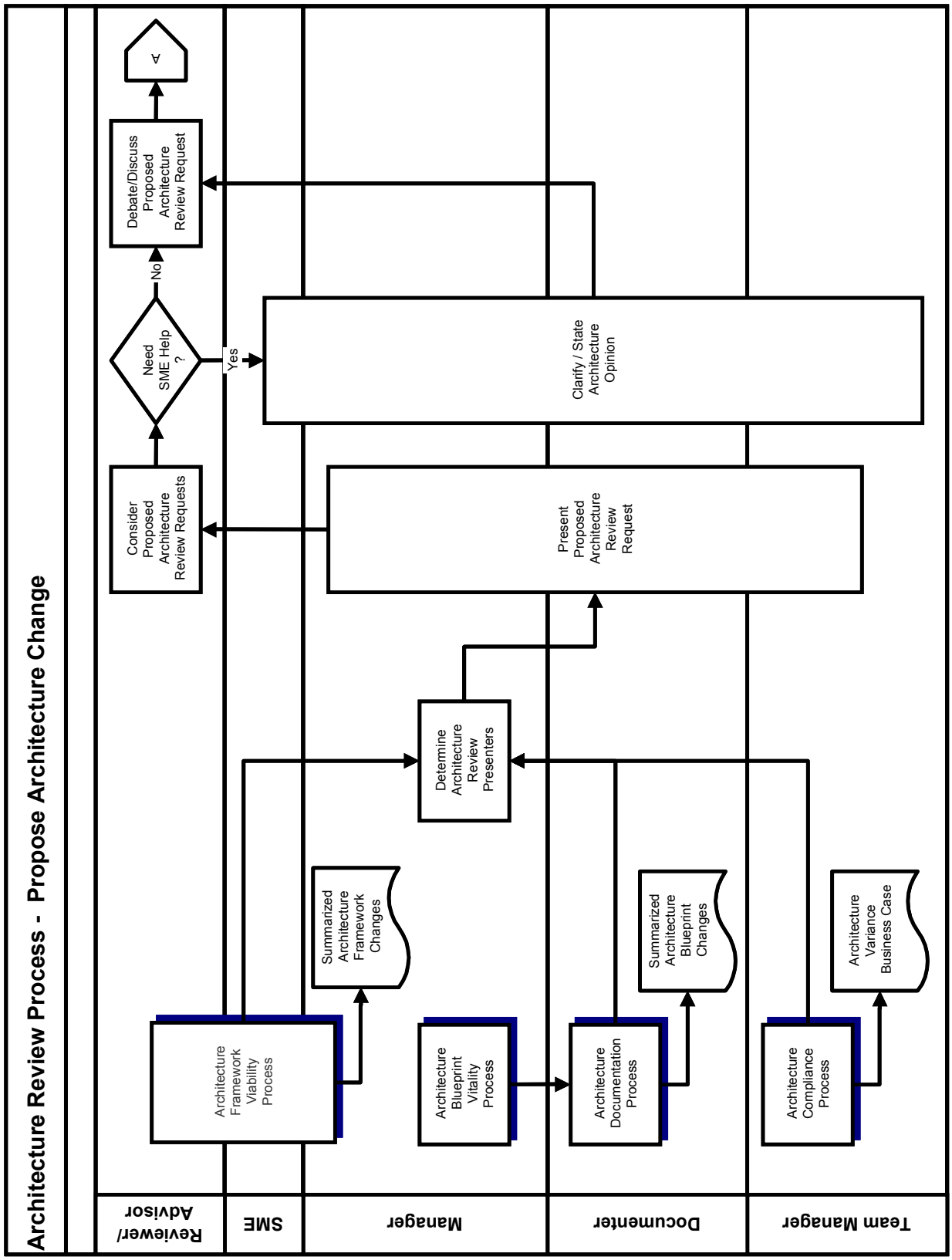
The Architecture Review Process is typically part of a regularly scheduled Architecture Review meeting. Individual organizations should define the frequency of Review meetings, based on the needs of their organization.

The Architecture Review Process is triggered by the completion of the following Architecture Lifecycle Processes:

- Architecture Framework Viability Process
- Architecture Blueprint Vitality Process
- Architecture Documentation Process
- Architecture Compliance Process

Depending on the process that triggered the review, the Proposed Architecture Review Request will contain different information, as depicted in the following chart:

Process That Triggered Review	*Information For Review*
• Architecture Framework Viability Process	• Summarized changes to the Adaptive Enterprise Architecture Framework Manual
• Architecture Blueprint Vitality Process	• Summarized changes to the Architecture Blueprints
• Architecture Documentation Process	• Summarized changes to the Architecture Blueprints
• Architecture Compliance Process	• Architecture Variance Business Case


Architecture Review Process - Propose Architecture Change
Reviewer/ Advisor
SME
Manager
Documenter
Team Manager
A
Debate/Discuss Proposed Architecture Review Request
No
Need SME Help ?
Yes
Clarify / State Architecture Opinion
Consider Proposed Architecture Review Requests
Present Proposed Architecture Review Request
Determine Architecture Review Presenters
Summarized Architecture Framework Changes
Summarized Architecture Blueprint Changes
Architecture Variance Business Case
Architecture Framework Viability Process
Architecture Blueprint Vitality Process
Architecture Documentation Process
Architecture Compliance Process

PROCESS DETAIL

Determine Architecture Review Presenters, Present Proposed Architecture Review Request –Changes to the architecture can be triggered by the following processes:

- Architecture Framework Viability Process
- Architecture Blueprint Vitality Process
- Architecture Documentation Process
- Architecture Compliance Process

The Architecture Manager will determine the role best suited to present the changes to the Reviewers/Advisors. The Manager may choose to make the presentation or may choose a Team Leader, or Documenter to make the presentation.

Consider Proposed Architecture Review Requests – For each proposed change the Reviewers should consider:

- Impact on the Architecture Blueprint
- Physical implementation requirements
- Impact on installed applications or services
- Impact on existing installation standards
- Funding

The Reviewers may also request the assistance of an Advisor.

Clarify/State Architecture Opinion – During the consideration of the request, the Reviewer may seek technical opinions from Subject Matter Experts in regard to the requested change. The Reviewer may also ask for clarification of some of the information provided with the request.

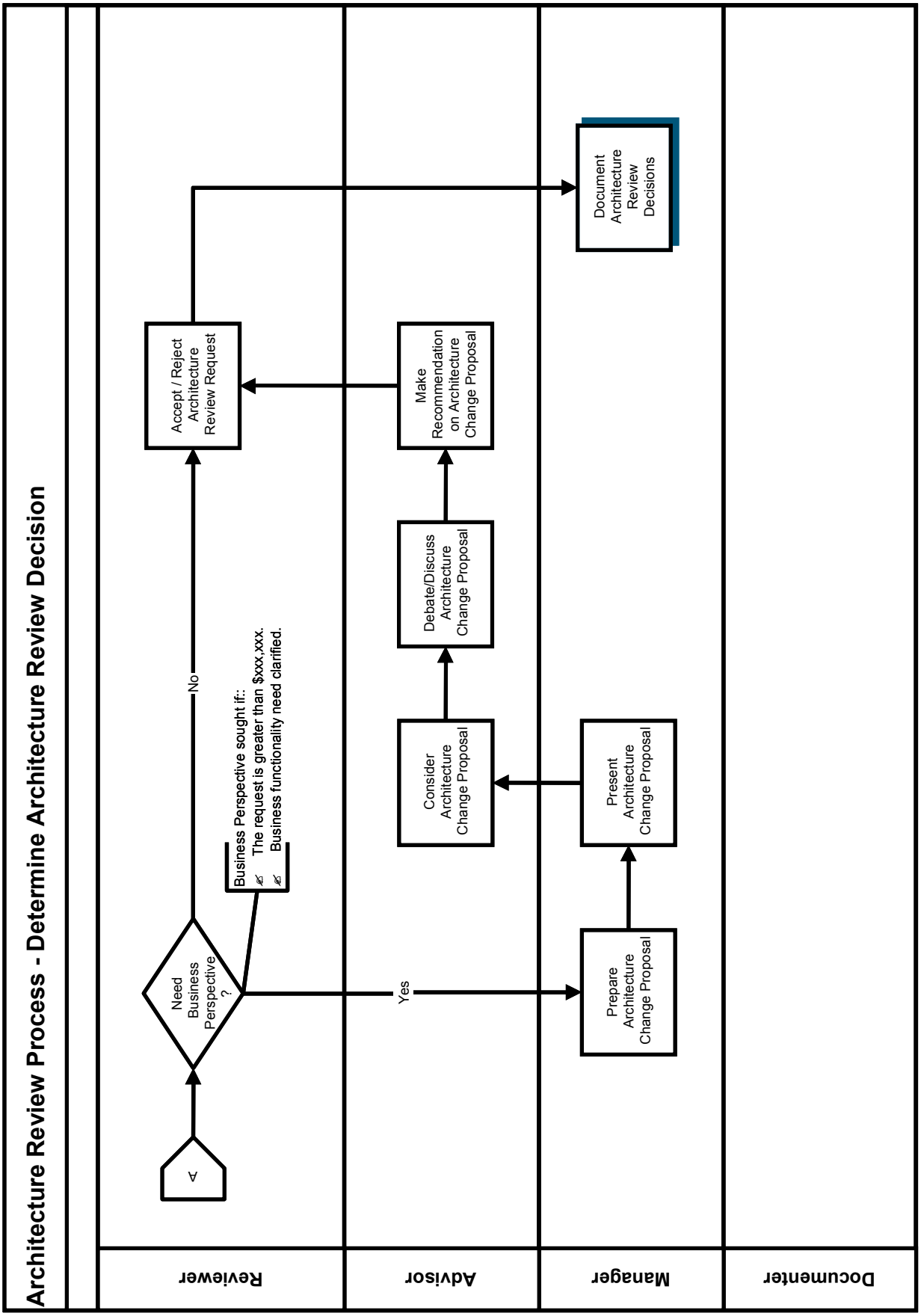
Debate/Discuss Proposed Architecture Review Request – The Reviewers weigh the pros and cons to make a decision toward accepting or rejecting the change. The Reviewers will also consider the immediate, as well as the long-term needs of the organization. It is essential that both perspectives be given proper consideration.

DETERMINE REVIEW DECISION

PROCESS OVERVIEW

Typically, organizations will set cost criteria for projects, above which additional business approval is required. If a request exceeds this limit or additional information is required related to the business functionality, the Manager may seek the opinion of the appropriate business Advisor on behalf of the Reviewers.

If no Advisor input is required, the process continues with the Accept/Reject Proposed Architecture Review Items process step, documented below.


Architecture Review Process - Determine Architecture Review Decision
Reviewer
Advisor
Manager
Documenter
A
Need Business Perspective ?
No
Yes
Business Perspective sought if::
The request is greater than $xxx,xxx.
Business functionality need clarified.
Accept / Reject Architecture Review Request
Make Recommendation on Architecture Change Proposal
Debate/Discuss Architecture Change Proposal
Consider Architecture Change Proposal
Prepare Architecture Change Proposal
Present Architecture Change Proposal
Document Architecture Review Decisions

PROCESS DETAIL

Prepare Architecture Change Proposal – When the Business perspective is needed, the Manager will prepare the proposals to be submitted to the Advisors. The proposal should contain information pertaining to the request and the business requirement to be addressed by the Advisor. This could vary from request to request.

Present Architecture Change Proposal – the government entity should determine when and how the presentation occurs, but the Architecture Manager will typically present the Architecture Change Proposal to the Advisors during a regularly scheduled Advisor meeting. The Advisors may ask for the requesting Team Leader or Documenter to attend the presentation to answer questions or make clarifications.

Consider Architecture Change Proposal – For proposed changes that need consideration from a business perspective, the Advisor should consider:

- Impact on the Business Architecture Blueprint
- Impact on the organization's IT Portfolio.
- Physical implementation requirements on the business
- Impact on installed applications or services that currently support the business.
- Funding

Debate/Discuss Architecture Change Proposal – The Advisors weigh the pros and cons from the business perspective to make a determination toward accepting or rejecting the change. As with the Reviewers, the Advisors will also consider the immediate, as well as the long-term needs of the organization.

Make Recommendation on Architecture Change Proposal – The Advisors will make recommendations to the Reviewer and Architecture Manager regarding whether to accept or reject the Proposed Architecture Review Items.

Accept/Reject Architecture Review Request – Based on the business case and the immediate and long-term needs of the organization, the Reviewer will either accept or reject the proposed architecture review request or line items. Note that each organization should determine whether Requests are accepted or rejected as a whole or whether the requests may be separated into line items addressed separately. Document Architecture Review Decisions: Whether a change was accepted or rejected, the results should be documented. This provides a better picture of the evolution of the decision process and history for the Enterprise Architecture Framework and Architecture Blueprint.

The documentation of the Architecture Review Decision is provided in the following sub-process model and description

DOCUMENT ARCHITECTURE REVIEW DECISION

PROCESS OVERVIEW

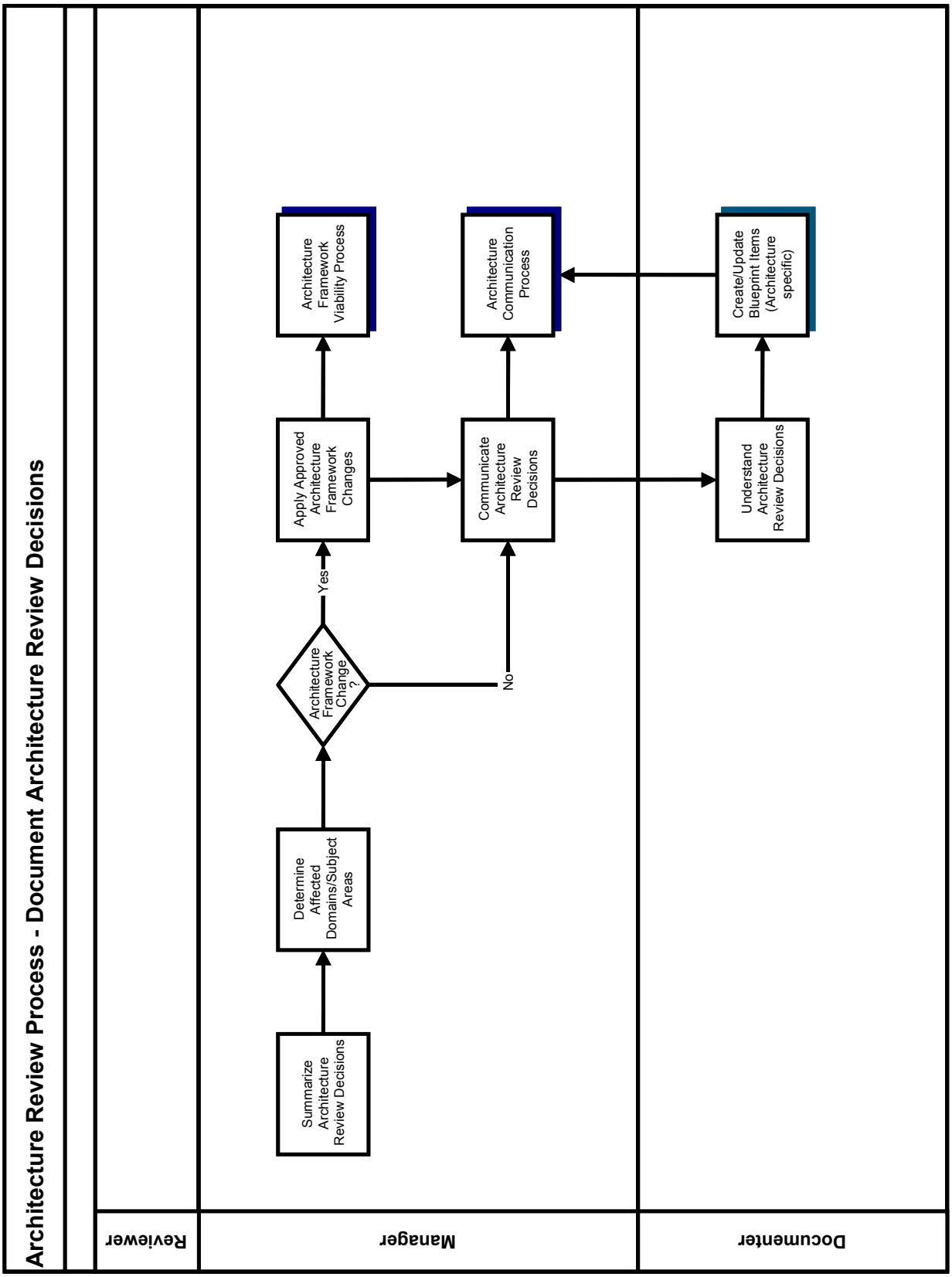
The results of the architecture change are documented regardless of whether a change was accepted or rejected. This provides a record of the decision process for the Enterprise Architecture Framework and Architecture Blueprint.

The process steps for documenting the review decision include

- Summarize Architecture Review Decisions
- Determine Affected Domains
- Apply Approved Enterprise Architecture Framework Changes
- Communicate Architecture Review Decisions
- Understand Architecture Review Decisions

NOTE: The following processes are sub-processes of the Architecture Documentation Process and are used for updating the Architecture Blueprints.

- Complete/Update Domain Blueprint
- Complete/Update Discipline Blueprint
- Create/Update Technology Areas
- Create/Update Product Components
- Create/Update Compliance Components


Architecture Review Process - Document Architecture Review Decisions
Reviewer
Manager
Documenter
Summarize Architecture Review Decisions
Determine Affected Domains/Subject Areas
Architecture Framework Change ?
Yes
No
Apply Approved Architecture Framework Changes
Communicate Architecture Review Decisions
Understand Architecture Review Decisions
Architecture Framework Viability Process
Architecture Communication Process
Create/Update Blueprint Items (Architecture specific)

PROCESS DETAIL

Summarize Architecture Review Decisions – The Architecture Manager will summarize the decision of the Reviewer meeting.

Determine Affected Domains – Multiple Domains may be affected based on the results of the review. The Manager should determine the affected Domains and the required updates.

Apply Approved Enterprise Architecture Framework Changes – These Enterprise Architecture Framework elements are maintained in the sub-process Confirm Architecture Governance Structure of the Architecture Framework Viability Process. After the updates are completed, the Architecture Blueprint Vitality Process is triggered to determine if the Architecture Blueprint also requires updating. This is a continuation of the Architecture Lifecycle processes.

Communicate Architecture Review Decisions – Major changes or decisions of the Architecture Review Process should be communicated to the IT community through the Architecture Communication Process. Domain-specific information should be provided to the Documenters of all Domains affected by the reviews.

Understand Architecture Review Decisions – The Documenters should understand the decisions communicated to them. Once they have an understanding, they should review the Architecture Blueprint and make updates as required to document the decisions. Update each level of the Architecture Blueprint affected by the review.

Create/Update Blueprint Items (Architecture specific) – Based on the review decision, the various Blueprint items should be updated within the affected architecture. The process model and details pertaining to updating the Blueprint Items specific to each of the architectures is provided within the respective sections of the Tool-Kit:

- Business Architecture – *Create/Update Business Architecture Blueprint Items*
- Information Architecture – *Create/Update Information Architecture Blueprint Items*
- Technology Architecture – *Create/Update Technology Architecture Blueprint Items*

Architecture Communication Process

The Architecture Communication Process ensures the contents of the enterprise architecture contents are communicated in a timely and accurate manner. This is a vital process in the success of the enterprise architecture. Without a thorough communication process, the enterprise architecture is simply a document, providing no real substance to the organization.

All users must have access to the latest version of the enterprise architecture documents and blueprints. A mechanism must exist to communicate the status and updated documentation to all users. Adequate communication of the enterprise architecture plays a vital role in ensuring that enterprise activities will be synchronized with the Architecture Blueprint and the organization's strategic plans.

The communication document should be available to contractors and vendors required to conform to the organization's enterprise architecture.

To ensure the shared enterprise architecture information meets the communication requirements, conduct a review of all audience members and their information needs. Some communication is automatically distributed; other times information is requested and subsequently distributed to the requester.

Any time the enterprise architecture makes a noticeable change due to an Architecture Review, Architecture Vitality, or Architecture Documentation Process, the information must be communicated to the Architecture Audience in a timely manner.

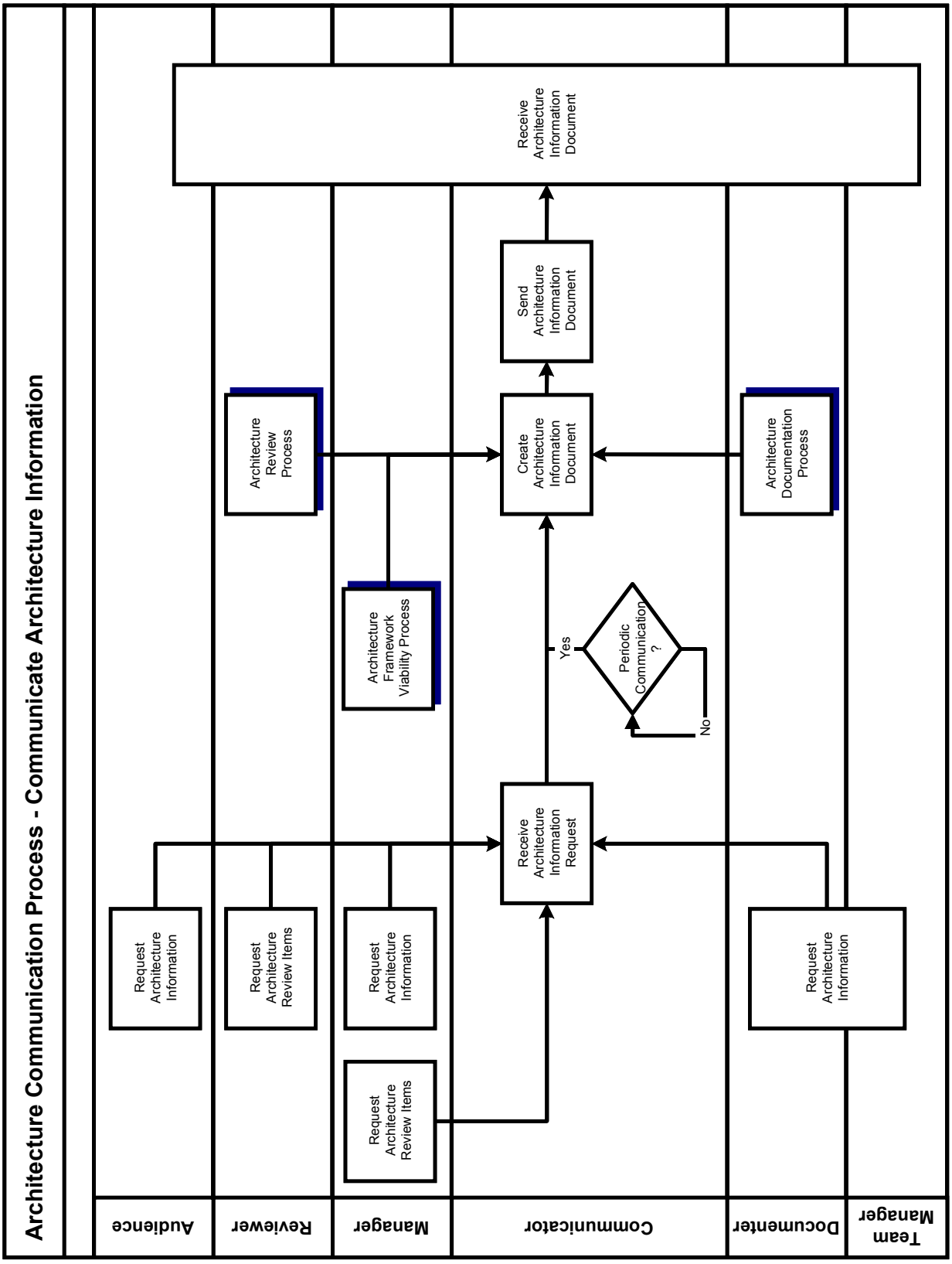
The process of communicating the documented enterprise architecture includes one sub-process to help determine, document and send the architecture communication document. The sub-process is entitled Communicate Architecture Information and includes a Process Model, followed by the process detail.

COMMUNICATE ARCHITECTURE INFORMATION

PROCESS OVERVIEW

The Architecture Communication is a set of communication "documents" that can be disseminated or requested from enterprise architecture information to the various Architecture Audience members. Some of the communication is best queried from the enterprise architecture information itself, while other communication is best summarized, with the added ability to query for the details.

This process model shows the Architecture Roles and Lifecycle processes that can trigger the production and delivery of the Architecture Communication Document.


Architecture Communication Process - Communicate Architecture Information
Audience
Reviewer
Manager
Communicator
Documenter
Team Manager
Request Architecture Information
Request Architecture Review Items
Request Architecture Information
Request Architecture Review Items
Request Architecture Information
Receive Architecture Information Request
Architecture Framework Viability Process
Architecture Review Process
Yes
Periodic Communication ?
No
Create Architecture Information Document
Send Architecture Information Document
Receive Architecture Information Document
Architecture Documentation Process

PROCESS DETAIL

Request Architecture Information – The Architecture Audience, Architecture Manager, and/or Architecture Documenter/Author can request architecture information. This can include requests such as:

- All information for a Domain or any of the Architecture Blueprint Levels
- All architecture blueprint information not reviewed in the last six months
- All Compliance Components for a specific Product (For example: Compliance Components for DB2 database.)
- All architecture blueprint information associated with a keyword (i.e., keyword: web)
- All product components that are classified as current in the technology architecture blueprint

The type of requests is dependent upon the requirements of the requesters. Organizations should determine such items as:

- What information can be shared
- At what point in the Architecture Lifecycle processes will sharing be allowed
- Which Architecture Roles should have access to what information
- The balance between need and efficiency

Request Architecture Review Items – During periodic Architecture Reviews, the information that is documented in the Architecture Blueprint or Enterprise Architecture Framework Elements, but not reviewed, should be collated and summarized for the Reviewers. The status allows the Architecture Communicator to gather the information and provide it in a Communication Document.

Create Architecture Communication Documents – The content of the Architecture Communication Document will vary based on the information collection trigger. The following processes provide the information for the document:

- Architecture Review Process
- Architecture Framework Viability Process
- Architecture Documentation Process

The following types of information are available to share:

- Architecture Blueprint information
- Enterprise Architecture Framework Elements
- Summaries of the Architecture Review
- Summaries of the Architecture Documentation effort
- Highlights from enhancements due to the Architecture Framework Viability Process

Send Architecture Communication Document – Based on what triggered the Architecture Communication Document to be produced, the document will be sent out to the appropriate Architecture Audience. Each organization should determine guidelines addressing the audience for each communication.

Receive Architecture Communication Document – The Architecture Audience member receives the requested Architecture Communication Document. The audience member receives information based on the following criteria:

- The audience member is a subscriber to the Architecture Communication Process
- The audience member is a requester of Ad-hoc Architecture Communication Document
- The audience member holds a primary Architecture Governance role
- Management has designated the audience member as a required receiver of specific Architecture Communication documents

Architecture Compliance Process

The Architecture Compliance Process describes the process to request a variance from the components approved within the organization. Having an established Architecture Compliance Process is an appropriate and tactically sound approach to managing information technology from an enterprise perspective.

In every organization, there will be circumstances that will preclude the use of the documented standards. A formal compliance process is essential to allow for the review and acceptance of variances from the enterprise-wide architecture standards. Members of the organization will be allowed to submit requests for deviation from the standard. These requests for deviation should be presented with an appropriate business case stating the reasons for the variance. Legitimate business cases will be reviewed, and those accepted will be documented as approved variances during the Architecture Review Process.

Results accepted from the Architecture Compliance Process review will flow into the Architecture Blueprint Vitality Process.

The compliance process consists of three sub-processes that determine, document and request architecture variances. These sub-processes include:

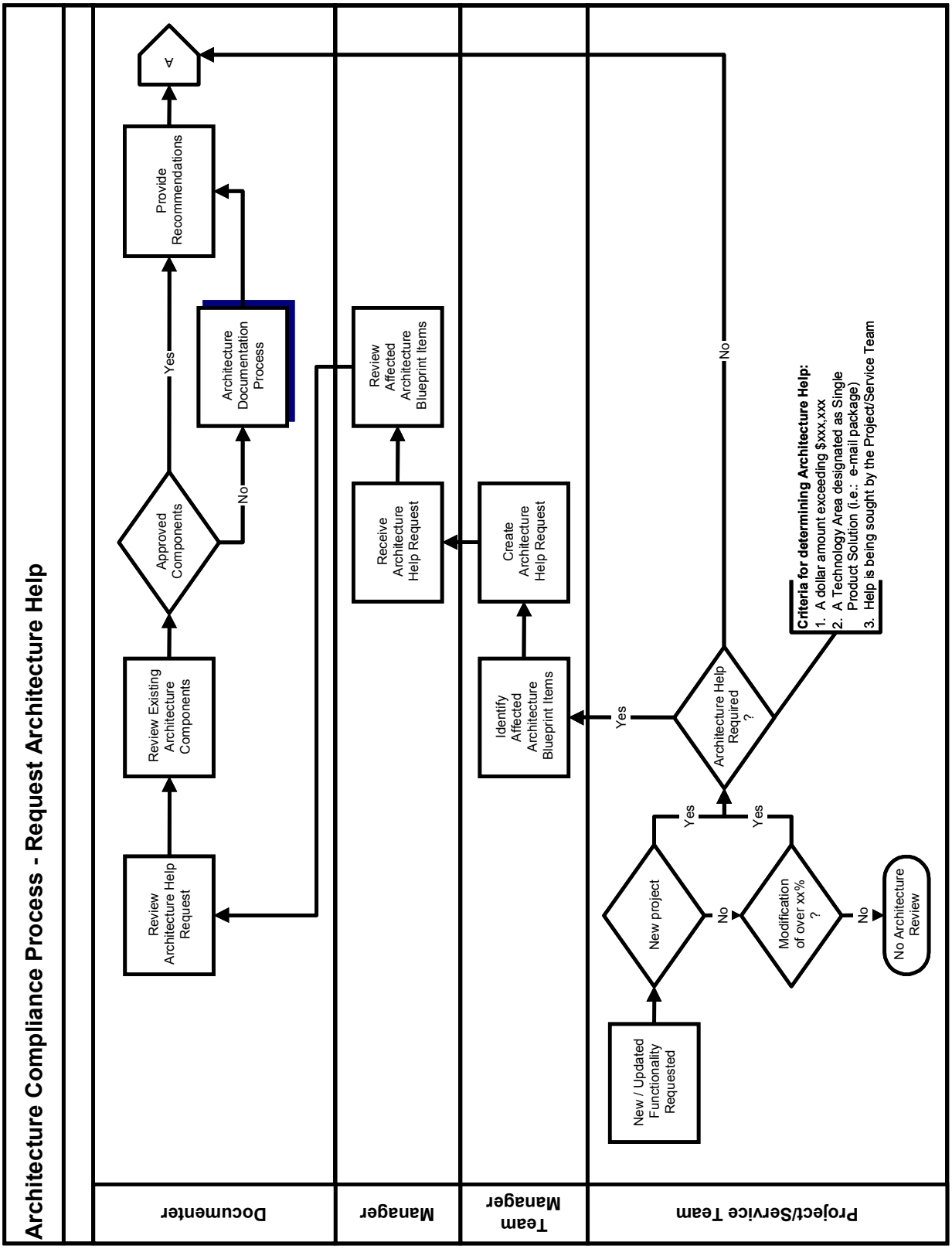
- Request Architecture Help
- Determine Options
- Create Architecture Variance Business Case

Each of the sub-processes follows the same format, providing a process model followed by the process detail.

Request Architecture Help

Process Overview

The Request Architecture Help Process describes the process for handling request for new functionality or updates to current functions. It is typical for organizations to set criteria, such as estimated project cost etc. to determine those projects that require reviews or recommendations based on the architecture The Documenters review the existing architecture component and provide recommendations to the project/service teams.


Architecture Compliance Process - Request Architecture Help
Documenter
Manager
Team Manager
Project/Service Team
New / Updated Functionality Requested
New project
Modification of over xx% ?
No Architecture Review
Yes
No
Yes
Yes
No
Architecture Help Required ?
Criteria for determining Architecture Help:
1. A dollar amount exceeding $xxx,xxx
2. A Technology Area designated as Single Product Solution (i.e.: e-mail package)
3. Help is being sought by the Project/Service Team
Identify Affected Architecture Blueprint Items
Create Architecture Help Request
Receive Architecture Help Request
Review Affected Architecture Blueprint Items
Review Architecture Help Request
Review Existing Architecture Components
Approved Components
No
Yes
Architecture Documentation Process
Provide Recommendations
A

PROCESS DETAIL

New/Updated Functionality Requested – When there is a request to create or update functionality in the organization's project or service teams, the scope of the request and document the requirements will need to be determined. Once this analysis is complete, review the possible solutions.

Based on the analysis of the requirements, determined whether a formal project will start or a production support request initiated. Identify architecture compliance reviews in the project plan schedule.

Project/Service Teams determine whether their project/enhancement requires a formal review to verify compliance with the documented architecture blueprint. This compliance review is required for either:

- All new projects, or
- Modifications of greater than x% on existing technology

If neither of these exists, the project/change requires no compliance review.

If a project/maintenance team requires help in reviewing their project or a new technology against the documented architecture blueprint, the Documenters are available to assist.

Architecture groups are required to review/assist a team if:

- The dollar amount of the solution being suggested is greater than $xxx,xxx.
- The technology area they are requesting a variance for has designated a single product solution. (Because of maintenance and inoperability issues, a single product has been designated as the only acceptable product in the currently documented architecture blueprint.)

Identify Affected Architecture Blueprint Items – The Team Leader should identify the Documenters impacted by the project/enhancement. This identification may not be complete until reviewed by the Architecture Manager, and Reviewers/Advisors.

Create Architecture Help Request – Team Leader will fill out an Architecture Help Request. This request allows the Architecture Manager to determine which of the Documenters can assist. The solutions may already exist in the Architecture Blueprint and the Architecture Manager will direct the Team Leader to the correct information.

Receive Architecture Help Request – Architecture Manager receives the Architecture Help Request and reviews it for completeness. The Architecture Manager will ask several questions to determine completeness, including:

- Is there enough information to determine possible solutions?
- Has contact information for the person requesting been supplied?
- Has the resolution date been communicated?

Review Affected Architecture Blueprint Items: The Architecture Manager, with help from the Reviewers and Advisors, will ensure that all affected domains/subject areas have been identified. They may also direct Team Leaders to possible solutions already approved and documented in the Architecture Blueprint.

Review Architecture Help Request, Review Existing Architecture Components, and Architecture Documentation Process: Based on the type of Architecture Help Request requested, the Documenters will set up time to aid the project/service team. The types of help requests:

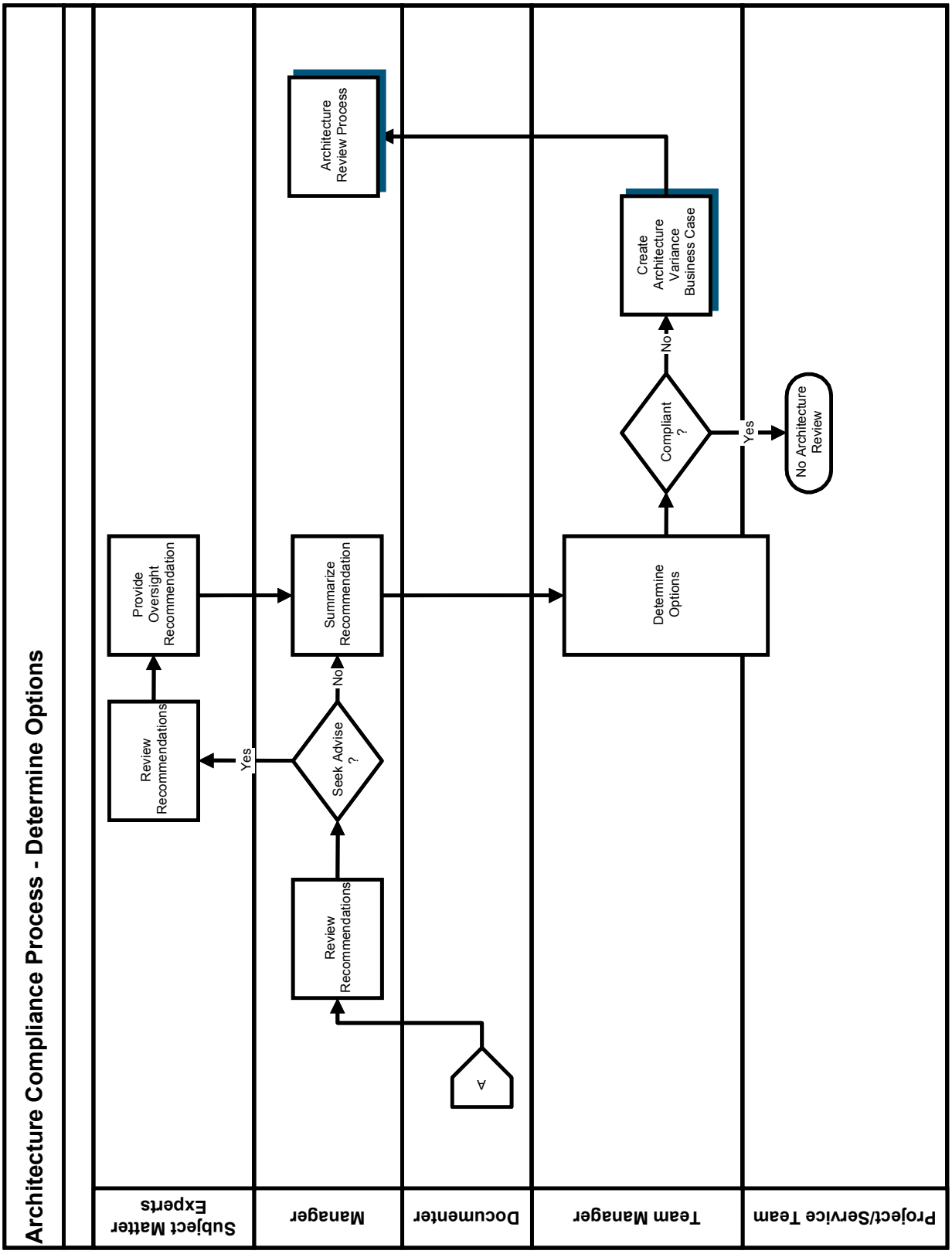
- Identifying or reviewing Business Architecture Components such as Business Drivers or other strategic elements that may be impacted
- Identifying or reviewing Process Components or Information Meta Components that may be impacted
- Identifying existing technology in the organization's products that may meet the requirements of the new or updated functionality requested.
- Conducting a technology scan to identify products that may meet the requirements of the new or updated functionality being requested. After finding potential products, execute the Evaluate Product/Compliance Component Process in the Architecture Documentation Process.
- Reviewing products that the Team Leaders bring forward to determine the possible fit into the documented architecture blueprint.

Provide Recommendations – Based on the reviews and evaluations conducted, the Documenters will make recommendations to the Architecture Manager. This information will be used to aid in the project/service team's selection of a solution for their functional requirements.

DETERMINE OPTIONS

PROCESS OVERVIEW

The Architecture Manager works with the SMEs to review, clarify and summarize the technology recommendations. Options for solving the functional requirements are reviewed and an option is chosen. If this option is compliant with the documented architecture blueprint, no further information is required. If not, an architecture variance business case is developed.


Architecture Compliance Process - Determine Options
Subject Matter Experts
Manager
Documenter
Team Manager
Project/Service Team
Provide Oversight Recommendation
Summarize Recommendation
Determine Options
Compliant ?
No
Yes
No Architecture Review
Create Architecture Variance Business Case
Architecture Review Process
Review Recommendations
Seek Advise ?
No
Yes
Review Recommendations
A

Process Detail

Review Recommendations – The Architecture Manager will review the recommendations presented by the Documenters. Based on this review, the Architecture Manager may seek advice from the Subject Matter Experts.

Review/Clarify Recommendations – The Subject Matter Experts aid the Compliance Process by reviewing and clarifying the recommendations provided by the Documenters.

Provide Oversight Recommendation – Once the Subject Matter Experts have reviewed and clarified the Recommendations, they provide their recommendation.

Summarize Recommendations – The Architecture Manager will prepare a summary from the Documenters' Recommendation and the Subject Matter Experts' Oversight Recommendation. This information is given to the Team Leader to aid the project/service team in determining a solution.

Determine Options – Various options for solving the functional requirements will be reviewed and an option will be chosen. If this option is compliant with the documented architecture blueprint, no further information is required.

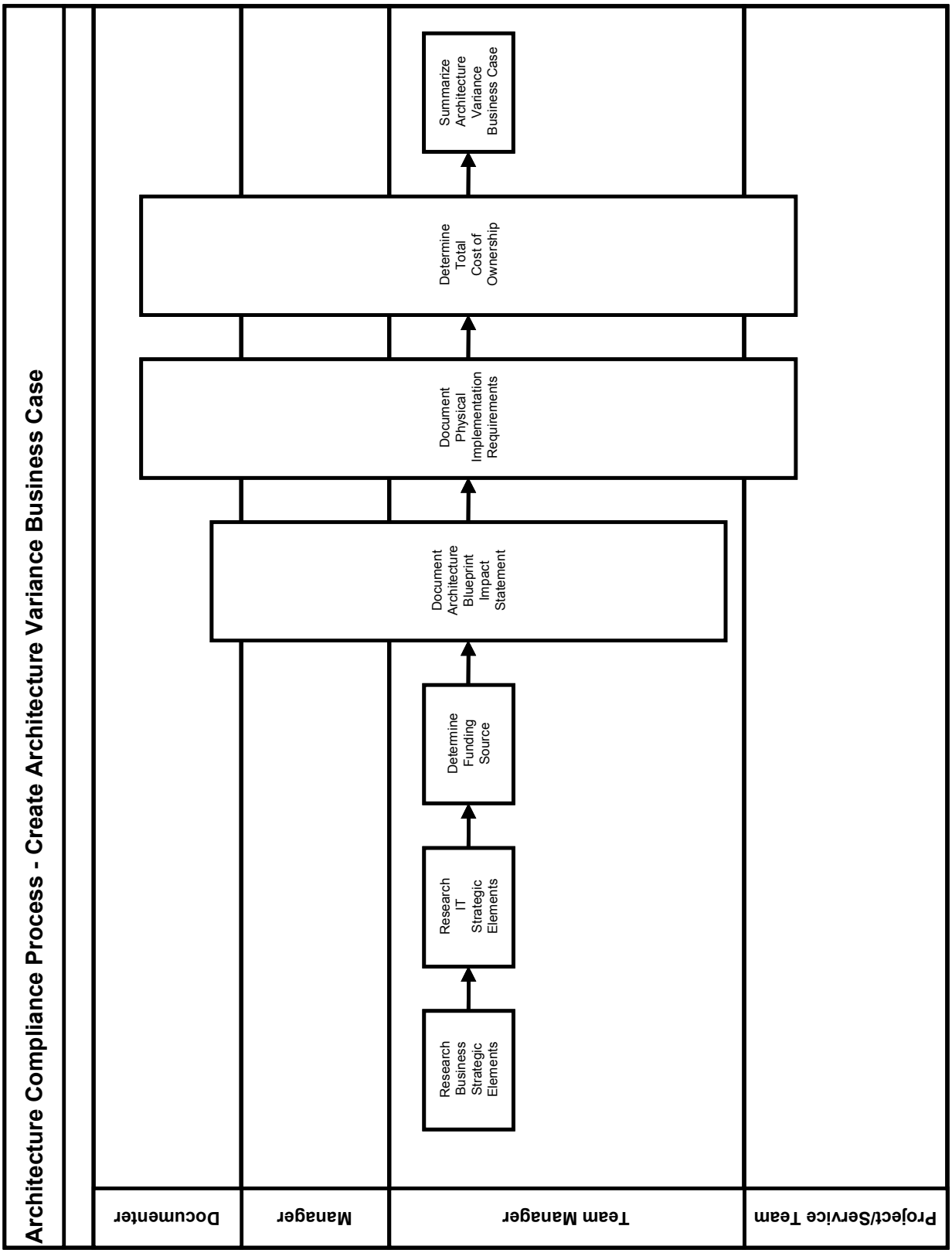
Create Architecture Variance Business Case – If the option chosen is not compliant with the documented architecture blueprint, the Team Leader will need to create a business case for requesting the architecture variance. This process is documented in the sub-process: Create Architecture Variance Business Case.

Once the Architecture Variance Business Case is documented, it will undergo the normal Architecture Review Process.

Create Architecture Variance Business Case

Process Overview

To create an Architecture Variance Business Case, the Team Leader will research Business and IT Strategic Elements and determine the funding sources to offset the cost of introducing a non-compliant product into the architecture blueprint. Then working with the rest of the team, the impact of the variance and the physical implementation requirements are documented. As part of this process, the costs associated with the variance are identified. All this information is summarized for presentation to the reviewers.


Architecture Compliance Process - Create Architecture Variance Business Case
Documenter
Manager
Team Manager
Project/Service Team
Research Business Strategic Elements
Research IT Strategic Elements
Determine Funding Source
Document Architecture Blueprint Impact Statement
Document Physical Implementation Requirements
Determine Total Cost of Ownership
Summarize Architecture Variance Business Case

PROCESS DETAIL

Research Business Strategic Elements – The Team Leader will research relevant business inputs. These can include updated Business Strategy Plans.

Research IT Strategic Elements – The Team Leader will research relevant technology inputs. These can include updated IT Strategy Plans.

Determine Funding Source – To show the offset of introducing a non-compliant product into the architecture blueprint, the Team Leader will identify the funding sources that will be responsible for the total cost of ownership during the product's lifecycle.

Determine Architecture Blueprint Impact Statement – With the help of the Documenters and the Architecture Manager, the Team Leader will craft an impact statement for the variance being sought.

Determine Physical Implementation Requirements – The Project/Service team, Team Leader, Architecture Manager and the Documenters will work together to document the physical implementation requirements that will be required for the new product and/or compliance component.

Determine Total Cost of Ownership – During the impact analysis, the Team Leader is responsible for identifying costs associated with the product such as the licensing fees, initial product cost, implementation cost, and on-going maintenance cost. These costs should include the cost of personnel required to maintain and enhance the product as it goes through its product lifecycle.

Summarize Architecture Variance Business Case – Once everything is determined and documented, the Team Leader should compile a summary of the technical and business inputs to present to the Reviewers.

Architecture Framework Viability Process

Architecture Framework Viability Process is the process that insures the content of the Adaptive Enterprise Architecture Framework Manual remains current and accurate. This is a major requirement of the governance processes.

To ensure Viability, the Enterprise Architecture Framework must be reviewed from a perspective of business strategic elements, IT strategic elements and recommendations for enhancements. Advisors should provide input for the business strategy and the IT strategy.

Any time business strategies or IT strategies make a noticeable shift, an architectural framework review may be required. Enterprise Architectural Framework reviews should occur every one to two years at a minimum.

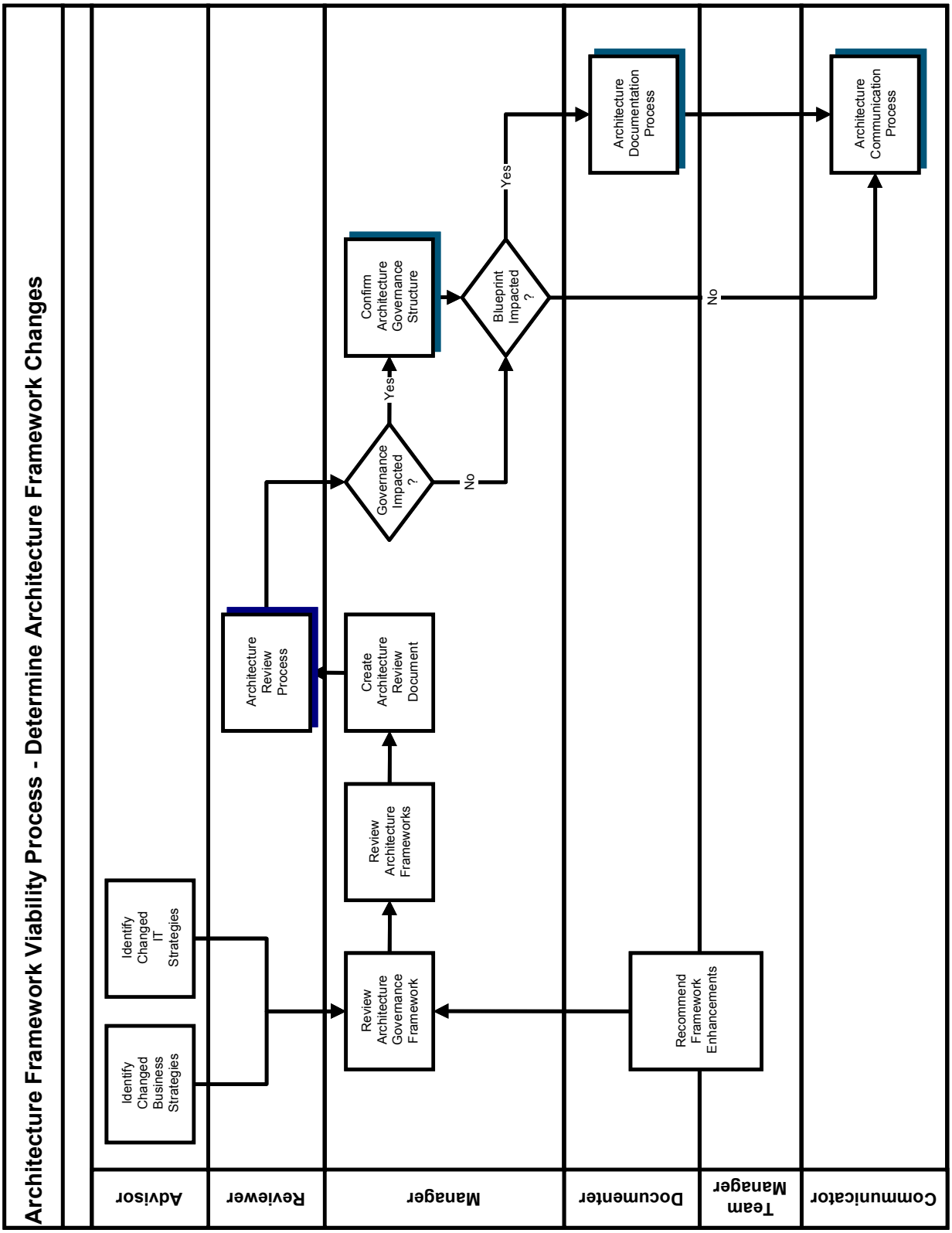
The process of routinely reviewing the documented Enterprise Architecture Framework is made up of one sub-process to help determine, document and request architecture changes. The process follows the format of a process model followed by the process detail.

DETERMINE ARCHITECTURE FRAMEWORK CHANGES

PROCESS OVERVIEW

The Enterprise Architecture Framework is a set of interrelated elements that provide the processes, templates, and governance to implement the Architecture Blueprints. Three events cause changes to the Enterprise Architecture Framework:

- Recommendations from the Documenters and Audience of the architecture for Enterprise Architecture Framework Element enhancements
- Shifts in Business Strategies provided to the Manager
- Shifts in IT Strategies provided to the Manager


Architecture Framework Viability Process - Determine Architecture Framework Changes
Advisor
Reviewer
Manager
Documenter
Team Manager
Communicator
Identify Changed Business Strategies
Identify Changed IT Strategies
Review Architecture Governance Framework
Review Architecture Frameworks
Create Architecture Review Document
Architecture Review Process
Governance Impacted ?
Yes
No
Confirm Architecture Governance Structure
Blueprint Impacted ?
Yes
No
Architecture Documentation Process
Recommend Framework Enhancements
Architecture Communication Process

PROCESS DETAIL

Identify Changed Business Strategies – The Business Advisor identifies and gathers relevant business inputs from updated Business Strategic Plans and forwards the information to the Architecture Manager. The Architecture Manager will need to research changes to the Business Drivers.

Identify Changed IT Strategies – The IT Advisor identifies and gathers relevant IT inputs from updated IT Strategic Plans and forwards the information to the Architecture Manager. The Architecture Manager will need to research changes to the Technology Drivers.

Recommend Framework Enhancements – While interacting with the Enterprise Architecture Framework elements, the Documenters and other users of the architecture may have suggestions for improvement that could benefit everyone. Consider these recommendations for new versions of the Adaptive Enterprise Architecture Framework Manual.

Review Architecture Governance Framework – Changes in the Business and IT Strategies or recommendations from the Documenters/users of the Enterprise Architecture Framework Elements may cause further enhancements to be identified. These enhancements need to undergo the Confirm Architecture Governance Structure sub-process to change the Architecture Lifecycle Processes, Architecture Governance Roles, and/or Enterprise Architecture Framework Elements. These changes can have a rippling effect on other components of the Enterprise Architecture Framework or the Architecture Blueprint.

Review Architecture Frameworks – Changes in the Business and IT Strategies may cause the Business Drivers to change. If the strategy changes have caused changes to the Business Drivers, there could be a rippling effect. Review each architecture framework to determine if the structure is still viable.

The other dimension of change may occur in the Architecture Framework enhancements to processes and/or templates. These could impact existing Architecture Blueprint documentation and communication tools.

Create Architecture Review Document – The Architecture Manager summarizes the business, information and technical inputs into a draft review document.

The governance inputs come from:

- Architecture Governance Framework Review Results
- Updated IT Strategic Elements
- Updated Business Strategic Elements

The business inputs come from:

- Business Architecture Framework Review Results
- Updated Business Strategic Elements

The information inputs come from:

- Information Architecture Framework Review Results
- Updated Business Strategic Elements

The technical inputs come from:

- Technology Architecture Framework Review Results
- Updated IT Strategic Elements

Architecture Review Process – Once the Architecture Review Document is prepared, it will be presented by the Architecture Manager to the Reviewers for the Architecture Review Process.

Confirm Architecture Governance Structure – All review items that impact the Architecture Governance Structure must go through this sub-process. Lifecycle processes, Governance Roles, and Enterprise Architecture Framework Elements are maintained in this sub-process.

Architecture Documentation Process – Based on the triggering event that caused the Architecture Framework to go back through the Architecture Documentation Process, the various levels of the architecture blueprint will need to be reviewed. Changes to the overarching Business Drivers will cause review of the Architecture Blueprint from the Domain/Subject level down.

The review during this process will address questions such as:

- Is a new piece of the architecture blueprint required?
- Is change required for classifications of existing pieces of the Architecture Blueprint?
- Is change required for the Disciplines, Domains or Subject Areas?

Document this information for submission to the Architecture Manager.

Architecture Communication Process – Communicate changes or enhancements to the Enterprise Architecture Framework or Architecture Blueprint to the Architecture Audience. The information, whether approved or rejected, should be available to the audience to aid in future service enhancements or Business/IT Portfolio additions.

Architecture Blueprint Vitality Process

Architecture Blueprint Vitality Process is the process that insures the architecture blueprint content remains current and accurate. This is a major requirement of the overall architecture lifecycle processes. To ensure Architecture Blueprint vitality, the Architecture Blueprint must be reviewed from a business strategy, an IT strategy and a study of technology directions. Input from the providers of the organization's strategic documents is essential and the subject matter experts must insure that technology solutions are extensible and sustainable.

Any time business strategies, IT strategies or technology solutions make a noticeable shift, an architectural review may be required. The enterprise will decide on the frequency of reviews that best suit their organization; however, these Blueprint Architectural reviews are typically conducted at a minimum of every four to six months.

The enterprise architecture review of projects should be included as a standard part of project plans. These reviews, along with compliance reviews, become the most prominent part of the Architecture Blueprint Vitality Process.

Once the Architecture Blueprint Vitality Process is initiated, the bulk of the changes will be documented in the Architecture Documentation Process. A Summary of the Architecture Blueprint Changes will be produced and presented as part of the Architecture Review Process.

DETERMINE ARCHITECTURE BLUEPRINT CHANGES

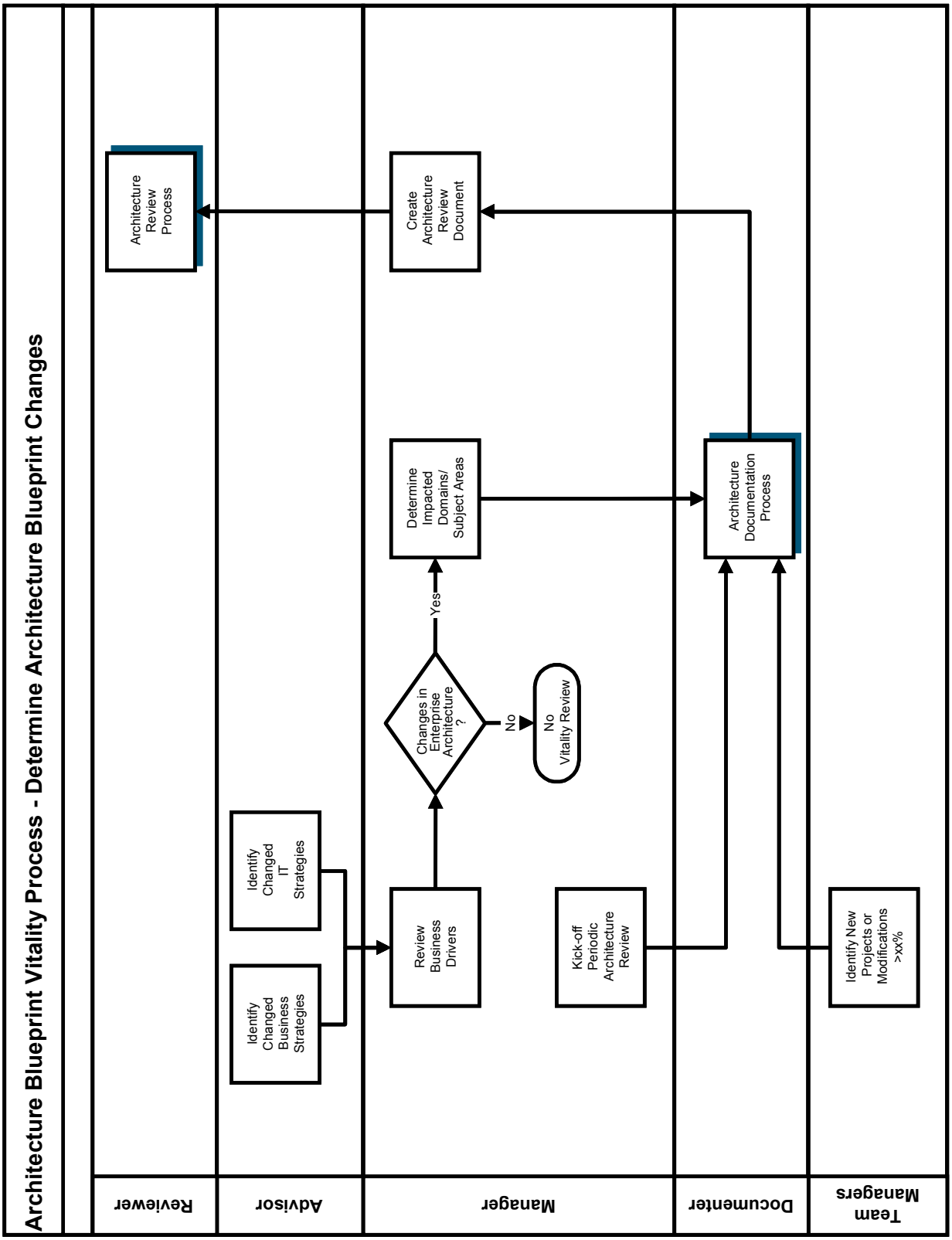
PROCESS OVERVIEW

Several events can trigger changes to the Architecture Blueprints:

- Business Strategic Elements cause the Business Drivers or priorities for the current Business Drivers to change
- IT Strategic Elements cause the Business Drivers or priorities for the current Business Drivers to change
- The Kick-off for Periodic Reviews
- The identification of new project or functionality

If the Strategy changes have caused changes to the drivers, there will be a rippling effect. Domains, Subject Areas, Disciplines and Perspectives that have relationships with the changed Business Drivers should be taken through the Architecture Documentation Process to verify they are still valid and updated as needed. The impacted areas are determined in preparation for an architecture review.

Architectural Blueprint reviews should become a standard part of project/service plans. These reviews, along with compliance reviews, become the most prominent trigger to the Architecture Documentation Process and Determine Architecture Blueprint Changes sub-process. When these reviews are complete, they should be summarized and presented to the Reviewers.


Architecture Blueprint Vitality Process - Determine Architecture Blueprint Changes
Reviewer
Advisor
Manager
Documenter
Team Managers
Architecture Review Process
Create Architecture Review Document
Identify Changed IT Strategies
Identify Changed Business Strategies
Review Business Drivers
Determine Impacted Domains/ Subject Areas
Changes in Enterprise Architecture ?
Yes
No
No Vitality Review
Kick-off Periodic Architecture Review
Architecture Documentation Process
Identify New Projects or Modifications >x%

PROCESS DETAIL

Identify Changed Business Strategies – The Business Advisor identifies and gathers relevant business inputs from updated Business Strategic Elements and forwards the information to the Architecture Manager. The Architecture Manager will need to research changes to the business as well, such as business principles, best practices and business industry trends.

Identify Changed IT Strategies – The IT Advisor identifies and gathers relevant IT inputs from updated IT Strategic Elements and forwards the information to the Architecture Manager.

Review Business Drivers – Changes in the Business and IT Strategic Elements may cause the Business Drivers to change. If the Strategy changes have caused changes to the drivers, there will be a rippling effect. Domains and Disciplines that have relationships with the changed Business Drivers should be taken through the Architecture Documentation Process to verify they are still valid and updated as needed.

Review the Business Drivers to determine whether any of the drivers require stronger emphasis in the Architecture Blueprints. For example, an item currently stated as a Best Practice may be elevated to a Principle or a Trend may be elevated to a Best Practice due to a change.

These types of changes will also affect the Domains/Subject Areas and Disciplines that are related to or conflicted with the changed Business Drivers.

Determine Impacted Domains/Subject Areas – Based on additions or changes to the Architecture Frameworks, identify the Domains/Subject Areas that are impacted in preparation for the review of the Architecture Blueprint.

Kick-off Periodic Architecture Review – Architectural Blueprint reviews should occur every four to six months at a minimum. Based on the audit stamp information, a Documenter/Author can determine which of the levels of the Architecture Blueprint may need to go through the Architecture Documentation Process.

Identify New Projects or Modifications > *x*% – The architecture review of projects and significant modification to existing technology should become a standard part of project/service plans. These reviews, along with compliance reviews, become the most prominent trigger to the Architecture Documentation Process and Determine Architecture Blueprint Changes sub-process.

Architecture Documentation Process – Based on the event that caused the Architecture Blueprint to go back through the Architecture Documentation Process, the levels of the architecture blueprint to be reviewed will be determined as follows:

- Changes to the overarching Business Drivers or periodic Architecture Review cycles will cause the Architecture Blueprint items to be reviewed.
- Changes triggered by project/change team requests will necessitate review of the specific technology areas and below.

The review during this process will address questions such as:

- Is a new piece of the Architecture Blueprint required?
- Is change required for classifications of existing pieces of the Architecture Blueprint?
- Is change required for the Disciplines, Domains or Subject Areas?

This information will be documented for submission to the Architecture Manager.

Create Architecture Review Document – The Architecture Manager summarizes the technical and business inputs into a draft review document.

The technical inputs come from:

- Architecture Blueprint Results (output from the Architecture Documentation Process)
- Summaries of recent technology and application revisions
- Details of any approved variances from standards

The business inputs come from:

- Updated Business Strategic Elements
- Updated IT Strategic Elements

Architecture Review Process – Once the Architecture Review Document has been prepared, it will be presented by the Architecture Manager to the Reviewers.

SUMMARY/CONCLUSION

To this point, the Toolkit has focused on the overarching principles and practices associated with an Enterprise Architecture Program. A well implemented and vital architecture program can provide the organization with data that can be used for many purposes.

In the following sections we will focus on the specifics associated with developing and maintaining the allied architectures framework and blueprints.

- Business Architecture
- Information Architecture
- Technology Architecture
- Solution Architecture

Each of these architectures can stand-alone, however the enterprise will realize highest return when the Business, Information and Technology Architectures have been developed in a manner that allows common elements to be shared. When this is achieved, the architectures can be mapped to each other allowing quick identification of dependencies across the organizations.

NASCIO Online
Visit NASCIO on the web for the latest information on the Architecture Program or to download the current version of the Enterprise Architecture Development Tool-Kit.

www.nascio.org

NASCIO EA Development Tool-Kit
Business Architecture

Version 3.0

October 2004

TABLE OF CONTENTS

BUSINESS ARCHITECTURE

State governments are complex organizations that are difficult to describe. Complex processes and relationships operate in a culture driven by budget. These complexities must be supported by a host of capabilities including information technology. Business architecture provides an operating discipline for describing and managing these complexities. This section of the Tool-Kit will be devoted to exploring and describing that part of Enterprise Architecture that is predominantly business related.

Development of NASCIO's Enterprise Architecture Tool-Kit is an on-going process. Each iteration of the Tool-Kit incorporates new knowledge and best practices as they are developed. NASCIO has generated this section of the Tool-Kit in response to its constituents, who have asked for a treatment of Business Architecture.

NASCIO is treating Enterprise Architecture as a program. As a program, Enterprise Architecture will continue to evolve and become more sophisticated. The reader is encouraged to treat this version of the Tool-Kit as one iteration in an ongoing process. The Tool-Kit will continue to evolve to reflect the changing nature of Enterprise Architecture. NASCIO is presenting Business Architecture as a first iteration in this evolution. The information provided in this version is not an exhaustive treatment of Business Architecture and therefore does not exhaustively detail every aspect of Business Architecture. It also is not NASCIO's intent to repeat within the Tool-Kit information that is readily available from other sources. However, NASCIO will present frameworks, approaches, and concepts that will assist the states in developing their enterprise architecture programs without prescribing a specific methodology. In that light, the Tool-Kit may include more than one view or approach to enterprise architecture allowing the reader to evaluate and use that content that is most relevant and useful in their particular circumstances.

Business Architecture should be viewed as the foundation or driver for the other components of an Enterprise Architecture. There are many definitions for Business Architecture, but for government enterprises, Business Architecture refers to the high-level representation of the vision, mission, goals, objectives, and business strategies that comprise the strategic business intent of government. That intent is then enabled through a variety of capabilities such as functions, processes, information, know-how, and technology critical to providing services to its citizens, agencies, bureaus, departments businesses, vendors, branches and others with whom the government interacts. Strategic business intent is not necessarily described explicitly. Nevertheless, whether the organization in focus is a state, or a branch within state government, strategic business intent will drive the development or further leveraging of technology and non-technology capabilities that are required to enable that intent.

Business architecture must start with an environmental context. That is, a contextual understanding of what is going on economically, politically, and in the way of citizen expectations. This includes identification and understanding of the trends, changes, market forces, fiscal and monetary policies and their immediate and latent effects on the economy, availability of capital, and labor. These environmental factors are spawning the transformation of government. It is important to realize that information technology is not only a tool for government, but also a driver for transforming the operations of government. Some of the trends in government include an increased emphasis on performance, accountability, improved financial management, improved service delivery and collaboration.

This contextual understanding provides the bounding and relevancy required to investigate market opportunities or citizen needs. Those opportunities and needs are then evaluated along with an understanding regarding who is able to fulfill those needs. This evaluation helps determine if a particular

need is best served by government or by the private sector. Once it has been determined that a particular need or desire is best served by government, government must develop its intentions, or its strategic business intent. Strategic business intent is made explicit through carefully articulated mission, vision, goals, objectives, and strategies. Performance measures are established as part of that intent in order to insure performance is perfectly aligned with intent. That intent is then enabled through capabilities that are delivered through management initiatives, programs and projects. Information technology is one of those capabilities. In fact, as with other capabilities, information technology can be stratified or broken down into manageable pieces that can be delivered or further leveraged through well scoped projects. Projects must be managed within portfolios as part of a program management discipline. This will insure that there is proper project to project communication and redundant efforts are avoided. This entire process is demonstrated with what can be termed the *Enterprise Architecture Value Chain* as shown in Figure 1. The four chevrons include examples of the kind of content that typically comprises these major activities.

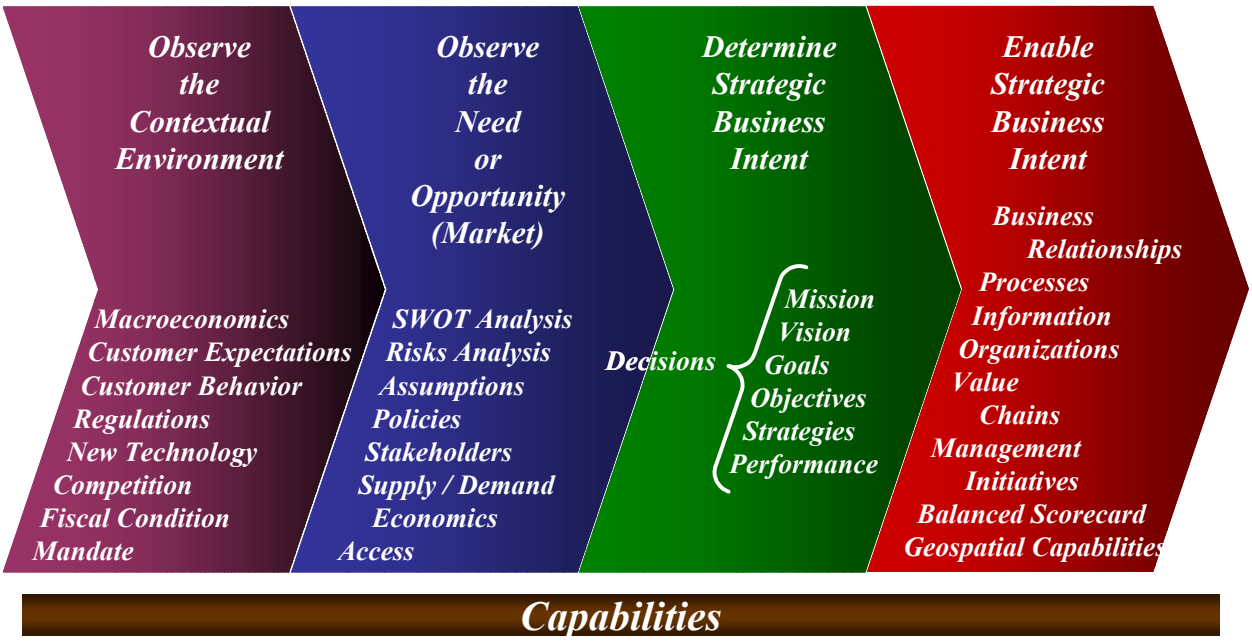


Figure 1. Enterprise Architecture Value Chain

It is termed a value chain as there is value added through the progression from environmental understanding through to enablement. This value adding process insures activities are properly executed within the realities facing government.

It is important to remember that there are many capabilities that enable strategic business intent that may not be predominantly based on information technology. Capability management, a part of enterprise architecture, explores, identifies, stratifies, evaluates and prioritizes capabilities to determine the best investment path for serving citizens.

Business architecture must also consider interaction with other governments, as well as delivery of services to citizens of other governments. Business Architecture includes this aspect as business interactions.

Business Architecture describes government business from an enterprise-wide perspective. Strategies, processes, organizations, locations, and information are all documented to show their existing place in the business model and their future significance. For any Enterprise Architecture effort to be successful, it must be linked to the business direction of the organization. This linkage is established in the Business Architecture.

Figure 2 shows how Business Architecture fits within the overall Enterprise Architecture Framework. Business Architecture serves as the business knowledge base for the Enterprise Architecture Program. It documents what, where, by whom, how, when and why the organization's business is performed. Essentially, business architecture describes how the business of government "fits" together.

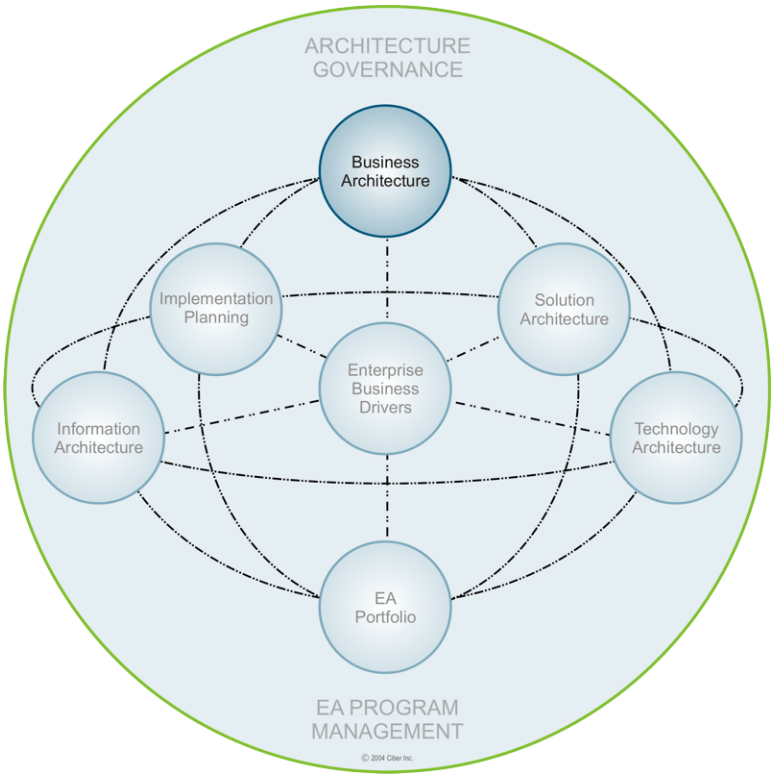


Figure 2. Business Architecture Touch-points

In addition to serving as the focal point for the Enterprise Architecture Program, Business Architecture can serve as a stimulus for developing detailed business plans, technology plans and business contingency plans. Business Architecture can also be used when performing impact analyses to adapt the organization to changing business needs.

Documenting the Business Architecture provides a clear understanding of the enterprise's current and future direction. The information documented in the Business Architecture supports the decisions of the executives and managers in their efforts to meet the business goals and objectives. Business priorities direct allocation of resources when Business Architecture is included in the Enterprise Architecture.

Business Architecture provides a demonstrable, repeatable approach for assuring the alignment of business processes, systems and resources throughout the enterprise. In addition, documentation of the Business Architecture provides a valuable tool for illustrating and communicating the business of the enterprise to all stakeholders. One of the benefits of Business Architecture is that it can serve as a vehicle for inclusion of the business side of government into the information technology planning process and for building consensus among groups.

Federal, state and local governments continually face mandates for inter-agency sharing of information and for providing bundled services. Business Architecture provides a business-based framework for developing solutions that operate across agencies and within the lines of business of federal, state and local governments. In developing Business Architectures, federal, state and local governments look at the architectures of their communicating partners, thus enhancing opportunities for interoperability between all governmental bodies, both vertically and horizontally. Inter-enterprise architecture refers to

extending the enterprise to include it communicating partners. An example of this is demonstrated with the exchange of criminal justice data within the justice community. Such information is shared between law enforcement, courts, corrections, and probation.

The pursuit of formal Enterprise Architecture Programs within organizations contributes to interoperability across enterprises. This is depicted in Figure 3.

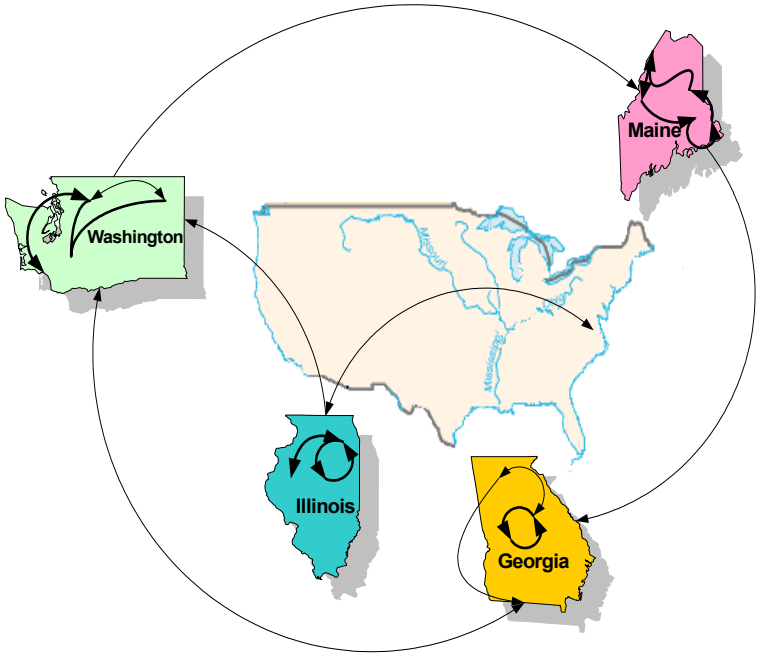


Figure 3. EA Enhances Interoperability Between All Government Bodies.

Definitions

When discussing Business Architecture and related topics, the terminology varies, including a variety of terms with the same or similar meanings, as well as varied meanings for the same term. To minimize any confusion in terminology, a glossary, which provides definitions of terms used throughout the Tool-Kit, is provided in Appendix A of the Tool-Kit document. A brief list of the terms and definitions used within this Business Architecture section are provided here:

- *Artifacts:* Artifacts constitute any object, or work product that is developed as a component of the enterprise architecture. Artifacts include trends, principles, mission, goals, objectives, strategies, capabilities, processes, process steps, entities, attributes, relationships, subject areas, application components, applications, data bases, etc.
- *Approach:* Approaches are devised to deliver work products that are consistent. An approach can be project specific or apply to the enterprise as a whole. For example, use of Unified Modeling Language (UML) case models versus entity relationship diagrams. These may be viewed as two different approaches for information modeling. *(see http://www.uml.org/)*
- *Baseline:* The current or "as is" state of the business environment, captured in a set of baseline business models.
- *Blueprint:* The dynamic depiction of the business, captured using standardized, structured processes and templates (framework). The Business Architecture Blueprint records the present direction of the enterprise and the direction the enterprise intends to pursue from a business perspective.
- *Business Architecture:* The high-level representation of the business strategies, intentions, functions, processes, information, and assets (e.g., people, business applications, hardware) critical to operating the business of government successfully.
- *Business Architecture Framework:* The combination of templates and structured processes that facilitate the documentation of the enterprise's business artifacts (e.g., strategies, processes, events) in a systematic and disciplined manner.
- *Business Domain Model*: A graphical or pictorial representation for describing business operations of the enterprise (Domains), independent of the agencies, bureaus, departments and/or offices that perform the operations or provide the services.
- *Business Domain:* A functional or topical subset of the business operations that is integral to the success of the enterprise. Examples of Domains might include:
  - Functional Domains
    - Education
    - Health and Social Services
    - Justice and Public Protection
    - Resource and Economic Development
    - Transportation and Engineering
  - Topical Domains
    - Customer
    - Location
    - Payments
- *Business Drivers:* Internal goals and strategies and external trends that influence the business.

- *Business Perspective:* A breakdown of the Business Domain based on a specific viewpoint, such as Who, What, Where, When, Why, How, or a logical combination of one or more of these viewpoints.
- *Business Portfolio:* The implemented baseline business environment, business processes, strategies and data of the business organization.
- *Business Architecture Perspective:* A breakdown of the Domain based on a specific viewpoint, such as Who, What, Where, When, Why, How, or a logical combination of one or more of these.
- *Framework:* In general, a framework will depict and define the relationship between enterprise architectures. Within an architecture, a framework will depict the relationships among the components. A framework depicts relationships between and among methodological work products. *(note: there is a diversity in the use of terms such as blueprint, framework, etc. In order to facilitate effective communication, definition of terms must be established in any enterprise architecture program initiative.)*
- *Gap:* The differences between the "baseline" business environment and the "target" business environment in key areas of the business (e.g. business needs, business processes, workload, ability to handle growth, users, interfaces).
- *Inter-enterprise Architectures:* Describes the relationships and interactions between the enterprise in focus and its trading partners/jurisdictions and customers.
- *Meta Models:* Meta models describe the artifacts or elements that comprise architecture domains. These are essentially data models – or entity relationship diagrams describing the artifacts, their attributes, and relationships. Meta models are essential to exploring and establishing the components of each architecture domain.
- *Migration:* The evolution from the baseline to the target state of the business environment.
- *Model:* The graphical representation or simulation of a process, relationship or information.
- *Operating Discipline:* An operating discipline is a "discipline for operations." It describes exactly what is to be done, when, by whom, why, and where. It is comprised of the following elements: a framework for describing the components and their relationships; meta models for describing the content of the framework; a methodology for navigating through the framework; approaches for delivering work products consistently; and service delivery for delivering work products in a particular engagement.
- *Repository:* An information system used to store and access architectural information, relationships among the information elements, and work products[1].
- *Strategic Element:* A strategic direction, driver or goal, used to establish a vision statement, business objectives, business plans and business drivers.
- *Target:* The desired future or "to be" state of the business environment, captured in a set of target business models.
- *Template:* An empty form that serves as a guide for capturing the business details that will ultimately reside in an Enterprise Architecture repository.

Business Architecture is the foundation for other parts of the Enterprise Architecture, providing context and guidance to keep the enterprise architecture focused on the strategies and goals of the government. Figure 4 illustrates the logical links and relationships of the Business Architecture to other parts of the Enterprise Architecture. The Business Drivers and enterprise circumstances influence the development of the Business Architecture Blueprint. The Blueprint, in turn, documents strategic initiatives, identifies potential investment benefits, and influences the development of the Technology, Information and Solution Architectures.

[1] A Practical Guide to Federal Enterprise Architecture v1.0, CIO Council, February 2001

Details pertaining to Motivation (why), Business Information Concepts (what), Business Cycles (when), Location/Logistics (where), Function (how), and People (by whom), are captured within a Business Architecture Blueprint as business models.

By capturing the information for these components in current business models (Baseline) and proposed business models (Target), deficiencies and gaps, including growth opportunities, are identified. Based on the analysis of the business drivers and the gaps, determinations are made regarding mitigation of gaps, migration strategies are developed to bridge the specific gaps and provide a roadmap to move to the target business model.

Pursuing a formal explicit Business Architecture offers many benefits to the Enterprise. These benefits are used to garner support for the Business Architecture effort, as well as the Enterprise Architecture effort as a whole. By presenting a holistic, seamless view of the Enterprise, the Business Architecture will:

- Provide a basis for Capital Planning and Change Management
- Facilitate cross agency and intergovernmental analysis and opportunities for integration
- Increase understanding of how the enterprise carries out its mission through documentation of its business transactions and functions
- Provide explicate documentation of regulatory compliance criteria throughout the Business Architecture Components
- Increase responsiveness to customers
- Increase collaboration and sharing of information across government-wide entities

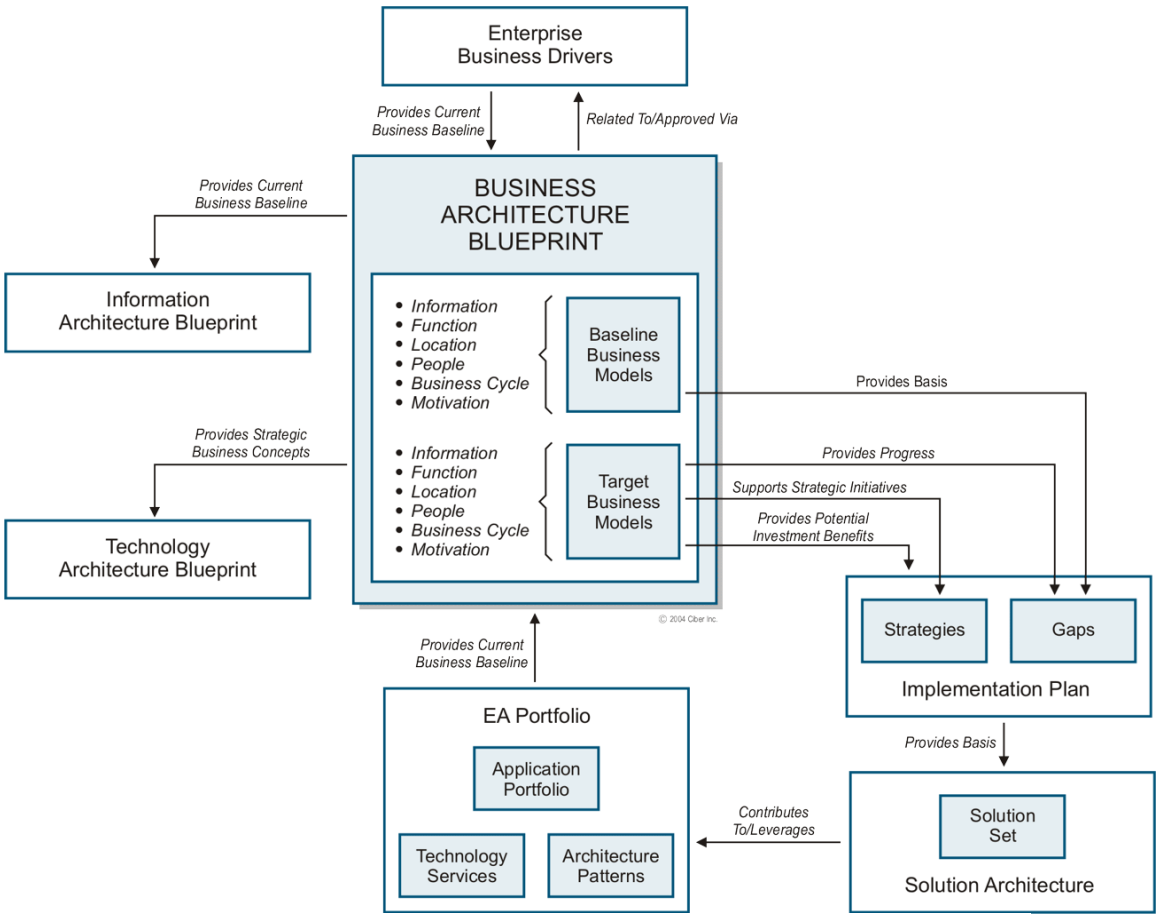


Figure 4. Business Architecture Touch-points

- Assess the impact and mitigate the risk of tactical decisions
- Increase project success rates
- Eliminate costly rework
- Identify opportunities to employ innovative technology[2]
- Enhance investment decision-making by providing ready access to information about technology and business linkages
- Reduce redundancy throughout the enterprise, which causes excess resource expenditures in human and financial capital
- Produce streamlined auditable processes
- Facilitate Business Process Reengineering (BPR), Business Process Consolidation (BPC), and Continued Process Improvement (CPI) etc.
- Ensure business focus is on the highest priority and mission critical efforts.

---

2 Federal Chief Information Officer (CIO) Council, Federal Architecture Working Group, *A Practical Guide to Federal Enterprise Architecture, Version 1.0,* February 2001.

This section of the Tool-Kit supports NASCIO's architecture program by providing government organizations a suggested structure (framework)for establishing an effective Business Architecture. As organizations develop the structure for their Business architecture, it is important that the processes and templates be flexible enough to guide the documentation of various business elements such as:

- Business drivers
- Business organizations / roles
- Business events
- Business functions
- Business locations
- Business information concepts

The development and maintenance of a vital Business Architecture requires the involvement of personnel in a variety of roles and responsibilities. Table 1 provides a reminder of the roles that apply across all of the architectures.

Table 1. Architecture Roles

Primary Roles	*Supportive Roles*
• Overseer • Champion • Manager • Documenter • Communicator • Advisor • Reviewer • Audience	• Subject Matter Experts (SMEs) • Services Teams • Project Teams • Procurement Manager • Project/ Services Communicator • Special Interest Groups • Enterprise Executive

Greater detail for these roles, including a brief description of each role, its responsibilities, its recommended implementation, etc. is provided in the Architecture Governance Section of this Tool-Kit (See *Architecture Governance Roles*). Appendix B also contains a Role & Responsibility Matrix which provides an "at-a-glance" reference of the responsibilities of each Architecture Governance role, the items acted upon, and the roles that interact regarding the responsibility. Each Enterprise should determine the roles that will best help their organization in developing their own Business Architecture. The following identifies the basic roles that are useful in developing Business Architecture:

- **Business Architecture Manager**- An executive responsible for items including, but not limited to:
  - Providing a "business needs" view of the enterprise with a focus on strategic planning, budgets, organization, policies and procedures (documenters)
  - Understanding the enterprise business architecture and communicating the architecture in such a way that business objects and process models can be developed
  - Understanding the current enterprise strategic direction and the relationships between elements of the organization and current endeavors.
- **Business Architecture Documenter-** A member of a team comprised of business modelers who are familiar with various aspects of enterprise-wide business processes. The team members are responsible for steering, shaping, and developing a Business Architecture Blueprint. These team members should be knowledgeable in both business and technology. The role of Documenter refers to the combination of those best suited to document the architecture, including business Subject Mater Experts.

- **Business Architecture Subject Matter Expert (SME) -** A member of an interdisciplinary team who ensures that the business functions, transactions and information are fully understood and correctly documented in the Business Architecture Blueprint. SMEs may also serve as Business Architecture Documenters.
- **Business Architecture Advisor** - An executive who provides clarity and support to the Business Architecture Manager. This Advisor serves as a champion for the Strategic Elements from both the business and technology communities within the enterprise. The Business Architecture Advisor will also provide guidance on enterprise architecture variance requests from a business and economic perspective.
- **Business Enterprise Executive** – An executive that provides Strategic Elements that give direction, goals and objectives to the enterprise. A Business Enterprise Executive is typically an executive role that is responsible for ensuring the enterprise goals and objectives are set by the governance organization. This individual must be an active sponsor and evangelist for business architecture.

This section provides concepts to improve understanding of Business Architecture and serves as guidance for enterprise architects and those assisting the architects in developing an enterprise architecture for their organizations.

Business Architecture Framework

The Business Architecture Framework is the combination of templates and structured processes that facilitate the documentation of the enterprise's business artifacts (e.g., strategies, processes, events) in a systematic, disciplined manner. The information captured should foster capital planning and other business decision-making by providing a picture of where the enterprise is today (baseline) and where the enterprise wants to be in the future (target). Having an accurate representation of the two classifications of the business (baseline and target) enables the identification of differences (i.e., gaps) between the two (Figure 5.). During Implementation Planning, analysis of the gaps, development of migration strategies, risk analysis, and development of business cases will draw upon the business architecture information.

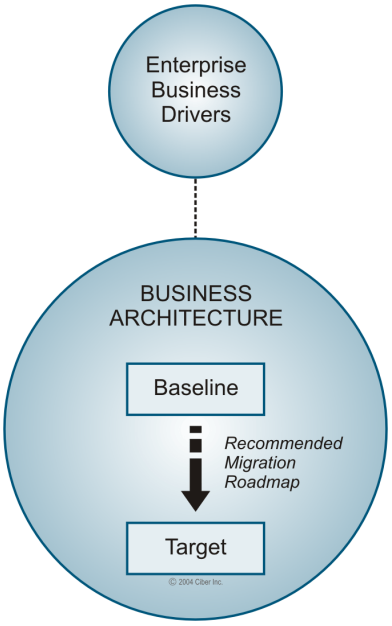


Figure 5. Business Architecture Flow

For each Business Domain, organizations should decide how much effort is appropriate for documentation of the baseline. The rationale for completing a baseline is to ensure adequate understanding of the current state for the purpose of developing a strategy for moving toward the target, while at the same time minimizing risk.

Documenting the Business Architecture by using structured processes and templates will:

- Provide information on strategic business drivers
- Show how those drivers are reflected today
- Furnish the roadmap to addressing those drivers in the future
- Provide valuable detail for making decisions and planning the investments (human capital or monetary capital) to further those drivers in the future.

The effective use of a Business Architecture Framework provides a standardized approach to capturing the details of the Business Architecture Blueprint by means of:

- Structured processes for documenting the Blueprint
- Templates for capturing the Blueprint detail

Standardization promotes broader understanding and can facilitate the integration and interoperability of solutions.

BUSINESS DRIVERS

The identification and development of Enterprise Business Drivers is an important business activity. Business Drivers include internal goals and strategies and external trends, such as legislation or regulatory items that influence the business. The Enterprise Business Drivers provide strategic business concepts for Business, Information and Technology Architectures. They also influence Implementation Planning and the enterprise solutions built as part of Solution Architecture.

Three common categories of Business Drivers include Principles, Best Practices and Trends:

- *Principles:* Principles are statements of preferred direction or practice. Principles constitute the rules, constraints and behaviors that a bureau, agency or organization will abide by in its daily activities over a long period of time. Principles are also business practices and approaches that the organization chooses to institutionalize to better provide services and information.
- *Best Practices:* Best Practices are practices and approaches that have proven successful over time at providing services and information.
- *Trends:* Trends are emerging influences within the business world that impact how services and information are provided. Trends include governmental trends as well as architecture specific tends, i.e. technology trends, information management trends, etc.

BUSINESS ARCHITECTURE BLUEPRINT STRUCTURE

A Business Architecture Blueprint refers to the dynamic depiction of an organization's business, captured using standardized, structured processes and templates. The Business Architecture Blueprint records the present direction of the enterprise and the direction the enterprise intends to pursue from a business perspective. The Business Architecture Blueprint is comprised of Business Domains, Business Architecture Perspectives, and Business Architecture Components.

Figure 6 provides a pictorial view of the relationship between the business architecture blueprint elements. The graphic displays these pieces working together to ensure the complete documentation of the Business Domains that form the Business Architecture Blueprint.

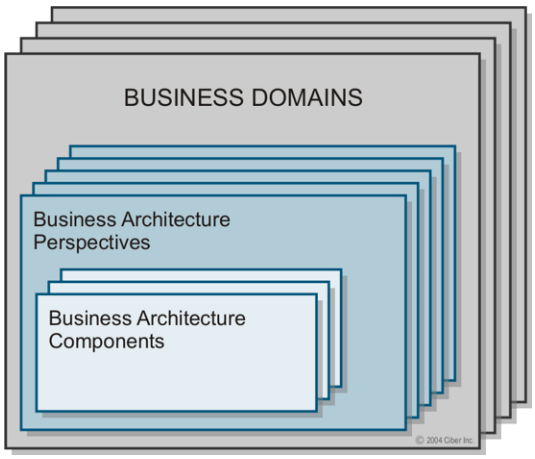


Figure 6. Business Architecture Blueprint Structure

Business Domains – Business Domains are the natural divisions of the business architecture and are based on either functional or topical scope. Business Domains represent the highest level of the business architecture blueprint. A few examples of functional and topical domains include:

- Functional Domains
  - Education
  - Health and Social Services
  - Justice and Public Protection
  - Resource and Economic Development
  - Transportation and Engineering
- Topical Domains
  - Customer
  - Location
  - Payments.

A Business Domain Model represents how the State's Business service offerings are arranged and used for defining the business needs, business processes, and business information concepts. Each enterprise should design its own model based upon its unique mandates and needs. This high-level representation departs from an organization structure to allow business functionality to cross departments and agencies. This cross-functionality helps in the development of enterprise business solutions that apply across the enterprise and reduces the type of solutions often referred to as stovepipes, silos or islands of information.

Organizations may choose to break out exceptionally large Domains into more manageable pieces. These logical subsets are typically referred to as Disciplines. The Business Domain Template can be customized to document each subset (Discipline) by adding a section for identifying the associated Domain. *Business Architecture Blueprint Samples – Set 2* includes an example of a Domain, Discipline, Business Architecture Component and Gap Component.

Business Architecture Perspectives – A Business Architecture Perspective is simply a breakdown of the Domain based on a specific viewpoint. Documenting each domain entails interviewing numerous stakeholders and collecting a wide range of detail.

The purpose of defining Business Architecture Perspectives is to create focal areas to assist Documenters as they conduct interviews and document the details of the Business Domain.

The Zachman Framework[3] is a widely recognized and frequently implemented framework for depicting the enterprise. John Zachman established six questions, or interrogatives: What, How, Where, Who, When and Why, which are addressed from various views. Business Architecture constitutes the top two rows of the Zachman Framework, which he refers to as the Planner's view (Contextual) and Owner's view (Conceptual).

The number of Business Architecture Perspectives and the viewpoint or focus of each Perspective, are determined within each organization based on the environment and circumstances. Once the Business Architecture Perspectives are determined, the same Perspectives or a sub-set of the Perspectives are typically used across all Business Domains.

An organization could decide to define one Business Architecture Perspective for each of the interrogatives addressed in the Zachman Framework: Who (people), What (assets), When (business cycles), Where (locations/logistic), Why (motivations) and How (functions). However, organizations may choose to define a least one of their Business Architecture Perspectives to address a combination of two or more of these interrogatives.

An example of this might be the creation of a Business Architecture Perspective, called Strategic Business, that focuses on the combination of "who" and "why" (Figure 7). This Business Architecture Perspective would cover components such as strategic direction, drivers and goals, organizational roles and responsibilities, business objectives and plans. This combination of viewpoints into a single Business Architecture Perspective is fairly common because the "who" and "why" topics are so often considered together. Creating one or more Business Architecture Perspectives that address a combination of the interrogatives allows the interviewers to address several aspects with fewer individuals.

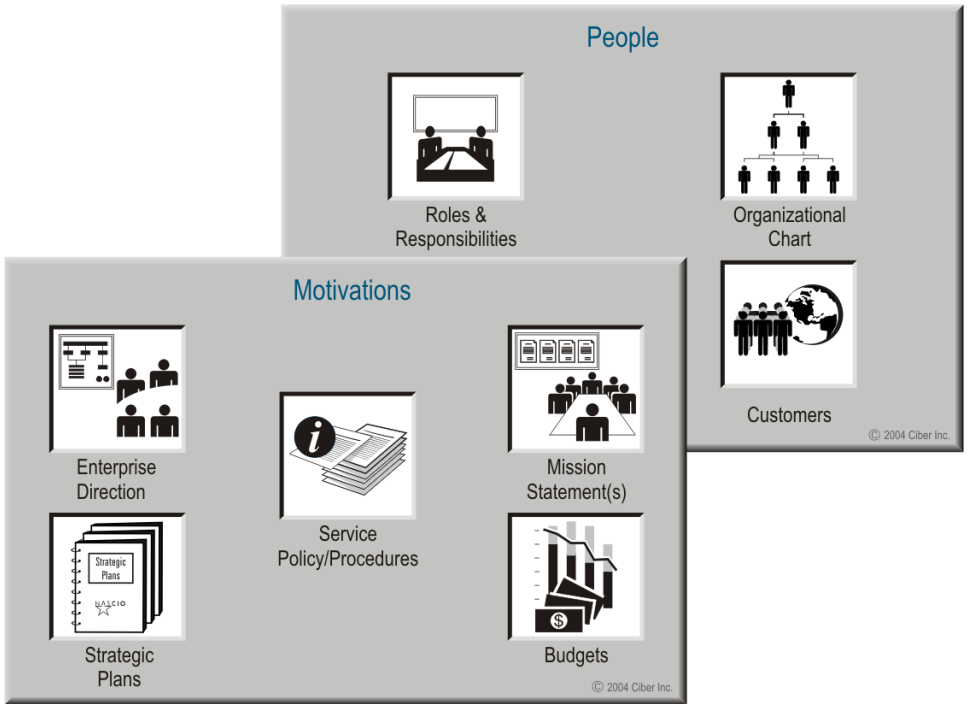


Figure 7. Sample Perspective – Strategic Business

[3] Zachman Framework, http:/www.zifa.com

During interviews, each documenter can be assigned to a specific Business Architecture Perspective. By utilizing this method, the documentation team divides the work and ensures that the detail documentation covers all perspectives. By setting scope and boundaries, the Business Architecture Perspectives facilitate full coverage of the Business Domains while breaking the Domains down into manageable pieces. This is important because state government domains are complex. Project management is made easier by using this breakdown because the project deliverables can be managed by Business Architecture Perspective. The following list provides one example of a breakdown of Business Architecture Perspectives. Government organizations are encouraged to develop their own Business Architecture Perspectives that are representative of the culture of their organization.

- *Strategic Business* – a view with the primary focus on motivating factors (why) and organizations (who) involved with the domain or process
- *Strategic Services* – a view with the primary focus on service performed (how) and the business cycles for these services (when)
- *Strategic Information* – a view with the primary focus on the information assets (what) important to the enterprise
- *Strategic Infrastructure* – a view with the primary focus on the locations and logistics (where) of the processes in the domain

Business Architecture Components – Business Architecture Components specifically identify what information, service, location/logistics, organizational roles/responsibilities, and strategies will be used for implementation of the Business Domain.

These elements of the Blueprint will be addressed in greater detail in the Business Architecture Documentation process models, however, there is one additional component that is introduced here: the Gap Component.

Gap Components –The Gap Component resides as a component of the Implementation Plan. Contributions to the Gap Component come from Business, Information, and Technology architectures. As part of the Business Architecture Documentation Process, once the baseline and target detail has been confirmed for any given Business Domain, the gaps can be identified and documented as appropriate. The documentation of these gaps, along with the migration strategies for closing the gaps, provides the roadmap for moving toward the target architecture. Information regarding gap closure that is not affordable in absolute or ROI terms and won't be pursued should also be included in the documentation. The graphic in Figure 8 shows the critical link between the Business Architecture Blueprint and the Gap Component, which is part of Implementation Planning.

For example a baseline and target scenario might be:

Baseline: "substantial data about regulated trucking firms resides in separate business units within the department of transportation. Duplication and redundant activities are common. Trucking firms may easily avoid the necessary permitting processes."

Target: "Data will be maintained in a common customer database that will be used to support improved identification, processing, and management of trucking firms under 'regulation XYZ.' As a result, payment of permits will increase, etc."

The Gap Analysis must include the gaps between baseline and target components and the roadmap or delivery process for change management.

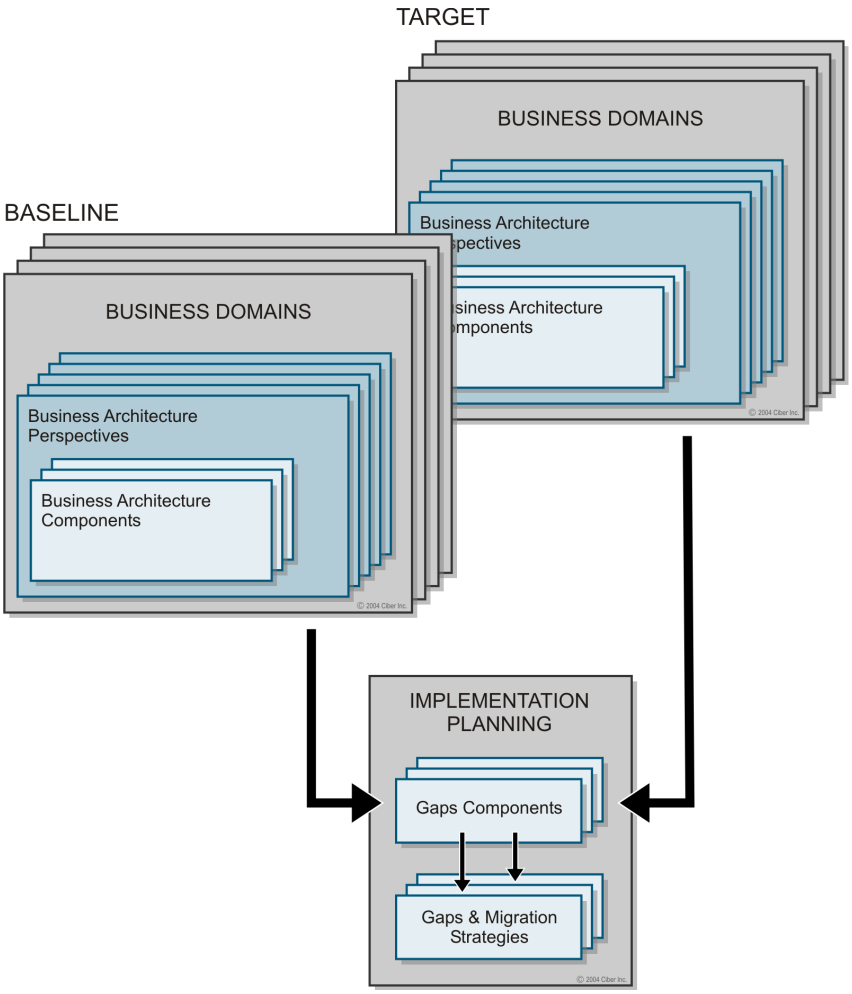


Figure 8. Business Architecture Contributes to Implementation Planning

BUSINESS ARCHITECTURE DEVELOPMENT

The process of developing Business Architecture begins with initiating the Business Architecture Documentation Process. This documentation process allows the architecture teams to capture, analyze, and document details about the business of government, which is included in the Business Architecture Blueprint.

Figure 9 provides a graphical representation of the workflow path for the architecture team as they move through the processes and sub-processes of the Business Architecture Documentation Process.

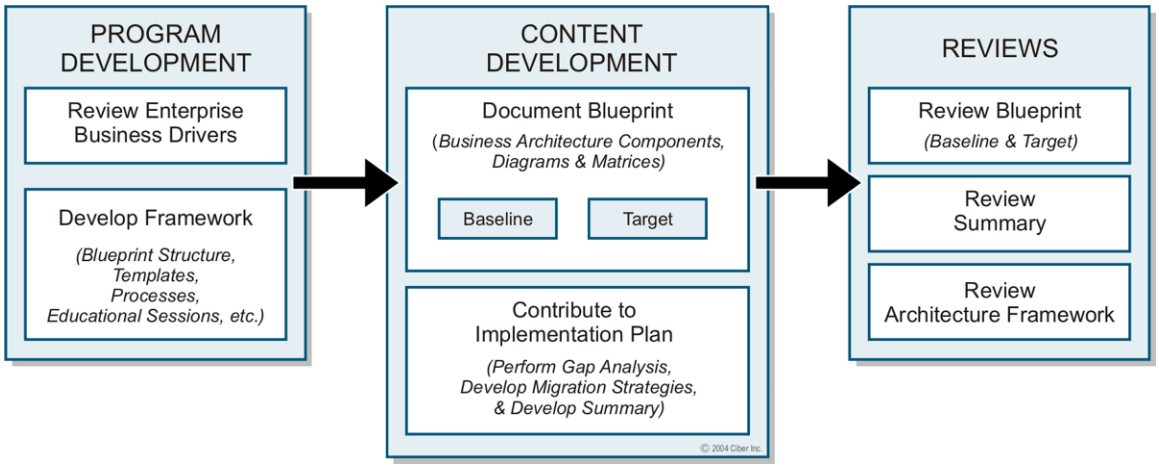


Figure 9. Business Architecture Development Work Flow

During the Business Architecture Documentation Process, details of where government business is today and where it wants to be in the future are captured. After the details of today's and the future's business are captured and documented, a roadmap of how to get to the future state is developed. This occurs as part of Implementation Planning.

It is expected that the majority of effort will be directed toward establishing the target strategic business intent. Strategies describe "how" the intent will be accomplished. Strategies are enabled through capabilities. Capabilities must be defined, stratified, evaluated and prioritized. Once prioritized, capabilities will be delivered or further leveraged through management initiatives, programs and projects. Every government organization will have different capabilities. One strategy might be to learn about common needs and leverage capabilities across the enterprise to meet those needs collectively.

The Documenters develop the Business Architecture Blueprint by interviewing Business Subject Matter Experts regarding various functional and topical areas. The explicit definition of the business model is then captured in what is referred to as the Business Architecture Blueprint. Diagrams and matrix information about the defined pieces of the business are created during this process to show the relationships and associations of all the business definitions.

The Business Architecture Documentation Process describes the systematic process for developing and maintaining the Business Architecture Blueprint. The Business Architecture Documentation Process consists of several sub-processes, including:

- Initiate Business Architecture Documentation Process
- Develop Business Architecture Framework

- Conduct Business Architecture Work Sessions
- Create/Update Business Architecture Blueprint Items.

The structure for each sub-process of this Business Architecture Documentation Process follows the same format:

- Introductory material (where applicable)
- Process model
- Narrative description of the process
- Template for capturing Blueprint detail (where applicable)
- Narrative description of the detail to be captured utilizing the template.

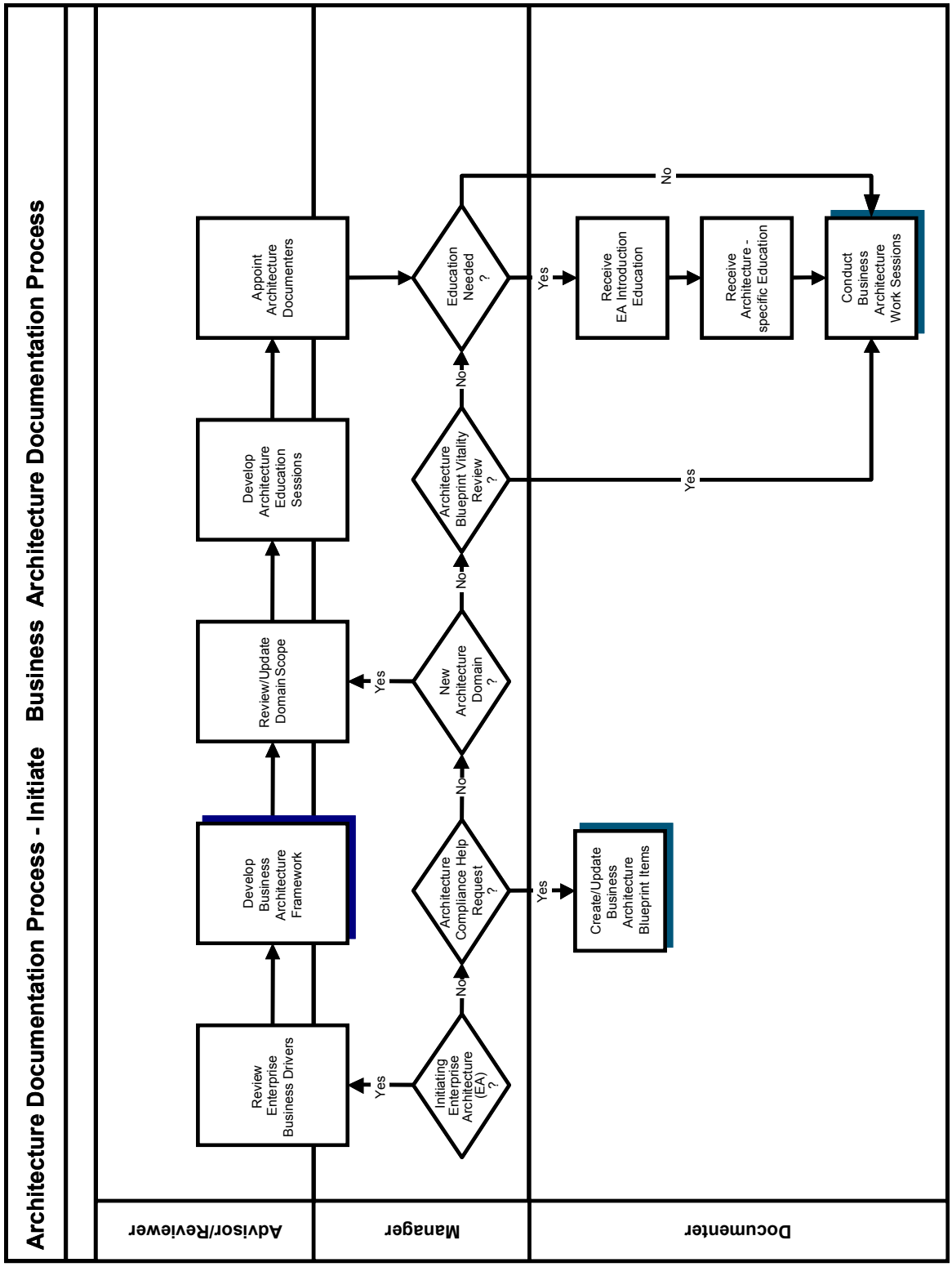
Initiate Business Architecture Documentation Process

PROCESS OVERVIEW

The Initiate Business Documentation Process presented here is similar to the generic process model provided in the Architecture Governance Section of the Tool-Kit. This model and narrative provides the initial process steps that are specific to the Business Architecture.

The Business Architecture Documentation Process can be triggered by the following processes/activities:

- Initiating Enterprise Architecture (EA)
- Architecture Compliance Help Request
- Architecture Blueprint Vitality Review
- New Business Architecture Domain.


Architecture Documentation Process - Initiate Business Architecture Documentation Process
Advisor/Reviewer
Manager
Documenter
Review Enterprise Business Drivers
Develop Business Architecture Framework
Review/Update Domain Scope
Develop Architecture Education Sessions
Appoint Architecture Documenters
Initiating Enterprise Architecture (EA) ?
Architecture Compliance Help Request ?
New Architecture Domain ?
Architecture Blueprint Vitality Review ?
Education Needed ?
Create/Update Business Architecture Blueprint Items
Receive EA Introduction Education
Receive Architecture - specific Education
Conduct Business Architecture Work Sessions
Yes
No

PROCESS DETAIL

Review Enterprise Business Drivers – It is important for the Business Architecture team to understand and become familiar with the Enterprise Business Drivers. While the development of the Enterprise Business Drivers is typically an overarching activity of Business, the Business Architecture team may become aware of circumstances or shifts from documented drivers and can contribute to the vitality of the Enterprise Business Drivers.

Develop Business Architecture Framework – The information documented within the Business Architecture Framework will play an important role in the development of the Business Architecture Blueprints. The NASCIO Business Architecture Framework provides structured processes and templates for capturing this information in a consistent and systematic manner. An organization may decide to use the framework elements as described in the NASCIO Tool-Kit, or may choose to develop a modified version, or may choose to use processes, templates and governance structures other than the examples provided in this Tool-Kit.

Review/Update Domain Scope – Review the definition of the domain and add any detail that will be helpful in identifying the documentation team members. Also add any information that will help the team develop the appropriate level of documentation for this domain.

Develop Architecture Education Sessions– The Architecture Education Sessions provide high-level overviews of the Enterprise Architecture Program and prepare Documenters for their role in the Business Architecture effort. Developers of education materials should consider inclusion of the following materials:

- Purpose
- Presenters
- Intended audience
- Session structure
- Prerequisites
- Syllabus
- Objectives
- Class materials for both instructors and attendees.

Appoint Architecture Documenters – At this point, the Documenters are appointed from subject matter experts familiar with the business side of the enterprise. The team is comprised of modelers familiar with various aspects of enterprise-wide business and responsible for steering, shaping, and developing the Business Architecture Blueprint.

The educational sessions described below, are progressive in nature. The sessions will be conducted after the architecture team is identified:

Receive EA Introduction Education – Documenters should receive initial training that covers the overview of enterprise architecture and architecture governance.

Receive Architecture-specific Education – After receiving initial enterprise architecture training, the Documenters will receive specialized instruction addressing the business architecture documentation templates and processes to be used to document the Business Architecture Blueprint. The documentation used during the sessions will contain detail relative to each specific Business Domain.

Conduct Business Architecture Work Sessions – Applying knowledge gained in the two education sessions, Documenters will begin development of the Business Architecture Blueprint documentation. The detail of the Work Sessions is presented in a separate process. (See *Conduct Business Architecture Work Sessions*).

Create/Update Business Blueprint Items - If architecture compliance help is requested, the various Blueprint items should be updated. The process model and details pertaining to updating the Blueprint items is presented in a separate process. (See *Create/Update Business Architecture Blueprint Items*).

Develop Business Architecture Framework

PROCESS OVERVIEW

In this Tool-Kit, the term Architecture Framework is used to refer to the combination of the structural elements of the architecture, such as the templates and the structured processes for documenting, reviewing communicating, implementing and maintaining the architecture,

Each governmental organization should develop a Business Architecture Framework based on their individual circumstances and build a team with the appropriate blend of business and technical Subject Matter Experts. The NASCIO Tool-Kit is designed to provide a jumpstart for organizations as they develop their architectures, not to provide a methodology. The framework elements provided in this Tool-Kit represent a sampling of the structural elements an organization should consider as they build their Business Architecture and is by no means exhaustive, nor is it intended to be prescriptive

There are many methodologies for developing architectures. Regardless of the methodology selected, the structure for capturing Business Architecture Blueprint detail should be consistent and concise to ensure uniform documentation and communication across the enterprise.

Architecture Documentation Process - Develop Business Architecture Framework
Advisor/Reviewer
Manager
Documenter
Develop Business Architecture Processes/ Templates
Identify/Define Enterprise Business Domains
Select Initial Business Domains for Documentation
Identify/Define Business Architecture Perspectives

PROCESS DETAIL

Develop Business Architecture Processes/Templates – Developing the processes and templates for capturing pertinent architecture detail, as well as defining and documenting the governance structure to support the architecture activity, is a step that is critical when initiating EA or any of the underlying architectures. Each enterprise must decide upon the methodology that best suits their organization. The best methodology for an organization is one that addresses the resource and time constraints of that enterprise.

The use of a repository or automated tool for the capture and storage of the architecture documentation should be considered. Developing, using and maintaining the Enterprise Architecture is greatly simplified when the information and models are readily available to all stakeholders. There is a large amount of information collected and documented within an EA with many interrelations between the parts of the EA. It is best if all the EA information, models and products are placed in a robust EA repository to maximize the potential for reuse.

Identify/Define Enterprise Business Domains - A Business Domain is a major functional or topical subset of the business operations such as public safety, and health and human services. These domains are integral to the operations of the enterprise. Business Domains provide the natural divisions of the business architecture based on scope and are the main building blocks of the business architecture blueprint. Each organization must identify its own Business Domains. The process of identifying Business Domains across the enterprise is, in itself, a valuable undertaking and most often begins with the Business Domain Model.

Business Domain Model – The Business Domain Model is a graphical representation describing business operations of the enterprise independent of the agencies, bureaus, departments and/or offices that perform the operations or provide the services. Therefore, a Business Domain Model is essentially a graphical representation of all of the Business Domains within an enterprise. The Business Domain Model provides a foundation from which the other levels of the Business Architecture can be developed.

A Business Domain Model will:

- Help in identifying "hot spots" for those domains that the organization feels should be documented further
- Facilitate cross-agency analysis to identify opportunities for collaboration and simplification
- Provide a single point of reference of the enterprise business for agencies, oversight bodies, IT decision makers, business partners, vendors, and citizens
- Facilitate identification of common business processes, information requirements, and opportunities for reengineering across the enterprise
- Aid in identification of redundancies and gaps
- Assist in the definition of user applications in the Solutions Architecture.

The purpose of building the Business Domain Model is to understand the essence of the business of the governmental enterprise so that intersections between functional and topical services are identified. Additionally, considering the overall enterprise will lead the team to discover things that are not being addressed currently. This understanding will help the Documenters in the domain selection process. The number of possible domains within a governmental enterprise can be very large. Resource and time constraints will not allow most enterprises to document every domain. Refining the many business activities and agencies of the government down to the fundamentals of how – in business terms – the enterprise achieves its various missions makes domain selection a manageable process.

Understanding the detail about the business needs that are captured within the Business Domains aids in determining scope, understanding the objectives, and directing the focus. The two most common ways to scope the Business Architecture effort are:

- *Functionally*: Allows the business, as a whole, to be divided into functional areas that can be explicitly documented to aid in consistency of the Business Architecture Blueprint detail.
- *Topically*: Allows the business to focus on a single subject and explore all impacts and touch points that the subject has across the enterprise.

    It is through the topical Business Domains that interoperability and cost reductions can become apparent, for it is within the topical business domains that the redundancies across functional areas are identified. Opportunities for collaboration across functional areas for consolidated solutions are also typically identified during the documentation of topical Business Domains.

A combination of functional and topical divisions will be required to fully illustrate the strategic needs of the enterprise. Regardless of the method chosen for dividing the enterprise into manageable pieces, consistency is important. Without it, duplication and interoperability issues can arise.

There are many approaches to modeling the business of the enterprise. A Business Domain Model might be citizen-centric if that is a mandate for the enterprise, or it might be functionally focused if cross-agency cooperation is a priority. The Federal Business Reference Model (BRM) is a good example of a functionally-focused business model. It organizes the federal government's business into four areas: services for citizens, mode of delivery, support of delivery of services, and management of government resources.

Another option is a model based on what some refer to as Pillars of Government or Communities of Practice. This model could list functional business domains such as Education and Transportation on the vertical axis with topical domains such as Human Resources, Citizens, and Payments as beams along the horizontal axis. This allows the Documenters to visualize all the points of impact, or touch-points, across the enterprise. The use of the pillar and beam concept allows an intersection as the beams pass through the pillars.

Another choice for a business model might be as simple as a spreadsheet listing of all business functional and topical domains within the enterprise. Samples of these Business Domain Models can be found in *Samples – Business Domain Model Samples*.

The creation of a business model is an instinctive and repetitive process. A conceptual understanding of governmental business can help to produce a comprehensive model. However, the creation of a business model begins with the best understanding at hand and changes whenever new information is available.

Though Business Domains selected for inclusion in the Business Domain Model may be domains common across government enterprises or unique to a specific enterprise, the process of identifying these domains typically follows the same basic steps:

- Gather data to develop a listing of lines of business and business functions (use budget documents or send a form for feedback)
- Analyze and compile feedback into a master list (probably an Excel spreadsheet)
- Identify logical groupings (functional and topical)
- Create a cross-functional matrix
- Create a model which best represents the focus of the enterprise as reflected in the Business Drivers (citizen centric, functional, etc.)

- Identify the intersections and areas that are common among the various agencies/departments of the organization.

Select Initial Business Domains for Documentation - As a first step, identify every Domain, providing the Domain Definition and Boundary (the first two sections of the Domain Template). This will establish an overview of the topic to be addressed and will identify possible overlaps between the Domains. Once Business Domains have been identified, the Documenters must prioritize the domains to determine which are the most crucial candidates for complete documentation. Documentation of Domains is typically completed in phases. This prioritization and selection process is necessary because the list of possible Domains within an enterprise is large. Fully documenting every domain within federal, state or local government could overwhelm even the most committed architecture team. Care should be taken to select a reasonable number of domains.

To reach the best balance between an all-inclusive architecture and one that can be realistically achieved, select domains that support the Business Drivers of the enterprise. Also keep in mind the needs of the stakeholders. To the extent possible, consider the future demands on the architecture so the details documented within the architecture can accommodate future changes and growth. Future iterations of the Business Architecture may focus on new areas of the enterprise, based on the business urgencies identified at that time, and can build on what is already documented.

Each organization must identify its own priorities regarding which domains should be the focus for further development. Business strategic elements and cross-functional goals provide vital information for determining the prioritization. Specific circumstances of each enterprise such as legislative mandates, federal regulation, budgetary constraints, competing resources, organizational readiness, pain points, and delivery timeframes will all be additional considerations as Advisors/Reviewers work to define a manageable number of Business Domains for their enterprise.

Business Strategic Elements - All governmental organizations have strategic elements that are documented in some manner. By reviewing and considering the existing documents, the architects, with assistance from Business Subject Matter Experts, can utilize the strategic planning of the enterprise in the Business Architecture Domain Selection Process.

Strategic Elements Documentation can include:

- State/Local Business Strategy Plan documents
- Agency Business Strategy Plan documents
- Mission, Vision and Goals
- Business Initiatives
- IT Strategy documents
- Value Statements
- State of the State Address
- Budget documents
- Interviews of key enterprise executives.

Gathering the recommended documentation may prove difficult in some cases, as only partial documentation may exist within an enterprise or access may not be granted to the existing documentation. In these cases, it is possible to derive business strategy from alternate sources. The objective is to gather strategic information from whatever sources are available. The goal is to develop a good picture of the

enterprise's strategic objectives, the business goals of the enterprise, and the services that they desire to provide or are mandated to provide.

In the absence of specific documentation, options include:

- Survey state agency leaders and other primary stakeholders
- Study trends in state and local government through journals, professional organizations and the Internet for issues that apply to the enterprise
- Review legislative mandates
- Ask IT employees who interact with the business side of government what they are being asked to provide and where their pain points are
- Look at strategic plans from other states for ideas and ask, "Do these apply to my enterprise?".

Cross-functional Selection Matrix - Cross-functional goals are important considerations in the selection process. Documenters can glean valuable insight by creating a matrix with the topical functions along the x-axis and the functional domains along the y-axis; the points of intersection will illustrate the cross-functional activities. For samples of cross-functional matrices, see *Samples – Federal Relationship Matrix.*

Identify/Define Business Architecture Perspectives – A perspective is simply a breakdown of the Domain into manageable pieces based on a specific viewpoint. Each Business Architecture Perspective provides a specific view of the Business Domain that deals with designated types of architecture information and components.

Each of the components documented will be further broken down into two classifications – baseline and target. It may be difficult to fully capture the baseline. This effort should be "fast" and "thin."

- Baseline, the "as is" or "current" state of the enterprise, indicates where the enterprise is today.
- Target, the "to be" or "proposed" state of the enterprise, depicts where the enterprise wants to be and/or what the enterprise is trying to achieve within a certain scope and timeframe.

The number of Business Architecture Perspectives and the view or focus of each Perspective is determined by each organization based upon its specific environment and circumstances. Table 2 provides a sampling of typical Business Architecture Perspectives.

Table 2. Potential Business Architecture Perspectives

Perspective	*Description*
Strategic Business Intent Who / Why *Organization and Motivation*	The components addressed within this Business Architecture Perspective define why and by whom business operations are performed. The manner in which the enterprise carries out its mission and the links from the business motivations and organization of the enterprise to the remaining Enterprise Architecture elements are identified within this Business Architecture Perspective.
Organizational Dynamics *Who* *Organization*	The components addressed within this perspective define the organization and organizational dynamic model that is most appropriate for fulfilling the strategic business intent.

Perspective	Description
Strategic Services *When / How* *Scheduling and Process*	This Business Architecture Perspective promotes understanding when and how the various business services are or will be conducted. Proper understanding of the Strategic Services involves two key points: • This Business Architecture Perspective simply addresses the descriptions of the business requirements that are or will be fulfilled through modernization. • The business model represents current thought on how exchanges should be logically grouped in the future. This representation will likely evolve as it modernizes and begins to reengineer key business services and support those functions
Strategic Information *What* *Data*	The focus of Strategic Information is on identifying and defining the information captured across the enterprise. Emphasis is placed on understanding what, in the form of informational assets, the enterprise cares about.
Strategic Infrastructure *Where* *Location*	The locations where business is performed and the logistics mechanisms used to perform strategic business activities are documented within the Strategic Infrastructure Perspective. Understanding where the state or local government conducts business, or plans to conduct business, aids in determining the types of services that can be supplied/distributed from a location. Ultimately the Strategic Infrastructure Perspective relates the logistics mechanisms that are used to perform strategic business activities to the business locations that perform those activities.

Once the Business Architecture Perspectives are determined within the enterprise, the same Perspectives are repeated across all Business Domains.

There is no template for the documentation of Business Architecture Perspectives. The set of Perspectives is defined once by each enterprise and serves as a classification of detail for each Domain.

Conduct Business Architecture Work Sessions

PROCESS OVERVIEW

The Business Architecture work sessions are intended to produce the documentation that initially populates the Architecture Blueprint. The Business Architecture is best documented by members of the business community. Ongoing Documenter meetings with the appropriate mix of business and technical Subject Matter Experts are required to document and maintain the vitality of the Domain's architecture blueprint. The first session will include:

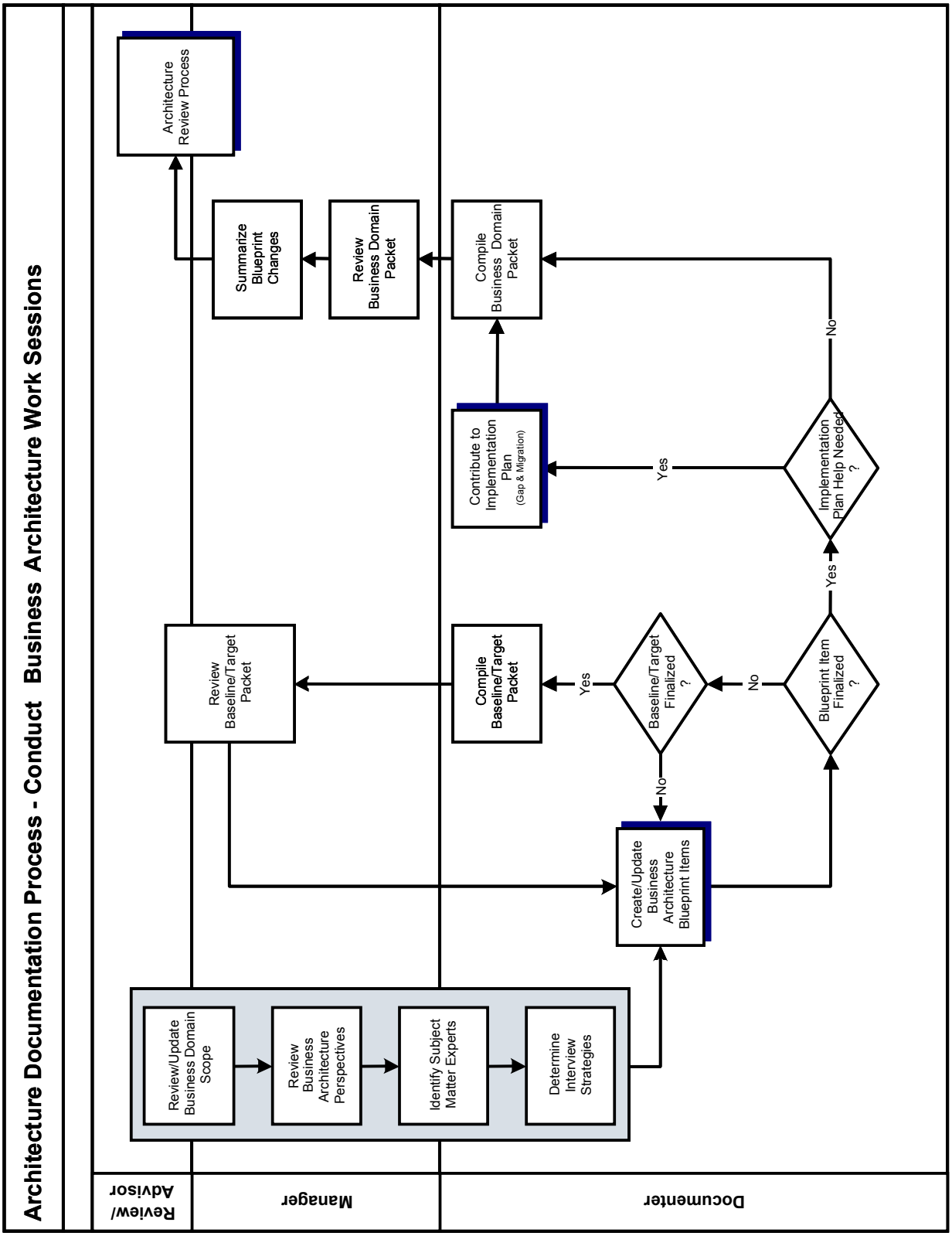
- Defining roles and responsibilities
- Reviewing architecture blueprint documentation requirements
- Determining expectations of on-going meetings.

After the first meeting, on-going working sessions are triggered from Architecture Lifecycle Processes including:

- The need to complete the Domain documentation
- Architecture Review Process

- Architecture Compliance Process
- Architecture Blueprint Vitality Process.

The creation of diagrams for the Business Architecture components provides a pictorial view for identification of the organization's business needs. Analyzing the various pieces within the enterprise facilitates the process of articulating the foundation of the Architecture. Individual components can be more easily defined and enable better communication of the business concepts. The relationships between various pieces can also be built into summary level views.


Architecture Documentation Process - Conduct Business Architecture Work Sessions
Reviewer/ Advisor
Manager
Documenter
Review/Update Business Domain Scope
Review Business Architecture Perspectives
Identify Subject Matter Experts
Determine Interview Strategies
Create/Update Business Architecture Blueprint Items
Blueprint Item Finalized ?
No
Yes
Implementation Plan Help Needed ?
Yes
No
Contribute to Implementation Plan (Gap & Migration)
Compile Business Domain Packet
Review Business Domain Packet
Summarize Blueprint Changes
Architecture Review Process
Baseline/Target Finalized ?
No
Yes
Compile Baseline/Target Packet
Review Baseline/Target Packet

PROCESS DETAIL

Review/Update Business Domain Scope - The initial definition of the Domain, determined during the Domain selection process, should be provided to the Documenters. The Documenters will update the basic definition as necessary and identify parameters for setting boundaries within the Business Architecture Domain. During this process, the scope of the individual efforts for further developing the business architecture components can be defined in greater detail. The Documenters/Authors are responsible for gathering all necessary information to complete the Domain documentation. Reference the sample Business Domain template for an example of the detail captured for each Domain (See *Business Domain Template*).

An important activity during the documentation/update of the Business Domain scope is the mapping of the Business Drivers that are significant to the Domain, along with indication of conflicts and the description of any conflict that exists.

Review Business Architecture Perspectives – For each Business Domain, the Documenter team is responsible for determining the level of detail that will be captured from each of the Business Architecture Perspectives (Who, What, When Where, Why and How or combinations of these, as determined by the organization). The set of Perspectives that will be utilized by the organization is defined as part of the Develop Business Architecture Framework process. The same set of Business Architecture Perspectives is considered for each Business Domain. The use of Business Architecture Perspectives allows simplification and organization of the Business Architecture documentation.

Identify Subject Matter Experts – Individuals who are experts in a segment of the business are determined. For the functional scope, identify the Subject Matter Experts for each of the Business Architecture Perspectives. Examples of Subject Matter Experts and their areas of expertise from the typical Business Architecture Perspectives could include, but are not limited to, the following:

- Strategic Business experts in:
  - *Strategic Elements*: Strategic direction, vision statements, goals, objectives, and policies
  - *Organizational Structure and Roles/Responsibilities*: Resource management reporting as well as cross-functional groups and informal reporting structures
  - *Business Function*: Main business activities that are conducted regardless of the business process to perform those activities.
- Strategic Services experts in
  - *Business Services*: Services conducted on behalf of external or internal customers, and the transactions that occur to support various business activities within this functional scope.
  - *Master Schedule*: The schedule upon which these services are conducted and any dependencies between these scheduled services.
- Strategic Information experts in:
  - *Strategic Information/Assets*: Assets that are vital to the day in and day out operations of this functional scope, including information that is required to help decision makers.
  - *Assets/Information Relationships*: The relationships between the various pieces of strategic information/assets. What is beneficial to understand as a group rather than individually? As decisions are made, what additional information would be beneficial to make an informed decision?

- Infrastructure experts in:
  - *Business Location*: The various channels by which the services and information within this business function scope are delivered.
  - *Business Logistics*: The various types of devices or transportation methods used to support these business locations.

Determine Interview Strategies – Interview meeting topics should be determined in one of the first working sessions. Interview questions should be designed to streamline the interview process and get the most information in minimum time.

Approaches for determining interview strategies can be based on:

- The business component/view to be documented. This format captures components such as strategic elements and organization charts.
- Functional topics. An example of a functional topic is "asset management." This format captures Strategic Transactions, Functional Breakdown, and Strategic Information.
- A specific Information Asset. An example of an information asset is "Customer." This also aids in capturing Strategic Transactions, Function Breakdown, and Strategic Information. Additionally, it can be used to capture the details concerning Application Areas and Infrastructure components.
- Business Cycle activities of a specific Information Asset. An example of this is documenting the various components around Inventory from ordering to consumption. Show the creation, utilization, and obsolescence of a given information asset. This can aid in capturing transaction architecture, application areas, and infrastructure components.
- Documenting the baseline activities followed directly with the target activities for a given topic. Often, the ability to stay on the same topic in a given timeframe assists in capturing the information around that topic, both where the business is today and where the business wants to be tomorrow, and can keep the creativity rolling without starting and stopping based on baseline and target. This can be done for both topical and functional domains.

Create/Update Business Architecture Blueprint Items – The Blueprint items include Business Architecture Component detail and process diagrams. . The sample Business Architecture Component template provides an example of the detail that is typically captured. A separate process model and narrative for this sub-process will provide greater detail (See *Create/Update Business Architecture Blueprint Items*)**.** When the Baseline or Target documentation is complete, a summary should be compiled and the Baseline or Target documentation should be submitted for review. The Reviewers can add valuable insight from an over-arching perspective.

Compile Baseline/Target Packet, Review Baseline/Target Packet – At the completion of Baseline, and again at the completion of the Target, a documentation packet should be complied and sent for review. This is beneficial to the documentation process as it allows feedback from the perspective of the Manager, Reviewers and Advisors at strategic points throughout the documentation process.

Contribute to Implementation Plan – After the Blueprint items have been finalized, Documenters will also contribute to the Implementation Plan if needed. Contributions include completing the detail for the Gap Components, performing a Gap Analysis, developing Migrations Strategies, and creating a summary of Gap and Migration results.

A copy of the Gap Component template, narrative for capturing the detail, and a sample template with completed Gap Component Blueprint detail can be found later in this section. (See *Gap Component Template* and *Blueprint Samples – Gap Component*).

Compile Business Domain Packet – A packet containing the completed Blueprint documentation will be compiled in preparation for formal review.

- If the Gap Analysis and Migration Strategies have been completed as a contribution to Implementation Planning, the detail that was compiled into the Gap & Migration Summary document will also be included in the Business Domain Packet. (For a sample of the Gap & Migration Summary, see *Gap & Migration Summary Format Sample*)

Review Business Architecture Domain Packet – The Business Architecture Manager will verify the contents of the Domain Packet and work with the Documenters to make modifications as necessary.

Summarize Blueprint Changes – After contents of the packet are verified, the Manager will summarize any changes that have been made to the Business Architecture Blueprint for tracking purposes and forward the packet to the reviewers for the formal Architecture Review Process.

Architecture Review Process – The governing bodies will review the Business Domain Packet for content and scope and either accept the Domain information into the architecture or reject the Domain information for reasons specified on the Domain template.

Business Domain Template

TEMPLATE OVERVIEW

The Business Domain Template provides a tool for documenting domain details in an electronic format. After the initial domain definition is completed and domains have been selected, the details of the domain are completed. The visual representation of the Business Domain Template, provided on the following page, is followed by the detailed description of its contents. The development of domains is a process that will evolve and change as information is gathered and documented.

It is anticipated that additional Business Domains may be identified during the lifecycle of the Business Architecture. Stakeholders are also encouraged to provide feedback and suggestions whenever it is apparent that the feedback will enhance the architecture.

Important items to keep in mind when determining the breakout of Domains are:

- Business Domains should not be too broad.

  In defining the scope of each business domain, it is important to keep in mind the Subject Matter Experts that will need to work together. Do the SMEs have similar:

  - responsibilities?
  - products and services they provide?
  - strategies and goals driving their efforts?

  Answers to these questions can help determine the division of Business Domains, as well as the level of documentation required for that domain.

- Business Domains should not be too narrow.

  Having Business Domains that are narrow in scope will cause the creation of many Domains, which in turn results in numerous documentation efforts that have high overheads in summarizations of baseline and target along with gap and migration strategy development.

- It is best to keep the number of Business Domains reasonable.

  The first scoping of the Business Domains may not be the permanent arrangement. The best Business Domain scope will surface naturally over time as the Architecture Blueprint is developed and used within your organization.

- Avoid spending excessive time determining terminology issues. Just as in metadata documentation, fine-tuning terminology can occupy a majority of the documentation time. Utilize the keywords and boundary statements to assist in identifying various terms and topics covered within the domain.

Business Domain

Definition			
Name			
Description			
Rationale			
Benefits			
Boundary			
Domain Type	☐ *Functional* ☐ *Topical*		
Boundary Scope Statement			
Associated Business architecture Perspectives			
Perspectives addressed within this Domain			
Related Enterprise Business Drivers			
Related Principles			
Reference #s, Statements or Links	*Conflict*	*Support / Conflict Detail*	
	☐		
	☐		
Related Best Practices			
Reference #s, Statements or Links	*Conflict*	*Support / Conflict Detail*	
	☐		
	☐		
Related Trends			
Reference #s, Statements or Links	*Conflict*	*Support / Conflict Detail*	
	☐		
	☐		
Keywords			
Keywords / Aliases			
Current Status			
Business Domain Status	☐ *In Development* ☐ *Under Review* ☐ *Accepted* ☐ *Rejected*		
Audit Trail			
Creation Date		*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

TEMPLATE DETAIL

Definition

Domain Name – The Business Domain team and/or the architecture review committee will determine the domain name.

Description – An appropriate description of the domain in a paragraph or two that provides sufficient clarity to the reader about the domain.

Rationale – A paragraph containing the reason or basis for this domain being included in the architecture.

Benefits – A paragraph or bulleted statements that provide the benefits associated with the Domain.

Boundary

Domain Type – Identify the type of domain, functional or topical. Examples of domain types:

- Functional Domains
  - Education
  - Health and Social Services
  - Justice and Public Protection
  - Resource and Economic Development
  - Transportation and Engineering
- Topical Domains
  - Customer
  - Location
  - Payments.

Boundary Scope Statement – The boundary scope statement provides parameters for identifying the boundaries for the domain. This section includes statements about what is included, as well as items that are related to, but excluded from, the domain. If excluded items are identified, it is beneficial to include a reference to the domain where information on those items can be found.

Associated Business Architecture Perspectives

Typically, the same perspectives are covered under each domain; however; your enterprise may choose to address only certain perspectives for a specific domain based on circumstances. In this area of the template, provide a list of the perspectives that are currently addressed within this domain

Related Enterprise Business Drivers

To minimize the amount of documentation required, general support of the business drivers is assumed. Therefore, not every Principle, Best Practice and Trend is specifically documented for each domain.

Principles, Best Practices and Industry Trends should be documented if:

- The driver is directly related to the domain (i.e. the reason for the domain or purpose of the domain is directly tied to the given driver).
- The driver will have a significant impact on the domain.
- There is a conflict between the driver and the domain.

Related Principles

Reference Numbers, Statements or Links: The overarching general rules that hold true across the enterprise architecture. The principles are developed and documented as Business Drivers at the most global level of the enterprise architecture.

Conflict*:* Verify that the development of the domain does not conflict with the established principles. This is a yes/no answer.

Support/Conflict Detail:

- For supported principle: Include details regarding the relationship between the domain and the principle
- For conflict: Include sufficient detail to describe the conflict.

Related Best Practices

Reference Numbers, Statements or Links: Best practices identify industry processes related to the implementation of the enterprise architecture that will assist in the maintenance and expansion of an adaptive enterprise architecture. They are based on experience and proven results. The best practices are documented as Business and Technology drivers and apply to the enterprise-wide concept of architecture.

Conflict: Verify that the development of the Domain does not conflict with the established best practices. This is a yes/no answer.

Support/Conflict Detail:

- For supported best practice: Include details regarding the relationship between the domain and the best practice
- For conflict: Include sufficient detail to describe the conflict.

Related Trends

Reference Numbers, Statements or Links: Marketplace, industry, technology trends have an effect on the deployment of information technology. Provide description of emerging trends to stimulate discussion regarding what is possible. Identifying these trends and having an awareness of their impact will allow IT decision makers to develop more informed, effective decisions. The trends are documented as Business and Technology drivers and apply to the enterprise-wide concept of architecture.

Conflict: Verify that the development of the Domain does not conflict with the established Industry and Technology Trends. This is a yes/no answer.

Support/Conflict Detail:

- For supported trend: Include details regarding the relationship between the domain and the trend
- For conflict: Include sufficient detail to describe the conflict.

Keywords

Keywords / Aliases - List any keywords and/or aliases that can be used to assist in searching the Architecture Blueprint for these Business Architecture Components. This information will be helpful for anyone that is looking for information regarding similar business elements.

Current Status

Document the status of the Business Domain documentation, indicating whether it is in development, under review, accepted, or rejected.

- *In Development* – The architecture team is currently drafting and/or reviewing the Business Domain content.
- *Under Review* – The architecture team has completed the Business Domain documentation and has submitted the documentation to the governing body for inclusion in the architecture.
- *Accepted* – The completed Business Domain documentation has been approved by the EA governing body and the content is an official part of the architecture. Once accepted into the architecture, the content is referred to as the Blueprint.
- *Rejected* – The Business Domain has been rejected by the governing body for reasons documented below in the Audit Trail section.

Audit Trail

Creation Date – Provide the date the domain was created.

Created By – List all individuals and their titles that helped in the creation of this Business Domain.

Date Accepted/Rejected – Provide the date the Business Domain was accepted into the architecture or rejected.

Reason for Rejection – If the Business Domain was rejected, document the reason for the rejection.

Last Date Reviewed – Document the most recent date the Business Domain was taken through the Architecture Vitality Process.

Last Date Updated – Document the most recent date at which any item in the Business Domain documentation was changed.

Reason for Update – Document the reason for the update to the Business Domain. This information should be a detailed description of the change, which can be used for future reference.

Create/Update Business Architecture Blueprint Items

PROCESS OVERVIEW

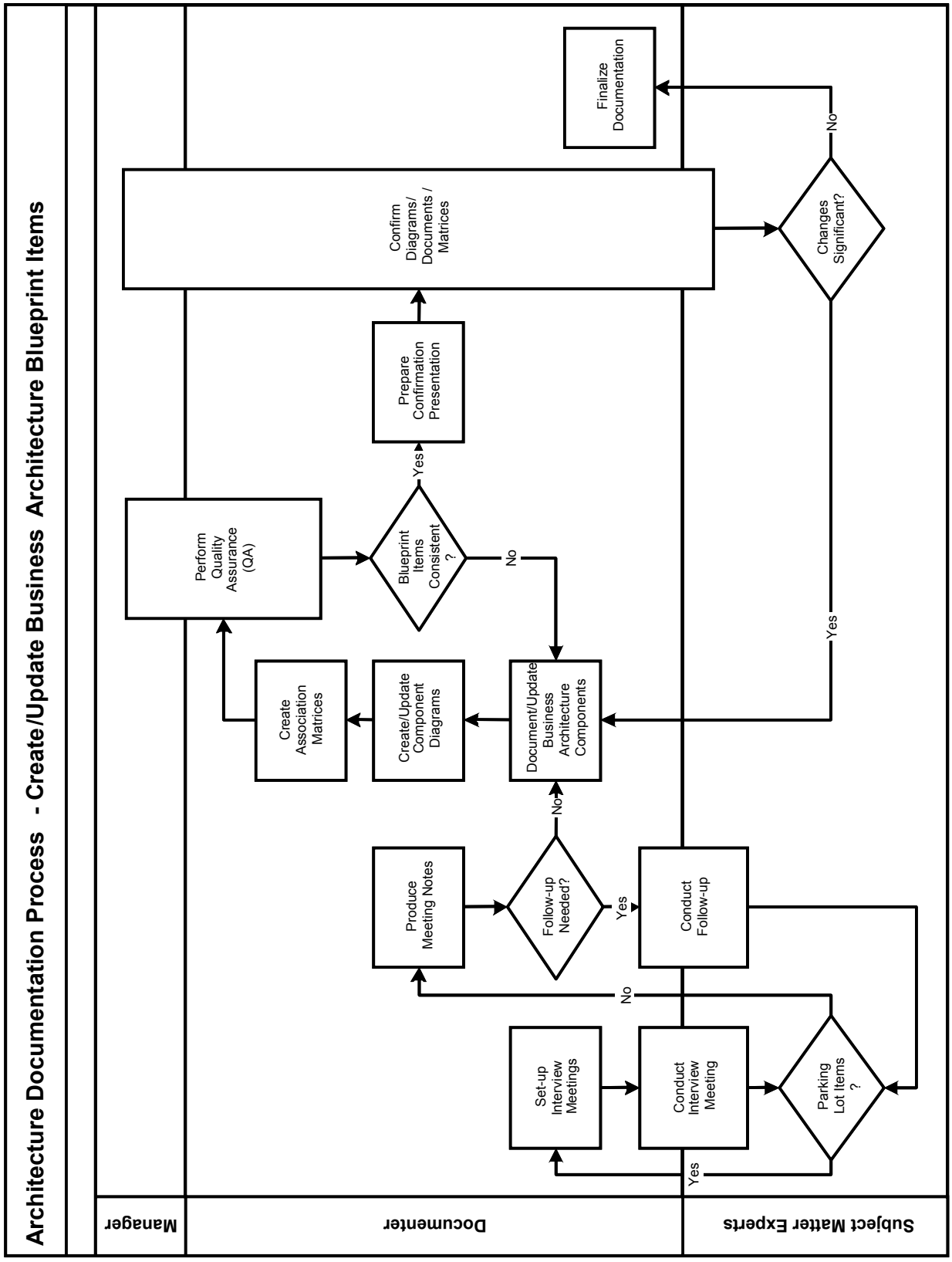
The Business Architecture Blueprint items consist of the Business Architecture Components and the diagrams that illustrate the various components and their relationships. Business Architecture Components refer to the individual elements that are documented as part of the Business Architecture Blueprint. Business Architecture Components specifically identify what information, services, location/logistics, organizational roles/responsibilities, and strategies will be used for implementation of the Business Domain.

Business Architecture Components are identified during the Business Architecture interview process and documented within each of the Business Architecture Perspectives as appropriate. The Business Domain team members, along with the Subject Matter Experts, determine the information to be documented as Business Architecture Components, and which Business Architecture Perspective is most applicable. For example, the business locations, and communication modes available from those locations, would be components documented within the Strategic Infrastructure Perspective. Within the documentation, references that identify relationships to other Business Architecture Components are also documented. Business Architecture components will cover items that answer the following example questions:

- What does the business care about? Components address the various assets of the business.
- How is business conducted? Components address the various functions of the business.

- Where are the locations critical to the business? Components address the mapping of the locations and communication modes available to/from those locations.
- Who affects or is affected by any given piece of the business? Components address the various roles and responsibilities and who fulfills those duties.
- When does something happen? Components address the various scheduled and unscheduled business events that affect the delivery of the services.
- Why is business done this way? Components address the policies, procedures, strategies and motivations that impact the decision making for the business.

This process, which results in defining/updating the Business Architecture Blueprint items, collects, organizes and documents a large volume of detail about the governmental organization's business. The detail is collected via interviews with a mix of Subject Matter Experts, from executives through line managers. Getting good results from interviews of key staff requires a team composed of individuals that are experienced, have knowledge of their business area, and are committed to the enterprise architecture process.


Architecture Documentation Process - Create/Update Business Architecture Blueprint Items
Manager
Documenter
Subject Matter Experts
Finalize Documentation
Confirm Diagrams/ Documents / Matrices
Changes Significant?
No
Yes
Prepare Confirmation Presentation
Perform Quality Assurance (QA)
Blueprint Items Consistent ?
Yes
No
Create Association Matrices
Create/Update Component Diagrams
Document/Update Business Architecture Components
Produce Meeting Notes
Follow-up Needed?
No
Yes
Conduct Follow-up
Set-up Interview Meetings
Conduct Interview Meeting
Parking Lot Items ?
No
Yes

PROCESS DETAIL

Set-up Interview Meetings - Once the subject matter experts have been identified and the interview strategy has been determined, the interview meetings can be scheduled. Allow at least two hours per session. No more than two sessions should be set up in the same day to allow Subject Matter Experts who attend both sessions to have a break from this style of overarching thinking.

Conduct Interview Meetings – Meetings are typically organized around a specific topic within the subject area scope. The topics were determined during the interview strategy session, which usually takes place in one of the first working sessions. At times, new topics will surface during the interviews. These should be aligned to the original strategy to assure that all aspects of this topic are addressed in the interviews. It is best to assign each interviewer a specific Business Perspective for which they are responsible.

Although everyone will be involved in the interviews from a general view, it helps to give each interviewer an area of focus based on the Business Perspectives to be covered for the given Domain. Before the interviews, each interviewer should plan questions based on their assigned perspective. This will help to ensure the coverage of all aspects. It is also helpful to have a different individual assigned as a scribe. This will allow the interviewers to focus their attention primarily on the interviewing process and less on taking notes.

Produce Meeting Notes – Knowledge of who participated in providing the subject matter is very useful. During the interview sessions, Subject Matter Experts or various architecture participants may be asked to follow up with action items or to share documentation and research on specific items. For this reason, notes of these meetings should be taken, reproduced and distributed as with any other formal meeting. Parking lot issues or unresolved items often result during interview meetings. These items need to be compiled, returned to the person interviewed for feedback, and documented in the interview strategies or the summary documentation.

Conduct Follow-up – Following interview meetings with subject matter experts, some items may require resolution or additional action. These activities may include, but are not limited to, the following:

- Changes to Interview Strategy: Based on interview feedback, the style and/or strategy of subject matter expert interviews may be changed.
- Resolution of Items: Dissention or ambiguity may necessitate resolution and/or direction from Architecture Subject Matter Experts, Executives, Manager or Reviewers.
- Clarification: The Documenters may need additional information on a topic.
- Parking Lot Items: Items that are currently out of the defined scope, but have been identified as potentially requiring future action, are documented for further research and resolution.

Document/Update Business Architecture Components – The Documenters capture detail about each of the Business Architecture Components such as keywords, critical references, stakeholders and applicable standards. The Business Architecture Component Template is a form that can be used for documenting this detail. (See *Business Architecture Component Template).* Note that although the components may be used on multiple diagrams and matrices, the detail for each component is documented only once.

Create/Update Component Diagrams - The documenters will place Business Architecture Components on various diagrams to show the flows and relationships. These diagrams may include but are not limited to:

- IDEF activity models
- Workflow models
- Activity tree models
- UML models
- Use case models
- Class models
- State diagrams
- Node connectivity diagrams.

Create Association Matrices – After the modeling/ documentation is drafted, associations between the business architecture components can be created. Coordination with the other modelers/documenters should occur so that all business components for a specific Business Domain are included in the matrices. The various perspectives should be reviewed to make certain that nothing is missing or incorrectly represented.

Examples include:

- Strategic Elements that have no corresponding business plan
- Business functions that do not support a Strategic Element
- Transactions that have no association to Strategic Information
- Strategic Information that has no association with Business Functions.

Perform Quality Assurance (QA) – The various Business Architecture documents, models, and matrices require verification by the architecture team prior to confirming them with the Subject Matter Experts. This quality assurance step allows the team to verify that the various business components are utilizing the same glossary of terms and that the team's understanding of the various components of the business architecture is the same.

Prepare Confirmation Presentation – The Documenters will compile the information from the meeting notes, the documented components and associations, and the quality assurance check. The information will be utilized to confirm the accuracy of the information captured.

Confirm Diagrams/Documents/Matrices – Once the architecture team has verified consistency in how they are defining and representing the various business components, the team will confirm the models/documents/matrices with Business and Technical Subject Matter Experts. This should be an interactive session where modifications and enhancements are noted. Some of the changes can occur in the session while others will take more time and will be conducted in "pick-ups" after the session. If the changes to the models/documentation/ matrices take place outside the session, an electronic copy of the changes should be sent out for approval. If the changes were significant, the potential exists to call another meeting to confirm those changes.

Finalize Documentation – When the component detail has been confirmed, update the status and audit trail detail. The final action is to submit all Business Architecture Component detail for inclusion in the Business Architecture documentation.

Business Architecture Component Template

TEMPLATE OVERVIEW

Business Architecture Components include the definition and gap identification for specific business components. The Documenters, along with Subject Matter Experts, determine the detail applicability to the overall architecture effort that will be included in these components. Each Business Architecture Component reviewed, whether accepted or rejected, will be documented using this Business Architecture Component Template.

The Business Architecture Component Template provides an instrument for documenting the Business Architecture Component details in an electronic format. The visual representation of the Business Architecture Component Template, provided on the following page, is followed by a detailed description of the contents to be captured.

Important items to keep in mind when determining the Business Architecture Component include:

- The sections included in the Business Architecture Component template identify some of the major pieces of information that can be gathered for a Business Architecture Component.

  As an organization sets up their business architecture framework, they will want to determine the pieces of information that are of most value to their overall EA effort. The level of detail documented within the Business Architecture Blueprint will also need to be maintained as part of the vitality process..

- Industry trend and best practice scans are helpful in capturing information regarding existing Business Architecture Components within a given Business Domain.

- There is more than one way to determine the level of detail to be documented as Business Architecture Components.

  Documenters preferring bottom-up analysis will begin by capturing a list of components from which they determine the level of documentation detail needed to best communicate the needs of the Business Domain.

  Those preferring top-down analysis will determine and document the overall Business Domain concepts or topics first, and proceed to identify and document components that address each topic.

- Documentation of Business Architecture Components within a Business Domain can become an area for boundary debate.

  When components span functional areas, a question can arise as to which documentation team is responsible for documenting which components. A decision should be made as to whether the component should be documented under multiple business domains, or all Subject Matter Experts should come together to document the component once under a specific Business Domain.

Business Architecture Component

Definition	
Name	
Description	
Rationale	
Benefits	
Component Classification	
Classification	☐ *Baseline* ☐ *Target*
Associated Business Architecture Perspective	
Business Architecture Perspective	
Keywords	
Keywords / Aliases	
Business Architecture component Type	
Component Type	
Critical References	
Related Business Architecture Components	

Business Architecture Component	*Relationship*	*Business Architecture Component*	*Relationship*

Standards Organizations			
Name		*Website*	
Contact Information			
Government Bodies			
Name		*Website*	
Contact Information			
Stakeholders/Roles			
Stakeholders			
Roles			
Reason for Stake			
GAP Component			
GAP Component Names			

CURRENT STATUS			
Business Architecture Component Status	☐ *In Development* ☐ *Under Review* ☐ *Accepted* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date		*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

TEMPLATE DETAIL

Definition

Name – Provide the name for the Business Architecture Component.

Description – Document the description of the Business Architecture Component in a paragraph or two that provides sufficient clarity to the reader about the component.

Rationale – Document a paragraph or two containing the reason or basis for this Business Architecture Component being included within the architecture.

Benefits – Document a paragraph or bulleted statements that provide the benefits associated with the Business Architecture Component.

Component Classification

Classification - Provide the classification for the Business Architecture Component:

- *Baseline:* The "as is" or "current" state of the component within the enterprise. Baseline indicates the component exists within the enterprise today.
- *Target:* The "to be" or "proposed" state of the component within the enterprise. Target indicates the component should be included or added to the enterprise within a certain scope and timeframe.

Associated Business Architecture Perspective

Business Architecture Perspective Name – Provide the name of the Business Architecture Perspective for which this Business Architecture Component is developed.

The following are sample Business Architecture Perspectives:

- Strategic Business
- Strategic Services
- Strategic Information
- Strategic Infrastructure.

Keywords

Keywords / Aliases - List any keywords and/or aliases that can be used to assist in searching the Architecture Blueprint for these Business Architecture Components. This information will be helpful for anyone that is looking for information on similar business elements.

Business Architecture Component Type

Component Type - This allows the type of information, and associated type of deliverables captured in the template, to be explicitly identified. Table 3 provides a list of the available component types, based on the sample Business Architecture Perspectives:

Table 3. Business Architecture Component Types

Primary BA Perspective	*Business Architecture Component Types*
Strategic Business	Strategic Direction, Drivers and Goals
	Organization – Roles and Responsibilities
	Business Objectives and Plans
Strategic Services	Significant Business Events
	Significant Business Cycles
	Business Function
Strategic Information	Strategic Information
Strategic Infrastructure	Strategic Business Locations
	Business Logistics

Critical References

Related Business Architecture Components – List all related Business Architecture Components and their relationship to this specific component. The information provided here is valuable for creating matrices that show relationships between the various components of the Business Architecture.

Standards Organizations – List all Standards Organizations that supply standards associated with this Business Architecture Component. Provide contact information for each organization, as well as URLs for websites, if available.

Government Bodies – List all Government Bodies that provide policies and/or mandates associated with this Business Architecture Component. Provide contact information for each Government Body, as well as URLs for websites, if available.

These are research references only, and are used in identifying items that may need to be escalated to review during gap analysis and migration strategies.

Stakeholder Information

To identify stakeholders, use questions such as:

- Who is directly impacted by this component or a change to this component?
- Who may have to change the way they do business?
- Who may benefit financially?

Stakeholders – Provide a list of stakeholders for this Business Architecture Component. Stakeholders are those who are affected by or will have an effect on the Business Architecture Component. If stakeholder title is not known, provide a description of the role the person or group performs in the Roles section. Stakeholders are typically agencies, departments, etc.

Roles – This section provides a place to present the roles and/or responsibilities for this Business Architecture Component. This is especially helpful when a title for the stakeholder is not known. Roles ensure the accountability for all Business Architecture Components and ensure that all stakes in the component are documented when interviewing the Subject Matter Experts. Examples of roles could include Project Manager or Documenter, etc.

Roles can also show IT stakeholders that utilize this information, resulting in better service and closer alignment to the business needs.

Reason for Stake – This optional section provides a place to note the reason that the stakeholder or role has a vested interest in this Business Architecture Component. This is helpful when the reason is not apparent or there are specific circumstances that should be noted. Consideration should be given to the interest of the stakeholder and not only to management, for often the same question posed to these groups results in different responses. The information presented here should take the opportunity to clarify the relationship of the stakeholders.

Gap Component

This section is documented for any Business Architecture Component that will be impacted by the move from baseline to target. If nothing will change, the gap statement can just say "no gap."

Gap Component Names – As gaps are identified, list the names for Gap Components for this Business Architecture Component. The Gap Component Template will be used to document the gaps that exist between this Business Architecture Component and other Business Architecture Components, as well as Impact Statements and Migration Strategies. The gap can be documented from the following perspectives:

- From the perspective of the baseline Business Architecture Component that is being updated, replaced or removed when migrating to the target.
- From the perspective of the target Business Architecture Component that is being added to, replaced or enhanced when migrating from the existing baseline.

Current Status

Document the status of the Business Architecture Component, indicating whether the documentation for the component is in development, under review, accepted, or rejected.

- *In Development* – The architecture team is currently drafting and/or reviewing the Business Architecture Component content.
- *Under Review* –The architecture team has completed the Business Architecture Component documentation and has submitted the documentation to the governing body for inclusion in the architecture.
- *Accepted* – The completed Business Architecture Component documentation has been approved by the EA governing body and the content is an official part of the architecture. Once accepted into the architecture, the content is referred to as the Blueprint
- *Rejected* – The Business Architecture Component has been rejected by the governing body for reasons documented in the Audit Trail section.

Audit Trail

Creation Date – Provide the date the Business Architecture Component was created.

Created By – List all individuals and their titles that helped in the creation of this Business Architecture Component.

Date Accepted/Rejected – Provide the date the Business Architecture Component was accepted into the architecture or rejected.

Reason for Rejection – If the Business Architecture Component was rejected, document the reason for the rejection.

Last Date Reviewed – Document the most recent date the Business Architecture Component was taken through the Architecture Vitality Process.

Last Date Updated – Document the most recent date that any item in the Business Architecture Component documentation was changed.

Reason for Update – Document the reason for the update to the Business Architecture Component.

Gap Component Template

TEMPLATE OVERVIEW

Once the baseline and/or target detail has been documented for any given Business Architecture Component, the gaps that are identified will be documented utilizing the Gap Component Template. The documentation of these gaps, along with the migration strategies for alleviating these gaps, provides the roadmap for achieving the target architecture. The Architecture Team, along with the Subject Matter Experts, determines the information applicable to the overall gap documentation. Each gap that is reviewed, whether it is accepted or rejected, will be documented using this Gap Component Template.

The Gap Component Template provides an instrument for documenting architecture gap details in an electronic format. The visual representation of the Gap Component Template is followed by a detailed description of the contents to be captured.

Important items to keep in mind when determining the various Gap Components are:

- A Gap Component can be documented to cover more than one business component.

  For example an organization could have a communication gap (various divisions or teams are having problems understanding the needs of the other groups because of terminology differences). A Gap Component could be created to identify the lack of a common enterprise vocabulary of terms. This Gap Component may be identified as having a relationship to many Business Architecture Components from functions, to organizations, to impeding a strategy/goal.

- Not all identified gaps need to be mitigated and resolved.

  Priority of the gaps will be accomplished during implementation planning. It is a good practice to document the gaps as they are identified. This helps everyone to understand that the gap has been identified. The migration strategies may include the decision not to address the gap, along with the reason for the decision..

- Documentation of gaps can identify areas where control points for security, regulatory compliance, and/or privacy need to be increased or fortified.

  Once documented, the risk to the enterprise can be assessed and prioritization for mitigating the gaps can be determined.

Gap Component Template

Definition	
Name	
Gap Statement / Description	
Rationale	

Gap Classification	
Related Architecture Blueprint	☐ *Business Architecture* ☐ *Information Architecture* ☐ *Technology Architecture*
Architecture Level	☐ *Component* ☐ *Discipline/Perspective* ☐ *Domain/Subject Area* ☐ *Other* _____
Gap Types	☐ *New* ☐ *Over-utilized* ☐ *Obsolete* ☐ *Change* ☐ *Under-utilized* *Replace by:* _____

Impact Position					
Area Affected	*Level of Impact*				*Position Statement*
	High	*Medium*	*Low*	*None*	
Business Impact	☐	☐	☐	☐	
Information Impact	☐	☐	☐	☐	
Technology Impact	☐	☐	☐	☐	

Related Gap Component Detail

Baseline Component Detail

Component Name	*Component Type*

Target Component Detail

Component Name	*Component Type*

Keywords	
Keywords / Aliases	

STAKEHOLDER INFORMATION			
Stakeholders			
Roles			
Reason for Stake			
MIGRATION INFORMATION			
Migration Strategies			
CURRENT STATUS			
Gap Component Status	☐ *In Development* ☐ *Under Review* ☐ *Accepted* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date		*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

TEMPLATE DETAIL

Definition

The definition section provides a brief synopsis of the Gap Component:

Name – Provide the name for the identified Architecture Gap.

Gap Statement/Description – Document the description of the Architecture Gap in a paragraph or two that provides sufficient clarity to the reader about the component.

Rationale – Document a paragraph or two containing the reason or basis for this Architecture Gap being included within the architecture. (Optional)

Gap Component Classification

The classification section provides more detail regarding the categorization for the identified Gap:

Related Architecture Blueprint – Select the architecture blueprint where the gap exists.

- Business Architecture
- Information Architecture
- Technology Architecture

Architecture Level – Select the level at which the gap was identified

Component – such as:

- Business Architecture - Business Architecture Component
- Information Architecture - Process Component or Information Meta Component
- Technology Architecture - Product Component or Compliance Component.

Discipline/Perspective - such as:

- Business Architecture Perspective
- Technology Architecture Discipline.

Domain/Subject Area – such as:

- Business Architecture Domain
- Technology Architecture Domain
- Information Architecture Subject Area

Other: if selected, specify.

Gap Types – List all applicable values that describe the nature of the identified gap:

- *New:* Items that were identified in the target blueprint, but did not exist in the baseline blueprint, reflect new business or technology components. Customer needs, legislative mandates, and technology changes are examples of drivers that cause the creation of these items.
- *Change:* Adapting components to accommodate changing business requirements. Improvement efforts are a consistent source of change and enable the organization to streamline operations, increase efficiency, reduce waste, and save money.
- *Under-utilized:* Identification of components that are not realizing full potential and can provide insight into efficiency improvements.

- *Over-utilized:* The concept of diminishing returns helps identify those components that are being tasked past the point for which originally slated.
- *Obsolete:* When a baseline component does not appear in the target architecture blueprint, it is no longer a valid component for the organization. Obsolete items may be replaced with new components or removed altogether unless identified in another Business Architecture Component. If selected, a replacement component must be specified. If the component will be removed, specify "none".

Impact Position

This section describes the impact the Gap has on the business, information and/or technology.

Level of Impact:

- *High:* Gap has a significant impact on the ability of the business to operate effectively. In these cases, significant resources are being allocated to minimize the effects of this gap on operations.
- *Medium:* Gap has an impact on daily operations; however, work-arounds are minimizing the effects of this gap on operations.
- *Low:* Gap has a minor impact. Daily operations are not affected.
- *None:* Gap has no impact on business operations.

Position Statement - Provide a position statement regarding the impact of the gap on the business, information and/or technology. When developing the impact position statement, consider impacts on the following items:

- Overall Enterprise Architecture
- Physical Environment
- Business Community
- Technical Community.

Related Gap Component Detail

This section lists the specific components involved in the identified Architecture Gap Component. The following information is captured for both the baseline and target components.

Additional lines may be added if needed.

Component Name – Provide the name for the impacted component.

Component Type – Specify the associated component type. The type will differ depending on whether the component is from the Business Architecture, Information Architecture or the Technology Architecture.

The Business Architecture includes items like the examples listed in Table 4. The component types listed in the table are based on the sample Business Architecture Perspectives.

Table 4. Component Type by Business Architecture Perspective

Associated BA Perspective	*Business Architecture Component Types*
Strategic Business	Strategic Direction, Drivers and Goals
	Organization – Roles and Responsibilities
	Business Objectives and Plans
Strategic Services	Significant Business Events
	Significant Business Cycles
	Business Function
Strategic Information	Strategic Information
Strategic Infrastructure	Strategic Business Locations
	Business Logistics

The Information Architecture consists of the following component types:

- Process Components
- Information Meta Components.

The Technology Architecture consists of the following component types:

- Product Components
- Compliance Components

Keywords

Keywords / Aliases - List any keywords and/or aliases that can be used to assist in searching the Blueprint for these Gap Components. This information will be helpful for anyone that is looking for information on similar elements.

Stakeholder Information

To identify stakeholders, use questions such as:

- Who is directly impacted by this component or a change to this component?
- Who may have to change the way they do business?
- Who may benefit financially?

Stakeholders – Provide a list of stakeholders for the Gap Component. Stakeholders are those who are affected by or will have an effect on the gap. If stakeholder title is not known, complete the Roles section. Stakeholders are typically agencies, departments, etc.

Roles – Provides the roles and/or responsibilities for this Gap Component. This is especially helpful when a title for the stakeholder is not known. Roles ensure the accountability for all Business and Technical components and ensure that all stakes in the component are documented when interviewing the Subject Matter Experts. Examples of roles could include Project Manager or Documenter, etc.

Roles can also show IT stakeholders who utilize this information in order to provide better service and establish closer alignment with the business needs.

Reason for Stake – This optional section provides a place to specify the reason that the stakeholder or role has a vested interest in this Gap Component, especially if the reason is not apparent or there are specific circumstances that should be noted. Consideration should be given to the interest of the stakeholder and not only to management, for often the same question posed to these groups results in different responses. The information presented here should clarify the relationship of the stakeholders.

Migration Information

This section is documented for any Business, Information and/or Technology Architecture component that will be impacted by the migration.

Migration Strategies – List the alternatives available for migration or links to reference Migration Strategy documents .

These strategies should identify the following items, as applicable:

For Business: List the alternatives available for migration from the baseline to target.

- Human capital required to migrate
- Human capital being migrated
- Physical capital required to migrate
- Physical capital being migrated
- Training
- Impacts on existing solutions
- Considerations for conversion.

For Technology - Document the migration requirements for:

- Existing Product Components classified as emerging that are moving to the classification of current
- Existing Product Components classified as current that are moving to either twilight or sunset.

These strategies should identify the following items, as applicable:

- Existing user base and technical staff
- Training for existing user base
- Training for existing technical staff
- Impacts on existing technology areas
- Considerations for conversion
- Recommendations for the technology area in:
- New development
- Modifications (corrections & enhancements)
- Possibilities for user-base expansion (reuse).

Current Status

Document the status of the Gap Component, indicating whether the component is in development, under review, accepted, or rejected.

- *In Development* – The architecture team is currently drafting and/or reviewing the Gap Component content.

- *Under Review* –The architecture team has completed the Gap Component documentation and has submitted the documentation to the governing body for inclusion in the architecture.
- *Accepted* – The completed Gap Component documentation has been approved by the EA governing body and the content is an official part of the architecture. Once accepted into the architecture, the content is referred to as the Blueprint.
- *Rejected* – The Gap Component has been rejected by the governing body for reasons documented in the Audit Trail section.

Audit Trail

Creation Date – Provide the date the Gap Component was created.

Created By – List all individuals and their titles that helped in the creation of this Gap Component.

Date Accepted/Rejected – Provide the date the Gap Component was accepted into the architecture or rejected.

Reason for Rejection – If the Gap Component was rejected, document the reason for the rejection.

Last Date Reviewed – Document the most recent date the Gap Component was taken through the Architecture Blueprint Vitality Process.

Last Date Updated – Document the most recent date that any item in the Gap Component was changed.

Reason for Update – Document the reason for the update to the Gap Component.

SAMPLES

Business Architecture Blueprint Samples – Set 1

NASCIO

Business Domain

DEFINITION	
Name	Transportation (Business Domain)
Description	Improve the efficiency and effectiveness of projects within the Department of Transportation Information Systems division.
Rationale	Delivering solutions to meet the state's transportation system needs is a complex task, involving many people across numerous business units. The business units have adapted their practices based on the characteristics of their environment and the resources – both tools and people - available to meet needs. This has led to the development of processes and tools that do not necessarily correspond with those used at headquarters and/or other districts.
Benefits	• Documented current transportation project and program life cycle processes • A single point of reference for how the State Transportation Improvement Program (STIP) is created • Consistent and accurate reporting of the baseline business practices and processes related to the creation and development of transportation projects, as well as the program and maintenance of the transportation system, available in one official database • A list of business units and roles responsible for the activities related to the transportation project life cycle • Process information that is available in a common format to everyone
BOUNDARY	
Domain Type	☒ Functional ☐ Topical
Boundary Scope Statement	This domain is limited to those activities directly related to identifying transportation system needs, developing a transportation project and developing a statewide transportation program (STIP).
ASSOCIATED BUSINESS ARCHITECTURE PERSPECTIVE	
Perspectives addressed under this Domain	Strategic Business Strategic Transaction Strategic Information

RELATED ENTERPRISE BUSINESS DRIVERS		
Related Principles		
Reference #s, Statements or Links	*Conflict*	*Support / Conflict Detail*
Coordinate with other organizations in developing land-use policies.	☐	The coordination regarding land-use policies is essential to the Transportation Project domain.
Honor the Highway and Transportation Commission's commitment to deliver the transportation program. • Complete projects on time and within budget and work to deliver the transportation program within budget. • Develop and implement a project delivery process that is faster and capable of handling a larger program. • Structure the contract and timing of the award to facilitate the earliest completion and least disruption to the public.	☐	Creation of this domain is a direct result of the Highway and Transportation Commission's commitment to deliver the transportation program
Manage the state's resources to fund transportation priorities. • Increase the ability to fund current transportation priorities while providing adequate flexibility to address emerging needs. • Maximize the use of all resources. • Identify additional funding sources. • Retain existing revenue streams and identify additional funds.	☐	The creation of this domain supports this principle directly.
Provide a safe transportation system.	☐	The creation of this domain supports this principle directly.

Related Best Practices		
Reference #s, Statements or Links	*Conflict*	*Support / Conflict Detail*
• Providing standard methodology for managing projects. • Having responsibility for process and project reporting and tracking. • Ensuring similar projects are executed in a similar way. • Having funding and information needed to speed up or slow down project delivery. • Providing a process for resource allocation and capacity management.	☐	This best practice is critical to the successful implementation of the Transportation Program
• Strategic leadership, including strategic planning and implementation, public and private partnerships, performance measurement and accountability • Program delivery, including funding and finance, workforce retooling, environmental streamlining and stewardship and internal organizational structure • Systems operations, including congestion and incident management, as well as operations adjustments for security and safety	☐	Directly affects the Transportation Project domain and its program delivery
Benefits of transportation coordination; range of programs and potential players, mechanisms states are using to create effective coordinating bodies.	☐	Directly affects the Transportation Project domain
Related Trends		
Reference #s, Statements or Links	*Conflict*	*Support / Conflict Detail*
Some successful partnerships that State Councils have had with the Department of Transportation.	☐	Directly supported by this domain
Improving and preserving existing facilities; renewal in the midst of traffic; increased federal aid not likely; alternate fuel vehicles will affect tax collection; rising traffic congestion; labor and skill shortages (DOT vacancies); public global warming concerns; environmental opposition for even modest projects.	☐	Directly supported by this domain

KEYWORDS			
Keywords/Aliases	FTIP, Transportation Program		
CURRENT STATUS			
Business Domain Status	☒ *In Development* ☐ *Under Review* ☐ *Accepted* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	3/30/04	*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update	New Domain		

Business Architecture Component

Definition	
Name	Build Public Trust (Business Architecture Component)
Description	One of the 3 strategic element found in the strategic plan
Rationale	Supports the organization's mission
Benefits	• Listen and analyze what others are asking the transportation department to do. • Communicate timely, accurate and consistent information to transportation partners, elected officials and the general public • Provide a tool that captures all information in a central location which identifies processes, data definitions, transactions and allows for reports to be produced in a timely manner

Component Classification	
Classification	☒ *Baseline* ☒ *Target*

Associated Business Architecture Perspective	
Business Architecture Perspective	Strategic Business

Keywords	
Keywords / Aliases	First and Best, Build Public Trust

Business Architecture Component Type	
Component Type	Strategic Direction, Drivers and Goals

Critical References

Related Business Components

Business Architecture Component	*Relationship*	*Business Architecture Component*	*Relationship*
Be the first and best source of information about the organization	Strategy to Strategy		
Business plan FY 2003-2008	Strategy to Strategy		
Demonstrate responsible use of taxpayers money	Strategy to Strategy		
Deliver Transportation Project	Strategy to Function		
Identify Transportation Needs	Strategy to Function		
Track Transportation Program	Strategy to Function		

Standards Organizations

Name		*Website*	
Contact Information			

Government Bodies			
Name		*Website*	
Contact Information			
STAKEHOLDERS/ROLES			
Stakeholders	Budget, Department of Transportation		
Roles	Information Coordinator, Project Managers, Elected Officials, Transportation Partners		
Reason for Stake			
GAP COMPONENT			
GAP Component Names	Terminology and Definitions		
CURRENT STATUS			
Business Architecture Component Status	☒ *In Development* ☐ *Under Review* ☐ *Accepted* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date		*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Reviewed	2/25/03	*Last Date Updated*	
Reason for Update	Annual Review of Strategic Plan identified shift in focus		

Gap Component Template

DEFINITION	
Name	Terminology and Definitions (Gap Component)
Gap Statement / Description	"Terms" are being used inconsistently across the Department of Transportation. Requests for information are not producing correct or usable results because the requester is not using the same language as the functional unit providing the response. Also, reports are being produced containing information that cannot be understood or interpreted by the recipients. Explaining the report's content is ineffective because the report's producer is using terminology differently than the report's recipient.
Rationale	• A clearly defined set of common business terms will facilitate the complex communication process within the Department of Transportation. • Employees at different physical locations and within different functional units will be able to speak the same language, resulting in greater understanding across the organization. • Employees will be able to clarify, by asking the right questions, exactly what information they are being asked to provide. • Employees will be able to derive the same answer for the same question, or at least determine that they do not have access to the information being sought. • The Department of Transportation's stakeholders will benefit by receiving more accurate information about the work that is being done by the Department of Transportation.
GAP CLASSIFICATION	
Related Architecture Blueprint	☒ *Business Architecture* ☐ *Information Architecture* ☐ *Technology Architecture*
Architecture Level	☐ *Component* ☐ *Discipline/Perspective* ☒ *Domain/Subject Area* ☐ *Other* _____
Gap Types	☐ *New* ☒ *Change* ☐ *Under-utilized* ☐ *Over-utilized* ☐ *Obsolete – replace by:* _____

IMPACT POSITION					
Area Affected	*Level of Impact*				*Position Statement*
	High	*Medium*	*Low*	*None*	
Business Impact	☒	☐	☐	☐	The Transportation Department's Director recently stated that clear communication is the greatest challenge and the greatest failure at the Transportation Department. Communication is impossible unless both parties understand the terminology being used. The interview participants stated that clearly defined terminology is needed to enable them to be more effective in their jobs. Lack of clearly defined terminology is having a significant impact upon the current business processes and therefore should be given High priority.
Information Impact	☒	☐	☐	☐	Affects the datamarts
Technology Impact	☒	☐	☐	☐	Affects the directory services

RELATED GAP COMPONENT INFORMATION	
Baseline Component Detail	
Component Name	*Component Type*
Build Public Trust	Strategic Direction, Drivers & Goals
Target Component Detail	
Component Name	*Component Type*
Build Public Trust	Strategic Direction, Drivers & Goals
Improve communication between managers, supervisors & their reports	Significant Business Events
Hold managers accountable for communication	Organization – Roles and Responsibilities

KEYWORDS	
Keywords /Aliases	Dictionary, Glossary, Lexicon

STAKEHOLDER INFORMATION			
Stakeholders	Department of Transportation, DOT Partners		
Roles	Managers, Supervisors, technical and executive personnel		
Reason for Stake	Partners and vendors: they require a consistent understanding of information about the work that is being done by the Department of Transportation.		
MIGRATION INFORMATION			
Migration Strategies	Five data center personnel 1 week to migrate and/or create datamarts Introduction of directory level server Resources for loading datamarts		
CURRENT STATUS			
Gap Component Status	☐ *In Development* ☐ *Under Review* ☒ *Accepted* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	2/25/03	*Date Accepted / Rejected*	3/30/04
Created By			
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

Business Domain

Definition	
Name	Public Safety (Business Domain)
Description	This domain entails all activities associated with protecting the citizens of the state of Kansas. This includes prevention, and response regarding a variety of public safety events. In the criminal justice discipline, this goes on to include prosecution, adjudication, incarceration, probation/parole, and criminal registrations.
Rationale	To maintain social order, to protect natural resources and property, to protect human life and safety, to organize for concerted response.
Benefits	Enhanced public safety. Assets are protected. Quality of life is improved. Crime is reduced.

Boundary	
Domain Type	☒ Functional ☐ Topical
Boundary Scope Statement	This does not include the functions handled at an international, national, or local level.

Associated Business Architecture Perspective	
Perspectives addressed under this Domain	Strategic Business Strategic Transaction Strategic Information

Associated Business Architecture Disciplines	
Related Disciplines	law enforcement, fire safety statistics, liquor retail licensing, disaster mitigation, disaster response, preventive police patrol.

Related Enterprise Business Drivers

Related Principles		
Reference #s, Statements or Links	*Conflict*	*Support / Conflict Detail*
The priority and preferred approach to public safety is prevention and mitigation rather than response.	☐	This principle supports this domain.

Related Best Practices		
Reference #s, Statements or Links	*Conflict*	*Support / Conflict Detail*
	☐	

Related Trends		
Reference #s, Statements or Links	*Conflict*	*Support / Conflict Detail*
Drug abuse is on the rise and has a direct relationship to the incidence and severity of crime.	☒	This trend is in direct conflict with ensuring public safety.
There is an increased use of fire retardant construction materials and techniques	☐	This trend is in direct support of ensuring public safety.

KEYWORDS			
Keywords/Aliases	Public safety police fire disaster risk management attorney jail victim plaintiff		
CURRENT STATUS			
Business Domain Status	☒ *In Development* ☐ *Under Review* ☐ *Accepted* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	5/24/04	*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

Business Discipline

Definition	
Name	State Police (Business Discipline)
Description	This discipline is in place to enforce state law, mitigate disasters, augment local enforcement operations, and provide security for larger or more critical public events and facilities.
Rationale	There is a need for a state wide capability for law enforcement that is not directly linked to any particular locality. The state police fulfill this capability.
Benefits	Enhanced public safety. Assets are protected. Quality of life is improved. Crime is reduced.

Boundary	
Boundary Scope Statement	This does note include the functions handled at an international, national, or local level. The state police can act at a local level based on need.

Associated Business Architecture Domain	
Related Domain	Public Safety

Related Enterprise Business Drivers

Related Principles

Reference #s, Statements or Links	*Conflict*	*Support / Conflict Detail*
The priority and preferred approach to public safety is prevention and mitigation rather than response.	☐	This principle supports this discipline.
The public prefers that the response be delivered by the lowest level of government capable of delivering the appropriate response – i.e., the public will prefer the local police department handle an incident. Then escalate to the county sheriff. Then escalation to the state police level. Then escalation to the FBI.	☐	This principle supports this discipline.

Related Best Practices

Reference #s, Statements or Links	*Conflict*	*Support / Conflict Detail*
	☐	
	☐	

Related Trends

Reference #s, Statements or Links	*Conflict*	*Support / Conflict Detail*
Drug abuse is on the rise and has a direct relationship to the incidence and severity of crime.	☒	This trend is in direct conflict with ensuring public safety.
There is an increased incidence of aggressive driving	☒	This trend is in direct conflict with ensuring public safety.

KEYWORDS			
Keywords/Aliases	State police, response, law enforcement, escalation		
CURRENT STATUS			
Business Discipline Status	☒ *In Development* ☐ *Under Review* ☐ *Accepted* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	5/24/04	*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

Business Architecture Component

Definition	
Name	Reduce highway fatalities (Business Architecture Component)
Description	This goal is to achieve increased safety of the motoring public.
Rationale	Improve highway safety.
Benefits	Quality of life, safer highways, enhanced transportation, greater efficiency in the transportation system, protection of life, health and property.
Component Classification	
Classification	☐ *Baseline* ☒ *Target*
Associated Business architecture Discipline	
Business Architecture Discipline	Ensure the public's safety
Associated Business architecture Perspective	
Business Architecture Perspective	Strategic Business
Keywords	
Keyword / Aliases	Safety, accident, fatality, injury, transportation, goal
Business Architecture Component Type	
Component Type	Goal (i.e., a set of broad, fundamental aims the organization is expected to accomplish to fulfill its mission). Often general in nature (even fuzzy) and deal with "what" the organization wishes to accomplish but not "how" it will be accomplished. Does not include specific measures or dates.
Critical References	
Related Business Architecture Components	

Business Architecture Component	*Relationship*	*Business Architecture Component*	*Relationship*
Fatalities will be reduced by 35% by EOY 2008 (this is an objective)	Goal to supporting objective		

Standards Organization			
Name		*Website*	
Contact Information			

Government Bodies			
Name		*Website*	
Contact Information			
Stakeholders/Roles			
Stakeholders			
Roles			
Reason for Stake			
COMPONENT LIFECYCLE INFORMATION			
GAP Component			
GAP Components	Lack of common wireless communication capability between fire, police, and EMS.		
CURRENT STATUS			
Business Architecture Component Status	☒ *In Development* ☐ *Under Review* ☐ *Accepted* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	5/24/04	*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

Gap Component

Definition	
Name	Lack of common wireless communication capabilities (Gap Component)
Gap Statement / Description	Fire, police and EMS use different wireless capabilities and therefore often do not communicate in a timely manner to coordinate resources in response to an incident.
Rationale	Common wireless communications capabilities are required to ensure all related first responders can communicate and coordinate resources.

Gap Component Classification	
Architecture Blueprint	☒ *Business Architecture* ☒ *Information Architecture* ☒ *Technology Architecture*
Architecture Level	☒ *Component* ☐ *Discipline* ☐ *Domain* ☐ *Other* _____
Gap Type(s)	☒ *New* ☒ *Change* ☐ *Under-utilized* ☐ *Over-utilized* ☐ *Obsolete – replace by:* _____

Impact Position					
Area Affected	*Level of Impact*				*Position Statement*
	High	*Medium*	*Low*	*None*	
Business Impact	☒	☐	☐	☐	Business architecture of related disciplines become interoperable
Information Impact	☒	☐	☐	☐	Information broker is established to share information at the point in time of need, involving all necessary participants based on the incident type.
Process	☒	☐	☐	☐	Business processes will be affected within allied disciplines
Technology Impact	☒	☐	☐	☐	Significant change in communication networks, protocols, equipment and operating processes.

Related Gap Component Information

Baseline Component Detail

Component Name	*Component Type*

Target Component Detail

Component Name	*Component Type*
Fatalities will be reduced by 35% by EOY 2008	Objective
By EOY 2008, 80 % of police, fire, and EMS responders will be able to communicate at the point of need	Objective
Through the use of shared 800 MHz frequencies, radio networks will be interconnected	Strategy

KEYWORDS			
Keywords/Aliases	Radio frequency, first responders, point of need, common, shared		
STAKEHOLDER INFORMATION			
Stakeholders	First responders, motoring public		
Roles	Managers, supervisors, first responders and public		
Reason for Stake	Responders need capability, public needs the service		
MIGRATION INFORMATION			
Migration Strategies	See the state radio plan (reference number).		
CURRENT STATUS			
Current Status	☐ *In Development* ☒ *Under Review* ☐ *Accepted* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	5/25/04	*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

Business Domain Model Samples

PILLARS OF GOVERNMENT

One example of a high-level business model is characterized in Figure 10. A vertical beam is used to represent a functional Business Domain. Functional governmental Business Domains are distinct, yet can be grouped. The groupings of these functional and distinct Business Domains are based on areas that share common functions. The terms Pillars of Government or Centers of Interest refer to functional Business Domains.

A horizontal beam is used to represent Topical Business Domains. Topical Business Domains allow the business to focus on a single topic and visualize all the points of impact or touch-points across the enterprise. Examples of topical Business Domains would be Human Resources, Citizens, and Payments.

The use of the pillar and beam concept allows an intersection as the beams pass through the pillars. This helps to identify where there is common usage of the topical business area within the architecture domain.

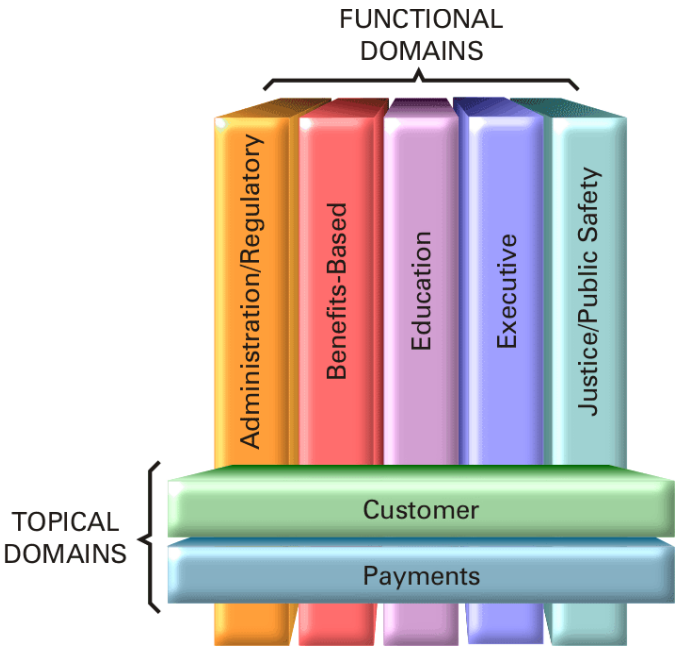


Figure 10. Sample Business Domains

FEDERAL BUSINESS REFERENCE MODEL (BRM)

Another example of a Business Model is the Federal Business Reference Model (BRM) illustrated in Figure 11. The Federal BRM describes the Federal Government's Lines of Business and its services to the citizen – independent of the agencies, bureaus, and offices that perform the business operations and provide the services.

The BRM identifies three *Business Areas* that provide a high-level view of the operations the Federal Government performs – Services to Citizens, Support Delivery of Services, and Internal Operations/ Infrastructure. The three Business Areas comprise a total of 35 external and internal *Lines of Business* – the services and products the Federal Government provides to its citizens; and 137 *Sub-Functions* – the lower level activities that Federal Agencies perform. [4]

[4] http://www.feapmo.gov/fea.asp

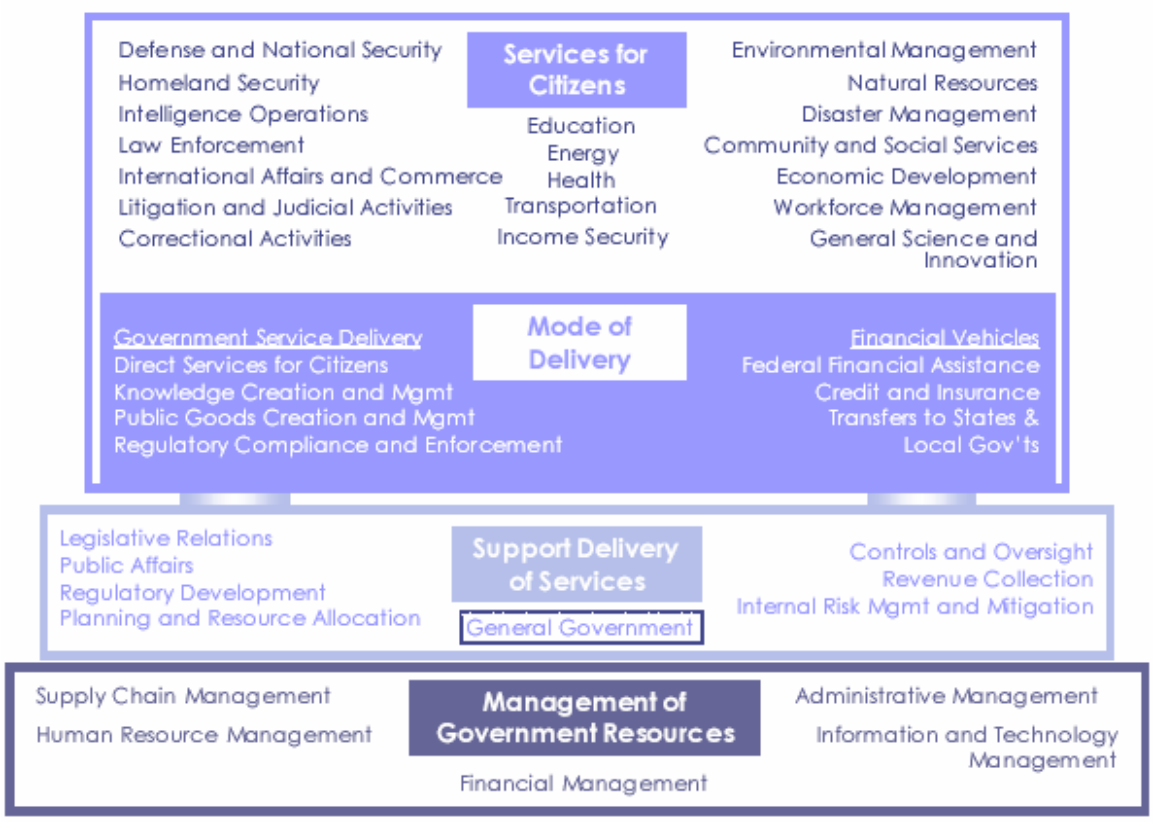


Figure 11. Federal Business Reference Model (BRM)

SPREADSHEET BUSINESS DOMAIN MODEL

A spreadsheet is a good method for capturing intersections between functional and topical areas of the enterprise business. The following samples illustrate only a small part of the actual spreadsheet developed by the Documenters. In the first sample the Agencies are listed on the y-axis and the functions are listed on the x-axis. In this case, the Architecture team included a column to identify services classes, Government to Citizen, Government to Schools, etc., since that information was important to the mission of this state.

This team did not develop the model further, but used the matrix itself as the Business Domain Model[5].

[5] State of Indiana, Division of Information Technology *Agency Mapping,* February 2003.

Line of Business	Business Function	Service Class	Accounts, Board Of	Attorney General	Auditor Of State	Budget Agency	Administration	Ethics Commission	Governor	House Of Representatives	Tax Review Board	Election Commission
Service Class:	G2C: Government to Citizen											
	G2B: Government to Business											
	G2G: Government to Government											
	G2S: Government to Schools											
	I-Ops Internal Operations											
Public Asset Management	Cultural Activities and Artifacts											
	Public Funds											
	Public Records / Data Management											
	Facilities Mgt.											
	Fleet Mgt.											
Defense and Security Ops	Anti-Terrorism											
	Bio-Terrorism											
Public Health	Illness Prevention											
	Immunization Management											
	Public Health Monitoring											
	Food Assistance											
	Housing Benefits											
	Medical Services											
	Monetary Benefits											

The sample on the following page is from the Federal Government. It is a similar matrix, but in this case the team used the matrix to organize and understand the functions and their intersections and built a simplified model, the BRM, which distilled governmental agencies and functions to an easily understood format.

FEDERAL RELATIONSHIP MATRIX[6]

Agency Mappings

Services to Citizens Business Area*

Analytical Summary
Average Number of Agencies per Sub-Function is 5
Average Number of Agencies per Line of Business is 10
Average Number of Lines of Business per Agency is 10
Average Number of Sub-Functions per Agency is 19

		USAID	USDA	Commerce	Education	Energy	HHS	HUD	DoI	DoJ	DoL	State	Transportation	Treasury	EPA	FEMA	GSA	NARA	NASA	NSF	NRC	OPM	SBA	SSA	VA	# of Agencies
Public Asset Management	Cultural Archives and Artifacts																									0
	Public Funds							X					X				X						X			4
	Public Facilities		X	X		X	X	X	X			X	X	X	X		X	X								12
	Public Records/Data Management			X				X					X	X	X		X	X		X				X		9
Defense and National Security Ops	Anti-Terrorism			X					X			X	X	X	X	X	X									8
	Border Control		X	X					X			X	X	X										X		7
	Intelligence Gathering								X				X	X												3
	Military Operations												X													1
	Weapons Control			X		X						X		X							X					5
Public Health	Illness Prevention	X					X														X				X	4
	Immunization Management	X					X																		X	3
	Public Health Monitoring	X	X	X			X						X		X											6
Energy Management	Energy Distribution					X			X																	2
	Energy Production					X			X																	2
	Energy Resource Management			X					X				X							X						4
Domestic Economy	Business/Industry Development		X	X					X		X	X	X	X	X		X		X				X			11
	Monetary Control								X				X	X												3
Social Services	Burial Services																									0
	Community Development		X	X				X	X				X	X	X		X						X			9
	Food Assistance		X																							1
	Housing Benefits							X	X							X										3
	Medical Services						X									X									X	3
	Monetary Benefits					X	X				X	X				X								X	X	7
Marketable Asset Management	Financial Asset Management			X				X						X												3
	Personal Property Management			X						X			X	X			X									5
	Real Property Management			X				X					X				X									4
Diplomacy & Foreign Relations	Conflict Resolution	X										X														2
	Foreign Socio-Econ and Political Dev.	X	X	X							X	X		X	X											7
	Treaties and Agreements	X		X								X		X	X				X					X		7
Disaster Management	Disaster Monitoring and Prediction	X		X				X				X	X		X	X	X									8
	Disaster Preparedness/Planning	X		X		X	X	X				X	X		X	X	X						X			11
	Disaster Repair and Restore	X	X	X				X	X			X	X		X	X	X						X			11
	Emergency Response	X		X		X	X		X			X	X		X	X	X									10
Education	External Training and Education	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X		X			X	X	X	X	20
	Advising and Consulting	X	X	X				X	X		X		X	X	X		X	X				X	X			13
	Promote Education	X			X																					2
Research & Development & Science	Data & Statistics Development			X	X	X		X	X	X	X		X	X	X		X	X					X	X		14
	Scientific Research and Development	X	X	X		X	X		X				X		X				X	X						10
	Socio-Economic Research & Development	X		X		X	X	X		X	X		X											X		9
	Technology Research & Development			X		X	X		X	X		X	X	X			X		X		X					11
Transportation	Air Traffic Control												X													1
	Land Transportation			X					X				X		X		X									5
	Maritime Transportation								X				X													2
	Space Operations												X													1
Workforce Management	Job Creation			X							X		X		X								X			5
	Labor Rights Management										X	X	X				X									4
	Worker Safety										X		X		X		X									4
Recreation and Natural Resources	Conservation Planning		X	X					X				X		X											5
	Land and Monument Management		X	X					X				X		X											5
	Tourism Management			X					X				X	X	X			X								6
Insurance	Insurance Issuing		X					X					X			X							X	X	X	8
	Insurance Services		X					X					X			X							X	X	X	8
Consumer Safety	Firearms and Explosives Safety												X	X												2
	Antitrust Control			X									X													2
	Consumer Products Quality Assurance		X	X			X		X				X	X	X		X									8
	Monetary Protection													X												1
Trade	Export Promotion	X	X	X										X	X								X			6
	Merchandise Inspection		X	X					X				X	X	X											6
	Tariff/Quotas Monitoring			X									X	X	X											4
	Trade Law Enforcement			X									X	X												3
Environmental Management	Environmental Monitoring			X		X			X		X		X		X					X						7
	Environmental Remediation								X				X		X											3
	Pollution Prevention and Control			X					X		X		X		X		X				X					7
Legal	Judicial Hearings							X		X	X		X													4
	Legal Defense								X																	1
	Legal Investigations							X	X	X			X		X									X		6
	Legal Prosecution/Litigation							X	X	X		X	X		X		X						X	X		9
	Resolution Facilitation									X			X		X		X									4
Regulated Activity Approvals	License Issuing and Control		X	X			X				X		X	X							X		X			8
	Permit Issuing and Control		X	X			X		X	X	X		X	X	X						X		X			11
Revenue Collection	Debt Collection									X				X												2
	Tax Collection								X					X											X		3
	Other Revenue Collection													X													1
Law Enforcement	Criminal Apprehension			X					X	X			X	X			X										6
	Criminal Incarceration									X																	1
	Criminal Investigation and Surveillance			X					X	X		X	X	X	X		X										8
	Citizen Protection									X																	1
	Crime Prevention																									0
	Intellectual Property Protection			X						X				X													3
	Leadership Protection											X	X	X													3
	Property Protection				X				X	X			X	X			X										6
	Substance Control								X	X		X	X	X													5
Federal Financial Assistance	Grants Assistance			X	X	X	X	X	X	X			X		X	X					X						11
	Loans Assistance	X	X	X	X		X	X						X	X	X								X		X	11
	Subsidies		X	X																							2
Total Lines of Business Performed		7	15	20	4	9	9	17	9	9	11	21	15	19	6	14	4	6	3	5	2	12	9	5		
Total Sub-Functions Performed		17	21	45	6	14	17	17	38	23	15	20	56	38	36	13	26	5	7	3	6	4	16	12	8	

[6] Federal Chief Information Officer (CIO) Council, Federal Architecture Working Group, *FEA_BRM_Agency Mappings_Rev_1*, July 2002.

Gap & Migration Summary Format Sample

The Gap & Migration Summary should summarize the key findings regarding the gaps and migration strategies for the given Domain. The following outline provides an example of the items typically covered, and the general structure of a Gap & Migration Summary Report.

Outline	*Description*
EXECUTIVE SUMMARY	A summary of the key findings of gaps identified for the Domain
INTRODUCTION	Provides description of background information to support the report
Overview	Provides greater detail regarding the scope of this effort and the methodology used in completing this document.
Goals and Objectives	Present the gap topics and migration strategy options for the Domain
Scope and Approach	Describe the scope of the effort, including any limitations or constraints and outline the approach used in the effort.
BASELINE SUMMARY	Summarize the Domain baseline component results from the various perspectives
TARGET SUMMARY	Summarize the Domain target component results from the various perspectives
GAPS	There can be several Gaps *(Repeat this section, along with Migration Strategies section for each gap identified.)*
Gap Name 1	The name for the identifying the Architecture Gap.
Gap Statement	The Gap Statement is a brief description of the identified gap topic, representing the current or "as-is" status of that topic.
Gap Description	The Gap Description is a detailed description of the gap topic, including background and scope
Goal(s)	This is a statement of the target status of the gap topic. Information found in the Rational Section of the Gape Component Template may assist in determining the future state. If this information is not available, other means will need to be employed to collect this data, i.e. interviews with key subject matter experts and senior management.
Benefit(s)	A statement of the advantages offered by moving to the target status of the gap topic
Priority	A statement of the relative importance of moving to the target status of the gap topic
Migration Strategies	Each Gap can have multiple Migration Strategies *(Repeat this section for each migration strategy identified for this Gap)*
Migration Strategy 1	Provide strategy statement
Strategy Description	A description of the actions that might be taken to move to the target status of the gap topic
Benefits of Strategy	A list of the advantages posed by employing the migration strategy
Drawbacks of Strategy	A list of the disadvantages presented by the migration strategy.
Degree Strategy Meets Goals	An analysis of the ability of the migration strategy to meet all of the goals of the gap topic
Cost, Time & Resources	A relative ranking of the investment required to implement the migration strategy

Outline	*Description*
OVERARCHING MIGRATION STRATEGIES	Describe the migration strategies that could be effective for more than one gap topic
CONCLUSION	Summarize the key findings.
APPENDICES	Include items such as Gap & Migration Summary charts and interview statements for each Gap,

Gap & Migration Strategy Chart Sample

The following table provides an example of a Gap/Migration Overview chart that might appear in the executive summary of a Domain Summary Report

Gap	*Associated Migration Strategies*
Terminology & Definitions	Develop a custom set of common business terms
	Compile a set of common business terms from existing documentation and by researching other Operational Areas
	Compile an initial set of common business terms from existing documentation and by researching other like areas on the Internet. Follow up with interviews across the functional units to validate, modify and append terms and definitions to the initial list
Data Collection & Storage	Develop standard formats or layouts for the same types of data and determine the best storage media for that data.
	Document the layouts or formats of the same types of data and share that documentation.
	Develop a standard format or layout for the same types of data and move the distributed data to a central data repository.
Data Visibility & Accessibility	Identify those times in the Project Life Cycle when the lack of information is creating a problem and address each occurrence individually.
	Create a common data repository and publish information at specified intervals.
	Create a common data repository and allow users to extract whatever information they need, whenever they need it.
Policy & Procedures	Identify and implement fully the existing policy and procedures across the organization.
	Continue the Enterprise Architecture effort to document both the business and technical aspects of the organization in a central, maintainable repository.
	Continue the development of Business Rules for implementation of the processes and procedures that can be automated.
Archival of Project Data	Develop a “datamart” of project data accessible to all functional units.
Change Tracking & Change Reporting	Determine the types of design changes that should generate notification and who should receive that notification.
	Allow the functional units to “pull” their design change data at will.
Agreements	Integrate the Agreements data and processes into the Transportation Project life cycle.

Roles & Responsibilities	Identify the roles associated with data creation and maintenance responsibilities and indicate the CRUD activities performed.
	Identify the roles associated with data creation and maintenance responsibilities and indicate the way in which each role is involved.
	Identify the roles associated with data creation and maintenance responsibilities and indicate the way in which the data is used and the way in which each role is involved.

SUMMARY/CONCLUSION

The Business Architecture provides a business-based framework for developing solutions that operate across agencies and within the lines of business of state and local governments.

It is through the pursuit of formal Business Architecture that provides:

- A demonstrable, repeatable approach to assuring business alignment throughout the enterprise
- A clear understanding of the enterprise's current and future direction
- Identification of opportunities for interoperability between all government bodies both vertically and horizontally
- A clear map between the business of federal, state and local government and IT's enablement of the defined business intentions
- A valuable tool for illustrating and communicating the business of the enterprise to all stakeholders
- Context and guidance to keep the enterprise architecture focused on the strategy and goals of the state or local government
- A method to deliver services and information in a consistent and structured manner.

The Business Architecture describes and interrelates operational elements required to realize the enterprise's business objectives. The Business Architecture is the collection of knowledge and relationships between strategy, people, functions, information, applications and infrastructure.

NASCIO Online
Visit NASCIO on the web for the latest information on the Architecture Program or to download the current version of the Enterprise Architecture Development Tool-Kit.

www.nascio.org

NASCIO EA Development Tool-Kit
Information Architecture

Version 3.0

October 2004

TABLE OF CONTENTS

INFORMATION ARCHITECTURE

Development of NASCIO's Enterprise Architecture Tool-kit is an on-going process. Each iteration of the Toolkit will incorporate new knowledge and best practices as they are developed. NASCIO is treating Enterprise Architecture as a program. As a program, EA will continue to evolve and become more sophisticated. The reader is encouraged to treat this version of the Tool-Kit as one iteration in an ongoing process. The Tool-Kit will continue to evolve to reflect the changing nature of EA. NASCIO is presenting Information Architecture as a first iteration in this evolution. This version is not an exhaustive treatment of Information Architecture and so it does not include every aspect of Information Architecture. The Tool-Kit content is not intended to repeat information that is readily available from other sources.

Information is one of the most important assets to any enterprise. Information, frequently defined as the organization of data into usable formats, must be transferred quickly, accurately, in the desired format and be understandable to the user. Information Architecture addresses the informational needs of the enterprise.

The objective of Information Architecture is to manage the information of the enterprise. Information Architecture aligns the Business Processes to the information systems that support these processes, promotes information sharing and facilitates cross-agency information exchanges. Using the set of business processes that provide a view of the functions of the enterprise, the Information Architecture will provide the organization with a high level model of its critical information.

Figure 1 shows how Information Architecture fits within the overall Enterprise Architecture Framework. Information Architecture provides the terminology and definitions for the organization's information assets as well as the processes that affect or are affected by the information.

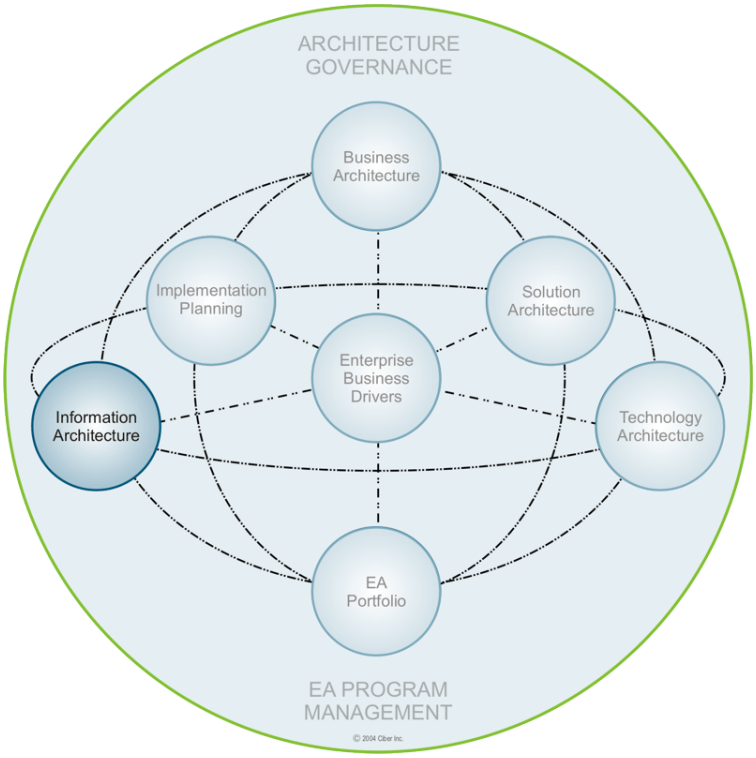


Figure 1. Information Architecture Touch-points

Information Architecture provides a demonstrable, repeatable approach in assuring the alignment of information assets and business processes throughout the enterprise. Documenting the Information Architecture provides a clear understanding of the enterprise's current and future information needs and provides insight into the business processes and their associated information for all enterprise architects. Utilizing the detail documented in the Information Architecture provides the basis for the sharing of information throughout the enterprise as well as across organizational boundaries.

State and local governments continually face mandates for inter-agency sharing of information and providing bundled services. The Information Architecture focus is on shared data elements, or those elements that are involved in information exchange, so that information solutions will operate across agencies and within the lines of business of state and local governments. It is through the Information Architecture that these shared data elements coalesce into the metadata of the enterprise. These shared data elements are exposed through examination of the business processes. This is depicted in Figure 2

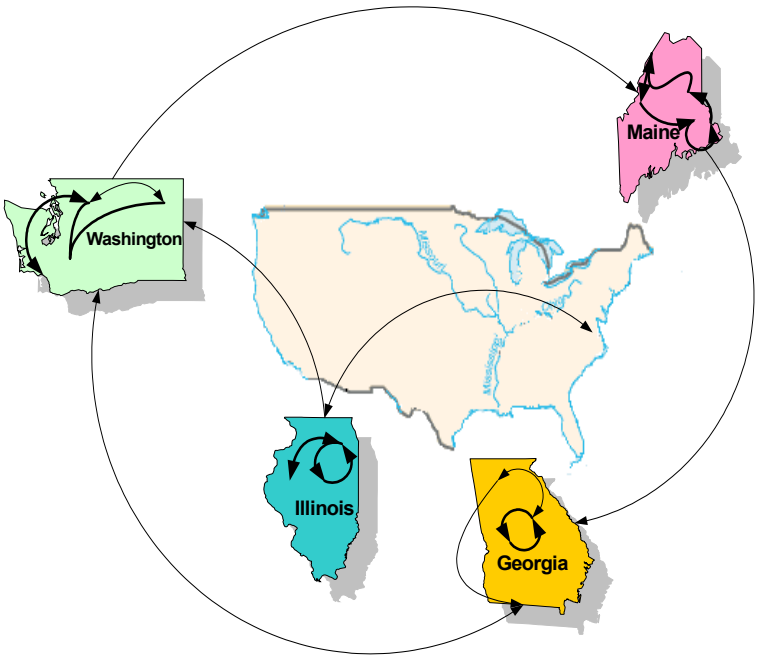


Figure 2. EA enhances interoperability between all government bodies.

The purpose of this section of the Tool-Kit is to provide an introductory understanding of the Information Architecture and a guide in the basics for the development and documentation of Information Architecture. This is accomplished by providing:

- A basic understanding of the terminology used for an Information Architecture
- Definition and organization of an Information Architecture Blueprint
- Sample processes that outline the steps necessary to build the Information Architecture Blueprint
- Collection of start-up templates for populating the Information Architecture Blueprint.

Definitions

When discussing Information Architecture and related topics, the terminology varies, including a variety of terms with the same or similar meanings, as well as varied meanings for the same term. To help minimize any confusion in terminology, a glossary that provides definitions of terms used throughout the Tool-Kit is provided in Appendix A. A brief list of the terms and definitions used throughout the Information Architecture section are provided here:

- *Baseline*: The current or "as is" state of the information environment, captured in a set of baseline information models.
- *Blueprint:* The dynamic depiction of information (content), captured using standardized, structured processes and templates (framework). The Information Architecture Blueprint records the present direction of the enterprise and the direction the enterprise intends to pursue from the perspective of the enterprise information requirements.
- *Cardinality:* Cardinality helps describe the nature of a relationship between two entities. A relationship's cardinality is the number of objects on one side of a relationship that may be related with objects on the other side.
- *Component:* Within this Tool-Kit, component refers to a level of architectural detail. The component level detail is captured utilizing a respective template. Component levels addressed in Information Architecture are Process Information Meta Components.
- *Conceptual Information Model:* Defines the functional requirements and the business users' view of the information.
- *Data:* The atomic bits of fact that constitute the raw material of knowledge about our business. The home address of an individual is data. It is atomic (not divisible) because to divide it renders it useless.[1]
- *Data Element:* A unit of data for which the definition, identification, representation, and permissible values are specified by the means of a set of attributes.[2]
- *Data Element Concepts:* An object, any part of the conceivable or perceivable work, that can be represented in the form of a data element, described independently of any particular representation (the combination of a value domain, data type, and if necessary, a unit of measure or a character set.)[3]
- *Enterprise:* Represents an organization in total, including all subordinate entities, encompassing corporations, small businesses, non-profit institutions, government bodies, as well as other kinds of organizations.
- *Framework:* The combination of the templates and structured processes that facilitate the documentation of the architecture in a systematic and disciplined manner.

  In this Tool-Kit, the term Architecture Framework is used to refer to the combination of the structural elements of the architecture, such as the structure of the Blueprint, the templates and the structured processes for documenting, reviewing communicating, implementing and maintaining the architecture.
- *Gap:* The difference between the "baseline" environment and the "target" environment.
- *Information:* The organization of data into usable formats. Information encompasses both structured (data marts, databases, database tables and data exchanges) and unstructured information (web content, jpeg or video files, and documents).
- *Information Architecture:* The compilation of the business requirements of the enterprise, the information, process entities and integration that drive the business, and rules for selecting, building and maintaining that information.
- *Information Relationship:* The description of how one Entity/Class is related to another.

[1] Mosshamer, E. L., A Word on Semantics: Data, Information, Knowledge, Insight, Illinois Mathematics and Science Academy
[2] ISO/IEC 11179-1:1999(E)
[3] ISO/IEC 11179-1:1999(E)

- *Information Subject Area:* Topical or functional categories of the business processes that are integral to the operations of the enterprise, such as Customer, Product/Service, etc.
- *Logical Information Model*: Shows the main functional [information] components and their relationships within a system [an enterprise] independent of the [system and] technical detail of how the functionality is implemented.[4]
- *Metadata:* Literally, "data about data." Metadata includes data associated with either an information system or an information object, for purposes of description, administration, legal requirements, technical functionality, use and usage, and preservation.[5] Therefore, metadata gives us detail about both what the data means and how it's stated. Metadata is one of the greatest critical success factors to sharing information because it provides business users, developers and data administrators with consistent descriptions of the enterprise's information assets.
- *Migration:* The evolution from the baseline to the target state.
- *Model:* The graphical representation or simulation of a process, relationship or information, along with the narrative that supports the diagram.
- *Repository:* An information system used to store and access architectural information, relationships among the information elements, and work products.[6]
- *Target:* The desired future or "to be" state of the business information environment, captured in a set of target information models.
- *Template:* The empty form that is provided as a guide for capturing details that need to be documented and ultimately will reside in a repository.

Information Architecture differs from Data Architecture in that it encompasses both structured (data marts, databases, database tables and data exchanges) and unstructured information (web content, jpeg or video files, and documents). Information Architecture also includes the defining of business functional processes and delineates the relationship of the data element concepts to the processes. Within Information Architecture, the relationships between Business Domains and business processes are documented, as well as the information, business rules, and organizational roles/responsibilities that are part of each process.

In the NASCIO Tool-kit, the remaining elements of Information Architecture reside in the appropriate sections. For example, the strategic information needed for the conceptual components resides in the Business Architecture section, while the Technology Architecture section addresses information-related standards and tools such as:

- Database engines
- Metadata repositories
- Content management tools/standards
- Document management tools/standards
- Data analytical reporting tools/standards
- Information naming standards
- Information modeling denotation standards

[4] http://msdn.microsoft.com/architecture/enterprise/default.aspx?pull=/library/en-us/dnea/html/eaarchover.asp#eaarchover_topic3
[5] http://www.getty.edu/research/conducting_research/standards/intrometadata/4_glossary/index.html
[6] Federal Chief Information Officer (CIO) Council, Federal Architecture Working Group, A Practical Guide to Federal Enterprise Architecture, Version 1.0, February 2001.

- Diagramming and process symbol standards.

Because information standards are covered within the Technology Architecture (Information Domain), Enterprise Architecture teams may want to consider the development of the Information Domain of the Technology Architecture prior to the Information Architecture effort.

Models

The conceptual, logical, and physical models of the Information Architecture are designed to translate business information from the business user view (conceptual) to the actual physical information objects, such as, database tables, web content, or documents, in the systems where the information resides.

Conceptual Model - The conceptual model defines the information in the language of the business or non-technical end user. It is the most abstract model and the purpose is to define the functional, business view of the data.

Logical Model - The logical model follows the conceptual model. The purpose of the logical model is to depict business information including business relationships and business semantics adopted within the enterprise. The logical data model should be developed independent of the technical details of how the information is implemented. In this manner the information models are built to address the business objectives and requirements.

Physical Model - The physical models are defined/mapped from/to the logical models. At this level, the models are solid, defining tables, document, content and views that are specific to the implementations of the information for the enterprise. Physical designs are predefined in purchased solutions; therefore, when working with purchased solutions, the designs existing in the purchased solution are mapped to the logical.

For the baseline or current environment, Information Architecture will develop the Process Components and the conceptual, logical and physical levels of the Information Meta Model Components.

For the target or future environment, the Information Architecture will define the Process Components and conceptual level only of the Information Meta Model Components. The target logical and physical models will be developed within Solution Architecture, as will the physical model.

By capturing the information for these components in current information models (Baseline) and proposed information models (Target), deficiencies and gaps can be identified. Based on the analysis of the business drivers and the gaps, migration strategies can be developed to bridge the gaps and provide a roadmap to move to the target information model. The Information Architecture teams contribute to the documentation of the Gap Components, perform gap analysis and develop migration strategies as part of Implementation Planning.

Information Architecture clarifies business relationships and enhances understanding of the business rules the enterprise has adopted. A government organization may want to use this baseline for exploring and implementing changes relative to how information is used and what business rules related to information the enterprise will adopt.

Information Architecture offers many benefits to the Enterprise. These benefits can be used to garner support specifically for the Information Architecture effort as well as for Enterprise Architecture as a whole. These benefits include:

- Create understanding of the business semantics for both baseline and target
- Facilitate communication and understanding throughout the vitality processes
- Promote understanding and validation of the flow of control
- Increase understanding of business interactions
- Leverage linkage across government-wide entities
- Increase collaboration and sharing of information
- Reduce information redundancy
- Increase information re-use
- Improve process interoperability across the enterprise
- Alignment to the Federal Enterprise Architecture
- Facilitate cross agency analysis
- Increase responsiveness to citizens.

The development and maintenance of a vital Information Architecture requires the involvement of personnel in a variety of roles and responsibilities. Table 1 provides a reminder of the roles that apply across all of the architectures.

Table 1. Architecture Roles

Primary Roles	*Supportive Roles*
• Overseer • Champion • Manager • Documenter • Communicator • Advisor • Reviewer • Audience	• Subject Matter Experts (SME) • Services Teams • Project Teams • Procurement Manager • Project/ Services Communicator • Special Interest Groups • Enterprise Executive

Greater detail for these roles, including a brief description of the role, its responsibilities, recommended implementation, etc. are provided in the Architecture Governance Section of this Tool-Kit (see *Architecture Governance Roles*). Appendix C also contains a Role & Responsibility Matrix, which provides an "at-a-glance" reference of the responsibilities of each Architecture Governance role, the items acted upon, and the roles that interact regarding each responsibility. The governmental entity must determine the roles that will best enable their organization to develop their own Information Architecture. The following identifies the roles that are basic to developing an Information Architecture and provides brief role descriptions:

- The Information Architecture Manager is an executive who manages the existing and future information assets and ensures these assets are consistently maintained. Additionally this manager is familiar with the business, the design of information assets that relate to the business and the standards put forward by the Information Architecture Domain.

- The Information Architecture Documentation team is comprised of modelers knowledgeable of various aspects of enterprise-wide business processes and information and responsible for steering, shaping, and developing an Information Architecture Blueprint. These team members should be knowledgeable in business and the applications of technology. The role of Documenter refers to the combination of those best suited to document the architecture, including Subject Mater Experts in Business Process and Information Meta Components.
- The Information Architecture Subject Matter Expert (SME) is a member of an interdisciplinary team that ensures that the business processes and information are fully understood and correctly documented from a business perspective in the Information Architecture Blueprint. The SMEs may also serve as Information Architecture Documenters.
- The Information Owner is ultimately accountable for the information asset and business process. The owner is also responsible for ensuring the quality and determining the Security Classification for the Information. The Owner is the role that defines the nature of the business information, including its place in business process functions. The owner perspective is essential to directing the day-in and day-out management of the business information and the future information needs of the business. The Owner enforces the information policies and procedures developed by the Stewards.
- The Information Steward is responsible for information content and for using and managing information in a practical manner. This includes ensuring appropriate usage of the information within the rules established by the owner. Given the constraints of the owners, the steward can manage the information for the use they need, but the steward is then responsible for communicating and verifying new uses for and changes to the information with the information owner.[7]
- The Information Custodian is responsible for assuring integrity of the information captured, for proper handling of the information (not the content), and for assuring the information is available when needed.

The actual ownership of business information created at or obtained within the enterprise belongs to the enterprise, not to any particular line of business, role or individual. Information or data gathered or produced for business purposes cannot be "owned" by a single individual or line of business unit within the enterprise. Protection of privacy, compliance with legal requirements and fiduciary requirements mandate that the enterprise owns the information and data. For members of the enterprise's community to make informed and timely decisions, accurate versions of the business information that are relevant to their decision-making must be readily available. Therefore, the roles outlined above refer to the responsibilities and accountabilities in relationship to the content, rather than actual ownership of the information.

Information Architecture Framework

The Information Architecture Framework refers to the structural elements of architecture, namely the combination of the templates and structured processes that facilitate the documentation of the enterprise's information artifacts (e.g., processes and metadata) in a systematic manner. The information captured provides a picture of where the enterprise is today (baseline) and where the enterprise wants to be in the future (target) related to information requirements. Having an accurate representation of the two

[7] ComputerWorld, March 15,2004, "Data Stewards Seek Data Conformity". Mary Brandel—www.computerworld.com/databasetopics/businessintelligence/datawarehouse/story/0,10801,91146,00.html

classifications of the business information/processes (baseline and target) enables the identification of differences (i.e., gaps) between the two and formulation of the steps necessary to move from one to the other (Figure 3.).

Documenting the Information Architecture using the Information Architecture Framework will:

- Provide insight into strategic information and process requirements/needs
- Show how those requirements/ needs are met today / not met today
- Furnish the roadmap to furthering those requirements / needs in the future
- Provide valuable detail for making decisions and planning the investments (human capital or monetary resources) to further those requirements / needs into the future.

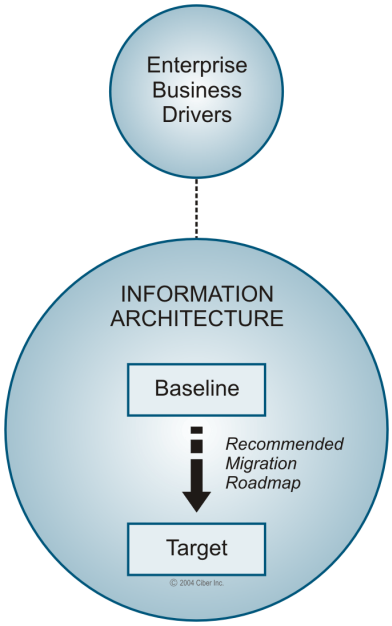


Figure 3. Information Architecture Flow

This section of the Tool-Kit supports NASCIO's architecture program by providing municipal, county and state governments a framework for establishing an effective Information Architecture Blueprint. This framework provides the processes and templates to guide the documentation of various information elements such as:

- Information organizations / roles
- Business information concepts
- Process activity.

The effective use of an Information Architecture Framework provides a standardized approach to capturing the details of the Information Architecture Blueprint by means of:

- Processes for documenting the Blueprint
- Templates for capturing the Blueprint detail.

Standardization promotes broader understanding and facilitates the integration and interoperability of solutions.

BUSINESS DRIVERS

The identification and development of Business Drivers is an important part of developing Enterprise Architecture. Business Drivers refer to the global influences on business that are captured within the architecture to show their acceptance and adoptability into the environment. Though these global influences can be of numerous types, three common categories of Business Drivers are Principles, Best Practices and Trends.

- *Principles:* Principles are statements of preferred direction or practice. Principles constitute the rules, constraints and behaviors that a bureau, agency or organization will abide by in its daily activities over a long period of time. Principles also encompass the business practices and

approaches that the organization chooses to institutionalize to better provide services and information.

- *Best Practices:* Best Practices are behavioral patterns and/or approaches that have proven successful over time for providing services and information.
- *Trends:* Trends are emerging influences within the business world that impact how services and information will be provided. Trends include governmental trends as well as architecture specific tends, i.e. technology trends, information management trends, etc.

INFORMATION ARCHITECTURE BLUEPRINT STRUCTURE

An Information Architecture Blueprint refers to the dynamic depiction of information captured using standardized, structured processes and templates. The Information Architecture Blueprint provides the basis for managing the enterprise information to maximize sharing of data across the enterprise. The Information Architecture Blueprint is comprised of Information Subject Areas, Process Components, and Information Meta Components.

Figure 4 provides a pictorial view of the relationship between the Information Architecture Blueprint elements. The graphic displays how these pieces work together to ensure the complete documentation of the Information Subject Areas and components that form the Information Architecture Blueprint.

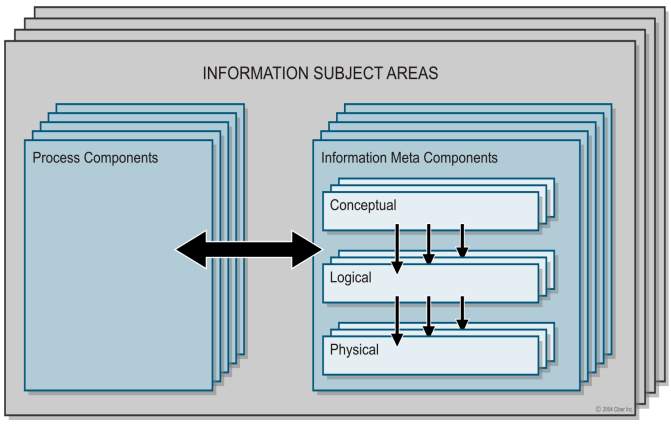


Figure 4. Information Architecture Blueprint Structure

Information Subject Areas – An Information Subject Area is a topical or functional division of the Enterprise's information. Unlike Business Domains it is not recommended to mix them. Examples of typical subject areas for shared information are:

- Customer / Customer Management
- Vendor/Supplier / Vendor Management
- Product/Service / Product/Service Management
- Organization / Organization Management
- Employee / Human Resource Management
- Geography / Location Management
- Calendar / Time Management

Information Subject Areas might vary somewhat within specific organizations, but this basic set will serve to categorize information for most enterprises. Each organization should determine the definition and scope of the subject areas that best reflect the information requirements of their organization. The detail captured within each Subject Area will cover topics such as:

- Information about them (e.g. Information about the Customer)
- The actions performed on/against them (e.g. Actions performed on a Product)

- The actions performed by them (e.g. Actions performed by the Customer)
- The actions performed for them (e.g. Actions performed for the Customer)

Process Components – The Process Components define the business functional processes and delineate the relationship of the data element concepts to the processes. Information Architecture Process Components specifically identify the business domain and/or information subject area that relate to each business process and the information, business rules, and organizational roles/responsibilities that are part of the process. There may be instances when additional decomposition of components is useful. Books and classes on developing use cases and decomposition levels are readily available.

Information Meta Components – The Information Meta Components serve to identify and define the shared information. The Information Meta Components are first identified as Data Elements or Data Element Concepts with the help of the Business SMEs. The Information Documenters refine this Conceptual model into the Logical and Physical layers of the Information Architecture.

These elements of the Blueprint will be addressed in greater detail in the Information Architecture Documentation process models; however, there is one additional component that is introduced here: the Gap Component.

Gap Components – In reality, the Gap Component resides as a component of the Gap Analysis and Migration Plan. However, contributions to the Gap Component come from Business, Information, Solutions and Technology architectures. As part of the Information Architecture Documentation Process, once the baseline and target detail has been confirmed for any given Data Element/Concept (Information Meta Component, conceptual detail) or process component, identified gaps between the Information Architecture Components are documented. The documentation of these gaps, along with the migration strategies for alleviating these gaps, provides the roadmap for achieving the target architecture. The graphic in Figure 5 shows the critical link between the Information Architecture Blueprint and the Gap Component, which is part of Implementation Planning.

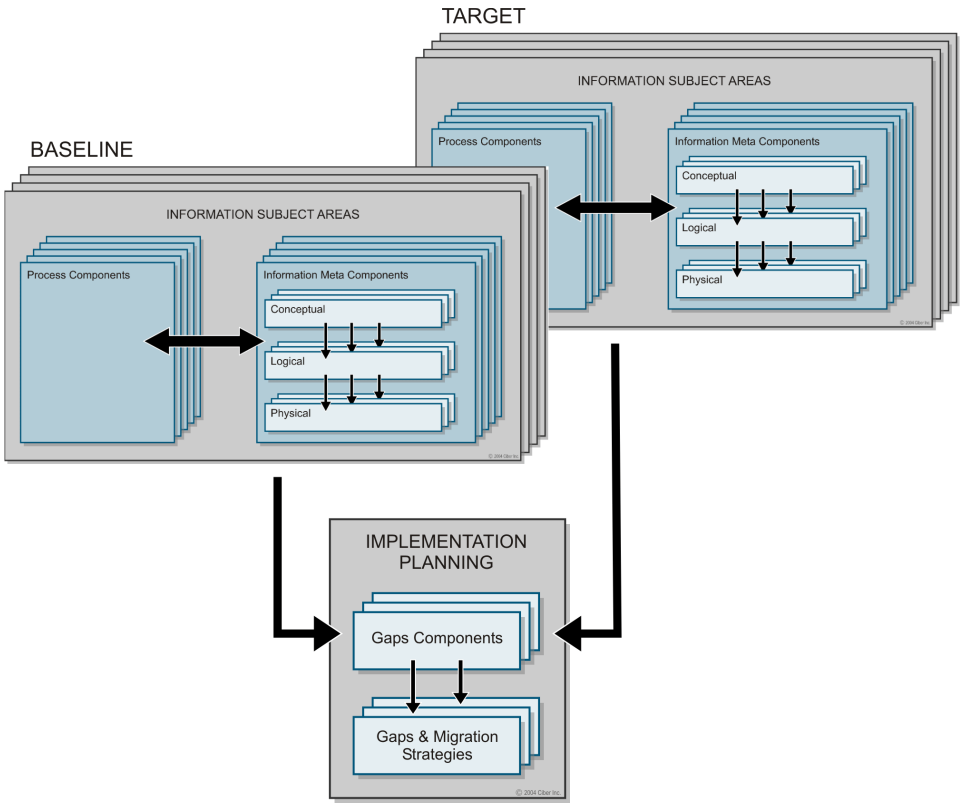


Figure 5. Information Architecture Contributes to Implementation Planning

INFORMATION ARCHITECTURE DEVELOPMENT

The Information Architecture Process begins with the Information Architecture Documentation Process, which allows the Architecture teams to capture, analyze, and document details about the information included in the Information Architecture Blueprint.

Figure 6 provides a graphical representation of the workflow path for the architecture team as they move through the processes and sub-processes of the Information Architecture Documentation Process.

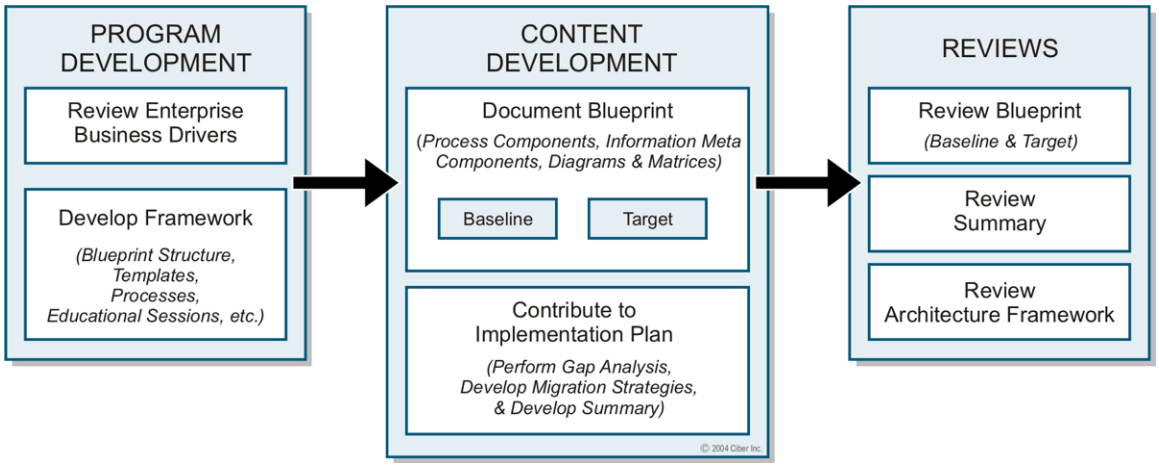


Figure 6. Information Architecture Documentation Work Flow

The Documenters develop the Information Architecture Blueprint by interviewing Subject Matter Experts regarding various functional and topical areas. The explicate definition of the information model is then captured in what is referred to as the Information Architecture Blueprint. Diagrams and matrix information about the defined information assets are created during this process to show the relationships and associations of all the information definitions.

The Information Architecture Documentation Process describes a systematic approach for developing and maintaining the Information Architecture Blueprint. The Information Architecture Documentation Process consists of several sub-processes, including:

- Initiate Information Architecture Documentation Process
- Develop Information Architecture Framework
- Conduct Information Architecture Work Sessions
- Create/Update Information Architecture Blueprint Items

The structure for each sub-process of this Information Architecture Documentation Process follows the same format:

- Introductory material (where applicable)
- Process model
- Narrative description of the process

- Template for capturing Blueprint detail (where applicable)
- Narrative description of the detail to be captured utilizing the template

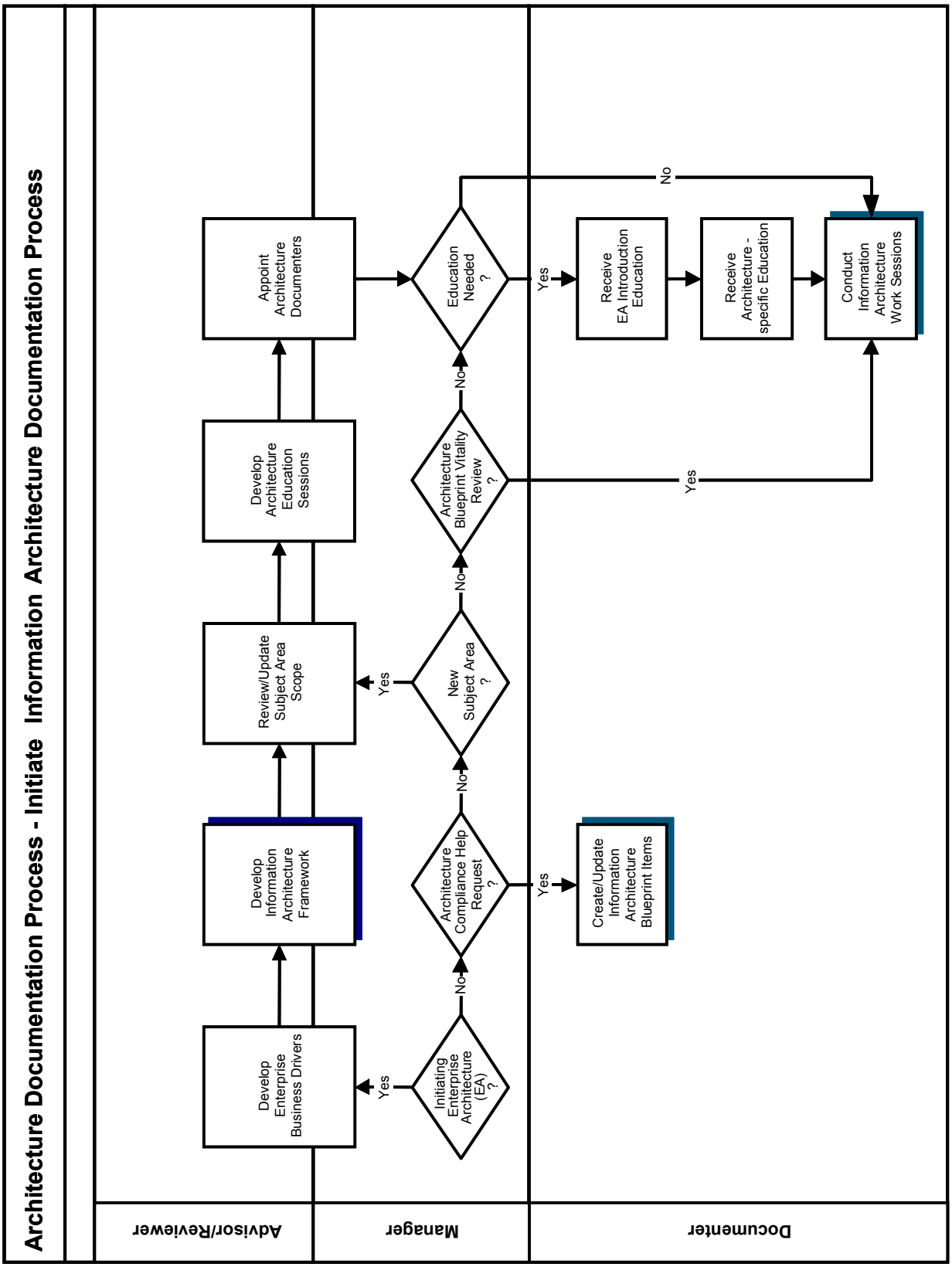
Initiate Information Architecture Documentation Process

PROCESS OVERVIEW

The Initiate Architecture Documentation Process presented here is similar to the generic process model provided in the Architecture Governance Section of the Tool-Kit. This model and narrative provides the initial process steps that are specific to the Information Architecture.

The Information Architecture Documentation Process can be triggered by any of the following processes/activities:

- Initiating Enterprise Architecture (EA)
- Initiating one of the constituent architectures
- Architecture Compliance Help Request
- Architecture Blueprint Vitality Review
- New Process or Information Meta Component


Architecture Documentation Process - Initiate Information Architecture Documentation Process
Advisor/Reviewer
Manager
Documenter
Develop Enterprise Business Drivers
Develop Information Architecture Framework
Review/Update Subject Area Scope
Develop Architecture Education Sessions
Appoint Architecture Documenters
Initiating Enterprise Architecture (EA) ?
Architecture Compliance Help Request ?
New Subject Area ?
Architecture Blueprint Vitality Review ?
Education Needed ?
Create/Update Information Architecture Blueprint Items
Receive EA Introduction Education
Receive Architecture - specific Education
Conduct Information Architecture Work Sessions
Yes
No

PROCESS DETAIL

Review Enterprise Business Drivers – It is important for the Information Architecture team to understand and become familiar with the Enterprise Business Drivers. While the development of the Enterprise Business Drivers is typically an overarching activity of Business, the Information Architecture team may become aware of circumstances or shifts from documented drivers and can contribute to the vitality of the Enterprise Business Drivers.

Develop Information Architecture Framework – The information documented within the Information Architecture Framework will play an important role in the development of the Information Architecture Blueprint. The NASCIO Information Architecture Framework provides structured processes and templates for capturing this information in a consistent and systematic manner. An enterprise may decide to use the framework elements as described in the NASCIO Tool-Kit, or may choose to develop a modified version, or may choose to use processes, templates and governance structures other than the examples provided in this Tool-Kit.

Review/Update Subject Area Scope – Review the definition of the Subject Area and add any detail that will be helpful in identifying the documentation team members. Also add any information that will help the team developing the documentation for this Subject Area.

Develop Architecture Education Sessions – Introductory and Information Architecture-specific sessions should be developed. The purpose of the Introduction to Enterprise Architecture Educational Session is to provide a high-level overview of the Enterprise Architecture Program. This session can be provided to executives, legislators or anyone within the organization that would benefit from an overview of Enterprise Architecture. The architecture-specific session should be designed to prepare Documenters for their role in the documentation effort. This session typically includes a review of the governance structure and overview of the templates they will be utilizing to document the detail for the architecture and processes they will follow or will affect their documentation efforts. Developers of training materials should consider inclusion of the following materials:

- Purpose
- Presenters
- Intended audience
- Session structure
- Prerequisites
- Syllabus
- Objectives
- Class materials for both instructors and attendees

Appoint Architecture Documenters – The Documenters will be appointed from subject matter experts familiar with the information needs of the enterprise. The team is comprised of modelers familiar with various aspects of enterprise-wide business and responsible for steering, shaping, and developing the Information Architecture Blueprint.

Receive EA Introduction Education – Documenters will receive initial training that covers an overview of enterprise architecture and architecture governance.

Receive Architecture-specific Education – After receiving initial enterprise architecture training, the Documenters will receive specialized instruction addressing the Information Architecture templates and documentation processes they will use to document the details of the Information Architecture Blueprint relative to their specific Information Subject Area.

Conduct Information Architecture Work Sessions – Applying knowledge gained in the first two education sessions, Documenters will begin development of the Information Architecture Blueprint documentation. The detail of the Work Sessions is presented in a separate process. (See Conduct Information Architecture Work Sessions).

Create/update Information Architecture Blueprint Items – If architecture compliance help is requested, the various Blueprint items should be updated. The process model and details pertaining to updating the Blueprint items are presented in a separate process. (See Create/Update Information Architecture Blueprint Items).

Develop Information Architecture Framework

PROCESS OVERVIEW

NASCIO's Information Architecture Framework provides a clear and consistent methodology to support communication and implementation of the Information Architecture. The combination of processes and templates are designed to facilitate the documentation of the Enterprise Information Architecture. An enterprise may decide to use the NASCIO Tool-Kit or it may choose another methodology. Regardless of the methodology selected, the structure for capturing Information Architecture Blueprint detail should be consistent and concise to ensure uniform documentation and communication across the enterprise.

Architecture Documentation Process - Develop Information Architecture Framework
Advisor/Reviewer
Manager
Documenter
Develop Information Architecture Processes/ Templates
Document Information Security Classifications
Identify/Define Information Subject Areas (Topical/Functional)
Identify Information Subject Area Owners/ Stewards
Select Initial Information Subject Areas for Documentation

PROCESS DETAIL

Develop Information Architecture Processes/Templates – Developing the processes and templates for capturing pertinent architecture detail, as well as defining and documenting changes to the overall governance structure that supports the architecture activity, is a critical step when initiating Enterprise Architecture or any of the underlying architectures. Each enterprise must decide upon a methodology that best suits their organization. The methodology that is best for an organization is the one that addresses the resource and time constraints for that enterprise.

During the development of the Information Architecture process and template designs is a good time to consider the use of a repository or automated tool for the capture, storage, and presentation of the architecture documentation. There is a considerable amount of documentation within an Enterprise Architecture and many interrelations between the underlying architectures. The use and maintenance of the Enterprise Architecture is greatly simplified when the architecture documentation and models are readily available to all stakeholders.

There are many methods and tools used for capturing the detailed information regarding the processes, events, agencies, information and conditions involved in an architecture project. One example of a tool that embodies the principles of both business and information architecture is the JIEM (Justice Information Exchange Model).[8] JIEM is a Web-based software application developed by SEARCH, The National Consortium of Justice Information and Statistics, for the Department of Justice that enables data collection, analysis, and reporting by users and researchers (For additional detail, see *Justice Information Exchange Model* at the end of this document).

While the JIEM tool was created specifically for meeting the needs of the courts and justice agencies, the methodologies regarding the capturing of detailed information surrounding the processes, events, agencies, information and conditions apply to any organization striving to focus on the enterprise-wide exchange of information.

Document Information Security Classifications – The standards for all security classifications reside within Technology Architecture under the Security Domain. Documenters will coordinate with the Technology Architect to determine appropriate classifications.

There are numerous methods used to classify information. For example, the US Department of Defense has various rules to categorize classified documents. These guidelines reflect a military style of classification, such as Top Secret, Secret, Confidential, and Unclassified data. The Security Classifications influence anyone who creates, dispenses or modifies information. They must understand and follow Security Classification policies.

A simple Security Classification for business use could be:

- External – Security Classification is defined outside the Enterprise, for example, information from Homeland Security.
- Privileged – This is a private Security Classification and would cause serious harm to the business of the Enterprise if breached.
- Sensitive – In this Security Classification, information obtained by unsecured parties would cause moderate harm to the business of the Enterprise.

[8] SEARCH – The National Consortium of Justice Information and Statistics, JIEM Reference Model, Version 1.0.1, May 2004

- Public—Information available to the Public for the use of all Citizens.

Identify/Define Information Subject Areas - An Information Subject Area is a topical/functional division of the Enterprise's information. All shared information in the enterprise is categorized into one of the Subject Areas. These Subject Areas can have actions performed against them, by them, for them or have data captured about them, etc. (e.g. data captured about customers/vendors, etc., actions performed by customers/vendors/employees, etc.). Each organization should determine the definition and scope of the subject areas that best reflect the information requirements of their organization. Subject Areas serve as categories for capturing Metadata and Processes.

The documentation team (Documenters and Subject Matter Experts) defines the scope of each of the Subject Areas for their organization, reviews the definition of the Subject Area and adds any detail that will be helpful in developing the documentation for this Subject Area. The Reviewers, in the evaluation of the Subject Areas, examine the scope to assure that there is no overlap or duplication of Subject Areas.

Identify Information Subject Area Owners/Stewards – Information gathered or produced for business purposes cannot be "owned" by a single individual or Line of Business unit within the State; however, individuals have accountability for the creation and management of the information. These responsible individuals need to be identified so that the accurate information data elements, concepts and process information can be documented for each subject area.

Select Initial Information Subject Areas for Documentation - Once the Information Subject Areas have been identified; the Advisors prioritize the subject areas to determine the most crucial candidate for initial documentation. Considerations in the selection process include the need for information exchange or information sharing, support of the Business Drivers, and any subject area that is a source of Metadata definitions. The specific circumstances of each enterprise such as legislative mandates, federal regulation, budgetary constraints, competing resources, organizational readiness, pain points, and delivery timeframes will all be additional considerations.

Conduct Information Architecture Work Sessions

PROCESS OVERVIEW

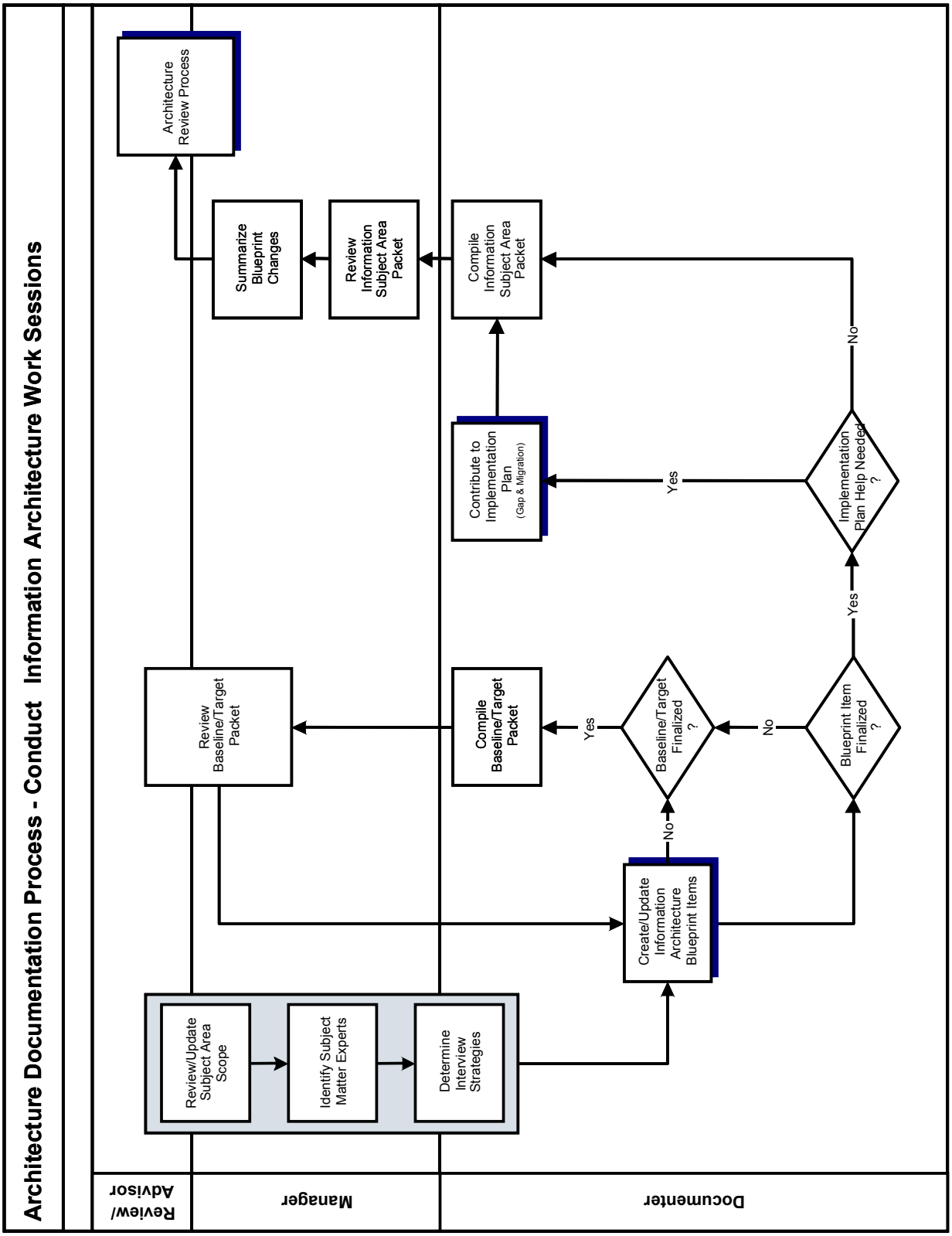
The Information Architecture work sessions are intended to produce the documentation that initially populates the Information Architecture Blueprint. Ongoing Documenter meetings are required to maintain the vitality of the Information Architecture Blueprint. The first session will include:

- Defining roles and responsibilities
- Reviewing architecture blueprint documentation requirements
- Determining expectations of on-going meetings

After the first meeting, on-going working sessions are triggered from Architecture Lifecycle Processes, including:

- Architecture Review Process
- Architecture Compliance Process
- Architecture Blueprint Vitality Process.

The creation of diagrams for the Information Architecture components provides a pictorial view for identification of the organization's information needs. Analyzing the various pieces within the enterprise facilitates the process of articulating the foundation of the architecture. Individual components can be more easily defined and will enable better communication of the information concepts. The relationships between various pieces can also be built into summary level views.


Architecture Documentation Process - Conduct Information Architecture Work Sessions
Reviewer/ Advisor
Manager
Documenter
Review/Update Subject Area Scope
Identify Subject Matter Experts
Determine Interview Strategies
Review Baseline/Target Packet
Compile Baseline/Target Packet
Baseline/Target Finalized ?
Yes
No
Create/Update Information Architecture Blueprint Items
Blueprint Item Finalized ?
Yes
No
Implementation Plan Help Needed ?
Yes
No
Contribute to Implementation Plan (Gap & Migration)
Compile Information Subject Area Packet
Review Information Subject Area Packet
Summarize Blueprint Changes
Architecture Review Process

PROCESS DETAIL

Review/Update Subject Area Scope - The basic definition of each Subject Area, as defined in the Initiate Information Architecture process, is provided to the Advisors/Reviewers. The Documenters will update the definition as necessary and identify parameters for setting boundaries within the Subject Area. In this process, the scope of the individual efforts for further developing the Information Architecture Components can also be defined in greater detail.

Identify Subject Matter Experts – In this process, experts in a particular segment of the business are determined. Based on the subject area scope, Subject Matter Experts that understand the functional/topical areas are identified. These individuals include the Subject Area Experts, Information Owners and Information Stewards.

Determine Interview Strategies – Interview meeting topics should be determined in one of the first working sessions. Interview questions should to be designed to streamline the interview process and get the most information in minimum time. Interview questions should address the six interrogatives from the Zachman Framework.[9] These interrogatives are who, what, where, when, why and how.

The following provide several ways to determine interview strategy:

- Based on Business Processes. An example of this is documenting the process activities of the various components around inventory from ordering to consumption. Show the creation, utilization, and obsolescence of a given information asset. This can aid in capturing information components such as process flows with additional information about data usage and location.
- Based on a specific information asset. An example of an information asset is "Customer." This can be used to capture the details concerning the Data Element/Concept component such as industry descriptors and security classifications.
- Based on documenting the baseline activities followed directly with the target activities, for a given topic. Often the ability to stay on the same topic in a given timeframe assists in capturing the information around that topic, both where the business is today and where the business wants to be tomorrow. This can really help keep the creativity rolling without starting and stopping based on baseline and target.

Create/Update Information Architecture Blueprint Items – The Blueprint items include both the process and information components being developed. In developing these components the following blueprint items can be created:

- Diagrams
- Information Meta Component details
- Process Component details
- Matrices

A separate process diagram and narrative for this sub-process will provide greater detail (See *Create/Update Information Architecture Blueprint Items*).

[9] Zachman Framework, www.zifa.com

Compile Baseline/Target Packet, Review Baseline/Target Packet – At the completion of Baseline, and again at the completion of the Target, a packet containing the documentation should be complied and sent for review. This is beneficial to the documentation process as it allows feedback from the perspective of the Manager, Reviewers and Advisors at strategic points throughout the documentation process.

Contribute to Implementation Plan – After the Blueprint items have been finalized, Documenters will also contribute to the Implementation Plan if needed. Contributions include completing the detail for the Gap Components, performing a Gap Analysis, developing Migrations Strategies, and creating a summary of Gap and Migration results.

A copy of the Gap Component template, narrative for capturing the gap detail, and a sample of the template with completed Gap Component Blueprint detail can be found in the Business Architecture section. (See *Business Architecture - Gap Component Template* and *Business Architecture Blueprint Samples – Gap Component).*

Compile Information Subject Area Packet – A packet containing the completed Blueprint documentation will be compiled in preparation for formal review.

If the Gap Analysis and Migration Strategies have been completed, the detail that was compiled into the Architecture Summary document will also be included in the Information Subject Area Packet.

Review Information Subject Area Packet – The Information Architecture Manager will verify the contents of the Information Subject Area Packet and work with the Documenters to make modifications as necessary.

Summarize Blueprint Changes – After contents of the packet are verified, the IA Manager will summarize any changes that have been made to the Information Architecture Blueprint for tracking purposes and forward the packet to the reviewers for the formal Architecture Review Process.

Architecture Review Process – The packet is either accepted into the architecture or rejected by the IA governing bodies.

Create/Update Information Architecture Blueprint Items

PROCESS OVERVIEW

The Information Architecture Blueprint items consist of the Process Components and the Information Meta Components; the diagrams on which the various components and their relationships are illustrated; various matrices that show the associations between the Information Architecture Components, and the other Components in the Enterprise Architecture Blueprint.

Information Architecture Components refer to the individual elements that are documented as part of the Information Architecture Blueprint (i.e. Process Components and Information Meta Components). Information Architecture Components specifically identify what process, information, business rules, and organizational roles/responsibilities will be used for implementation of the Information Subject Area.

Information Architecture Components are identified during the Information Architecture interview process and documented within each of the subject areas as appropriate. The Information Architecture

Documenters, along with the Subject Matter Experts who are not already part of the documentation team, determine the information to be documented as Information Architecture Components. Within the documentation, references that identify relationships to other Information Architecture Components are also documented.

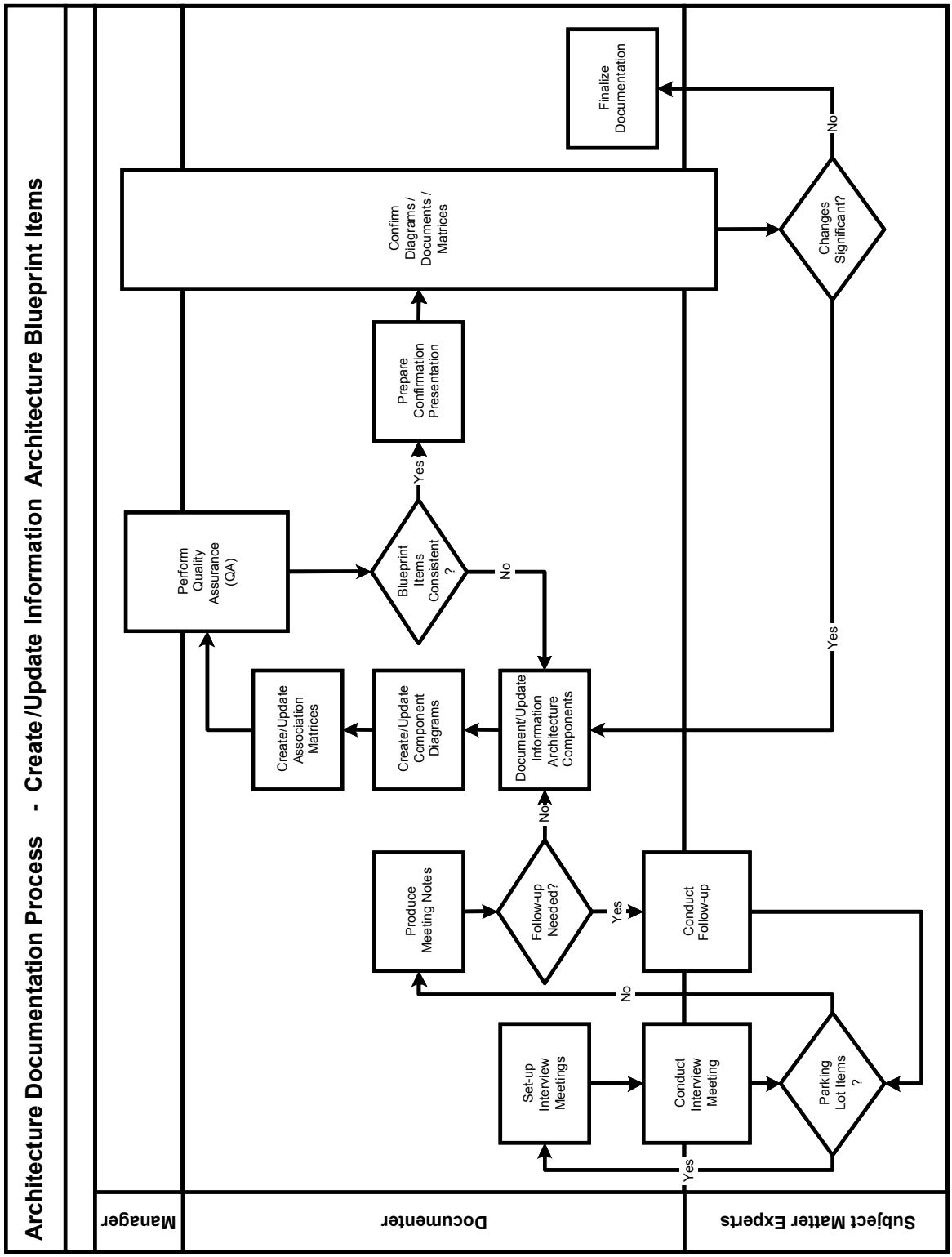
The Information Architecture Process Components perspective will encompass items that answer the following questions:

- *How are the information assets used by the business and in which processes?*
- *Who executes those processes?*
- *Where are those processes executed?*
- *When are the processes used, and in which business cycle?*
- *Why are the processes important to the business?*

The Information Architecture Meta Components perspective will cover items that answer the following questions:

- *What information is vital to the business*?
- *Who owns/stewards the information asset?*
- *Who uses the information assets?*
- *Where are the information assets captured and stored?*
- *What are the business rules for the information asset?*
- *What is the security classification of the information asset?*

IA Components address the various information assets and processes of the business. They identify the information assets and processes that are critical for information exchange.


Architecture Documentation Process - Create/Update Information Architecture Blueprint Items
Manager
Documenter
Subject Matter Experts
Set-up Interview Meetings
Conduct Interview Meeting
Parking Lot Items ?
Yes
No
Produce Meeting Notes
Follow-up Needed?
Yes
No
Conduct Follow-up
Document/Update Information Architecture Components
Create/Update Component Diagrams
Create/Update Association Matrices
Perform Quality Assurance (QA)
Blueprint Items Consistent ?
Yes
No
Prepare Confirmation Presentation
Confirm Diagrams / Documents / Matrices
Changes Significant?
Yes
No
Finalize Documentation

PROCESS DETAIL

Set-up Interview Meetings – Once the subject matter experts that are not already part of the documentation team have been identified and the interview strategy has been determined, the Interview meetings can be scheduled. Allow at least two hours per session. No more than two sessions should be set up in the same day to allow Subject Matter Experts attending both sessions to have a break from this style of overarching thinking.

Conduct Interview Meeting – Meetings are typically organized around a specific topic within the subject area scope. The topics were determined during the interview strategy session, which typically happens in one of the first working sessions. At times new topics will surface during the interviews. These should be aligned to the original strategy to assure that all aspects of this topic are addressed in the interviews.

Although everyone will be involved in the interviews from a general view, it helps to give each interviewer an area of focus based on the perspectives of Who, What, Where, When, Why and How. Before the interviews, each interviewer should plan questions based on their assigned perspective. This will help to ensure the coverage of all aspects. It is also helpful to have a separate individual assigned as a scribe. This will allow the interviewers to focus their attention primarily on the interviewing process and less on taking notes.

It is very important that everyone understands that all participants of the interviews are equal. All opinions are valid and important. During the interview is not the time to establish priorities. These interviews are designed to gather and document all viewpoints.

Besides gathering detail from the perspective of the six interrogatives as stated earlier, another useful interview strategy is, for each information component relationship or process that is identified during the interviews, to ask questions that will identify the Supplier, Input Information, Output Information and Customer (SIPOC[10]). This will ensure the appropriate mapping of Process Component to Information Meta Components.

Produce Meeting Notes – Knowledge of who participated in providing the subject matter is very useful. During the interview sessions, Subject Matter Experts or various architecture participants may be asked to follow up with action items or to share documentation and research on specific items. For this reason, notes of these meetings should be taken, reproduced and distributed as with any other formal meeting. Parking lot issues or unresolved items often result during interview meetings. These items need to be compiled, returned to the interviewee for feedback and documented in the interview strategies or in the summary documentation.

Conduct Follow-up – Following interview meetings with subject matter experts, some items may require resolution or additional action. These activities may include, but are not limited to, the following:

- *Changes to Interview Strategy:* Based on interview feedback, the approach and/or strategy of Subject Matter Expert interviews may be changed
- *Resolution of Items:* Dissention or ambiguity may necessitate resolution and/or direction from Architecture Subject Matter Experts, Executives, the IA Manager or Reviewers

[10] SIPOC is a tool used in the Six Sigma methodology. It was originated by Deming & Scholtes.

- *Clarification:* The Documenters may need additional information on a topic
- *Parking Lot Items:* Items that are currently out of the defined scope, but have been identified as potentially requiring future action, should be documented and submitted to the IA Manager.

Document/Update Information Architecture Components – The Documenters capture detail about each of the Information Architecture components such as keywords, critical references, stakeholders and security classifications. The Process Component and Information Meta Component Templates provided at the end of this section are forms that can be used for documenting this detail. See *Process Component Template and Information Meta Component Template.*

Static components (Information Meta Components) and dynamic components (Process Components) are tightly integrated with one another. These components, which are mutually dependent, determine, guide and validate each other. The Process Components provide the process flow, definitions and dynamic business rules The Information Meta Components provide entity definitions, relationships and structural business rules. Table 2 describes the relationships between Process Components and Information Meta Components. This tight integration of purpose for the Process and Information Meta Components guides the NASCIO approach for developing Information Architecture.

Table 2. Process Components and Information Meta Components Relationships

Process Component → Information Meta Component	*Information Meta Component → Process Component*
• Sets the scope of the processing required. • Helps identify the entities in the information component. • The context of the process component helps create the entity definitions. • Iteration in the process may help define cardinality, e.g., one-to-many relationship. • The semantics of the process definition may provide the reasoning behind a relationship. • The sequence of transaction steps identifies existence dependencies for the entity relationships.	• Sets the scope of the information required. • Information component relationships help identify processes. • The context of the information component helps define prerequisites. • Cardinality on relationships may imply the need for iteration in a process. • The data element concept definitions may help clarify the need for a process, and provide a single name and meaning for words in the process definitions.

The Documenters, working with the SMEs capture the Process Component detail**.**

The Information Meta Components, which refer to descriptive information about data, projects, models and multimedia products, are defined by the business SMEs who are most familiar with the business information needs. The Documenters, working with the SMEs capture the Information Meta Component detail**.** The Information Meta Components include, but are not limited to, directories, catalogues, catalogue methods, and dictionaries.

Generally, the 20-year rule, proposed by the National Research Council's Committee on Geophysical Data, has been the major guideline in the development and use of Information Meta Components. The 20-year rule states, "Will someone 20 years from now, not familiar with the data or how it was obtained, be able to find data sets of interest and then fully understand and use the data solely with the aid of the documentation archived with the data set?"

Note that although the components may be used on multiple diagrams and matrices, the detail for each component is documented only once.

Create/Update Component Diagrams - The documenters will place Information Architecture Components on various diagrams to show the flows and relationships. These diagrams should depict the entities, relationships and attributes. Modeling at this stage must maintain a logical level of abstraction and is intended to develop a business information model. Each organization should determine the diagramming technique they are going to use. These diagrams can include, but are not limited to:

- Conceptual ERD / Conceptual Class Diagram
- Data Flow diagram
- IDEF
- State transition
- Process mapping – on flows in process mapping.

Compliance with the organization's modeling standards should be maintained. Logical models may later be translated into physical models that will be used for the solution designs.

Create/Update Association Matrices – As part of the documentation, associations between the information architecture components can be created in the form of matrices. Coordination with the other modelers/documenters should occur so that all components for a specific Information Subject Area are included in the matrices. The process and metadata perspectives should be reviewed to make certain that nothing is missing or incorrectly represented (i.e. ensure that there is no process that utilizes information prior to it being created, and there is no information that is created and never utilized.).

Examples can include:

- Processes that have no corresponding data element/concepts
- Information that has no association with Business Processes
- Information that has no organization/role that utilizes it
- Processes that have no business function they are fulfilling.

Perform Quality Assurance (QA) – The various information architecture documents, models, and matrices require verification by the architecture team prior to confirming them with the Subject Matter Experts. This quality assurance step allows the team to verify that the various information components are utilizing the same lexicon of terms and that the team's understanding of the various components of the information architecture is the same. The team will also verify that the process flows are correct so that information is created prior to being utilized and that all created information is utilized.

Prepare Confirmation Presentation – The Documenters will compile the information from the meeting notes, the documented components, diagrams and associations matrices, and the quality assurance check. The information will be utilized to confirm the accuracy of the information captured and update the various pieces of information to take to the Subject Matter Experts. A summary agenda of the presentation details will aid comprehension of the numerous documents produced. The Documenters need to determine which documents are of most importance for review in a formal meeting and which can be sent-out for review and comments.

Confirm Diagrams/Documents/Matrices – Once the architecture team has verified consistency in how they are defining and representing the various information components, the team will confirm the

models/documents/matrices with the Subject Matter Experts. This should be an interactive session where modifications and enhancements are denoted. Some of the changes can happen right in the session; others take more time and will be conducted in "pick-ups" after the session. If the changes to the models/documentation/ matrices happen outside the session, an electronic copy of the changes should be sent for approval. If the changes were significant, the potential exists to call another meeting to confirm those changes as well.

Finalize Documentation – When the component information has been confirmed, update the status and audit trail detail. The final step is to submit all Information Architecture Component information for inclusion in the Information Architecture documentation.

Process Component Template

TEMPLATE OVERVIEW

Information Architecture Process Components include the definition and gap identification for specific Process Components. The Documenters, along with the Subject Matter Experts, determine the information applicability to the overall architecture effort that will be included in these components. Each Information Architecture Process Component reviewed, whether accepted or rejected, will be documented using this Process Component Template.

The Process Component Template provides an instrument for documenting the Process Component details in an electronic format. The visual representation of the Process Component Template, provided on the following page, is followed by a detailed description of the contents to be captured.

Important items to keep in mind when addressing Process Components are:

- Documentation of the business processes should never go to the procedural or individual person's "desk level".

  If the documentation goes to that level of detail, the documentation has moved from process documentation into procedural documentation. Procedural documentation is too low of a level for an Enterprise Architecture effort. Procedures can be referenced from within the documentation of a process, but the actual procedure should not be included as part of the Information Architecture Blueprint.

- Utilizing a standard of Verb-Noun for naming process steps aids in readability and consistency.

  Example: Capture Licensee Address

  The use of Verb-Noun convention keeps the process/activity step names consistent and easy to read. It can also help to prevent process steps from spanning beyond a single process activity/step.

- The Information Architecture Blueprint is a "living" document.

  A documented process should be confirmed and validated as it is implemented. Changes will occur, and should be documented to correctly reflect the current implementation of the business process.

Process Component

Definition	
Name	
Description	
Rationale	
Benefits	
Component Classification	
Classification	☐ *Baseline* ☐ *Target*
Related Domain / Subject Area	
Business Domain	
Information Subject Area	
Keywords	
Keywords/Aliases	
Process component Type	
Component Type	☐ *Process* ☐ *Process Step*
Process Identifier	
Component Deliverable	

Business Rules		
Owner	*Classification*	*Rule Statement*
	☐ *Baseline* ☐ *Target*	
	☐ *Baseline* ☐ *Target*	

Critical References			
Related Business Components			
Business Architecture Component	*Relationship*	*Business Architecture Component*	*Relationship*
Related Information Components			
Supplier	*Input Information Component*	*Output Information Component*	*Customer*

Stakeholders/Roles			
Stakeholders			
Roles			
Reason for Stake			
RELATED GAP COMPONENT			
Gap Components			
CURRENT STATUS			
Process Component Status	☐ *In Development* ☐ *Under Review* ☐ *Accepted* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date		*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Updated by			
Reason for Update			

TEMPLATE DETAIL

Definition

Name – Provide the name for the Process. This is typically in verb-noun format.

Description – Document the description of the Process Component in a paragraph or two that provides sufficient clarity to the reader about the component.

Rationale – Document a paragraph or two containing the reason or basis for this Process Component being included within the architecture.

Benefits – Document a paragraph or bulleted statements that provide the benefits associated with the Process Component.

Component Classification

Classification - Provide the classification for the Process Component:

- *Baseline:* The "as is" or "current" state of the component within the enterprise. Baseline indicates the component exists within the enterprise today.
- *Target:* The "to be" or "proposed" state of the component within the enterprise. Target indicates the component should be included or added to the enterprise within a certain scope and timeframe.

Related Domain / Subject Area

Business Domain/Information Subject Area – List the Business Domain or Information Subject Area to which this process belongs. This will ensure the appropriate mapping of Process Component to Business Domain or Information Subject Area.

Keywords / Alias

Keywords/Aliases - List any keywords/alias that can be used to assist in searching the Enterprise Repository for these Process Components. This information will be helpful for anyone that is looking for similar Process Components (i.e. What else is this known as?).

Process Component Type

Component Type – Provide the component type: process or process step component.

Process Identifier – List the process step number or other identifier that indicates the order of the process steps. This information is necessary to provide a link between this supporting detail and the process box on the diagram. There are various numbering schemes that can be used. For example, ISO provides numbering standards. Each enterprise should use the numbering scheme that best suits their environment.

Component Deliverable – To determine the Component Deliverable ask questions such as:

- What does this process produce?
- What is the end product of this process?

Business Rules

When defining the business rules, utilize "rule words," such as:

- Must or Should
- Not
- No
- Only if

Owner – List which business unit is responsible for this business rule.

Classification – Provide the classification for the business rule specifying whether the rule exists today or is proposed for the future.

- *Baseline:* The "as is" or "current" state of the component within the enterprise. Baseline indicates the component exists within the enterprise today.
- *Target:* The "to be" or "proposed" state of the component within the enterprise. Target indicates the component should be included or added to the enterprise within a certain scope and timeframe.

Rule Statement – Provide a statement that defines, constrains, asserts business structure, controls or influences the behavior of the Process Component.

Critical References

This section is documented for any Business or Information Component that is related to this Process Component.

Business Architecture Component – Provide the names of each Business Component that this Process Component is related to. This will ensure the appropriate mapping of Process Component to Business Components.

Relationship – Provide a brief description of the relationship to this specific Process Component.

Related Information Components– For each information component relationship, provide the Supplier, Input Information Component, Output Information Component and Customer (SIPOC[11]). This will ensure the appropriate mapping of Process Component to Information Meta Components.

Stakeholder Information

To identify stakeholders, use questions such as:

- Who is directly impacted by this component or a change to this component?
- Who may have to change the way they do business?
- Who may benefit by the change?

Stakeholders – Provide a list of stakeholders for this Process Component. Stakeholders are those who are affected by or will have an effect on the Process Component. If stakeholder title is not known, provide a description of the role the person or group performs in the Roles section. Stakeholders are typically agencies, departments, etc.

Roles – This section provides a place to present the roles and/or responsibilities for this Process Component. This is especially helpful when a title for the stakeholder is not known. Roles ensure the

[11] SIPOC is a tool used in the Six Sigma methodology. It was originated by Deming & Scholtes.

accountability for all Process Components, ensuring that all stakes in the component are documented when interviewing the Subject Matter Experts. Examples of roles could include Project Manager or Planner, etc.

Roles can also show IT stakeholders that utilize this information, which will provide better service and alignment to the business needs.

Reason for Stake – This optional section provides a place to note the reason that the stakeholder or role has a vested interest in this Process Component. This is helpful when the reason is not apparent or there are specific circumstances that should be noted. Consideration should be given to the interest of the stakeholder and not only to management, for often the same question posed to these groups results in different responses. The information presented here should clarify the relationship of the stakeholders.

Related Gap Component

This section is documented for any Information Architecture Process Component that will be impacted by the move from baseline to target. If nothing will change, the gap statement can just enter a phrase such as "No Gap".

Gap Components – As gaps are identified, list the Gap Components for this Information Architecture Process Component. The Gap Component Template will be used to document the gaps that exist between this Information Architecture Process Component and other Information Architecture Process Component, as well as Impact Statements and Migration Strategies . The gap can be documented from the following perspectives:

- From the perspective of the baseline Information Architecture Process Component that is being updated, replaced or removed when migrating to the target.
- From the perspective of the target Information Architecture Process Component that is being added to replaced or enhanced when migrating from the existing baseline.

Current Status

Document the status of Information Architecture Process Component, indicating whether the component is in development, under review, accepted, or rejected.

- *In Development* – The architecture team is currently drafting and/or reviewing the Process Component content.
- *Under Review* – The architecture team has completed the Process Component documentation and has submitted the documentation to the governing body for inclusion into the architecture
- *Accepted* – The completed Process Component documentation has been approved by the EA governing body and the content is an official part of the architecture. Once accepted into the architecture, the content is referred to as the Blueprint
- *Rejected* – The blueprint has been rejected by the governing body for reasons documented below in the Audit Trail section.

Audit Trail

Creation Date – Provide the date the Information Architecture Process Component was created.

Created By – List all individuals and their titles that helped in the creation of this Process Component.

Date Accepted/Rejected – Provide the date the Information Architecture Process Component was accepted into the architecture or rejected.

Reason for Rejection – If the Information Architecture Process Component was rejected, document the reason for the rejection.

Last Date Reviewed – Document the most recent date the Information Architecture Process Component was taken through the Architecture Vitality Process.

Last Date Updated – Document the most recent date that any item in the Information Architecture Process Component documentation was changed.

Updated By – List all individuals and their titles that helped in the update of this Information Architecture Process Component.

Reason for Update – Document the reason for the update to the Information Architecture Process Component.

Information Meta Component Template

TEMPLATE OVERVIEW

Information Architecture Meta Components include the definition and gap identification for specific metadata components. The Documenters, along with the Subject Matter Experts, determine the information applicability to the overall architecture effort that will be included in these components. Each Information Architecture Meta Component reviewed, whether accepted or rejected, will be documented using this Information Meta Component Template.

The Information Meta Component Template provides an instrument for documenting the Information Meta Component details in an electronic format. The visual representation of the Information Meta Component Template, provided on the following page, is followed by a detailed description of the contents to be captured.

Important items to keep in mind when addressing Information Meta Components are:

- It is not necessary to capture the metadata for every piece of information within the enterprise.

  Metadata can be captured for all information within an enterprise. However, as with everything in Enterprise Architecture, it is important to keep in mind the value of capturing the detail versus the cost of capturing and maintaining that information.

  For metadata on information that is not highly secured or used throughout the cross functional groups within the enterprise, the value of the metadata may not outweigh the cost of collecting, capturing and maintaining it.

- Information exchanges and analytical information are good areas of focus.

  As noted in the reference to the JIEM tool, it is the information exchanges and the analytical information that need the attention to detail in the metadata documentation effort. It is these pieces of information that will cost the enterprise the most if data is not clearly defined and data quality is not maintained.

Information Meta Component

PART 1 – CONCEPTUAL CONTENT *(Data Element/Data Element Concept[12])*	
DEFINITION	
Name	
Industry Description	
Industry Description Provider	
Description	
Rationale	
Benefits	
COMPONENT CLASSIFICATION	
Classification	☐ *Baseline* ☐ *Target*

CRITICAL REFERENCES	
Data Element/Concept	*Relationship*
Process Component	*Relationship*
Application	*Relationship*
Conceptual Information Model	*Link or Identifier*

STAKEHOLDER DETAIL	
Stakeholders	*Reason for Stake*

[12] ISO/IEC 11179-1:1999(E)

INFORMATION SECURITY CLASSIFICATION			
Security Classification			
KEYWORDS			
Keywords / Alias			
VALID VALUES / EXAMPLES			
Valid Values			
Examples of the Data Element/Concept			
BUSINESS RULES			
Owner	*Classification*	*Rule Statement*	
	☐ *Baseline* ☐ *Target*		
	☐ *Baseline* ☐ *Target*		
	☐ *Baseline* ☐ *Target*		
	☐ *Baseline* ☐ *Target*		
CURRENT STATUS			
Data Element/Concept Status	☐ *In Development*	☐ *Under Review*	☐ *Accepted* ☐ *Rejected*
CONCEPT SECTION AUDIT TRAIL			
Creation Date		*Date Accepted / Rejected*	
Created by			
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Updated by			
Reason for Update			

PART 2 – LOGICAL AND PHYSICAL CONTENT (LOGICAL CONTENT)	
ENTITY/CLASS DEFINITION	
Entity/Class Name	
Description	
Source Name	
Source Type	

Critical References	
Logical Information Model	*Link or Identifier*

Related Attributes					
Attribute Name	*Attribute Description*	*Sample Data*	*Representation Class*	*Information Security Classification*	*Information Security Rules*

Relationships					
Relationship Name	*Entity/Class Name (1)*	*Relationship*	*Cardinality*	*Entity/Class Name (2)*	*Relationship Description*

PART 2 – LOGICAL AND PHYSICAL CONTENT (PHYSICAL CONTENT) (Data Dictionary Section)	
TABLE / CONTENT / DOCUMENT DEFINITION	
Table Name/ Content Location	
Description	
Source Name	
Source Type	

Related Columns				
Document Name /Column Name	*Associated Attribute*	*Column Data Type / Length*	*Column Null Indicator*	*Column Comment*

CURRENT STATUS					
Logical/Physical Content Status	☐ *In Development*	☐ *Under Review*	☐ *Accepted*	☐ *Rejected*	
INFORMATION ARCHITECTURE AUDIT TRAIL					
Creation Date		*Date Accepted / Rejected*			
Created by					
Reason for Rejection					
Last Date Reviewed		*Last Date Updated*			
Updated by					
Reason for Update					

TEMPLATE DETAIL

Because the method of capturing the Data Elements/Concepts will vary from organization to organization, this template is designed so that it can be used as two separate templates if that is better suited to the style of an organization. It is up to the discretion of the Documenters in collaboration with their Advisors and Managers to decide the best approach for their organization.

Part 1 of the Information Meta Component Template is designed to capture the business or conceptual view of the Enterprise's information. Part 2 is designed to capture the Logical and Physical views of the information. The conceptual and logical data models must be developed in partnership with the SMEs. Their understanding of the business information, and rules must be fully leveraged in the development of conceptual and logical model. The template is designed for the capture of both structured and unstructured information.

TEMPLATE PART 1 – CONCEPTUAL CONTENT

Definition

Name – Provide the name for Data Element/Data Element Concept.

Industry Description – For Data Elements/Concepts that are industry standards provide the Industry Description. This is optional. If the Data Element/Concept is not an Industry standard, leave this blank and provide the enterprise description under Description.

Industry Description Provider – For Data Element/Concepts that have an industry description provide the group/organization/standards body that provided the description. This is required if Industry Description is provided.

Description – Document the enterprise's description of the Data Element/Concept in a paragraph or two that provides sufficient clarity to the reader about the concept. This is required if no Industry Description was provided.

Rationale – Document a paragraph or two containing the reason or basis for this Data Element/Concept being included within the architecture.

Benefits – Document a paragraph or bulleted statements that provide the benefits associated with the Data Element/Concept.

Component Classification

Classification - Provide the classification for the component:

- *Baseline:* The "as is" or "current" state of the component within the enterprise. Baseline indicates the component exists within the enterprise today.
- *Target:* The "to be" or "proposed" state of the component within the enterprise. Target indicates the component should be included or added to the enterprise within a certain scope and timeframe.

Critical References

Data Element/Concept – List all other Data Element/Concepts to which this Data Element or Data Element Concept is related. For each related Data Element/Concept, provide a brief description of the relationship to this specific Data Element/Concept.

Process Component – Provide the names of each process that this Data Element/Concept is related to. Providing this information will ensure the appropriate mapping of the Information Meta Component to Process Component.

Application – Provide the names of each application that this Data Element/Concept is related to and the relationship. This will ensure the appropriate mapping of the Information Meta Component to Application.

The references listed above are research references only, and are used in identifying items that may need to be escalated to review during gap analysis and migration strategies.

Conceptual Information Model – Provide the names of the Conceptual Information Models on which this Data Element/Concept appears and a link or identifier to indicate where the model can be found.

Stakeholder Detail

To identify stakeholders, use questions such as:

- Who is directly impacted by this component or a change to this component?
- Who may have to change the way they do business?
- Who may benefit financially?

Stakeholders – Provide a list of stakeholders for this Data Element/Concept. Stakeholders are those who are affected by or will have an effect on the Data Element/Concept. Stakeholders are typically agencies, departments, owners, stewards, custodians, etc.

If stakeholder title is not known, provide a description of the role the person or group performs. Roles ensure the accountability for all Data Elements/Concepts, ensuring that all stakes are documented when interviewing the Subject Matter Experts. Roles can also show IT stakeholders that utilize this information, which will provide better service and alignment to the business needs. Examples of roles could include Project Manager or Planner, etc.

Reason for Stake – This optional section provides a place to note the reason that the stakeholder or role has a vested interest in this Information Meta Component. This is helpful when the reason is not apparent or there are specific circumstances that should be noted. Consideration should be given to the interest of the stakeholder and not only to management, for often the same question posed to these groups results in different responses. The information presented here should clarify the relationship of the stakeholders. Please note a stakeholder can have more than one type of stake.

- **Owner -** Originator of the Data Element/Concept and has ultimate responsibility for the definition of the concept.
  - Enforcing the information policies and procedures developed by the Stewards
  - Ensuring the quality of the Data Element Concept.
  - Determining the Security Classification for the Data Element/Concept (who can have access to the Data Element/Concept and the type of access.).
- **Steward –** Responsible for data content.
  - Establishing attributes
  - Ensuring appropriate usage of the data within the rules established by the owner
  - Given the constraints of the owners, the steward can manage the data for the use they need
  - Communicating and verifying new uses for and changes to the data with the data owner
  - Using and managing data in a practical manner.

- **Custodian -** Responsible for assuring integrity of the data captured, for proper handling of data, (not the content), and assures the data is available when needed,:
  - Day to day management of the data
  - The proper handling of the data
  - Ensuring availability, backup, etc
- **Other Stakeholders** - Provide the type of stake and a sentence explaining the stake that the stakeholder / role have in this Data Element Concept. Stake types include:
  - Interested In -Reviews or makes decisions based on the information
  - Authorized to - Creates / Maintains the information
  - Works with - Uses the information to perform activities in their jobs.

Information Security Classification

Security Classification - Provide the Information Security Classification for this Data Element/Concept Each enterprise will use their own agency standards for the classification scheme that will be used to define an appropriate set of protection levels. A typical scheme would have the following classifications:

- Secret
- Confidential
- Sensitive
- Internal Use Only
- Public

Keywords

Keywords/Alias - List any keywords/alias that can be used to assist in searching the Enterprise Repository for these Data Elements/Concepts. This information will be helpful for anyone that is looking for information on similar Data Element/Concepts, i.e. "What else is this known as?"

Valid Values / Examples

Valid Values – If only a specific list of values is acceptable, please list them, or refer to the source of the list of values, i.e. List of Valid State Abbreviations.

Examples of the Data Element/Concept – Provide examples of the Data Element/Concept to aid in clarifying this specific Data Element/Concept from another. For example, if using a Data Element/Concept such as "External Organization", a Valid Value might be "Banks" and an example would be "US Bank".

Business Rules

When defining the business rules, utilize "rule words," such as:

- Must or Should
- Not
- No
- Only if

Owner – List which business unit is responsible for this business rule.

Classification – Provide the classification for the business rule specifying whether the rule exists today or is proposed for the future.

- *Baseline:* The "as is" or "current" state of the component within the enterprise. Baseline indicates the component exists within the enterprise today.
- *Target:* The "to be" or "proposed" state of the component within the enterprise. Target indicates the component should be included or added to the enterprise within a certain scope and timeframe.

Rule Statement – Provide a statement that defines, constrains, asserts business structure, controls or influences the behavior of the Data Element/Concept.

Current Status

Document the status of Data Element/Concept, indicating whether the component is in development, under review, accepted, or rejected.

- *In Development* – The architecture team is currently drafting and/or reviewing the Data Element/Concept content.
- *Under Review* – The architecture team has completed the Data Element/Concept documentation and has submitted the documentation to the governing body for inclusion into the architecture.
- *Accepted* – The completed Data Element/Concept documentation has been approved by the EA governing body and the content is an official part of the architecture. Once accepted into the architecture, the content is referred to as the Blueprint.
- *Rejected* – The Data Element/Concept has been rejected by the governing body for reasons documented below in the Audit Trail section.

Concept Section Audit Trail

Creation Date – Provide the date the Data Element/Concept was created.

Created By – List all individuals and their titles that helped in the creation of this Data Element/Concept.

Date Accepted/Rejected – Provide the date the Data Element/Concept was accepted into the architecture or rejected.

Reason for Rejection – If the Data Element/Concept was rejected, document the reason for the rejection.

Last Date Reviewed – Document the most recent date the Data Element/Concept was taken through the Architecture Vitality Process.

Last Date Updated – Document the most recent date that any item in the Data Element/Concept documentation was changed.

Updated By – List all individuals and their titles that helped in the update of this Data Element/Concept.

Reason for Update – Document the reason for the update to the Data Element/Concept.

TEMPLATE PART 2 – LOGICAL AND PHYSICAL CONTENT

This part of the template is used only for baseline and, during the Solution Architecture, for development of a target solution.

Entity/Class Definition

Repeat as many times as there are entities.

Entity/Class Name – Provide a unique name for the Entity/Class.

Description – Document the Enterprises' description of the Entity in a paragraph or two that provides sufficient clarity to reader about the Entity.

Source Name – The logical source of this entity / attribute where the Entity is related.

Source Type – Provide a statement as to where the entity originated, is utilized, or is the source of authority.

Critical References

Logical Information Model – Provide the names of the Logical Information Models on which this Data Element/Concept appears and a link or identifier to indicate where the model can be found.

Related Attributes

Attribute Name – Provide the attributes for the Entity.

Attribute Description – Provide a description of each attribute .

Sample Data – Provide examples of the information that will be in each attribute.

Representation Class – Provide the representation category - includes data type and size

Information Security Classification – Provide the classification scheme that will be used to define an appropriate set of protection levels.

- Secret
- Confidential
- Sensitive
- Internal Use Only
- Public

Information Security Rules – Provide rules stating when the Information Security Classification needs to be implemented, e.g. when this attribute is combined with other attributes, then it is classified.

Relationships

Each relationship will be documented from two perspectives. For example, documenting a relationship between a manager and an employee would include documentation from the manager perspective as well as from the employee perspective.
Example: Manager employs one or more employees. Employee is employed by one or more managers.

Relationship Name – Provide a name for the relationship to be used as a reference, in the form of Entity/Class1.Entity/Class2.

Example: Manager.Employee

Provide the following for each perspective:

- **Entity/Class Name (1)** – Provide the name of the first entity/class.
- **Relationship** – Provide the relationship between the two entities. The relationship is indicated by use of a verb or verb form (i.e. "employs", "is employed by", etc.)
- **Cardinality** – Provide the rule for the number of instances of the neighbor entity that is related to a single instance of the first entity. Expressed as :

  1:1 - for one instance of the first entity, there is a maximum of one instance of the second entity

  1:M - for one instance of the first entity, there can be many instances of the second entity

  M:M there are many instances of the first entity that have a relationship with many instances of the second entity

- **Entity/Class Name (2)** – Provide the name of the related (neighbor) entity/class.
- **Relationship Definition** – Provide the definition of the relationship in a paragraph or two that provides sufficient clarity regarding the purpose and nature of the relationship.

Table / Content / Document Definition

Repeat as many times as there are tables.

Table Name/Content Location – Provide a unique name for the table, document or content location.

Description – Document the Enterprise's description of the table in a paragraph or two that provides sufficient clarity to the reader about the table.

Source Name – provide the physical source of this table.

Source Type – Provide a statement as to where the entity originated, is utilized, or is the source of authority.

Related Columns

Document Name/Column Name – Unique name of the column as created on this table.

Associated Attribute – Provide a description of each attribute.

Column Data Type / Length – Provide the data type and length for this column. If this is unstructured data (i.e. jpeg, video, etc) note where content or analytic can be found. (E.g. Doc management tool, or an OLAP system)

Column Null Indicator – Please indicate if a record in this table can be created with this column set to "null" (i.e. Optional).

Column Comment – Provide any further information to help clarify the definition / use of this column.

Current Status

Document the status of the Logical/Physical Content, indicating whether the component is in development, under review, accepted, or rejected.

- *In Development* – The architecture team is currently drafting and/or reviewing the component detail.

- *Under Review* – The architecture team has completed the component documentation and has submitted it to the governing body for inclusion into the architecture.
- *Accepted* – The completed template, now known as a blueprint, has been approved by the EA governing body and is now an official part of the architecture.
- *Rejected* – The blueprint has been rejected by the governing body for reasons documented below in the Audit Trail section.

Audit Trail

Creation Date – Provide the date the logical or physical section of this artifact was created.

Created By – List all individuals that helped in the creation of the logical or physical section of this artifact and their titles.

Date Accepted/Rejected – Provide the date the logical or physical section of this artifact was accepted into the architecture or rejected.

Reason for Rejection – If the logical or physical section of this artifact was rejected, document the reason for the rejection.

Last Date Reviewed – Document the most recent date the logical or physical section of this artifact was taken through the Architecture Vitality Process.

Last Date Updated – Document the most recent date that any item in the logical or physical section of this artifact was changed.

Updated By – List all individuals and their titles that helped in the update of this logical or physical section of this artifact were created.

Reason for Update – Document the reason for the update to the logical or physical section of this artifact.

SAMPLES

Information Architecture Blueprint Samples

NASCIO

Process Component

DEFINITION	
Name	Handle Customer Call – Process Component
Description	This process describes the major steps in handling a customer call and providing resolution of that call.
Rationale	This is a primary vehicle to communicate with the citizens, therefore it is significant.
Benefits	Provide quality service to citizens. Improve the efficient and effective delivery of product and services. Enhance agency image an strengthen credibility
COMPONENT CLASSIFICATION	
Classification	☒ Baseline ☐ Target
RELATED DOMAIN / SUBJECT AREA	
Business Domain	Customer
Information Subject Area	Customer
KEYWORDS	
Keywords/Aliases	Customer, customer service, call handling, customer service center, customer service, customer relationship management (CRM), customer service agent, customer service representative, call routing, call center
PROCESS COMPONENT TYPE	
Component Type	☒ Process ☐ Process Step
Process Identifier	P1 (could use predecessor and successor notation, etc.)
Component Deliverable	Completed customer call

BUSINESS RULES

Owner	*Classification*	*Rule Statement*
Customer Call Center Manager	☒ *Baseline* ☒ *Target*	Agents should acknowledge customer within 5 seconds of call notification
Customer Call Center Manager	☒ *Baseline* ☒ *Target*	Subject of the call must be logged.
Customer Call Center Manager	☒ *Baseline* ☒ *Target*	If repeat call, then call history should be reviewed

Customer Call Center Manager	☒ *Baseline* ☒ *Target*	Resolution/commitment must be verified with customer

CRITICAL REFERENCES

Related Business Components

Business Architecture Component	*Relationship*	*Business Architecture Component*	*Relationship*
Build Public Trust	Enabler for building trust		
Service Delivery	This process component (Handling Call) directly supports call center consolidation goal		

Related Information Components

Supplier	*Input Information Component*	*Output Information Component*	*Consumer*
Caller	Contact information	• Call statistics	• Caller • Action Agent • Call Center Management
Caller	Request	• Call statistics • Resolution	• Caller

Stakeholders/Roles

Stakeholders	Call Center, Executive Branch
Roles	Consumer, citizen, governor, attorney general
Reason for Stake	Executive branch because they will hear from constituents.

RELATED GAP COMPONENT

GAP Components	Redundant call data

CURRENT STATUS

Process Component Status	☒ *In Development*	☐ *Under Review*	☐ *Accepted*	☐ *Rejected*

AUDIT TRAIL

Creation Date	05/13/04	*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Updated by			
Reason for Update			

Information Meta Component

PART 1 – CONCEPTUAL CONTENT *(Data Element/Data Element Concept)*	
DEFINITION	
Name	Call (Information Meta Component - Conceptual)
Industry Description	A transaction between a caller and a call agent, independent of the medium (telephone, web, video, mail, pda, instant message, etc)
Industry Description Provider	Call Center Industry Advisory Council (CIAC)
Description	
Rationale	Primary mechanism for gathering and disseminating information.
Benefits	Identifies the process supplier, consumer, nature of request
COMPONENT CLASSIFICATION	
Classification	☒ *Baseline* ☒ *Target*
CRITICAL REFERENCES	
Data Element Concept	*Relationship*
Media	The call must be able to process all customer contact media
Process Component	*Relationship*
Handle Customer Call	Primary data element
Application	*Relationship*
CRM package	Captures call data
Interactive Voice Response Unit (IVR)	Initial data gathering
Automatic Call Distributor (ACD)	Identifies agent and routes call, based on call data
Quality Assurance Package	Collects and analyses call data
Conceptual Information Model	*Link or Identifier*
Call – Conceptual Model	Samples – Conceptual Information Model

STAKEHOLDERS	
Stakeholders	*Reason for Stake*
Call Center Lead	Owner
ABC Company (Outsourcing agency)	Steward
Marketing Department	Steward
Database Administrator	Custodian
Governor	Assures Citizen Satisfaction

INFORMATION SECURITY CLASSIFICATION	
Security Classification	Public

KEYWORDS AND ALIAS	
Keywords / Alias	Customer contact, Call processing, transaction

VALID VALUES / EXAMPLES	
Valid Values	
Examples of the Data Element Concept	Emergency calls Tourist calls Legislative calls

BUSINESS RULES		
Owner	*Classification*	*Rule Statement*
Call center manager	☒ *Baseline* ☒ *Target*	All information needed to resolve call will be captured with initial contact
	☐ *Baseline* ☐ *Target*	
	☐ *Baseline* ☐ *Target*	

CURRENT STATUS				
Data Element/Concept Status	☒ *In Development*	☐ *Under Review*	☐ *Accepted*	☐ *Rejected*

CONCEPT SECTION AUDIT TRAIL			
Creation Date	05/13/04	*Date Accepted / Rejected*	
Created by			
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Updated by			
Reason for Update			

Information Meta Component

PART 1 – CONCEPTUAL CONTENT *(Data Element/Data Element Concept)*	
DEFINITION	
Name	Caller (Information Meta Component - Conceptual)
Industry Description	
Industry Description Provider	
Description	The party that calls the call center
Rationale	
Benefits	
COMPONENT CLASSIFICATION	
Classification	☒ *Baseline* ☒ *Target*

CRITICAL REFERENCES	
Data Element Concept	*Relationship*
Call	Primary concept
Process Component	*Relationship*
Handle Customer Call	Primary data element
Application	*Relationship*
CRM package	Captures call data
Interactive Voice Response Unit (IVR)	Initial data gathering
Automatic Call Distributor (ACD)	Identifies agent and routes call, based on call data
Quality Assurance Package	Collects and analyses call data
Conceptual Information Model	*Link or Identifier*
Party - Conceptual Diagram	Sample – Conceptual Information Model

STAKEHOLDERS	
Stakeholders	*Reason for Stake*
Call Center Lead	Owner
ABC Company (Outsourcing agency)	Steward
Marketing Department	Steward
Database Administrator	Custodian
Governor	Assures Citizen Satisfaction

INFORMATION SECURITY CLASSIFICATION			
Security Classification	Sensitive		
KEYWORDS AND ALIAS			
Keywords / Alias	Customer, contact, citizen, caller, requestor		
VALID VALUES / EXAMPLES			
Valid Values	Any		
Examples of the Data Element Concept	Bob H. Smith Tate's Rentals		
BUSINESS RULES			
Owner	*Classification*	*Rule Statement*	
Call Center manager	☒ *Baseline* ☒ *Target*	Individual caller names must be captured in First Name, Middle Initial, and Last Name format.	
Call Center Manager	☐ *Baseline* ☐ *Target*	Individual caller names must not include Company Names only Proper Names.	
Call Center Manager	☐ *Baseline* ☐ *Target*	Individual callers calling on behalf of a company must provide their name. The company they are calling on behalf of must be denoted as well.	
	☐ *Baseline* ☐ *Target*		
CURRENT STATUS			
Data Element/Concept Status	☒ *In Development* ☐ *Under Review* ☐ *Accepted* ☐ *Rejected*		
CONCEPT SECTION AUDIT TRAIL			
Creation Date	05/13/04	*Date Accepted / Rejected*	
Created by			
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Updated by			
Reason for Update			

PART 2 – LOGICAL AND PHYSICAL CONTENT (LOGICAL CONTENT)	
ENTITY/CLASS DEFINITION	
Entity/Class Name	Party (Information Meta Component – Logical)
Description	A person who interacts with the government entity in some capacity
Source Name	Party Management Database
Source Type	Oracle Database, Siebel Software

Critical References	
Logical Information Model	*Link or Identifier*
Party – Logical Model (Alternative A)	Samples – Logical Information Models (Sample 1)
Party – Logical Model (Alternative B)	Samples – Logical Information Models (Sample 2)

Related Attributes

Attribute Name	*Attribute Description*	*Sample Data*	*Representation Class*	*Information Security Classification*	*Information Security Rules*
Party Code	Unique identification of Party	1234567	Unique Key	Internal Use Only	Only used by internal systems
First Name	First Name of the Party	Bob Kathy	Name Class	Public / Internal Use Only	If first name, middle initial, and last name are combined then this attribute is classified: Internal Use Only
Middle Initial	One character initial of the party's middle name.	H E			If first name, middle initial, and last name are combined then this attribute is classified: Internal Use Only
Last Name	Last name of the Party	Smith Jones	Name Class		If first name, middle initial, and last name are combined then this attribute is classified: Internal Use Only
Picture	Picture of Party		Content	Sensitive	If combined with party type 'criminal' then classification is Public

Relationships					
Relationship Name	*Entity/Class Name (1)*	*Relationship*	*Cardinality*	*Entity/Class Name (2)*	*Relationship Description*
Party.Business Partner	Party	represents	1:1	Business Partner	Provides information regarding agent relationship of Party. A Party must represent one and only one Business Partner.
	Business Partner	is represented by	1:M	Party	Provides information regarding agent relationship of Party. A Business Partner must be represented by at least one Party. A Business Partner could be represented by many instances of Party.
Party.Party Assignment	Party	defines	1:M	Party Assignment	A Party must define one or many Party Assignments. e.g., a Party can be a "Citizen" and a "Taxpayer". A Party must have at least one Party Assignment.
	Party Assignment	is defined by	1:1	Party	Existence of a Party Assignment requires a relationship to one and only one Party. An instance of Party Assignment can pertain to only one Party instance.
Party.Address	Party	resides at	1:M	Address	A Party must have at least one residence. A Party can have many residents.
	Address	is residence for	1:1	Party	An instance of Address can pertain to one and only one Party. As instance of Address must pertain to at least one Party. (Note: Party Address is an Attributive Entity of Party.)

PART 2 – LOGICAL AND PHYSICAL CONTENT (LOGICAL CONTENT)					
ENTITY DEFINITION					
Entity/Class Name	Party Type (Information Meta Component – Logical)				
Description	Provides the means to identify the Party by the role they play with in the enterprise. A given party can play more than one role in the enterprise. For example a Party can play both the role of a "Citizen" and a "Tourist"				
Source Name	Party Management Database				
Source Type	Oracle Database, Siebel Software				
Critical References					
Logical Information Model		*Link or Identifier*			
Related Attributes					
Attribute Name	*Attribute Description*	*Sample Data*	*Representation Class*	*Information Security Classification*	*Information Security Rules*
Party Type	Includes the various types of parties that could interact with the government	Citizen Non-citizen Tourist Criminal Taxpayer	Type Class	Public , Sensitive	If party type is combined with party identification then Party Type is classified as Sensitive information.
Party Type Description	Provide description for the party type	A citizen is anyone through either birth or naturalization possesses rights and obligations of citizenship.	Name Class	Public	

PART 2 – LOGICAL AND PHYSICAL CONTENT (LOGICAL CONTENT)	
ENTITY DEFINITION	
Entity/Class Name	Party Type Assignment (Information Meta Component – Logical)
Description	Assigns the party type to the Party. This allows an individual party to be identified with the party types they are in the enterprise.
Source Name	Party Management Database
Source Type	Oracle Database, Siebel Software

Critical References	
Logical Information Model	*Link or Identifier*

Related Attributes

Attribute Name	*Attribute Description*	*Sample Data*	*Representation Class*	*Information Security Classification*	*Information Security Rules*
Party Type.Code	Includes the various types of parties that could interact with the government	Citizen Non-citizen Tourist Criminal Taxpayer	Type Class	Public , Sensitive	If party type is combined with party identification then Party Type is classified as Sensitive information.
Party.Code	Unique identification of Party	1234567	Unique Key	Internal Use Only	Only used by internal systems

Relationships					
Relationship Name	*Entity/Class Name (1)*	*Relationship*	*Cardinality*	*Entity/Class Name (2)*	*Relationship Description*
Party Type.Party Assignment	Party Type	defines	1:M	Party Assignment	Existence of an instance of Party must define one or many instances of Party Assignment. e.g., a Party can be a “citizen” and a “taxpayer.” A Party must be at least one Party Type.
	Party Assignment	is defined by	1:1	Party Type	The existence of an instance of Party Assignment requires a relationship to one and only one Party.

PART 2 – LOGICAL AND PHYSICAL CONTENT (LOGICAL CONTENT)					
ENTITY DEFINITION					
Entity/Class Name	Party Address (Information Meta Component – Logical)				
Description	A Party Address is a location where a person can be contacted directly or indirectly. Also allows the address to be given a primary address type. Provides the ability to capture the various addresses for a party.				
Source Name	Party Management Database				
Source Type	Oracle Database, Siebel Software				
Critical References					
Logical Information Model	*Link or Identifier*				
Related Attributes					
Attribute Name	*Attribute Description*	*Sample Data*	*Representation Class*	*Information Security Classification*	*Information Security Rules*
Party Address Identifier	The system assigned identifier that uniquely identifies a Party Address	1234567	Unique Key	Internal Use Only	Only used by internal systems
Party Identifier	Unique identification of Party	1234567	Unique Key	Internal Use Only	Only used by internal systems
Primary Address Type	Identifies if this address associated with a given Party is the home address or the work address	Home Work	Type Class	Public	
Address Line 1	Provide the first Address Line of the Party	1501 South Idaho Street	Address Line Class	Sensitive	
Address Line 2	Provide the second Address Line of the Party	Suite 200; Mail Stop 5	Address Line Class	Sensitive	
City	Provide the City in which the address can be found	Boise	City Class	Public, Sensitive	City when combined with address lines is classified as Sensitive information
State Province	Provide the state or province in which the city is located.	Idaho	State Class	Public, Sensitive	When combined with address lines is classified as Sensitive

Address Begin Date	The business date that the Address became effective.	January 15, 1987	Date/time	None	
Address End Date	The business date after which the Address is no longer effective.	December 12, 1992	Date/time	None	

Relationships					
Relationship Name	*Entity/Class Name (1)*	*Relationship*	*Cardinality*	*Entity/Class Name (2)*	*Relationship Description*

PART 2 – LOGICAL AND PHYSICAL CONTENT (PHYSICAL CONTENT) (DATA DICTIONARY SECTION)	
TABLE / CONTENT / DOCUMENT DEFINITION	
Table Name/ Content Location	Customer_Name_P (Information Meta Component – Physical)
Description	Customer Name physical table provides the structure to capture customer name information separate from customer address information.
Source Name	Customer_DB
Source Type	Oracle 9.1

Related Columns

Document Name /Column Name	*Associated Attribute*	*Column Data Type / Length*	*Column Null Indicator*	*Column Comment*
CUSTOMER_ID	Party Identifier	NUMERIC,7.0	NON_NULL	Primary key for the Customer ID
PRIMARY_CUSTOMER_ROLE	Party Type	ALPHA-NUMERIC, CHAR10	NULLABLE	Denotes if customer has preferred role they want to be associated with for information presentation
CUSTOMER_FIRST_NAME	First Name	ALPHA-NUMERIC, CHAR50	NULLABLE	Captures Customer First Name , No updates allowed to field if new name must create new customer record.
CUSTOMER_MIDDLE_INITIAL	Middle Initial	ALPHA-NUMERIC, CHAR50	NULLABLE	Captures Customer Middle Initial No updates allowed to field if new name must create new customer record.
CUSTOMER_LAST_NAME	Last Name	ALPHA-NUMERIC, CHAR50	NULLABLE	Captures Customer Last Name No updates allowed to field if new name must create new customer record.
BUSINESS_CUSTOMER_NAME	Company Name	ALPHA-NUMERIC, CHAR50	NULLABLE	Captures Customer Last Name No updates allowed to field if new name must create new customer record.

CUSTOMER_DUNNS_NUMBER		ALPHA-NUMERIC, CHAR25	NULLIBLE	For business customers a Dunns and Bradstreet ID must be denoted.
CREATION_DATE				
UPDATE_DATE				

PART 2 – LOGICAL AND PHYSICAL CONTENT (PHYSICAL CONTENT) (DATA DICTIONARY SECTION)	
TABLE / CONTENT / DOCUMENT DEFINITION	
Table Name/ Content Location	Customer_Address (Information Meta Component – Physical)
Description	Customer Address physical table provides the structure to capture customer address information. A given customer record captured in the Customer_Name physical table can have multiple addresses associated with it.
Source Name	Customer_DB
Source Type	Oracle 9.1

Related Columns

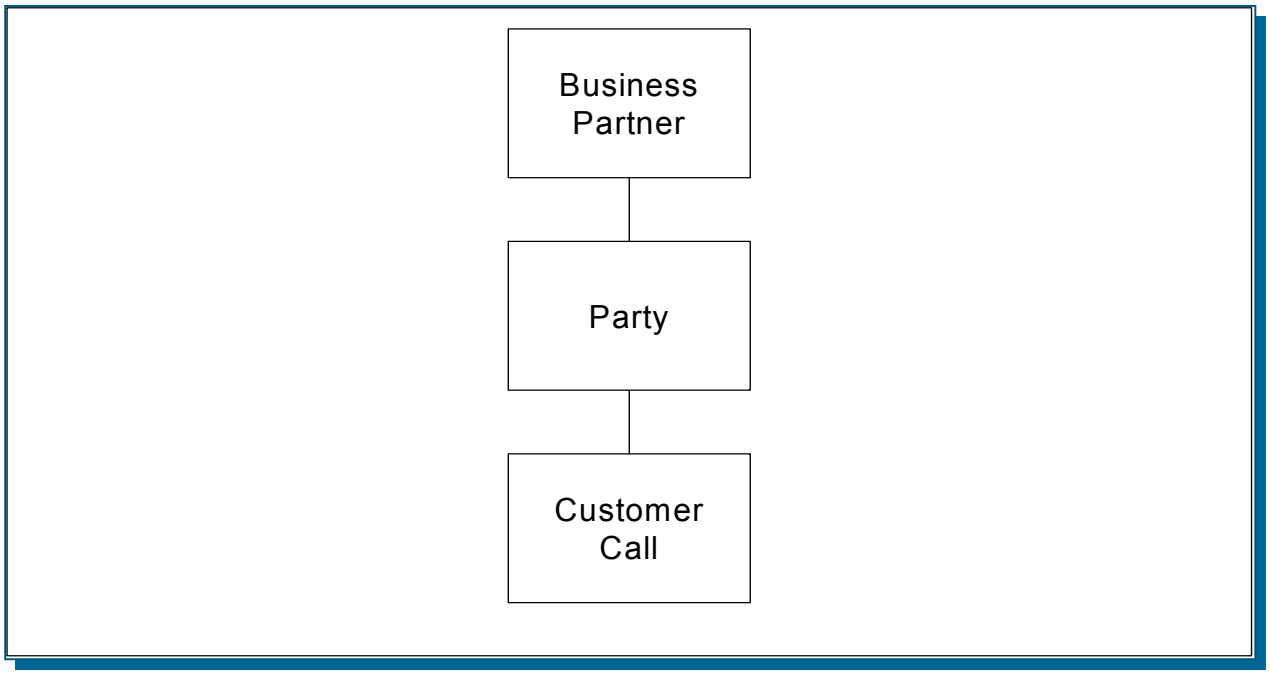
Document Name /Column Name	*Associated Attribute*	*Column Data Type / Length*	*Column Null Indicator*	*Column Comment*
Party Address Identifier	Party Address Identifier	NUMERIC,7.0	NON_NULL	Primary key for the Customer Address Table
Party Identifier	Party Identifier	NUMERIC,7.0	NON_NULL	Provides a foreign key relationship to the Customer Name table.
Customer_Address_Role	Primary Address Type	ALPHA-NUMERIC, CHAR10	NULLABLE	Provides a categorization of the usage of the address. Examples can include home mailing address, billing address, shipping address
Address_Line_1	Address Line 1	ALPHA-NUMERIC, CHAR50	NULLABLE	Captures Customer Address line 1 information
Address_Line_2	Address Line 2	ALPHA-NUMERIC, CHAR50	NULLABLE	Captures Customer address line 2 information
City	City	ALPHA-NUMERIC, CHAR50	NULLABLE	Captures City associated with Customer Address.
State Province	State Province	ALPHA-NUMERIC, CHAR4	NULLIBLE	Captures standardized State or Province Codes from ISO
Creation_Date		TIMESTAMP	NON_NULLIBLE	Creation date of the Customer Address Record
Update_Date		TIMESTAMP	NULLIBLE	Last update date of the Customer Address Record

PART 2 – LOGICAL AND PHYSICAL CONTENT (PHYSICAL CONTENT) (DATA DICTIONARY SECTION)				
TABLE / CONTENT / DOCUMENT DEFINITION				
Table Name/ Content Location	Criminal Picture Library (Information Meta Component – Physical)			
Description	Criminal Picture Library provides storage of pictures for all prison inmates from 2/01/1997 until current.			
Source Name	Alphabetical Criminal Picture Folders			
Source Type	Windows NT Server			
Related Columns				
Document Name /Column Name	*Associated Attribute*	*Column Data Type / Length*	*Column Null Indicator*	*Column Comment*
{InmateID}.jpg	*Picture*	.jpg		These files contain the pictures of inmates. Pictures are retaken annually. History of all pictures can be found in the library based on archiving rules.

CURRENT STATUS					
Logical/Physical Content Status	☒ *In Development*	☐ *Under Review*	☐ *Approved*	☐ *Rejected*	
INFORMATION ARCHITECTURE AUDIT TRAIL					
Creation Date	5/12/04		*Date Accepted / Rejected*		
Created by					
Reason for Rejection					
Last Date Reviewed			*Last Date Updated*		
Updated by					
Reason for Update					

Conceptual Information Model

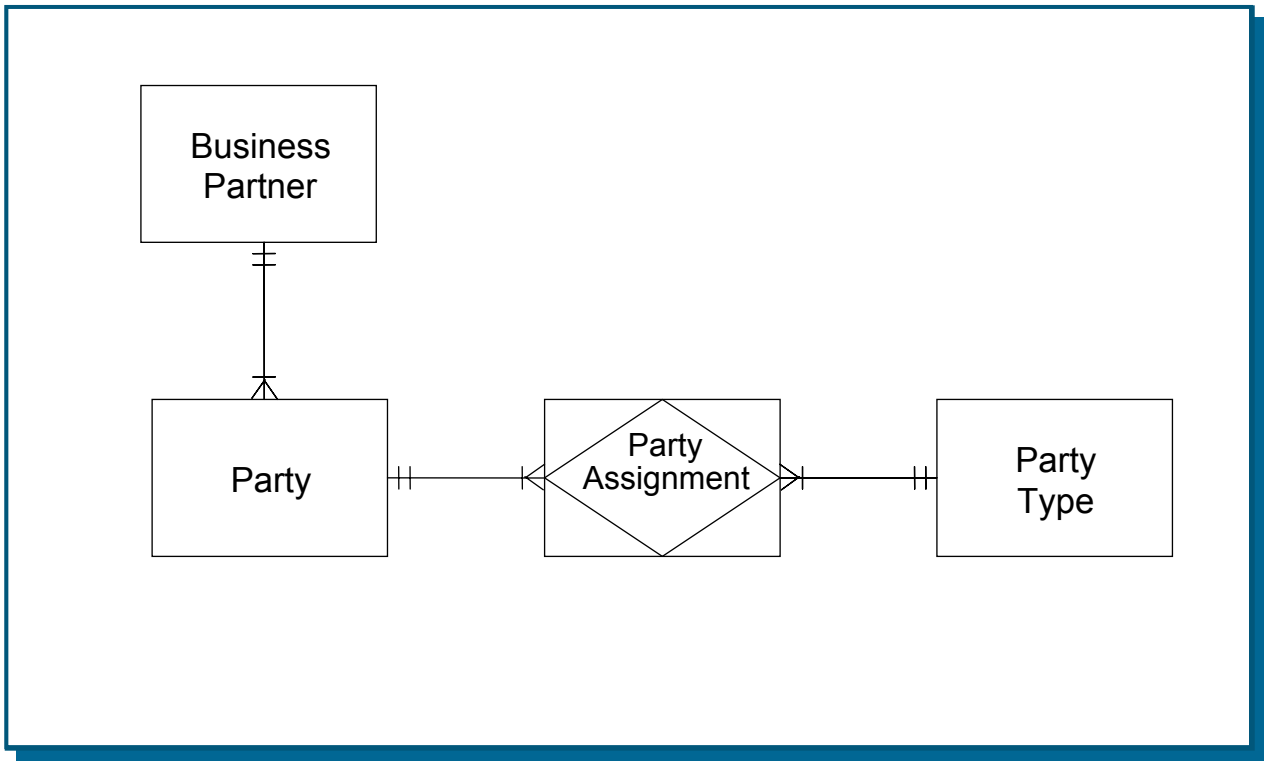
This diagram is referenced in the Blueprint sample: Party (Information Meta Component - Conceptual)



Logical Information Models

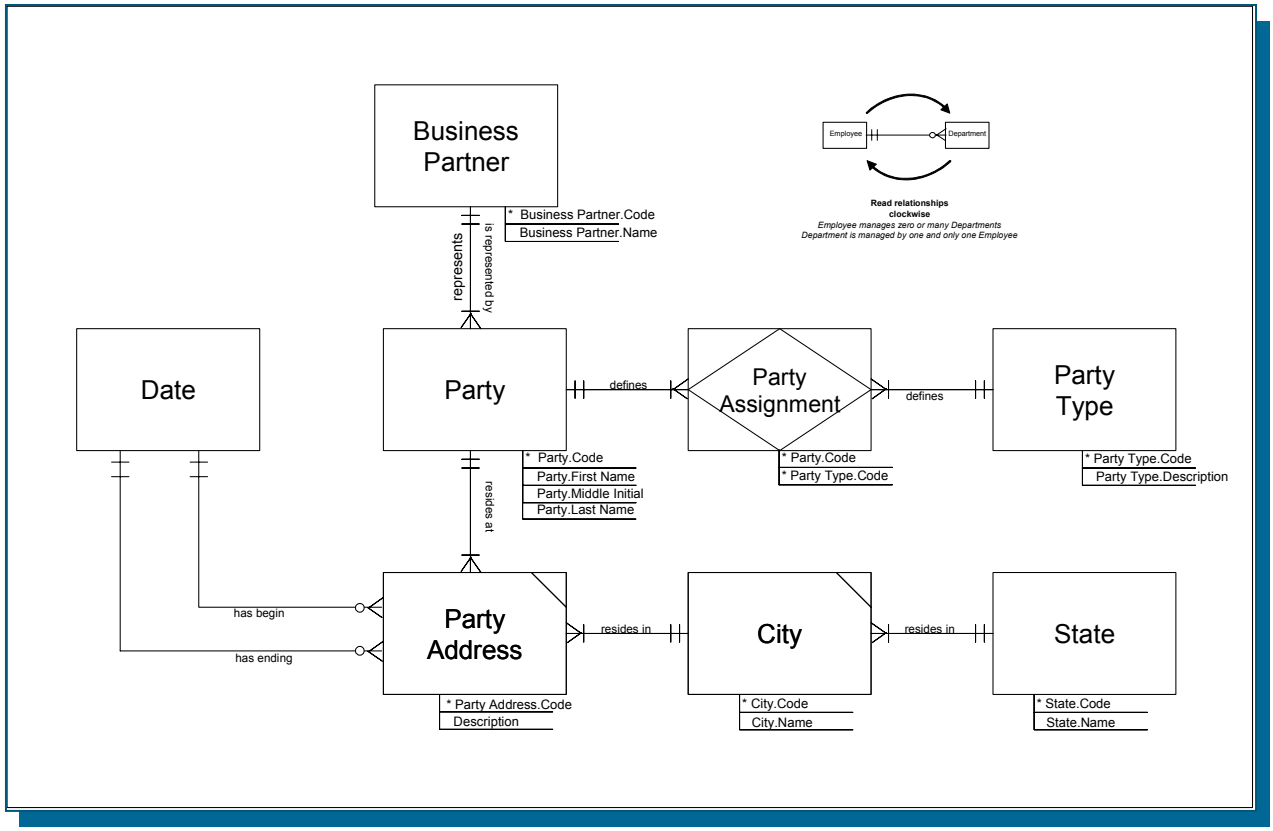
SAMPLE 1 – ALTERNATIVE A

This diagram is referenced in the Blueprint sample: Party (Information Meta Component – Logical)



SAMPLE 2 – ALTERNATIVE B

This diagram is referenced in the Blueprint sample: Party (Information Meta Component – Logical)
Note: Optionally modify the templates to accommodate graphical representations such as process models, data models, organizational charts, business interaction models, Rummler-Brache cross functional flow charts, etc.



SUMMARY/CONCLUSION

The Information Architecture provides a business-based framework for developing solutions that operate across agencies and within the lines of business of state and local governments.

It is through the pursuit of a formal Information Architecture that the following are provided:

- A demonstrable, repeatable approach to assuring critical information exchange throughout the enterprise
- A clear understanding of the enterprise's current and future direction
- Identification of opportunities to leverage linkage across government-wide entities and increase collaboration and sharing of information
- A means to increase information re-use and reduce information redundancy throughout the enterprise.

The Information Architecture identifies and inter-relates the information assets of the enterprise to enable sharing and exchange of critical information. Though enterprise typically refers to the organization as a whole, the development of Information Architecture can also be accomplished at an agency level. For example, in North Carolina, Information Architecture is primarily done by the agencies with only a portion of the information provided at the enterprise (statewide) level.

JUSTICE INFORMATION EXCHANGE MODEL

The Justice Information Exchange Model (JIEM) consists of a conceptual framework that defines universal dimensions of information exchange, a research and planning methodology for modeling the operational dynamics of this information exchange, and a Web-based software application (the JIEM Modeling Tool) that enables data collection, analysis, and reporting by users and researchers.[13]

SEARCH, The National Consortium of Justice Information and Statistics, developed this web-based tool to aid cities, counties and states in the development of information exchange elements within the justice arena.

The JIEM tool facilitates the documentation of the following characteristics:

- *Process* – Logically related events that are associated with an information exchange. These processes begin and end with an event and may contain multiple events.
- *Event* – There are two types of events (triggering and subsequent). A triggering event is a decision or action that causes the exchange of information. By contrast, a subsequent event is the next logical step in the process, which results from the information exchange.
- *Agency* – The entity that sends or receives information. While not all agencies may be involved in the initial transaction or exchange of information, the detail gathered during that interaction could be used by many other entities. The tool supports the identification of all agencies that have an interest in the data.
- *Condition* – The factor that affects the content or direction of the information exchange. Conditions basically determine what agencies receive specific information as part of the overall business process.
- *Information* – The content that is actually exchanged between entities. The information may include documents and/or specific data elements, images, video, etc. and can be exchanged via paper, electronic medium, and/or other forms of communication.

By focusing on the identification of key decision points, and the information that flows between various justice entities at critical exchange points, the tool provides an enterprise-wide view of the exchange of information and empowers agencies to share information more efficiently, thereby increasing the safety and security of both employees and the general public.

One of the key benefits of this tool is the incorporation of a Global Justice XML Data Dictionary. This allows users to import data types and structures directly from the dictionary, eliminating the concerns around naming, data types and field size elements.

While the JIEM tool was created specifically for meeting the needs of the courts and justice agencies, the methodologies for capturing the detailed information surrounding the processes, events, agencies, information and conditions apply to any organization that is striving to focus on the enterprise-wide exchange of information.

[13] http://www.search.org/integration/pdf/JIEM.pdf

NASCIO Online
Visit NASCIO on the web for the latest information on the Architecture Program or to download the current version of the Enterprise Architecture Development Tool-Kit.

www.nascio.org

NASCIO EA Development Tool-Kit
Solution Architecture

Version 3.0

October 2004

TABLE OF CONTENTS

SOLUTION ARCHITECTURE

Introduction

Solution Architecture facilitates the development of architectural solutions for the enterprise and as such, is a critical part of the Enterprise Architecture with links to Business Drivers, Business, Information and Technology Architectures, and Implementation Planning as shown in Figure 1.

An "architectural solution" is defined as a response to any new architecture shift within the enterprise. These shifts are identified as gaps within the Business Architecture, Information Architecture, and Technology Architecture blueprints. The Solution Architecture is utilized for architecture related projects including the establishment of processes, business systems, and technical systems.

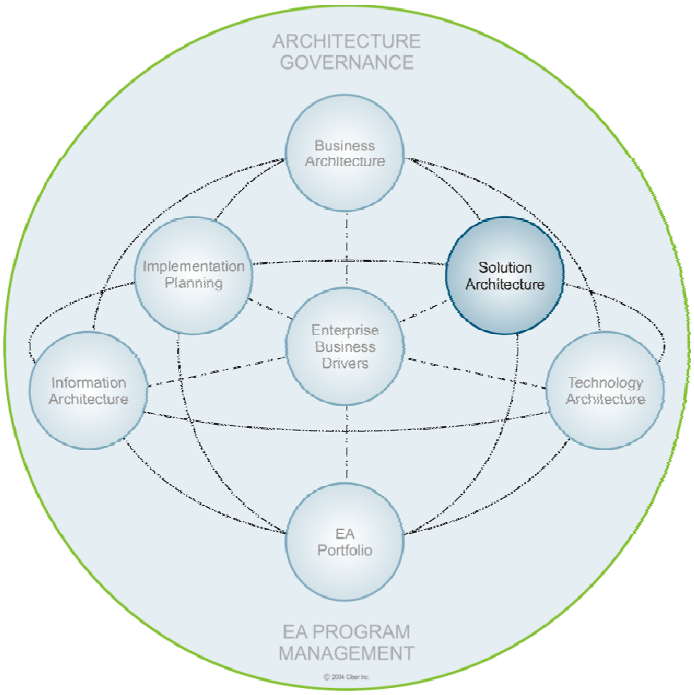


Figure 1. Solution Architecture Touch-Points

The Solution Architecture process guides the solution architect in documenting the requirements and design specifications necessary to fulfill a specific migration strategy identified during the Implementation Planning architecture process. The Solution Architecture process is initiated when an Implementation Planning effort has been approved and selected for execution. The Solution Architecture templates capture the detail of the solution project or effort in terms of scope, requirements, design specifications, and design models. Wherever possible, it links the solution set to the existing Enterprise Architecture artifacts to form integrated solutions.

The design of a solution is based on analysis of the migration strategy identified in the Implementation Plan and approved for development and implementation. The solution is intended to consider the long term goals of the enterprise and is specifically designed to achieve these goals; however, due to organizational constraints, (e.g., funds, human resources), it may be implemented in various iterations. The key, however, is that the whole solution is designed first, ensuring the high-level target is identified prior to implementation of any of the iterations. For all Solution Architecture efforts however, the deliverables consist of specific detailed solution requirements, solution design specifications, and solution design models.

Solution Architecture consists of the following:

- The Solution Architecture process that guides the identification of the requirements and design specifications of an enterprise solution.

- Solution Architecture templates that capture detail about the solution being created. The specific templates are:
  - *Solution Set Scope* – Describes the overall solution and links the solution to the Implementation Plan; defines a conceptual model of the solution.
  - *Solution Set Requirements* – Lists the various solution set requirements based on specific solution set types, views, and categories. These views examine the required functionality necessary to fulfill the Business Architecture, Information Architecture, and Technology Architecture requirements.
  - *Solution Set Design* - Lists the various solution set design specifications based on specific set types, views, and categories. In addition, they provide the information to assess the solution impacts to the current environment in the areas of capacity, training, business continuity, etc.

The organization's Enterprise Architecture methodology and the respective architectures (e.g., Business Architecture, Information Architecture, Technology Architecture) should be implemented and utilized for an organization to fully leverage the advantages of Solution Architecture. Figure 2 provides a visual representation of how the development of a Solution Set within Solution Architecture leverages the information captured in the Business, Information and Technology Blueprints.

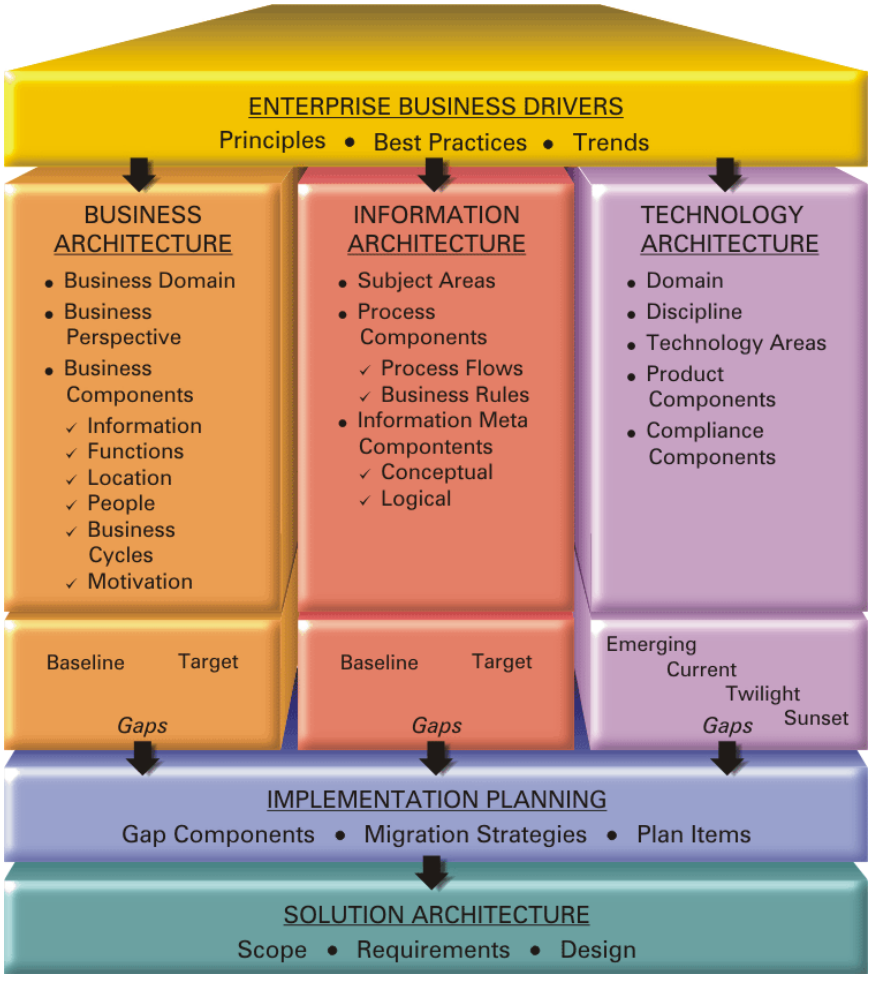


Figure 2. Solution Architecture Leverages Existing Architecture

In addition to the architectural blueprints developed within these architectures, further benefits of Solution Architecture can be realized by referencing and building the solution around the following organizational constructs:

- **The Enterprise Application Portfolio** – Current inventory of applications and components, complete with relationships to supported business processes, interfacing systems, supplied/required information and infrastructure configurations. The Application Portfolio can be very detailed and maintained by an extensive portfolio management system, or it may be a simple list of the business applications in use within the organization. The more detailed the inventory, the better able to enterprise is to access current capabilities and future requirements.
- **Design Models** – Pre-existing formats used to guide the development of the Solution Architecture artifacts (e.g., logical design). These models are typically graphical in nature and show the relationships among the elements of the solution. Models, which provide simplified abstract representations of complex information, are used for communication, analyzing, testing, simulating, or exploring options. The various types of models (e.g., Business Process Models, Software Models) approved for usage by the organization are created within the Business, Information and/or Technology Architectures and are leveraged when building a solution design.

  An example of a model used to document business processes is the SIPOC model. The SIPOC model depicts a business process in terms of the S (Supplier), I (Input), P (Process), O (Output), and C (Consumer). The unpopulated model, or template, is contained within the Information Architecture. The model is used to develop the unique solution model during the Solution Architecture process.
- Design Patterns – Design Patterns are pre-existing configurations that identify a collection of architecture components and describe commonly recurring structures, systems, and processes within the enterprise. A pattern provides the bundling of a set of commonly recurring subsystems or components necessary to solve a general solution design. In addition, a pattern specifies sub-system or component characteristics and responsibilities, and includes rules and guidelines for organizing these relationships. Patterns can help expedite the delivery of a solution because they can be used to quickly identify groups of components required to build a system or solution.

  The various patterns prescribed for usage by the organization are created as part of the Business, Information and/or Technology Architecture processes, and are leveraged when building a solution design. These patterns are bundled views of the current and future architecture processes that exist within the architecture inventory.

  A typical list of patterns would include design patterns (such as object oriented software design), analysis patterns (such as recurring and reusable analysis models), infrastructure patterns (such as N-tier), organizational patterns (such as structure of organizations and projects) and process patterns (which are used for process design).

Solution Architecture provides guidance for *what* is to be developed and *how* it fits into the overall enterprise. However, for IT related solutions, it does not recommend the specifics of the development life cycle (e.g., requirements gathering, analysis, usage of design tools, testing, or implementation tasks). These documents are characteristically a part of the organization's Technology Architecture methodologies.

BENEFITS

The quality of Solution Architecture is no better than the quality of the Business Architecture, Information Architecture, and the Technology Architecture. The focus is not on enabling a single solution, but on identifying and enabling the optimal portfolio of enterprise solutions.

Solution Architecture provides the following benefits to a governmental organization:

- Ensures that information and services are served holistically across the organization
- Identifies the solution patterns for the future state of the solutions architecture
- Is a quick start for project leaders, managers, and architects when developing solutions and services

The following are considered critical success factors to achieving enterprise wide, integrated solutions:

- Proven success in the development of Business Architecture and Information Architecture
- A holistic view of the enterprise
- Strong linkage among, and definition of, the business change requirements
- Business information requirements
- Information technology requirements that describe the business solutions requirements to support enterprise business strategies

To implement a Solution Architecture to the fullest extent, the following "Best Practices" apply:

- A solution should be architected with the life-cycle of the solution in mind
- Converge on a solution: Use scenario planning models to identify and access alternatives
- Personalization for ease of access
- All solutions to be "highly granular" and "loosely coupled"
- Solutions are built from existing Enterprise Architecture (EA) components
- Capture EA information, design models and solution sets in a robust EA repository to maximize the potential for reuse
- All solutions must conform to common enterprise-wide IT interoperability standards
- Establish and manage solution requirements

LINK TO IMPLEMENTATION PLANNING

Implementation Planning is the process that consolidates all the gaps and migration strategies for the purposes of assessing the potential architecture related work load needing to be addressed by the enterprise. The following information is provided to introduce the concept of Implementation Planning and remind the reader of the background information that is available to the Solution Architect upon initiation of the solution documentation process.

The Solution Architecture process is initiated for a specific solution effort contained in the Implementation Plan and proceeds after receiving approval. This approval, which occurs during the Implementation Planning architecture process, is based on several key factors including the effort's prioritization, cost/benefit analysis, enterprise architecture fit, commitment of resources, etc.

The Solution Architecture process also leverages the information developed during the Implementation Planning process. Information created during the Implementation Planning process and used during the Solution Architecture process includes the gaps identified as related to the solution effort and migration strategy, the high-level requirements, and the conceptual model that was created for this specific migration strategy.

For each project or effort that is approved to move into the Solution Architecture process, a conceptual model is required. The conceptual model:

- Should be in enough detail as to help determine the organizational areas that need to be interviewed to capture the Solution Set business requirements
- Will be used to validate the solution intent with the project sponsor
- Defines the business problem and presents a high level description of the proposed solution in terms of a set of integrated ideas and concepts about what it should do, how it should behave, and what it should look like – in terms that are understandable to the project sponsor

Definitions

When discussing Solution Architecture and related topics, the terminology varies, including a variety of terms with the same or similar meanings, as well as varied meanings for the same term. To minimize any confusion in terminology, a glossary, which provides definitions of terms used throughout the Tool-Kit is provided in Appendix A of the *Introduction/Architecture Governance* document. A brief list of the terms and definitions used within this Solutions Architecture section are provided here:

- *Architectural Patterns*: The expression of a fundamental structural organization or schema for a system or solution. It provides a set of predefined subsystems, specifies their responsibilities, and includes rules and guidelines for organizing the relationships between them.
- *Architecture Blueprint*: The dynamic detail of the business, information or technology captured utilizing standardized, structured processes and templates (framework).
- *Architecture Framework*: The combination of structured processes, templates and governance that facilitate the documentation of the architecture in a systematic manner.
- *Baseline*: Current or "as is" state of the business environment, captured in a set of baseline business models.
- *Business Architecture*: The high-level representation of the business strategies, intentions, functions, processes, information, and assets (e.g., people, business applications, hardware) critical to providing services to citizens.
- *Business Domain*: A functional or topical subset of business operations integral to the enterprise operations.
- *Business Portfolio*: The implemented baseline business environment (e.g., implemented business processes, strategies, data of the business organization).
- *Conceptual Patterns*: A pattern whose form is described by means of terms and concepts from a business, technology or application domain.
- *Design Patterns*: Structure that provides a scheme for refining the subsystems or components of a system, or the relationships between them. It describes commonly recurring structure of communicating components that solves a general design problem within a particular context.
- *Information Architecture*: The compilation of the business requirements of the enterprise. Includes the information, process entities, and integration that drive the business, as well as, rules for selecting, building and maintaining that information.

- *Logical Information Model*: Shows the main functional [information] components and their relationships within a system, independent of the technical detail of how the functionality is implemented.[1]
- *Solutions Architecture*: A process within the Enterprise Architecture that focuses on the development and implementation of the solution or service being created for the enterprise.
- *Solutions Architecture Model*: The graphical representation of concepts to portray a desired future state, as well as an undesirable current state. Used for communicating, analyzing, testing, simulating, or exploring options.
- *Solution Pattern*: The bundling of tested solutions or configurations commonly used together, which can be addressed as a whole.
- *Solution Set*: The combination of the scope, requirements, design specifications, and logical models that define the solution.
- *Target*: Desired future or "to be" state of the business environment, captured in a set of target business models.
- *Technology Architecture*: A disciplined approach to describing the current and future structure and inter-relationships of the enterprise's technologies in order to maximize value in those technologies.
- *Template*: The empty form, provided as a guide for details of the architecture to be documented. Ultimately, the content captured utilizing architecture templates is referred to collectively as the Blueprint and resides in the architecture repository.

Roles

Figure 3 identifies the basic roles that are necessary when developing a Solution Architecture effort:

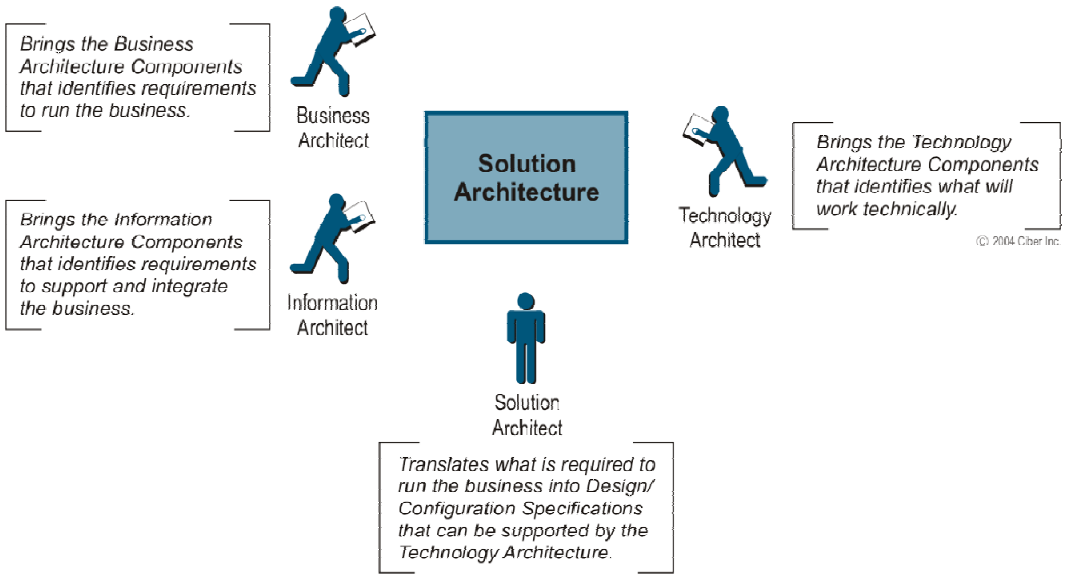


Figure 3. Solution Architecture Roles

[1] http://msdn.microsoft.com/architecture/enterprise/default.aspx?pull=/library/en-us/dnea/html/eaarchover.asp#eaarchover_topic3

Business Architect – Provides input concerning the elements necessary to run the business. This individual, or team, has a complete understanding of the artifacts and blueprints within the Business Architecture.

Information Architect – Provides input concerning the elements necessary to support and integrate the business and the key business information. This individual, or team, has a complete understanding of the artifacts and blueprints within the Information Architecture.

Technology Architect – Provides input concerning what infrastructure is required to support the application, infrastructure, or service being developed. This individual, or team, has a complete understanding of the artifacts, blueprints, configurations, and services within the Technology Architecture.

Solutions Architect – Translates the above elements into design and/or configuration specifications that can be supported by the Technology Architecture. This individual, or team, is the primary architect for this effort and is responsible for completing and delivering the solution design or model.

Solution Architecture Framework

The Solution Architecture framework is a combination of structured processes and templates that utilize existing architecture documents (such as business, information, and technology components as well as models and patterns) to design a desired business solution. The Solution Architecture framework, by allowing the development of a Solution Set, facilitates the rapid development and delivery of a solution in a systematic and well-disciplined manner.

By leveraging the components of the existing architectures, the solution that is developed will augment and extend the enterprise architecture. The solution's design identified within the Solution Architecture will enable the organization to accurately determine the impacts to all resources (e.g., dollars, people, systems). This ensures that the solution leverages the target architectural components and enhances the Enterprise Architecture, thereby mitigating the possibility of undesirable architectural components.

Designing the solution as prescribed in the Solution Architecture framework enables the identification of all architectural touch points, ensures involvement from architecture subject matter experts, and enables the implementation of specific items identified on the Implementation Plan. In addition, it completes the architecture loop by initiating the vitality of the Business, Information, and Technology Architecture artifacts affected by the modified or newly developed solution set.

The effective use of a Solution Architecture framework provides a standardized approach when identifying requirements and design specifications for enterprise solutions by means of:

- Solution Set structure
- Structured processes for documenting, developing, and implementing the solution set
- Templates for capturing the solution set scope, requirements, and design specifications

The standardized approach leveraged by the Solution Architecture framework promotes a broader understanding of the enterprise and facilitates the integration and interoperability of solutions.

Solution Set Structure

A Solution Set refers to the dynamic detail for a specified solution effort captured using the structured processes, and templates. This Solution Set provides the details of the Solution Set requirements and design specifications.

Unlike the Business, Information, and Technology Architectures, the Solution Architecture does not contain *baseline* or *target* information. Rather, it provides the process and structure to enable the development of a solution or a tightly coupled series of solutions. The combination of the scope, requirements, design specifications, and logical models that define the solution is referred to as a Solution Set.

After the Solution Set is completed and implemented within the enterprise, the Solution Architecture documentation is used for historical purposes only. The information created as part of the Solution Set is updated within the appropriate Business Architecture, Information Architecture, and/or Technology Architecture blueprints once the solution set is implemented within the enterprise.

The Solution Set is comprised of the Solution Set Scope, the Solution Set Requirements, and the Solution Set Design. The Solution Set contains the information necessary to implement the direction of the enterprise from business, information, and technology perspectives.

Figure 4 provides a pictorial view of the relationship between the Solution Set elements. The graphic displays these pieces working together to ensure the complete documentation of the solution set that forms the high-level design of the complete solution effort.

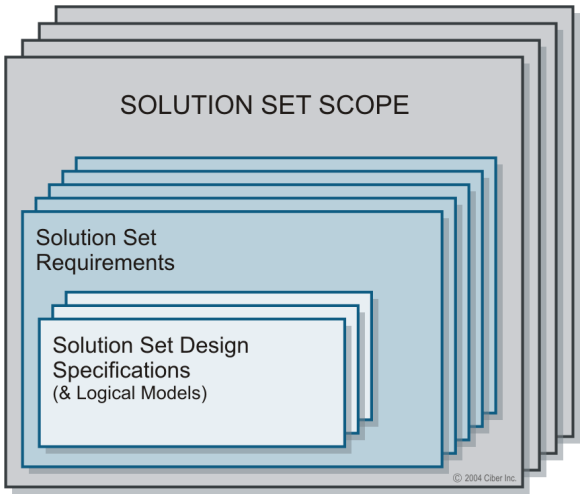


Figure 4. Solution Set Structure

SOLUTION SET SCOPE

The Solution Set Scope contains various details about the Solution Architecture effort being undertaken within the enterprise. It is unique in nature and typically addresses one effort contained on the Implementation Plan. A Solution Set Scope template should be filled out for each Solution Architecture effort undertaken.

The Solution Set Scope describes the solution in enough detail to aid in determining the overall scope of the effort. An initial high-level scope should have been captured when documenting the migration strategy for the associated gap component. The Solution Set Scope can be used by the Solution Architect to re-affirm the migration strategy and to document additional information about the proposed effort. If there are numerous migration strategies associated with the original Business Architecture, Information Architecture, or Technology Architecture gap component, each migration strategy would require a unique Solution Set Scope template.

When populated, this template provides the necessary background information for the effort. It contains a link to the proposed solution's conceptual model contained in the Implementation Plan. In addition, it links to the reference material that will be needed when completing the rest of the solution set requirements and design specifications. The information referenced will include such items as:

- The priority of the effort
- The associated business case
- A risk assessment
- The gap components that contained information on the business needs
- The potential migration strategies
- Associated Architecture Components
- The high-level scope and description of the effort

The Solution Set Scope template also references the original architecture blueprints that identified the future state that the solution set seeks to implement. These are the blueprints created during the Business, Information, and Technology Architecture efforts.

With the above information available, the Solution Architect can then fully populate the Solution Set Scope Template. The scope of the effort is detailed at a lower level, and the areas supporting the identification of the solution requirements are identified and documented.

The Solution Set Scope template is also used to identify the type of solution being designed. A description of the typical Solution Set types include:

- **Business Solution** – The solution will implement a business process, organizational, or other type of business solution. This may include new business processes, organizational structures, methodologies, etc.
- **Application Solution** – The solution involves the purchase and/or development of a traditional business system application.
- **IT Infrastructure Solution** – The solution involves the purchase and/or design of IT infrastructure components. This includes traditional IT infrastructure such as Networks, Platforms, etc. as well as the infrastructure to support the application development environment (e.g. Websphere, .NET, Java).

Once the solution type has been identified, the solution requirements and design specifications can be addressed. It may be possible for a Solution Set to consist of a business solution, an application solution, an IT infrastructure solution, or a mix of these types. This list is an example of the most common solution types. Organizations may identify additional solution types depending upon the needs of the organization.

The Solution Set templates provided in this Tool-Kit are designed to accommodate the documentation of multiple solution types within a single effort. Multiple types can be indicated in the Solution Set Scope template and the Solution Set Requirements and Design templates can be customized to address multiple solution types within a Solution Set by replicating the sections as needed.

Depending upon the intent, size, and complexity of the solution, the actual solution types will vary. For example, if the solution is small and will implement only business process changes, the only solution type that may need to be completed is that of "Business". However, if the solution is intended to encompass the implementation of a major new business system, it is highly likely that the Business, Application, and Infrastructure types will need to be completed to capture all the requirements and design considerations for the whole solution.

The types are referenced and utilized when documenting the solution requirements, the logical model, and the design specifications. However, due to the specific organizational processes and culture, the templates

may be leveraged as deemed necessary to support specific organizational needs. It is up to the discretion of the Documenters to decide the best approach for their organization.

SOLUTION SET REQUIREMENTS

The first part of designing the solution set involves gathering the functional requirements. These requirements are extrapolated from various Business, Information, and Technology Architecture components and from information previously identified in the Gap and Migration Strategies. During creation of the desired solution set type, the information is refreshed for timeliness and accuracy by working with the business users and sponsors of the project or effort. The requirements must be in sufficient detail to enable the development of the Solution Set Logical Model and the design specifications which will occur in subsequent phases of the process.

REQUIREMENTS VIEWS

To assist with the collecting of information, the Solution Set Type section on the template is further divided into various "views". The use of views helps the Solution Architect ensure all of the information for the solution has been collected, based on the various aspects or discrete focuses of the solution. The typical views that may be included when developing requirements include:

- *Business View* – Pertains to how business requirements will be addressed in the solution. This includes such requirements as financial, strategic planning, business cycles, organizational, business drivers, logistical, as well as policy and procedures. This view typically aligns with the information contained within the Business Architecture blueprint.
- *Security View* – Pertains to how security requirements will be addressed in the solution. These requirements may be in terms of physical security, human resource security, information security, and IT security. They are grouped into security categories known as management, operational, and technical security controls.
- *Information View* - Pertains to how information requirements will be addressed in the solution. This typically includes such requirements as process flows, information ownership, metadata, spatial data, data architecture, data standards, document management, knowledge management, and content management.
- *Application View* – Pertains to how application system requirements and design considerations will be addressed in the solution. This typically includes such categories as application functionality, application structure, performance, reliability, availability, and maintainability.
- *Usability View* - Pertains to how application system usability requirements and design considerations will be addressed in the solution. This typically includes the graphical user interface (GUI), any dialogs and queries that need to be performed by the application, any input forms to be developed, any user reports that the system needs to produce, and accessibility needs.
- *Infrastructure View* - Pertains to how IT infrastructure requirements and design considerations will be addressed in the solution and typically includes such categories as hardware, software, voice, middleware, and databases.
- *Integration View* - Pertains to how the results of the Solution Set will integrate with components of the existing environment. This includes such integration requirements as process, application, infrastructure, and those requirements external to the organization. It is also concerned with the impacts to the current environment in the form of training, resources, capacity, performance, and bandwidth. The integration requirements addressed in the solution may be categorized as training, capacity, performance, and managerial.

Categories

The Solution Set Requirements template also leverages the usage of 'categories' as a mechanism for classifying requirement sub-types. These category lists are for illustration purposes only and help to further identify the areas within the enterprise architecture that the Solution Architect will need to examine for potential component reuse. In addition, it will also help to identify those areas of responsibility for coordinating changes or solution dependencies. For a list of categories as defined on the Solution Set Requirements templates, please reference the specific template section of the manual.

Your organization may or may not leverage the use of categories. If they do, they may be similar to the categories discussed in the Requirements templates section; however, it is unlikely that they will perfectly match. The Solution Architect may choose to leverage the use of categories. If this is indeed the case, they may customize these categories to fit their environment and organizational standards.

Solution Set Design

Upon establishing all the necessary Solution Set requirements, the Solution Architect's attention turns to developing the Solution Set designs and logical models via the design process. The *Solution Set Design* template assists in the development of these solution set designs.

The Solution Set Design template is used to capture the various design specifications, dependencies, and other organizational and environmental impacts. It is linked to existing enterprise architecture artifacts, models, and patterns. If there are no existing artifacts that substantiate the logical model it is quite possible that architecture gaps may result. If gaps are identified the solution set may be rendered architecturally non-compliant and an architectural review should be executed to determine if the solution should move forward. Architecture gaps identified at this point become dependencies of the Solution Set and, if they are not resolved, it is quite possible for the effort to be put on hold or terminated.

The actual design specifications documented in the Solution Set Design are at the lowest level of documentation. These specifications address the specific requirements captured when the solutions architect completed the Solution Set Requirements. Once the specifications are captured in narrative, they can be consolidated and represented in the form of logical design models.

Logical models will later be used to produce physical design models. The development of the physical design models is beyond the scope of the Solution Architecture process. Development of the physical models for the solution is typically completed within the standard SDLC or business process development methodologies within the organization.

Logical Models

After the design specifications have been documented and the appropriate EA components for fulfilling the design specifications have been identified, the logical model can be developed. A logical model is utilized for both business and technical models. For proposed business solutions a process model is created. If the solution being presented is an IT solution then a logical architecture model is developed.

It is quite possible for the Solutions Architect to create multiple logical architecture models depending upon the complexity and scope of the solution set. For example, the Solution Architect may propose process changes to a manual effort to solve a specific business need as well as an automated solution involving the development of a new IT system.

This logical model is used to:

- Validate and communicate the view of the proposed solution set to the business community and the project sponsor
- Determine the feasibility of the solution (e.g., technical, economic, operational, managerial, organizational)
- Show how the system will satisfy the user requirements
- Reflect underlying business rules and activities rather than physical constraints and systems
- Depict WHAT the solution will encompass, not HOW it will be accomplished
- Capture the most critical and essential information in a fairly quick and concise manner

The logical model is captured in the form of a visual depiction of the solution with simple narrative about its included components.

After all the requirements are documented, the design specifications are identified, and the logical model is complete, the Cost/Benefit analysis and initial Project Plan should be augmented to include the additional information captured during this process. The Solution Set Design activity concludes with a decision whether to pursue the desired solution. If there are multiple solutions presented, a selection is made on which solution is preferred and the design portion of the solution begins.

SOLUTION ARCHITECTURE DEVELOPMENT

The process of developing the Solution Architecture begins with initiating the Solution Architecture Documentation Process. This documentation process enables the architecture teams to develop the Solution Architecture Framework and to capture, analyze, and document requirements and design details about a specific project or effort.

The work flow moves through the many layers of the process models and its sub-processes. Figure 5 provides a graphical representation of the high-level workflow path for the architecture team as they move through the processes and sub-processes of the Solution Architecture Documentation Process.

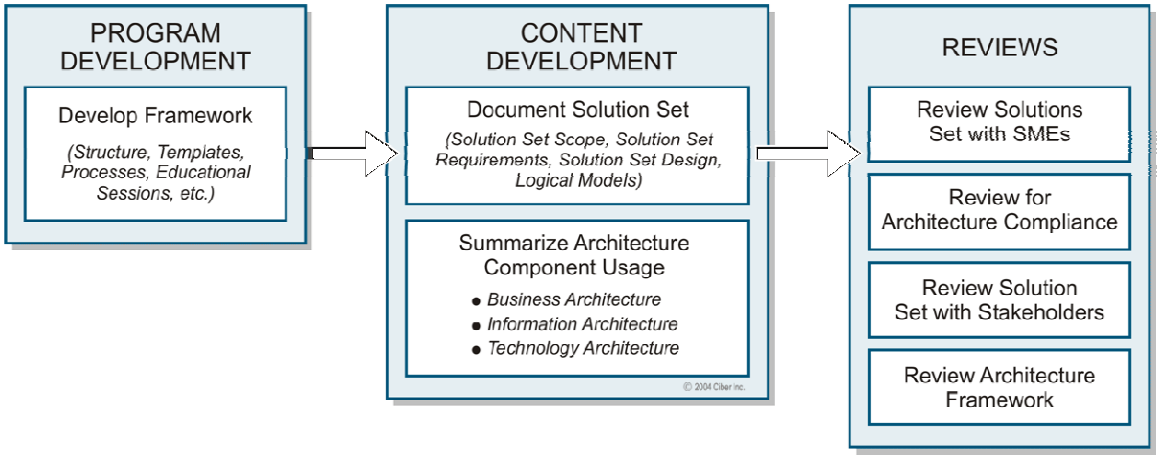


Figure 5. Solution Architecture Development Work Flow

The Solution Architecture Documentation Process encompasses two major development phases: the creation of the framework and the development of a Solution Set, utilizing the structured processes and templates defined. Once the framework is established and approved, it remains constant until the Solution Architecture vitality process is invoked. The development of a Solution Set, however, is executed each time an approved project is selected for execution from the Implementation Plan.

During the Solution Architecture Documentation Process for the Solution Set, details for a specifically selected solution are captured. This detail includes the scope of the particular project or effort, the functional and technical requirements, the design specifications, and lastly, the logical models that graphically depict the proposed solution.

The Documenters develop the Solution Set by interviewing various Subject Matter Experts regarding the solution specifics. These explicit details of the solution are captured in the Solution Set.

The Solution Architecture Documentation Process describes the systematic process for developing and maintaining the Solution Architecture Framework and various Solution Sets. The Solution Architecture Documentation Process consists of several sub-processes, including:

- Initiate Solution Architecture Documentation Process
- Conduct Solution Architecture Work Sessions
- Create/Update Solution Set Items

- Solution Set Vitality Review

The structure for each sub-process of this Solution Architecture Documentation Process follows the same format:

- Introductory material (where applicable)
- Process model
- Narrative description of the process
- Template for capturing Solution Set detail (where applicable)
- Narrative description of the detail to be captured utilizing the template

Initiate Solution Architecture Documentation Process

THE PROCESS OVERVIEW

The Initiate Solution Architecture Documentation Process presented here is similar to the generic process model provided in the Architecture Governance Section of the Tool-Kit. This model and narrative provides the initial process steps that are specific to the Solution Architecture.

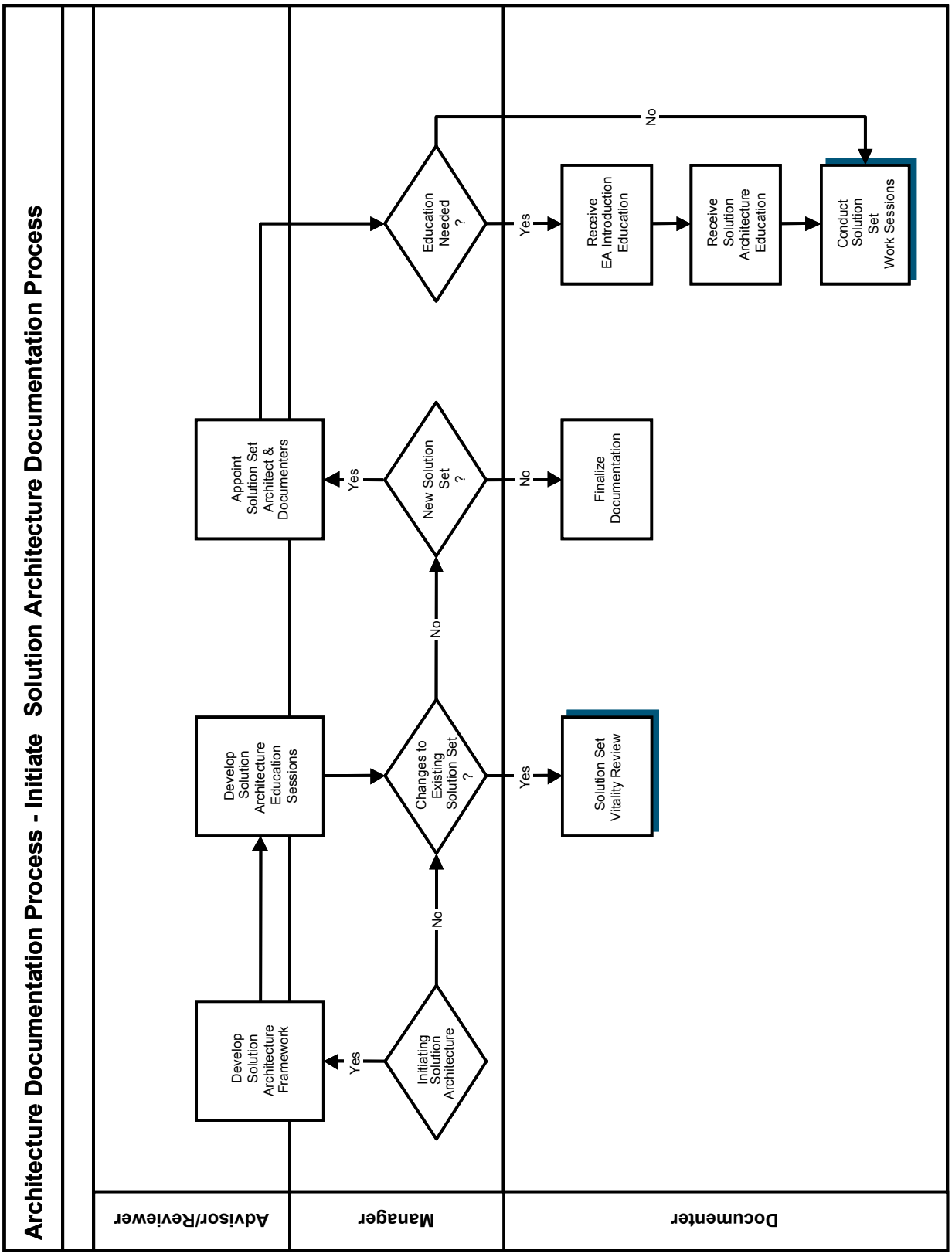
The Solution Architecture Documentation Process can be triggered by the following processes/activities:

- Initiating Solution Architecture (SA)
- Architecture Framework Vitality Review
- Solution Set Vitality Review
- New Solution Set

During the initiation of the Solution Architecture Documentation Process, the Solution Architecture Framework is developed. In this Tool-Kit, the term Architecture Framework refers to the combination of the structural elements of the architecture, including the structure of the templates and the structured processes for documenting, reviewing, communicating, implementing, and maintaining the Architecture Framework.

Each governmental organization should develop a Solution Architecture Framework based on their individual circumstances and build the unique Solution Set team with the appropriate blending of business and technical Subject Matter Experts. The NASCIO Tool-Kit is designed to provide a jumpstart for organizations as they develop their architectures, not to provide a methodology. The Framework elements provided in this Tool-Kit represent a sampling of the structural elements an organization should consider as they build their Solution Architecture and is by no means exhaustive, nor is it intended to be prescriptive.

There are many methods for designing solutions. Regardless of the one selected, the structure for capturing Solution Set detail should be consistent and concise to ensure uniform documentation and communication across the enterprise.


Architecture Documentation Process - Initiate Solution Architecture Documentation Process
Advisor/Reviewer
Manager
Documenter
Develop Solution Architecture Framework
Initiating Solution Architecture
Yes
No
Develop Solution Architecture Education Sessions
Changes to Existing Solution Set ?
Yes
No
Solution Set Vitality Review
Appoint Solution Set Architect & Documenters
New Solution Set ?
Yes
No
Finalize Documentation
Education Needed ?
Yes
No
Receive EA Introduction Education
Receive Solution Architecture Education
Conduct Solution Set Work Sessions

THE PROCESS DETAIL

Develop Solution Architecture Framework – By using the Solution Architecture Framework, the Solution Set detail is captured and the Solution Set is created. The NASCIO Solution Architecture Framework provides the structure, processes and templates necessary for capturing specific Solution Set information. An enterprise may decide to use the framework described in the NASCIO Tool-Kit or may choose other processes, templates, and governance structure.

Developing the processes and templates for capturing pertinent architecture detail, as well as defining and documenting the governance structure to support the architecture activity, is a step that is critical when initiating any of the architectures (e.g. Business, Information, Technology, and/or Solution Architecture). Each enterprise must decide upon the methodology that best suits their organization. The best methodology for an organization is one that addresses the resource and time constraints of that enterprise.

It is best to consider the use of a repository or automated tool for the capture and storage of the architecture documentation. The use and maintenance of the Enterprise Architecture is greatly simplified when the information and models are readily available to all stakeholders. There is a large amount of information collected and documented within an EA with many interrelations among the various EA components. It is best if all the EA information, design models and solution sets are placed in a robust EA repository to maximize the potential for reuse.

Develop Solution Architecture Education Sessions – The Solution Architecture Education Sessions provide a high-level overview of the Enterprise Architecture Program and prepare the Solution Set Documenters for their role in the Solution Architecture effort. Developers of education materials should consider inclusion of the following materials:

- Purpose
- Presenters
- Intended audience
- Session structure
- Prerequisites
- Syllabus
- Objectives
- Class materials for both instructors and attendees

Finalize Documentation – The Solution Architecture educational materials should be finalized and stored with the other Enterprise Architecture training materials.

Solution Set Vitality Review – If the Solution Set is being modified due to changes in scope, requirements, or design options, the various Solution Set items should be updated. In addition, if changes have occurred in Business, Information, or Technology Architecture blueprints that are referenced in a particular Solution Set, the Solution Set should be reviewed carefully to assess potential impacts. The process model and details pertaining to updating the Solution Set are presented in a separate process. (See *Solution Set Vitality Review*).

Appoint Solution Set Architect & Documenters – The Solution Set Architect and Solution Set Documenters are appointed from subject matter experts familiar with the business and technical views of the enterprise. The team is comprised of business analysts who have expertise in the various aspects of the specific business area needing the solution. They are responsible for steering, shaping, and developing the

scope and requirements of the solution set. If the Solution Set encompasses the design of a business application system or an IT infrastructure component, then it should also include the various technical subject matter experts that can adequately represent the identified technical area.

The team should also include a Solutions Architect who is knowledgeable about the various solutions development processes and methodologies. It is the Solution Architect's responsibility to ensure that the solution set is designed to:

- Meet the business need
- Leverage the Business, Information, and Technology Architecture blueprints previously created in the Enterprise

The educational sessions described below are progressive in nature. The sessions will be conducted after the architecture team is identified:

Receive EA Introduction Education – Documenters should receive initial training that covers the overview of enterprise architecture and architecture governance.

Receive Solution Architecture Education – After receiving initial enterprise architecture training, the Documenters will receive specialized instruction addressing the Solution Architecture documentation templates and Solution Architecture documentation processes to be used to document a Solution Set. If the Documenters and Solution Architect are expected to start work on the development of a specific Solution following the delivery of the education, the documentation used during the session should include specific project detail found in the associated Implementation Planning, Gaps, and Migration Strategies items.

Conduct Solution Set Work Sessions – Applying the knowledge gained in the two sessions, the Solution Architect and Documenters will begin development of the Solution Set. The detail of the Work Sessions is presented in a separate process. (See *Conduct Solution Architecture Work Sessions*).

Conduct Solution Set Work Sessions

Process Overview

The Solution Set Work Sessions are intended to produce the documentation that populates the Solution Set. The Solution Architecture is best documented by stakeholders involved in setting the scope, developing the requirements, and designing the solution. This will include various business and technical subject matter experts as well as those individuals who assisted in the development of the Implementation Plan item that identified the Solution Set project or effort. Ongoing Documenter meetings with the appropriate mix of business and technical Subject Matter Experts are required to document the specific solution set. The first session will include:

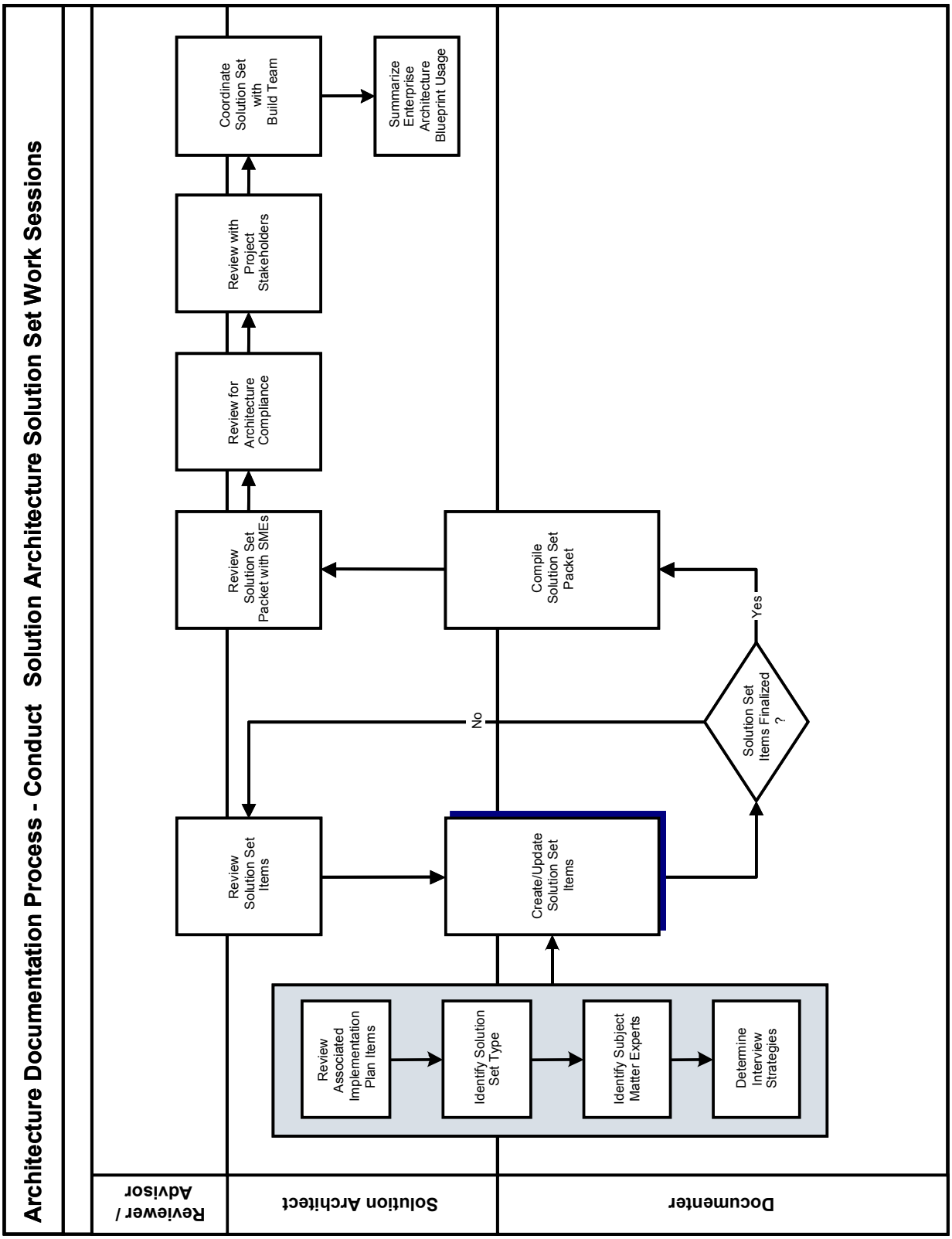
- Defining roles and responsibilities
- Reviewing Solution Set documentation requirements
- Determining expectation of follow-on meetings

After the first meeting, on-going working sessions are triggered from Architecture Lifecycle Processes including:

- The need to complete the Solution Set documentation
- Solution Set Vitality Process

The creation of the Solution Set provides the architectural design to solve a specific business need. Analyzing the various components of the Solution Set facilitates the process of articulating a design that can be readily developed and implemented. Individual requirements can be met by existing architectural components from the Business, Information, and Technology Architecture blueprints.

The Solution Set Work Sessions typically continue until the Solution Set design is complete and approved by the stakeholder. Work sessions may start again if the Solution Set scope changes, if additional requirements are identified, or if the logical models are modified by the introduction of new architecture components or architecture patterns. In addition, the work session may commence again if the original project is halted and restarted at a later date. If this occurs, it will be necessary to re-validate the original scope, requirements and proposed design. The re-validation is required because of the dynamic nature of the Business, Information, and Technology Architecture blueprints. If items within the blueprints have been updated while the project was inactive, and the original assumptions and conclusions may no longer be valid.


Architecture Documentation Process - Conduct Solution Architecture Solution Set Work Sessions
Reviewer / Advisor
Solution Architect
Documenter
Review Associated Implementation Plan Items
Identify Solution Set Type
Identify Subject Matter Experts
Determine Interview Strategies
Review Solution Set Items
Create/Update Solution Set Items
Solution Set Items Finalized ?
No
Yes
Compile Solution Set Packet
Review Solution Set Packet with SMEs
Review for Architecture Compliance
Review with Project Stakeholders
Coordinate Solution Set with Build Team
Summarize Enterprise Architecture Blueprint Usage

THE PROCESS DETAIL

Review Associated Implementation Planning Items – The project definition, scope, gap, and migration information developed as a part of Implementation Planning should be provided to the Documenters and the Solution Architect. The team will update the basic definitions as necessary and identify any additional information. During this process the scope of the solution is further developed and the Solution Set is defined in greater detail. The Documenters and Solution Architect are responsible for gathering all necessary information required to complete the Solution Set Scope template.

Identify Solution Set Type – Based on the information obtained from a review of the Associated Implementation Plan Items, the Solution Architect and the Documenters will determine the type of Solution Set being designed. The solution may consist of one or multiple types of solutions. This *may* include the following:

- **Business Solution** – The solution will implement a business process improvement, organizational change, or other type of business solution.
- **Application Solution** – The solution will involve the purchase and/or development of an application system.
- **IT Infrastructure Solution** – The solution will involve the purchase and/or design of IT infrastructure components

The identification of the solution set type is necessary so that the team can identify the appropriate resources to provide Solution Set requirements, contribute to design specifications, and assist with the development of the Solution Set logical models.

Identify Subject Matter Experts – Subject Matter Experts are experts in the area of the enterprise business and will assist in the identification of the scope of the Solution Set. These Subject Matter Experts will contribute to the development and detail of defining the Solution Set requirements, design specifications, and design models.

Additionally, the Subject Matter Experts with the detailed knowledge of the various specifications are identified. If the Solution Set involves organizational processes and information, these individuals may be the same Subject Matter Experts as previously identified. If the Solution Set involves the creation of an IT business system or related IT infrastructure, the Subject Matter experts will be from areas specific to the IT solution area. This may include Subject Matter Experts knowledgeable in application development methodologies, tool, and development environments. It may also include experts knowledgeable in technology infrastructure areas such as security and networks.

Determine Interview Strategies – Interview meeting topics should be determined in one of the first working sessions. Interview questions should be designed to streamline the interview process and get the most information in a minimum amount of time. In addition, it is sometimes helpful to hold the interviews in a location away from the interviewees primary work location. This will help focus discussions and avoid repeated work related interruptions.

Approaches for determining interview strategies can be based on:

- The Solution Set views necessary to complete the design. These views are intended to help the solution architect collect all the information for the solution and are based on various aspects or discrete focuses of the solution. The specific types of views that may be included when developing requirements include:

- **Business View** – Pertains to how business requirements will be addressed in the solution. This includes such requirements as financial, strategic planning, business cycles, organizational, business drivers, logistical, policy, and procedures. This view typically aligns with the information contained within the Business Architecture blueprints.
- **Security View** – Pertains to how security requirements will be addressed in the solution. These requirements may be in terms of physical security, human resource security, information security, and IT security. They are grouped into security categories known as management, operational, and technical security controls.
- **Information View** – Pertains to how information requirements will be addressed in the solution. This typically includes such requirements as process flows, information ownership, metadata, spatial data, data architecture, data standards, document management, knowledge management, and content management.
- **Application View** – Pertains to how application system requirements and design considerations will be addressed in the solution. This typically includes such categories as application functionality, application structure, performance, reliability, availability, and maintainability.
- **Usability View** – Pertains to how application system usability requirements and design considerations will be addressed in the solution. This typically includes the graphical user interface (GUI), any dialogs and queries that need to be performed by the application, any input forms that need to be developed, any user reports that the system needs to produce, and accessibility needs.
- **Infrastructure View** – Pertains to how IT infrastructure requirements and design considerations will be addressed in the solution and typically includes such categories as hardware, software, voice, middleware, and databases.
- **Integration View** – Pertains to how the results of the Solution Set will integrate with components of the existing environment. This includes such integration requirements as process, application, infrastructure, and those external to the organization. It is also concerned with the impacts to the current environment in the form of training, resources, capacity, performance, bandwidth, and so forth. The integration requirements addressed in the solution may be categorized as training, capacity, performance, and managerial.

- The functional requirements to be documented. This format captures the necessary Solution Set requirements that must be satisfied in order to meet the business need.
- Developing design specifications.
- Determining other organizational and system impacts.

Create/Update Solution Set Items – At this point in the process interviews will be conducted and the Solution Set documentation will be undertaken. The Solution Set items include the Solution Set Scope, the Solution Set Requirements, and Solution Set Design.

A separate process model and narrative for this sub-process will provide greater detail (See *Create/Update Solution Set Items*)**.**

Review Solution Set Items - The number and point of reviews should be determined for each Solution Set. For complex projects, it may be appropriate to have interim reviews at the completion of scope and again at the completion of the requirements. The Reviewers, who should include the project sponsor and designated representatives from the architecture community, can add valuable insight from an over-arching perspective.

Compile Solution Set Packet – When the Solution Set design specifications, solution impacts, and design model(s) are complete, a summary should be compiled and the various pieces of the Solution Set

documentation should be submitted for review. A packet containing the completed Solution Set documentation will be compiled in preparation for formal review. This is typically reviewed by the project manager, all project Subject Matter Experts, the chief architect, and representatives from the impacted functional areas.

Review Solution Set Packet with SMEs – The Solution Set Architect as well as the SMEs that contributed to the effort will verify the final contents of the Solution Set Packet and work with the Documenters to make modifications as necessary. This review provides the opportunity for those who participated in the definition of the requirements and/or design to see and provide feedback on the final product.

Review for Architecture Compliance – The Solution Architect will review the Solution Set Packet with the various architecture representatives, ensuring that the Solution Set is in compliance with the documented architecture components:

- Business Architecture – Business Architecture Components
- Information Architecture – Process and Information Meta Components.
- Technology Architecture – Product and Compliance Components.

If inconsistencies are found, the Solution Architect will work with the Documenters to make modifications as necessary, to recompile the Solution Set Packet and to start the review process again.

Review with Project Stakeholders – The Solution Architect will review the Solution Set Packet with the various stakeholders of the project (e.g., project sponsor) ensuring the Solution Set is designed to meet the original needs of the project. If for any reason the Solution Set does not meet the expectations of the stakeholders, the Solution Architect will work with the Documenters to make modifications as necessary, recompile the Solution Set Packet, and start the review process again.

Coordinate Solution Set with Build Team – When the Solution Set is approved, it must be referred to the team responsible for executing the Business Development Process or the SDLC. All information obtained in the Solution Set (e.g., project scope, requirements, design specifications, impacts, logical models) will be needed by the project team to actually develop and implement the solution. The Solution Architect will ensure that the Solution Set Packet is understood and accepted by the build team.

Summarize Enterprise Architecture Blueprint Usage – The Solution Architect will create a summarization of the BA, IA, and TA blueprints or patterns that were referenced when the Solution Set was designed. If the Solution Set Design identified gaps within the existing architecture, a list of those gaps, as well as the completion of the necessary gap component, will also be completed. The Enterprise Architecture Blueprint Usage report serves to identify the changes to the Application Portfolio as well as identify follow-on activities to address the gaps in the architecture blueprints.

Create/Update Solution Set Items

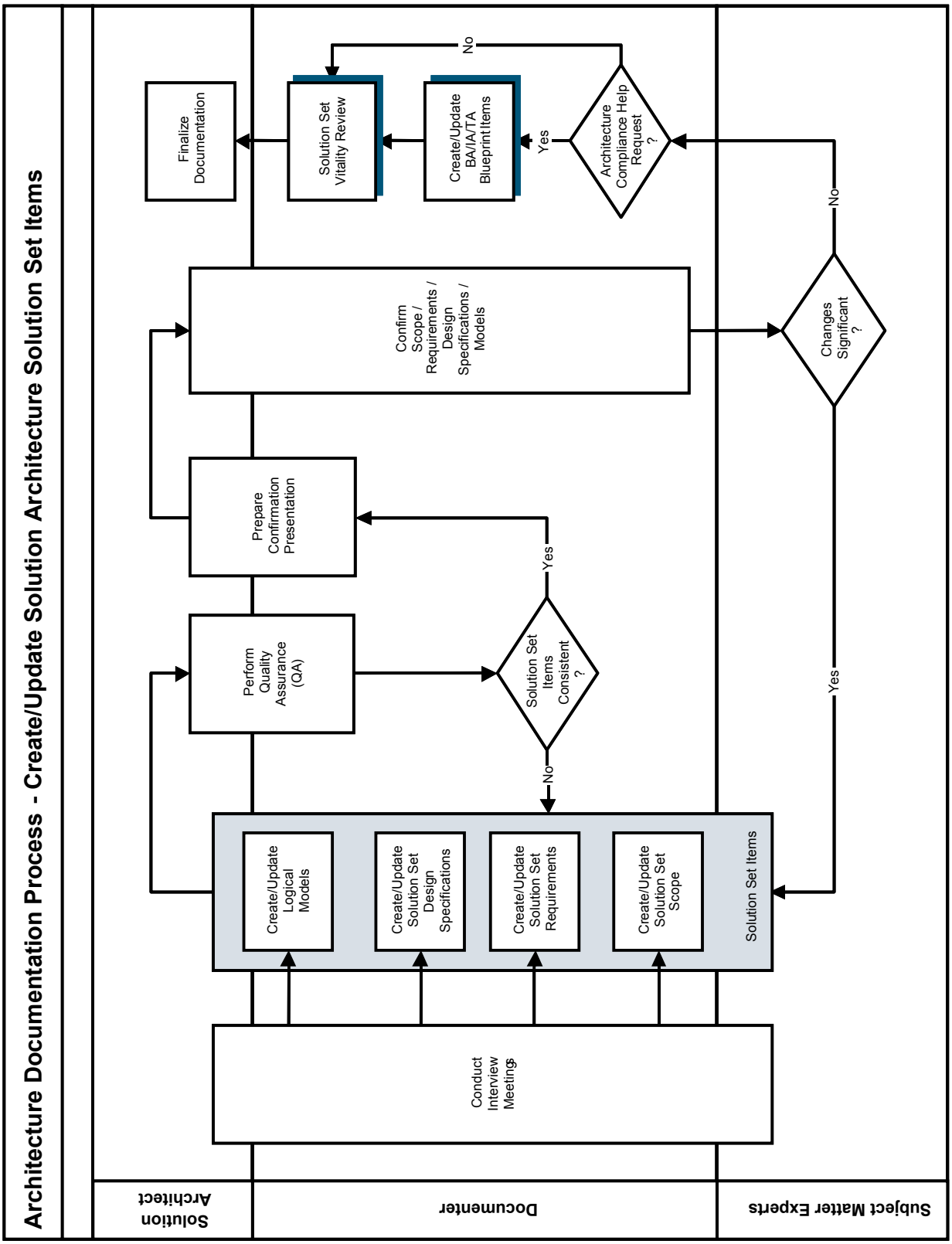
PROCESS OVERVIEW

The Solution Set items consist of the definition of solution scope, the solution requirements, design specifications, impacts, and logical models. These items, collectively known as a Solution Set, describe the overall design architecture for a specific solution effort or project.

Solution Set specifics are identified during the Solution Architecture interview process and documented within each of the Solution Set views as appropriate. The Solution Architecture team, and Subject Matter Experts determine the information to be documented and which Solution Architecture views are necessary to complete the solution design specifications.

For example, if the solution set type is an Application System, the views that would be documented might include: business, security, application, usability, and integration. The process would ensure that the Solution Architecture team collects the appropriate requirements, documents the matching design specifications, considers organizational and technical impacts, and lastly, builds the logical model for the solution.

This process, which results in defining/updating the Solution Set items, collects, organizes and documents the data that pertains to the specific solution. The detail is collected via interviews with a mix of Subject Matter Experts, from executives through line managers. Getting good results from interviews of key staff requires a team composed of individuals who are experienced and have both knowledge of their area and a commitment to the enterprise architecture process.


Architecture Documentation Process - Create/Update Solution Architecture Solution Set Items
Solution Architect
Documenter
Subject Matter Experts
Conduct Interview Meetings
Create/Update Logical Models
Create/Update Solution Set Design Specifications
Create/Update Solution Set Requirements
Create/Update Solution Set Scope
Solution Set Items
Perform Quality Assurance (QA)
Solution Set Items Consistent ?
No
Yes
Prepare Confirmation Presentation
Confirm Scope / Requirements / Design Specifications / Models
Changes Significant ?
No
Yes
Architecture Compliance Help Request ?
Yes
No
Create/Update BA/IA/TA Blueprint Items
Solution Set Vitality Review
Finalize Documentation

PROCESS DETAIL

Conduct Interview Meetings – When the subject matter experts have been identified and the interview strategy has been determined, the interview meetings can be scheduled. When obtaining and documenting the Solution Set requirements, allow at least two hours per session. More sessions may need to be conducted depending upon the complexity of the Solution Set and the various Solution Set views that need to be documented. It is also quite possible that several sessions will need to be conducted to document the Solution Set Design Specification and solution impacts. These sessions should allow enough time for the experts to identify all the design criteria.

Items that will contribute to successful interviews include:

- *Plan the Meeting Topics* – Meetings are typically organized around a specific view within the Solution Set. The views should have been determined during an interview strategy session, which is typically one of the first work sessions scheduled. Often, new requirements and views will surface during the interviews. If this occurs, these should be documented and the original strategy modified to assure that all views of the Solution Set area addressed in the interviews. It is best to assign each interviewer a specific Solution Set view for which they are responsible.

  Though everyone will be involved in the interviews from a general view, it helps to give each interviewer an area of focus based on the view to be covered for the proposed Solution Set. Before the interviews, each interviewer should plan questions based on their assigned view. This will help to ensure the coverage of all aspects. It is also helpful to have an individual assigned as a scribe. This allows the interviewers to focus their attention primarily on the interviewing process and less on taking notes.
- *Produce Meeting Notes* – Knowing who participated in providing the subject matter is very useful. During the interview sessions, Subject Matter Experts or various architecture participants may be asked to follow up with action items or to share documentation and research on specific items. For this reason, meeting notes should be taken, reproduced and distributed as they are done for any other formal meeting. Parking lot issues or unresolved items often result during interview meetings. These items need to be compiled, returned to the person interviewed for feedback, and documented in the interview strategies or the summary documentation.
- *Conduct Follow-up* – Following interview meetings with subject matter experts, some items may require resolution or additional action. These activities may include, but are not limited to, the following:
  - Changes to Interview Strategy: Based on interview feedback, the style and/or strategy of subject matter expert interviews may be changed
  - Resolution of Items: Dissention or ambiguity may necessitate resolution and/or direction from Architecture Subject Matter Experts, Executives, Managers or Reviewers
  - Clarification: The Documenters may need additional information on a topic
  - Parking Lot Items: Items that are currently out of the defined scope, but have been identified as potentially requiring future action

Create/Update Solution Set Scope – The Solution Architect and Documenters, with input from the appropriate Subject Matter Experts will define the scope of the Solution Set. This will also include boundary statements and links to the reference material that will be needed when completing the rest of the solution set requirements and design specifications. The Solution Set Scope template is a form that can be used for documenting this detail. See *Solution Set Scope Template.*

Create/Update Solution Set Requirements – The Documenters and Solution Architect capture detail about the Solution Set requirements, such as the specific views being addressed, the sub-category of the requirement, requirement statements, requirement owners, and the related EA components that identified the original business need. The Solution Set Requirements template is a form that can be used for documenting this detail. See *Solution Set Requirements Template.*

Create/Update Solution Set Design Specifications – The Documenters and Solution Architect capture detail about the Solution Set design specifications such as the specific views being addressed, the sub-category of the design specification, design specification statements, and the related EA components that satisfy the design. The Solution Set Design template is a form that can be used for documenting this detail. See *Solution Set Design Template.*

Create/Update Logical Models – Upon completion of documenting the Solution Set requirements, design specifications, organizational impacts, and technical impacts, the Solution Architect is ready to build the Solution Set Logical Model. The model is a graphical representation of the Solution Set and is typically inserted or referenced on the Solution Architecture Requirements Template. This template is a form that contains the design specifications and it can be used for referencing the logical model as well. See *Solution Set Design Template.*

Perform Quality Assurance (QA) – The various Solution Set items and models require verification by the architecture team prior to confirmation with the Subject Matter Experts. This quality assurance step allows the team to verify that the various components are utilizing the same glossary of terms and that the team's understanding of the various components of the Solution Set is the same.

Prepare Confirmation Presentation – The Solution Architect and Documenters will compile the information from the meeting notes, the documented Solution Set and associations, and the quality assurance check. This information will be utilized to confirm the accuracy of the information captured.

Confirm Scope/Requirements/Design Specifications/Models – Once the architecture team has verified consistency in how they are defining and representing the Solution Set, the team will confirm the requirements, design specifications and logical models with Business and Technology Subject Matter Experts. This should be an interactive session where modifications and enhancements are noted. Some changes can occur during the session, while others will take more time and will be conducted in "pick-ups" after the session. If the changes to the requirements/design specifications/models take place outside the session, an electronic copy of the changes should be sent out for approval. If the changes were significant, the potential exists to call another meeting to confirm those changes.

Create/Update BA/IA/TA Blueprint Items – If components are identified during the Solution Set documentation process that are needed for the particular Solution Set but do not currently exist as part of the architecture, the appropriate Business, Information or Technology Architecture Blueprints should be updated. However, this should be initiated via an Architecture Help Request so the proposed blueprint changes are coordinated with the appropriate architecture and governance community.

- For updates to the Business Architecture Components see Business Architecture – Create/Update Business Architecture Blueprint Items
- For updates to the Process and/or Information Meta Components see Information Architecture – Create/Update Information Architecture Blueprint Items
- For updates to the Product and/or Compliance Components see Technology Architecture – Create/Update Technology Architecture Blueprint Items

Solution Set Vitality Review – The Solution Architect and Documenters will perform a vitality review of all items in the Solution Set ensuring that the proposed Solution Set is still valid and does not need to be

updated to reflect the results of the Architecture Compliance Help Request or additions or updates to Business Architecture, Information Architecture, or Technology Architecture blueprints. If changes are necessary, then the team must initiate the *Solution Set Vitality Review* process.

Finalize Documentation – When the Solution Set detail has been confirmed, an update of the status and audit trail detail will occur. The final action is to submit all Solution Set details for inclusion in the Solution Architecture documentation.

Solution Set Scope Template

TEMPLATE OVERVIEW

The Solution Set Scope template provides an instrument for documenting the scope of the solution in an electronic format. The visual representation of the Solution Set Scope template is followed by a detailed description of the contents to be captured.

When populated, this template provides the necessary background information for the effort. It contains a link to the proposed solution's conceptual model contained in the Implementation Plan as well as links to all the reference material that will be needed when completing the rest of the solution set requirements and design specifications.

Important items to keep in mind when completing the Solution Set Scope template are:

- The Solution Set Scope template reuses critical information previously identified in the allied architecture processes.
- The information referenced on the Solution Set Scope template is used to ensure that the Solution Architect has a complete view of all the known information about the effort being undertaken. Various pieces of information, such as high-level requirements and dependencies, are contained in the associated gap and migration strategies. Other information, such as the proposed future state, is identified on the original Business Architecture, Information Architecture, or Technology Architecture blueprints.

  Project specific information, such as project dependencies, risk analysis, cost/benefit analysis, and the conceptual model designed for the solution are contained within the specific Implementation Planning item. The Solution Set Scope template brings all this information together.
- The Solution Set may address multiple solution types.

  It may be possible for a Solution Set to have a combination of a business solution and an application solution that need to be designed. If this is the case, a Solution Set Scope template and Solution Set Requirements templates should be completed for these Solution Set types.
- The conceptual model for the solution set is created as a part of Implementation Planning.

  The conceptual model, which will be used during the Solution Architecture process, is created during the Implementation Planning effort. The conceptual model and the high-level requirements that are documented during the Implementation Planning process are used to frame or scope the Solution Set effort.

Solution Set Scope

Definition				
Name				
Description				
Rationale				
Benefits				
Boundary				
Boundary Scope Statement				
Associated Implementation Plan Items				
Implementation Plan Project Identifier				
Plan Items Solution Set is Dependant Upon				
Plan Items Dependant Upon Solution Set				
Related Migration Strategies				
Selected Solution Set Conceptual Model				
Solution Set Types	☐ *Business*	☐ *Application*	☐ *IT Infrastructure*	
Keywords				
Keywords / Aliases				
Contact Information				
Project Sponsor				
Implementation Plan Coordinator				
Solution Set Architect				
Solution Set Contributors				
Contract Information				
Name				
Reference Number				
Contact Information				
Implications				
Current Status				
Solution Set Status	☐ *In Development*	☐ *Under Review*	☐ *Approved*	☐ *Rejected*

AUDIT TRAIL			
Creation Date		*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Updated By			
Reason for Update			

TEMPLATE DETAIL

DEFINITION

Name – The Solution Architect will determine the name for the solution set based on the associated Implementation Plan item. It should be followed by the type of template (e.g., Solution Set Scope, Requirements, or Design) because the name will be used again as the Plan name. Example: *Department of Human Resources Portal – Solution Set Scope*.

Description – An appropriate description of the solution being undertaken in a paragraph or two that provides sufficient clarity to the reader about the effort. It should clearly identify the specific migration strategy that is being undertaken and how this migration strategy impacts any other associated migration strategies (if necessary).

Rationale – An explanation of the reason(s) for this solution being designed and implemented. This could include linkages to strategic and/or operational plans or other business drivers

Benefits – A paragraph or bulleted statements that provide the benefits associated with the solution.

BOUNDARY

Boundary Scope Statement – The boundary scope statement provides parameters for identifying the boundaries for the solution. This section includes statements about what is included, as well as items that are related to, but excluded from, the solution. If this is an incremental solution it is important to denote that this is a portion of the overall solution.

ASSOCIATED IMPLEMENTATION PLAN ITEMS

Implementation Plan Project Identifier - Identify the associated Implementation Plan item that this Solution Set is addressing and follow it by the actual name of the Implementation Plan item name.

Plan Items Solution Set is Dependent Upon – List any other Implementation Plan items that are dependent upon this solution's implementation. This is important because if this solution is not completed the other plan items will also not be able to be completed. The list should contain the plan item number followed by the name of the plan item.

Plan Items Dependent Upon Solution Set – List any other Implementation Plan items that are dependent upon this solution's implementation. This is important because if this solution is not completed the other plan items will not be able to be completed either. The list should contain the plan item number followed by the name of the plan item.

Related Migration Strategies – Document the related Migration Strategy for the Solution. The Migration Strategy is part of the Implementation Plan.

Selected Solution Set Conceptual Model – Document the link to the associated Conceptual Model that was used to establish the high-level view of the solution set. This Conceptual Model is a part of the associated Plan Item number.

Solution Set Types – List the type of solution that will be designed for this Solution Set effort. The solution may consist of one or more solution types. This *may* include the following:

- **Business Solution** – The solution will implement a business process improvement, organizational change, or other type of business solution.

- **Application Solution** – The solution will involve the purchase and/or development of an application system.
- **IT Infrastructure Solution** – The solution will involve the purchase and/or design of IT infrastructure components

KEYWORDS

Keywords / Aliases - List any keywords that can be used to assist in searching the repository for information about the solution being designed and implemented. This information will be helpful for anyone looking for information regarding similar elements.

CONTACT INFORMATION

Project Sponsor - Identify the ultimate decision maker for the Solution Set. This may be the Project Sponsor, the Project Champion, or the Project Owner. This individual is typically responsible for (1) funding the solution, (2) ensuring that it remains a priority on the Implementation Plan, (3) providing the solution requirements, and (4) Approving/Accepting the Implemented Solution.

Implementation Plan Coordinator – Provide the name and contact information of the individual responsible for maintaining the detailed information on the Implementation Plan. This individual will be responsible for communication and coordinating external solution set requirements with the respective areas as well as with linked plan items.

Solution Set Architect – Identify the name of the primary architect who will be designing the solution. This will also be the individual who will work with the project team to obtain architectural review and approval of the design.

Solution Set Contributors - List the names and contact information of the individuals who will work with the Solution Architect to establish the requirements and design specifications for this solution set. One of the contacts should be identified as the solution set owner or business project manager. The designated persons should have sufficient knowledge of the solution set to be able to provide additional information or points of contact as needed. Other individuals listed should include Subject Matter Experts who will contribute to the various requirements (e.g. Security, Information).

CONTRACT INFORMATION

If this solution set is impacted by or is impacting an existing contract this relationship and an impact statement need to be documented. Contracts may impact specific Solution Set designs in terms of licensing requirements, simulations usage, authorizations, and so forth. The Solution Architect should also consider potential contract impacts to existing organizational contracts, contracts leveraged but owned by other government agencies, and contracts with customers or suppliers.

This section should be repeated for each contract that will be impacted by, or will impact, the specific Solution Set.

Name – List the specific contract name.

Reference Number – List the specific contract reference number that identifies the contract.

Contact Information – List the agency, vendor, or unit that provides ownership and review of the contract. In addition, list the address and telephone number of the contact point.

Implications – Document the specific contract implications that will occur if the Solution Set is approved and implemented. If the contract has impacted the Solution Set design, list what was impacted and how this impact is going to be resolved.

CURRENT STATUS

Solution Set Status – Document the status of the Solution Set, indicating whether the component is in development, under review, accepted, or rejected.

- *In Development* – The architecture team is currently crafting and/or reviewing the Solution Set detail.
- *Under Review* – The architecture team has completed the Solution Set documentation and it has been submitted for review. Possible reviewers may include members of the project team, the technical community, and the business community.
- *Accepted* – The Solution Set has been approved for submission to the appropriate build team.
- *Rejected* – The Solution Set has been rejected for reasons documented below in the Audit Trail section.

AUDIT TRAIL

Creation Date – Provide the date the Solution Set was created.

Created By – List the names and titles of the individuals who contributed to the creation of the Solution Set.

Date Accepted/Rejected – Provide the date the Solution Set was accepted or rejected.

Reason for Rejection – If the Solution Set was rejected, document the reason for the rejection. A Solution Set may be rejected for many reasons including, but not limited to, the following:

- Priority, resource, or timing issues rendered the Solution Set not viable at this time. Although the Solution Set is considered rejected for implementation, the original Implementation Planning items remain in effect should the project be re-initiated.
- The Solution Set represented one of several options for delivering the required functionality to the organization and another option was chosen. If this happens, the original Implementation Plan item should also be rejected and removed from the Implementation Plan.
- Predecessor projects were determined to have been necessary, so the Solution Set was put on hold until successful completion of the identified projects. Although the Solution Set is considered rejected for implementation, the original Implementation Planning items remain in effect should the project be re-initiated.
- Necessary architecture components were identified as missing from the existing Enterprise Architecture blueprint. In this event, the Solution Set project must wait until the architecture gaps are filled. Although the Solution Set is considered rejected for implementation, the original Implementation Planning items remain in effect should the project be re-initiated.

Last Date Reviewed – Document the most recent date the Solution Set was taken through the Solution Set Vitality Process. This will occur if the Solution Set has been changed after the solution design has previously been approved but not executed.

Last Date Updated – Document the most recent date that any item in the Solution Set documentation was changed.

Updated By – List the names and titles of the individuals who updated this Solution Set.

Reason for Update – Document the reason for the update to the Solution Set.

Solution Set Requirements Template

TEMPLATE OVERVIEW

The Solution Set Requirements template provides a tool for documenting the Solution Set requirements in an electronic format.

To aid the Solution Set Architect and Documenters, requirements are categorized into types, thereby enabling the team to identify the Subject Matter Experts with whom coordination is necessary during the development of the Solution Set. Some typical solution types may include:

- **Business Solution** – The solution will implement a business process improvement, organizational change, or other type of business solution.
- **Application Solution –** The solution will involve the purchase and/or development/modification of an application system.
- **IT Infrastructure Solution** – The solution will involve the purchase and/or design of IT infrastructure components.

When completely populated, this template provides the detailed requirements necessary to create the solution design.

REQUIREMENT VIEWS

The Solution Set Requirements template is designed to be generic in nature because each "view" requires documentation that is structurally similar. The template sections can be repeated as necessary to accommodate any combination of solution types and views. This keeps the template simple, while allowing for the documentation of specific requirements based upon the needs of the solution set.

The Solution Set Requirements template is organized by "views" and "categories". The various views and categories, defined below, help to further identify Subject Matter Experts and ensure that the necessary Solution Set requirements are identified. These views are also used when identifying the associated design specifications and the logical design models after data collection and analysis. The list of potential views for the Solution Set Requirements template is described below.

Business View

The Business View provides a tool for documenting business requirements that will be addressed in the solution. These requirements relate to anything causing changes or updates to the following:

- **Financial** – Monetary or accounting systems that systematically record, present, and interpret financial accounts.
- **Strategy and planning** – The processes that select, design and support decision making for the direction of the enterprise, including business drivers.
- **Policy** – The governing principle, plans or rules which guide organizational behavior.

- **Organizational** – The arrangement or organization structure of the enterprise and the related human resources systems,
- **Procedure** – The established sequence of steps in a process or activity.
- **Business Cycle** – The regular alternation of periods of business activity.
- **Logistical** – Procuring, maintaining, and transporting materials, personnel and facilities.

Most organizations have standard development methods that may include questionnaires to be used during interviews to populate the business requirements portions of the templates. The Software Engineering Institute[2] is a good source for questionnaire information.

Information View

The Information view examines and documents the data element and data element concepts needed for the solution. The categories associated with Information are in the form of Process Components and Meta Data Components. For a detailed explanation of these categories, please reference the Information Architecture section of the Tool-kit.

Security View

The Security View provides a tool for documenting how security requirements will be addressed in the solution. In addition, it also specifies the security processes, controls, and/or technologies that will be used to implement the solution depicted in the Solution Set logical models.

Most organizations have a standard development methodology that may include questionnaires to gather detail to populate the security portions of the templates. The National Institute of Standards and Technology[3] is a good source for questionnaire information and for detailed definitions of the categories used within the Security View area of the template.

Security Requirements can be expressed in many ways; however, one that is standard in the industry is "controls[4]". These features, often expressed as Managerial, Operational, and Technical Requirements, are gathered and used to identify the security specifications completed during the Solution Set Design.

The types of Security Controls are:

Managerial Controls – Address security topics that can be characterized as managerial. These controls are techniques and concerns that are normally addressed by management in the organization's computer security program. In general, these controls focus on the management of the computer security program and the management of risk within the organization. Topics generally covered in Management Controls include:

- Security Policy
- Security Program Management
- Security Risk Management
- Security & Planning in the SDLC
- Assurance

---

[2] http://wwwsei.cmu.edu/
[3] http://www.nist.gov/
[4] Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook

Operational Controls – Address security controls that focus on controls that are implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular environment, system, or group of systems. These often require technical or specialized expertise and often rely upon management activities as well as technical controls. Topics generally covered in Operational Controls include:

- Personnel/User Issues
- Contingencies & Disaster Planning
- Security Incident Handling
- Awareness, Training, & Education
- Security Considerations in Support & Operations
- Physical & Environment Security

Technical Controls - Focus on security controls that the computer system executes. These controls are dependent upon the proper functioning of the system for their effectiveness. The implementation of technical controls, however, always requires significant operational considerations and should be consistent with the management of security within the organization. Topics generally covered in Operational Controls include:

- Identification & Authentication
- Logical Access Control
- Audit Trails
- Cryptography

Application View

There are several categories of requirements that must be addressed when designing an application system. These categories include end-user services, application infrastructure, and application structure and usability. Wherever possible, application detail is leveraged from pre-existing documentation. Be careful not to baseline existing systems that exhibit significant deficiencies or do not satisfy a high percent of future requirements.

The Application View applies to various forms of Application development efforts including:

- **New Development** - A totally new system development implies that there is no existing system. You have a blank sheet of paper and total latitude in defining its requirements and design. In reality this is a rather rare occurrence.
- **Rewrites of an Existing System** – In a rewrite there is an existing system; however, the system may be limited in its ability to absorb major modifications (e.g., such as integrating with a new portal) while minimizing the impact to the rest of the system. Maintainability may have become an issue, vendors may have provided all or the bulk of the support, underlying platforms may have changed, and so forth. When this situation occurs, it is usually desirable to maintain the core functionality of the business system. As a result, the original system is re-written to accommodate the new environment (e.g., replacing a batch system with an online system, moving it from a centralized system to a distributed system), but the system performs the same function (e.g., payroll processing, license renewals).
- **Maintenance** – Incremental improvements to an existing system, regardless of the size of the changes.

- **Package Selection -** Package selection involves evaluating, acquiring, tailoring and installing third party software.
- **System Conversion** - A system conversion involves translating a system into a new environment. This includes conversions to a different programming language, operating system, computer, disk drives, Data Base Management System, etc. In the translation, the system is not redesigned. It is ported to the target environment, to the extent possible, on a line-for-line basis.

A sample list of the Application View categories, which are related to the characteristics of the application itself, include:

- **Functionality** – The specific functions that the application performs. This category covers the actual application capabilities itself such as reading, writing, calculating and displaying data, extracting, comparing, and loading data from other files and so forth.
- **Performance** - Performance requirements describe how fast the system must complete transformations, how many must be completed, and any limitations on the amount of utilization of the agents used to support the transformation (e.g., amount of machine time, amount of disk space).
- **Reliability** - Reliability defines the degree of accuracy required in the transforms. In billing this would be 100%. In weather forecasting it could be plus or minus 5% for a short term forecast.
- **Availability** - Availability defines the amount of time the system is available during the time periods when it is supposed to be available. This is usually defined as a percentage, qualified with standard deviations. Mean time to failure, by type of failure, further defines system availability.
- **Serviceability** - Serviceability addresses how quickly the system can be corrected when it is discovered to be unreliable or unavailable. This might be expressed as the mean time to fix. Mean time to fix is usually qualified by the type and severity of the failures. Serviceability can also be affected by the capability of remote system access and/or local service staff.
- **Localization** - Localization describes the ability to adapt the application to different languages, character sets, and cultures to support international users. This also relates to the capability of the system to match the business processes of the organization as well as changes to the look and feel, and navigational aspects of the GUI.
- **Portability** - Portability describes the need to be able to quickly adapt the application to run on different technology.
- **Maintainability** - Maintainability describes the need for people to be able to quickly and reliably identify where changes must be made to the system.
- **Testability** - Testability describes what is being tested, when testing must occur, the steps in testing, the properties to being tested, and the definition of the overall testing effort.
- **Extendibility** - Extendibility describes the system's ability to absorb major modifications to changes in any of the above requirements, while minimizing the impact to the rest of the system. This is usually described in terms of change scenarios accompanied with the probability that the change will be needed and the probable time frame in which it will occur. Extendibility also relates to the capability of the technology to expand without major additions to infrastructure. In the integration space this would mean an architecture would be initially capable of supporting several agencies and business process exchanges and without major changes be capable of adding many agencies and exchanges.
- **Retainability -** Retainability describes how the system manages the retention of various data items based on formal retention policies.

Usability View

Usability requirements describe the ergonomics of the system (e.g., ease of correctly interpreting the information on a screen). The categories defined within the Usability view may include:

- **GUI** – Graphic User Interface requires (GUI) a description of the user interface screens showing the graphics required and the graphic structure for the screen interface. This would include screen layouts and navigation between windows or screens.
- **Reports** – Reports outline the requirements for the presentation of information gathered from a database via pre-determined parameters that may or may not be run at scheduled intervals. This information can be used visually from displayed output data sets or output within hard copy.
- **Forms** – This is similar to the GUI because this is a representation of the expected detail that would be collected via a screen form. . It can also relate to the output generated from the on-line data entry.
- **Accessibility** – This lists the requirements to comply with accessibility needs of the application, such as those required by Section 508 of the Rehabilitation Act: Accessibility for People with Disabilities in the Information Age. Detailed information on Section 508 can be found at: http://www.usdoj.gov/crt/508/report2/standards.htm.
- **Queries** – This contains the detail necessary to build queries from the desktop.
- **Other** – Any other detail deemed necessary to meet the Usability Requirements

Infrastructure View

The Infrastructure View is intended to guide the Solution Architect in capturing all the requirements and design considerations involving the usage of IT infrastructure components or services. The Infrastructure View identifies the technical components in the architecture that are being introduced or changed, as well as any impacts on other technology components required for functionality. It also addresses the impact on roles, policies, and standards required within the infrastructure to support the solution.

Some examples of the various types of infrastructure can be seen in the list that follows. It is important to understand however, that this list is only representative of the typical EA categories used to classify IT Infrastructure and may not match those developed within your organization.

Examples of categories within an Infrastructure View include:

- **Voice & Video** (e.g., CTI, Telephones, IP Telephony, PBX, Video Conferencing, IVR)
- **Network – Software** (e.g., Protocols, Access Methods, DHCP, WINS, DNS)
- **Network – Hardware** (e.g., Switches, Routers, Hubs, Bridges, Content Services, RAS, Modems, Sniffers, LAN/WAN/MAN)
- **Security Systems** (e.g., Firewall, Intrusion Detection System, Access Control Servers)
- **Storage Devices** (e.g., SANs, RAID, Tape Drives/Libraries, Disk, Optical CDs, Removable Media)
- **Platform – Hardware** (e.g., Desktops, Laptops, Workstations, Servers)
- **Platform – Software** (e.g., Operation Systems for Mainframe, Mid-Range, Server)
- **Systems Management** (e.g., Change Control, Problem Resolution, Asset Management)
- **Productivity Tools** (e.g., Office XP, MS VISIO, MS Project, Word Perfect, Lotus)
- **Databases** (e.g., Relational, Hierarchical)
- **External Service Providers** (e.g., ISP, VPN, Voice Mail, Satellite, Paging, Cellular)

- **I/O Devices** (e.g., Printers, Monitors, Scanners, Copiers, Wireless Storage, Digital Camera, Facsimiles)
- **Utilities** (e.g., Performance Monitors, ISPF, JES2, Disc Defrag, Installation Utilities, TSO/E, CICS)

The Infrastructure View often leverages pre-existing infrastructure patterns where possible, thus enabling rapid development of the design and the solution set. These infrastructure patterns represent the bundling of various components of the Technology Architecture. These patterns help to jump-start the design process by identifying all the necessary infrastructure components required to deliver or develop the solution.

Some examples of infrastructure patterns that organizations often find useful pertain to the bundling of components that deliver application capabilities:

- *Transact* – Applications that store business data for long periods of time, such as online customer order and other transactions, usually working with only one record or possibly a few records at a time
- *Publish* – Applications with read-only data, such as state highway transportation project information published in Web pages and made viewable to the public
- *Collaborate* – Applications that allow users to share information contained in files and documents, such as a word processing documents shared by a development team or an e-mail driver customer support system

Publish patterns, for example, can be further defined as Client/Server Publish, Web Publish, and Stream Publish. Each pattern would contain all the necessary information for the client or front-end component (e.g., PC, kiosk), the server types needed (e.g., web server, database server, application server) and the technologies utilized to build the application (e.g., XML, XQL, HTML/HTTP). This information is useful to the Solution Architect because it lays out the various architectural components that are needed to design the solution.

In many organizations, the Solution Architect is initially aligned with a particular business unit. This enables the Solution Architect to focus on the specific needs of the business unit's application portfolio. However, this may also cause the Solution Architect to inadvertently build silo solution sets.

From an enterprise perspective, it may be more advantageous to align the Solution Architect by skill set as opposed to business unit, as it ensures reuse and application of various architecture components. For example, if the organization has built patterns, the Solution Architect can be aligned by skill set (e.g., Web Publishing) thus ensuring the systematic re-use of the components in the architecture pattern.

The knowledge of the specific business unit should have been captured within the Business Architecture. That data, along with the input from the various line of business subject matter experts, should ensure that the Solution Architect has the appropriate business-specific knowledge to develop the pattern-based design.

For more information about these types of infrastructure patterns and a discussion on the understanding, development and usage of infrastructure patterns in general, please refer to the book *Enriching the Value Chain: Infrastructure Strategies Beyond the Enterprise*[5]. This book, produced by META Group, provides an excellent dialog on patterns and other key infrastructure services.

[5] Bruce Robertson and Valentin Sribar. Enriching the Value Chain: Infrastructure Strategies Beyond the Enterprise. Intel Corporation and META Group. 2002.

Integration View

The Integration View examines how the solution will integrate with the existing environment. Integration can occur at several touch or exchange points in order to incorporate processes, application, infrastructure, and those elements external to the organization.

To further assist the Solution Architect in determining the possible integration requirements, the Integration View includes the usage of categories also. These categories, labeled Managerial, Operational, and Technical, encompass the following:

Managerial - Includes human resources, skills, and training. Some examples of Managerial integration are:

- Skills
- Training
- Staffing Levels
- Vendor Qualification

Operational – Includes those mechanisms implemented and executed by people. Integration of operational aspects must be evaluated for every part of the solution, for example:

- Hardware and System Support
  - Data Management Services
  - Security
  - Platform/Configuration
  - Network Services
  - Operations
    - Operator Activities Associated with Servers and Print Queues
    - DASD Backup and Restore
    - Software Distribution to Servers and PCs
    - Asset Management and Inventory
    - Disaster Recovery and Planning
- Application Services
- End User Services
- Services Desk
- Measurement/Reporting/Service Levels
- Service Continuity and Consistency
- Backup and Recovery
- Documentation
- Locations
- Process

Technical – Includes the physical IT application, system, and equipment integration requirements including:

- Performance
  - Response Time
  - Availability
  - Transaction Throughput
- User Numbers Supported
- Output
- Accuracy
- Timeliness
- Capacity
- Availability
- Performance
- Continuity
- Scalability/Adaptability

The views and categories listed here are examples of items that are commonly addressed during solution design. The Solution Set templates provide a means for capturing requirements for any combination of views and categories. Organizations may wish to customize templates to include the views and categories that are most commonly addressed during solution design within their environment.

The state of North Carolina has created a "System Design Template" that contains a detailed series of questions to ensure critical elements are addressed for each design. A copy of North Carolina's "System Design Template" is available by accessing SMART at NASCIO's website at www.nascio.org.

The visual representation of the Solution Set Requirements Template, provided on the following page, is followed by the detailed description of its contents.

Solution Set Requirements

Definition			
Name			
Keywords			
Keywords / Aliases			
Solution Set Type			
Type of Solution	☐ Business	☐ Application	☐ IT Infrastructure
Requirements View			
Requirements View Name			
Category Name			
Requirement Statement		Requirement Owner	Related EA Component
Category Name			
Requirement Statement		Requirement Owner	Related EA Component
Requirements View			
Requirements View Name			
Category Name			
Requirement Statement		Requirement Owner	Related EA Component
Current Status			
Solution Set Requirement Status	☐ In Development	☐ Under Review	☐ Approved ☐ Rejected
Audit Trail			
Creation Date		Date Accepted / Rejected	
Created By			
Reason for Rejection			
Last Date Reviewed		Last Date Updated	
Updated By			
Reason for Update			

TEMPLATE DETAIL

The methods utilized for capturing requirements vary by organization. As a result, this template is designed to expand the solution set types, views, and categories, as needed, to accommodate the specifics of the solution set and the uniqueness of the organization.

DEFINITION

Name – The name of the solution set followed by the words "Solution Set Requirements". The name of the Solution Set is obtained from the Solution Set Scope Template. For example: *Customer Service Center –Solution Set Requirements*

KEYWORDS

Keywords / Aliases – List any keywords that can be used in searching the repository for information about the solution being designed and implemented. This information will be helpful for anyone looking for information regarding similar elements.

SOLUTION SET TYPE

The solution set type is used to document the requirements specific to the type of solution being designed (e.g. business solution, application solution, IT infrastructure solution). This template area can be broken down into the various solution types and views so the Solution Architect can focus on the specific needs of a particular view independently. This is necessary because the resources required to gather specific requirements will typically be from different organizations.

Type of Solution – Check the box that represents the type of Solution Set being documented in this section of the template.

The Solution Set Type, along with the Requirements View sections, should be repeated for each solution type addressed by the Solution Set.

REQUIREMENTS VIEW

Within the Requirements View section, list each of the requirements within a specific solution set type. The most common views that may be documented for a solution set type include:

- **Business View** – Pertains to how business requirements will be addressed in the solution. This includes such requirements as financial, strategic planning, business cycles, organizational, business drivers, logistical, policy, and procedures. This view typically aligns with the information contained within the Business Architecture blueprints.
- **Security View** – Pertains to how security requirements will be addressed in the solution. These requirements may be in terms of physical security, human resource security, information security, and IT security. They are grouped into security categories known as management, operational and technical security controls.
- **Information View** - Pertains to how information requirements will be addressed in the solution. This typically includes such requirements as process flows, information ownership, metadata, spatial data, data architecture, data standards, document management, knowledge management, and content management.
- **Application View** – Pertains to how application system requirements and design considerations will be addressed in the solution. This typically includes such categories as application functionality, application structure, performance, reliability, availability, and maintainability.

- **Usability View** - Pertains to how application system usability requirements and design considerations will be addressed in the solution. This typically includes the graphical user interface (GUI), any dialogs and queries that need to be performed by the application, any forms to be developed, any user reports that the system needs to produce, and accessibility needs.
- **Infrastructure View** - Pertains to how IT infrastructure requirements and design considerations will be addressed in the solution and typically includes such categories as hardware, software, voice, middleware, and databases.
- **Integration View -** Pertains to how the results of the Solution Set will integrate with components of the existing environment. This includes such integration requirements as process, application, infrastructure, and those external to the organization. It is also concerned with the impacts to the current environment involving training, resources, capacity, performance, and bandwidth. The integration requirements are addressed in the solution and are typically categorized as managerial, operational, or technical.

The Requirements View section should be repeated for each view that the Solution Set addresses.

Requirements View Name – Provide the name of the view being completed for these requirements.

Category Name – The Requirement View Category allows for the division of Views into manageable subsets. Provide the name of the category that represents a logical subset of the Requirements View. For a list of potential categories for each of the Views, reference *Solution Architecture – Framework*. Example – Solution Set Type Name is *Application*, Requirements View Name is *Usability*, and the Requirements View Category is *Accessibility*.

The Category section should be repeated for each category within a view that the Solution Set addresses.

For each requirement:

Requirement Statement - List the requirements identified for this solution. These requirements should include sufficient detail to enable the completion of a resource assessment.

Requirement Owner - Document the name of the individual who will provide detail and ownership for the specified requirement. Also include contact information. If the specific requirement spans organizational functions, systems, locations, and providers, this may be more than one individual.

Related EA Component – List the related Business, Information, or Technology Architecture Component, associated Gap Component, and/or associated Migration Strategy component name that contained the original requirement for the Solution Set. This can be found as part of the documentation established during the development of the target architecture or during the Implementation Planning activities.

The Related EA Component represents the source of the requirement. It is possible, however, that the specific requirement was identified while creating the Solution Architecture Requirements and was not previously found in any of the existing EA component documentation. If this occurs, the Related EA Component field needs to identify this Solution Set Requirements Component as the source for the requirement.

The EA component type should be listed first and then be followed by the actual component name. Example: *Process Component (Target) – New Employee Orientation.* If it was identified during development of the template, the Related EA Component name may be *Solution Set Requirements Component - Employee Background Security Checks.*

CURRENT STATUS

Solution Set Requirement Status – Document the status of the Solution Set, indicating whether the component is in development, under review, accepted, or rejected.

- *In Development* – The architecture team is currently crafting and/or reviewing the Solution Set detail.
- *Under Review* –The architecture team has completed the Solution Set documentation and it has been submitted for review. Possible reviewers may include members of the project team, the technical community, and the business community
- *Accepted* – The Solution Set has been approved for submission to the appropriate build team.
- *Rejected* – The Solution Set has been rejected for reasons documented below in the Audit Trail section.

AUDIT TRAIL

Creation Date – Provide the date the Solution Set was created.

Created By – List the names and titles of the individuals responsible for the creation of the Solution Set.

Date Accepted/Rejected – Provide the date the Solution Set was accepted or rejected.

Reason for Rejection – If the Solution Set was rejected, document the reason for the rejection. A Solution Set may be rejected for many reasons including, but not limited to, the following:

- Priority, resource, or timing issues rendered the Solution Set not viable at this time. Although the Solution Set is considered rejected for implementation, the original Implementation Planning items still remain in effect should the project be re-initiated within a limited period of time.
- The Solution Set represented one of several options for delivering the required functionality to the organization and another option was chosen. If this happens, the original Implementation Planning item should also be rejected and removed from the Implementation Plan.
- Predecessor projects were determined to have been necessary so the Solution Set was put on hold until successful completion of the identified projects. Although the Solution Set is considered rejected for implementation, the original Implementation Planning items still remain in effect should the project be re-initiated within a limited period of time.
- Necessary architecture components were identified as missing from the existing Enterprise Architecture blueprint. In this event, the Solution Set project must wait until the architecture gaps are filled. Although the Solution Set is considered rejected for implementation, the original Implementation Planning items still remain in effect should the project be re-initiated within a limited period of time.

Last Date Reviewed – Document the most recent date the Solution Set was taken through the Solution Set Vitality Process. This will occur if the Solution Set has been changed after the solution design had previously been approved but not executed.

Last Date Updated – Document the most recent date that any item in the Solution Set documentation was changed.

Updated By – List the names and titles of the individuals that updated this Solution Set.

Reason for Update – Document the reason for the update to the Solution Set.

Solution Set Design Template

TEMPLATE OVERVIEW

The Solution Set Design template provides a tool to assist in documenting the design detail for the Solution Set.

The Solution Set Design template is used to capture various design specifications, dependencies and other organizational and environmental impacts. It also provides links to existing enterprise architecture artifacts, models, and patterns.

The design specifications documented in the Solution Set Design template address the specific requirements captured in the Solution Set Requirements. The design specifications, captured in narrative, will also be rendered on Logical Design Models, which provide a pictorial view of how the pieces work together to form the Solution Set. The detail from the Solution Set Design provides the basis for the physical design models, which is accomplished as part of the standard business process development or SDLC methodologies within the organization.

Important items to keep in mind when documenting the Solution Set Design Specification are:

- The Solution Set Design template provides the structure to leverage component detail that already exists within the architecture
- One design specification may meet one or more requirements
- Specifications should be in sufficient detail to enable the completion of a detailed design
- Links to the requirements ensure the Solution Set Requirements have been addressed.

The visual representation of the Solution Set Design template, provided on the following pages, is followed by the detailed description of its contents. The development of the Solution Set Design is a process that will evolve and change as information is gathered and documented.

Solution Set Design

Definition	
Name	
Keywords	
Keywords / Aliases	
Solution Set Type	
Type Name	
Design View	
Design View Name	
Category Name	
Design Specification Statements	*Related EA Component*
Related Requirements	*Relationship*
Category Name	
Design Specification Statements	*Related EA Component*
Related Requirements	*Relationship*
Design View	
Design View Name	
Category Name	
Design Specification Statement	*Related EA Component*
Related Requirements	*Relationship*

SOLUTION SET LOGICAL MODEL			
Source Document			
CURRENT STATUS			
Solution Set Design Status	☐ *In Development* ☐ *Under Review* ☐ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date		*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Updated by			
Reason for Update			

TEMPLATE DETAIL

The Solution Set Design Template is utilized to document the design considerations after a logical model has been approved.

DEFINITION

Name – The name of the Solution Set followed by the template name. The name of the Solution Set is obtained from the Solution Set Scope Template. For example: *Customer Service Center – Solution Design.*

KEYWORDS

Keywords/Aliases – List any keywords and/or aliases that can be used in searching the repository for information about the solution design. This information will be helpful for anyone looking for information regarding similar elements.

SOLUTION SET TYPE

Type Name - The name of the Solution Set followed by the solution type. For example: *Customer Service Center – Business Solution.*

The Solution Set type names for Solution Design should match the solution set type names for the Solution Requirements. One or more solution set types can be documented by repeating the Solution Set Type section for each type.

Design View

Design View Name – Provide the Design View Name. The Design Views within each Solution Set Type should also map to the Requirement Views covered by the Solution Set Requirements. Examples of Design Views include, but are not limited to:

- Business
- Information
- Application
- Infrastructure
- Security
- Integration
- Usability

Category Name – The category name allows for the division of Views into manageable subsets. The Categories documented for the Solution Set Design will match those used for Solution Set Requirements.

The following information should be documented for each category.

Design Specification Statements – List the design specifications identified for this design view. Specifications should be in sufficient detail to enable the completion of a detailed design.

- Security View - Specify the security classification for any associated data
- Information View - The Logical and Physical target (future) view of the information is captured in the Solution Architecture, however, because the level of detail for the Information View is similar

in structure to the detail captured for the baseline documentation in Information Architecture, the logical detail will be captured utilizing the template provided in the Information Architecture Section of the Tool-Kit.

- Integration View - List the specific integration dependency or integration specification identified for this solution. These items should be in sufficient detail to articulate the need, identify how it will impact the environment, and identify who should resolve this impact.

Related EA Component – List the EA component that is related to each design specification. EA components can come from the Business, Information and/or Technology Architectures. If the organization uses patterns (commonly bundled EA Components), the pattern can also be listed here.

If the design specification cannot be satisfied by any EA components identified to date, a gap should be identified so that steps can be taken to get the component documented within the architecture. This is accomplished by creating an EA Help Request. EA Help Requests are addressed as part of the EA Compliance Process (see *Governance: EA Lifecycle Processes – Compliance Process*). A standard phrase should be used to identify these gaps, such as "EA Help Request Needed". Use of a standard phrase to identify EA Component gaps will allow for queries on these items.

This gap is a Solution Set dependency. A Gap Component template should be used to document the Gap and it must go through the EA Governance Process. It should also be submitted to the Implementation Plan coordinator to be included as an action item on the Implementation Plan.

Related Requirements – List the requirements that these design specifications satisfy. The design specifications may satisfy, or partially satisfy, one or more requirements.

Relationship – For each Related Requirement, provide comments regarding the relationship between the specification and the requirement that will help to verify that all requirements have been addressed. This may include statements such as "Satisfies the application portion of the requirement" or "Fully satisfies the requirement".

Solution Set Logical Model

Source Document – Provide the name of the source document containing the logical model.

Current Status

Solution Set Design Status – Document the status of the Solution Set, indicating whether the component is in development, under review, accepted, or rejected.

- *In Development* – The architecture team is currently crafting and/or reviewing the Solution Set detail.
- *Under Review* –The architecture team has completed the Solution Set documentation and it has been submitted for review. Possible reviewers may include members of the project team, the technical community, and the business community
- *Accepted* – The Solution Set has been approved for submission to the appropriate build team.
- *Rejected* – The Solution Set has been rejected for reasons documented below in the Audit Trail section.

AUDIT TRAIL

Creation Date – Provide the date the Solution Set was created.

Created By – List the names and titles of the individuals that created the Solution Set.

Date Accepted/Rejected – Provide the date the Solution Set was accepted or rejected.

Reason for Rejection – If the Solution Set was rejected, document the reason for the rejection. A Solution Set may be rejected for many reasons including, but not limited to, the following:

- Priority, resource, or timing issues rendered the Solution Set not viable at this time. Although the Solution Set is considered rejected for implementation, the original Implementation Planning items still remain in effect should the project be re-initiated within a limited period of time.
- The Solution Set represented one of several options for delivering the required functionality to the organization and another option was chosen. If this happens the original Implementation Planning item should also be rejected and removed from the Implementation Plan.
- Predecessor projects were determined to have been necessary, so the Solution Set was put on hold until successful completion of the identified projects. Although the Solution Set is considered rejected for implementation, the original Implementation Planning items still remain in effect should the project be re-initiated within a limited period of time.
- Necessary architecture components were identified as missing from the existing Enterprise Architecture blueprint. In this event, the Solution Set project must wait until the architecture gaps are filled. Although the Solution Set is considered rejected for implementation, the original Implementation Planning items still remain in effect should the project be re-initiated within a limited period of time.

Last Date Reviewed – Document the most recent date the Solution Set was taken through the Solution Set Vitality Process. This will occur if the Solution Set has been changed after the solution design had previously been approved but not executed.

Last Date Updated – Document the most recent date that any item in the Solution Set documentation was changed.

Updated By – List the names and titles of the individuals that updated this Solution Set.

Reason for Update – Document the reason for the update to the Solution Set.

Solution Set Vitality Review

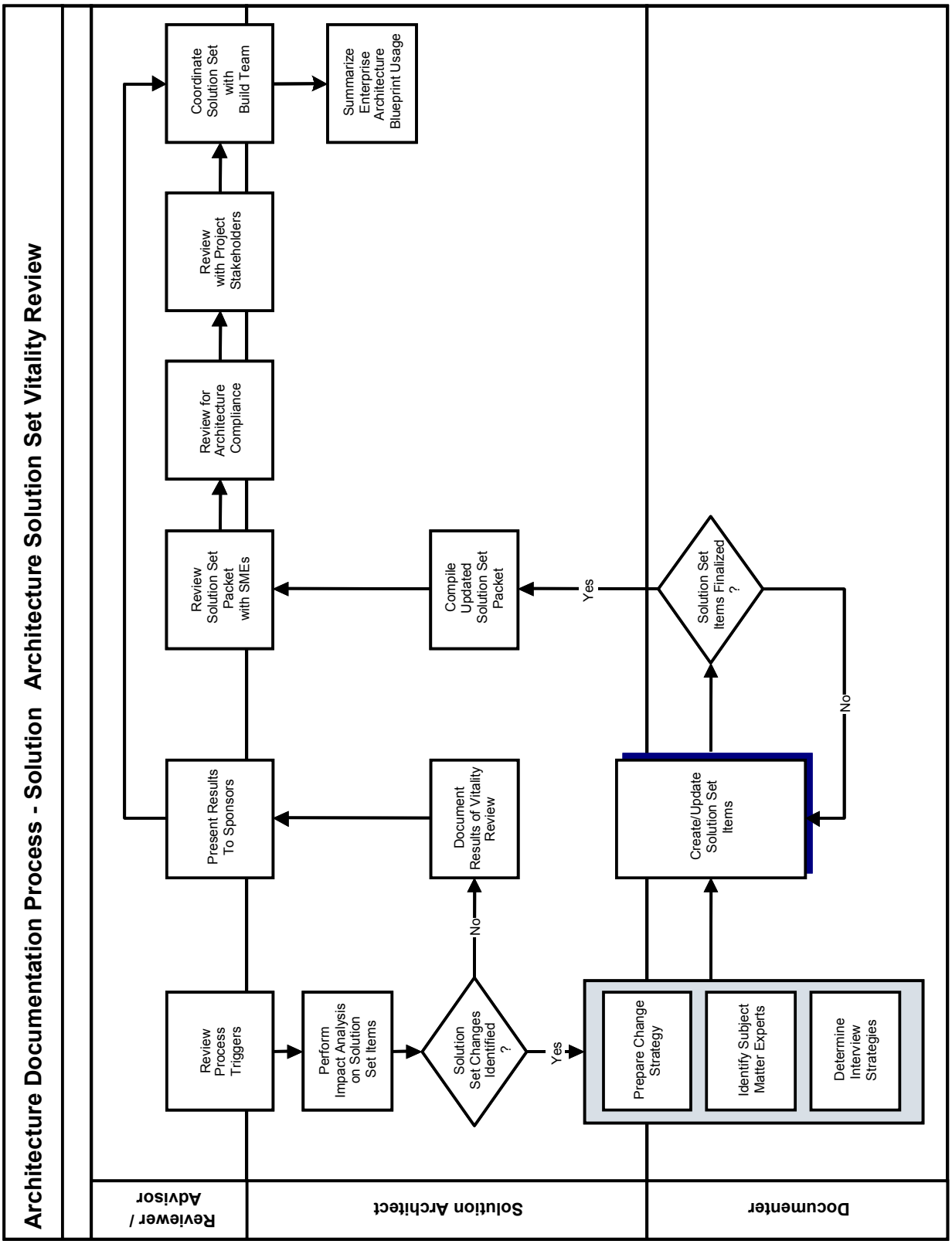
PROCESS OVERVIEW

The Solution Set Vitality Review is intended to ensure that the Solution Set that was originally designed to solve a particular business problem is still valid and in line with the stated business and technical goals, objectives, and directions of the organization.

There are many reasons for initiating a Solution Set Vitality Review. Some of these include:

- *Reactivation Of The Associated Implementation Planning Item* – If the Solution Set had been created but not implemented due to various organizational constraints, the Solution Set should be re-evaluated to ensure that the original assumptions and requirements are still valid. In addition, the Solution Set design and design models should be reexamined to ensure that they are leveraging current or preferred architecture blueprints. Any Implementation Planning items that were linked to the particular Solution Set (e.g., predecessor or successor efforts) should also be examined.
- *Changes to Enterprise Architecture Blueprints used within the Solution Set* – When the original Solution Set was developed, it referenced and the design was built based upon various Business, Information, and Technology Architecture components and design patterns. If any of these components or patterns changed while the Solution Set was on hold, the Solution Set design must be re-evaluated and potential design changes need to be addressed.
- *Business Driver Changes* – When the original Solution Set was developed the requirements and design may have been influenced by various Business Drivers (e.g., principles, best practices, trends). If any of these drivers changed while the Solution Set was on hold, the Solution Set design must be re-evaluated. This is to ensure the Solution Set is still aligned, and not in conflict with, the organization's business drivers.
- *External Organizational Influences* – New legislation, vendor performance, product shifts, or other external factors may cause the Solution Set to be re-evaluated. For example, new legislation, such as HIPAA regulations, may impact how the requirements were identified and how the solution was designed. This new legislation will need to be analyzed for impacts and the Solution Set will need to be redesigned to ensure compliance.
- *Internal Organizational Influences* – Many internal organizational events can occur that might impact the original Solution Set. These may include a new organizational structure, changes in the EA process, budgetary shifts, the implementation or shifts in development methodologies, new executive management, and/or changes to the existing operating environment. Any of these events may impact the Solution Set requirements and design specifications. Information about the new event, and how it may impact the organization, must be identified and the Solution Set must be redesigned to accommodate these changes.

The Solution Set Vitality Review may involve updating specific Solution Set elements or may conclude with the determination that the Solution Set is still vital as is. Regardless of the outcome, the Solution Architect must document the findings (or lack there of) and communicate this back to the various stakeholders identified within the process.


Architecture Documentation Process - Solution Architecture Solution Set Vitality Review
Reviewer / Advisor
Solution Architect
Documenter
Review Process Triggers
Perform Impact Analysis on Solution Set Items
Solution Set Changes Identified ?
No
Yes
Document Results of Vitality Review
Present Results To Sponsors
Review Solution Set Packet with SMEs
Review for Architecture Compliance
Review with Project Stakeholders
Coordinate Solution Set with Build Team
Summarize Enterprise Architecture Blueprint Usage
Prepare Change Strategy
Identify Subject Matter Experts
Determine Interview Strategies
Create/Update Solution Set Items
Solution Set Items Finalized ?
No
Yes
Compile Updated Solution Set Packet

THE PROCESS DETAIL

Review Process Triggers – The Solution Set Vitality process triggers should be gathered and reviewed in detail. If the triggering event is due to the re-activation of a previously approved Solution Set, all prior Solution Set documentation should be collected. The original Implementation Planning item, gap, and migration strategies should also be gathered for review by the Solution Set team. Careful attention should be placed on reviewing other Implementation Planning items to ensure that any linked plan items are also investigated for applicability or changes.

If the process triggers were due to any other planning or architecture change other than the re-activation of a Solution Set effort, then documentation describing the event should also be collected. Examples of this include:

- Enterprise Architecture Blueprint Changes
- Business Driver Changes
- External Organizational Influences
- Internal Organizational Influences

Perform Impact Analysis on Solution Set Items – Once the information that initiated or triggered the vitality process has been collected, the Solution Architect should review this information in detail and determine if the Solution Set will be impacted. All existing requirements, design specifications, and design models are evaluated against the vitality triggers. A list of these impacts should be created, as this will be necessary to identify the appropriate Subject Matter Experts to participate in the vitality review.

Document Results of Vitality Review – If no changes were identified upon completion of the vitality review, the Solution Architect documents that the review has taken place and that no impacts have been identified.

Present Results to Sponsors – The Solution Architect prepares and delivers a brief update to the sponsor indicating that the vitality review of the original Solution Set has been completed and that no impacts or changes have been identified.

Prepare Change Strategy – If Solution Set impacts have been identified, the Solution Architect and Documenters must determine the best approach for updating the Solution Set items. If the changes are minor and affect only the selection of a technology component for example, the team may decide to enhance and validate only the Solution Set Design. If business drivers or the business strategy has changed, these changes may impact the scope and requirements of the effort. In this case, the team will want to update all affected Solution Set artifacts and include all stakeholders in the review process.

Identify Subject Matter Experts – The list of the Subject Matter Experts who participated in the original creation of the Solution Set should be reviewed and validated. Those individuals should be asked to participate in the vitality review. If the vitality review was initiated due to Solution Set impacts caused by changes to the Enterprise Architecture, or changes in the organization, additional individuals may need to be brought in to the process to complete the revalidation. Subject Matter Experts may be identified and included in the interviewing process as well.

Determine Interview Strategies – Interview meeting topics should be determined in one of the first working sessions. Interview questions should be specifically focused on the impacts to the Solution Set as identified during the impact analysis step.

Create/Update Solution Set Items – At this point in the process, the interviews will be conducted and the Solution Set documentation updated. The Solution Set items that may need to be updated include the Solution Set Scope, Solution Set Requirements, and the Solution Set Design.

A separate process model and narrative for this sub-process will provide greater detail (See *Create/Update Solution Set Items*).

Compile Updated Solution Set Packet – When the Solution Set requirements, design specifications, solution impacts, and design model are updated, a summary should be compiled and the various pieces of the Solution Set documentation should be submitted for review. A packet containing the update Solution Set documentation will be compiled in preparation for formal review. The updated Solution Set Packet is typically reviewed by the project manager, all project Subject Matter Experts, the Chief Architect, and representatives from the impacted functional areas.

Review Solution Set Packet with SMEs – The Solution Set Architect, as well as the SMEs that contributed to the effort will verify the contents of the Solution Set Packet and work with the Documenters to make modifications as necessary.

Review for Architecture Compliance – The Solution Architect will review the Solution Set Packet with the various architecture representatives, ensuring that the Solution Set is in compliance with the documented architecture components:

- Business Architecture – Business Architecture Components
- Information Architecture – Process and Information Meta Components.
- Technology Architecture – Product and Compliance Components.

If inconsistencies are found, the Solution Architect will work with the Documenters to make modifications as necessary, to recompile the Solution Set Packet, and to start the review process again.

Review with Project Stakeholders – The Solution Architect will review the Solution Set Packet with the various stakeholders of the project (e.g., project sponsor) ensuring the Solution Set is designed to meet the original needs of the project. If for any reason the Solution Set does not meet the expectations of the stakeholders, the Solution Architect will work with the Documenters to make modifications as necessary, recompile the Solution Set Packet, and start the review process again.

Coordinate Solution Set with Build Team – When the Solution Set is approved, it must be referred to the team responsible for executing the Business Development Process or the SDLC. All information contained in the Solution Set (e.g., project scope, requirements, design specifications, impacts, logical models) will be needed by the project team to develop and implement the solution. The Solution Architect will ensure that the Solution Set Packet is understood and accepted by the build team.

Summarize Enterprise Architecture Blueprint Usage – The Solution Architect will create a summarization of the Business, Information, and Technology Architecture components or patterns that were referenced when the Solution Set was designed. If the Solution Set Design identified gaps within the existing architecture, a list of those gaps, as well as the completion of the necessary gap component documentation will also be completed. The Enterprise Architecture Blueprint Usage report and/or matrices serve to identify the changes to the Application Portfolio, to identify follow-on activities to address the gaps in the architecture blueprints, and to provide metrics on the reusability of the architecture.

SAMPLES

Project: Child Support Payments to Other States

SOLUTION SET SCOPE

The Solution Architecture effort used for populating the sample Solution Set is assumed to have been defined and approved as part of the Implementation Planning process. Information obtained and documented during that process is reprinted here to provide clarity and understanding to help the reader see how the Solution Set templates were used to capture the detail pertinent to the sample solution effort: *Child Support Payments to Other States*.

Baseline System

Currently the State receives child support payments that are destined for residents in other States. Initially, these payments are captured in the State's payment database; the payments are subsequently transferred to an out-of-State payment database. A balance listing is prepared by the State and forwarded to the Office of Child Support, Department of Human Services for distribution to the destination states. This office requests payment in the amount of the total due other States and the check, along with the printed check register, is mailed to the destination State for credit to the non-custodian parent's account. This requires several days to complete and in numerous cases the payments are late.

To be certified by the Federal Government, a system must be in place to EDI the payments to the destination States or utilize the Automated Clearing House to route the payments.

Target System

By taking the child support payments from the payments database and building an EDI or Automated Clearing House transaction, the receipt of the child support payment should result in a reduction of labor by the Child Support, Department of Human Services office. Additionally, the payments should be more accurate and the State's total payment amount can be broken down by non-custodial parent to be directly posted to the non-custodian parent's account.

Benefits

The following advantages should be gained by implementation of this change to the existing system:

- Faster processing of the out-of-State payments
- Non-custodial accounts in other States will be updated more quickly and accurately
- Payments to other States will be generated automatically by the system and required accounting and audit reports will be produced
- Reduction in cost by introduction of Business Process Improvements resulting in reduced processing steps
- Reduction in errors as each non-custodial parent's payment will be created in a transaction with the proper account number and other personal data
- Compliance with Federal Requirements to retain the certification and funding by the Federal Government

- Reduction in errors of processing and better audit controls

HIGH-LEVEL SYSTEM REQUIREMENTS

The following summarize the initial high-level system requirements for the EDI or Automated Clearing House processing of out-of-State non-custodial parent payment processing:

- Using the out-of-State Payment Database to generate payments by non-custodial parent accounts for custodial parents that reside in other States
- Assemble payments by Case Worker and display for review on their workstation
- Assemble Case Worker approved accounts by out-of-State
- Create a Check Register Report by State showing the non-custodial parent and the child support payment
- Create a payment transaction to be sent to the State of residence for the non-custodial parent and child
- Create transactions to be processed by the Payables Modules of the Child Support System to Produce an out-of-State Payment Check
- Create EDI or Automated Clearing House files to transmit to each state or local bank for distribution in the Automated Clearing House. Automatic back-up processes and/or procedures to re-transmit a State's file in the event of loss or missing
- Create machine-readable media to transfer to local bank in event of transmission failure
- Update the out-of-State Payment Database to indicate the payment has been sent to the proper State
- Create status reports on the transmission of files from the server to the proper State or bank
- Create supporting programs to list transaction files in the event of major system failure
- Revise the workflow within the Child Support, Department of Human Services office to match the new non-custodial parent audit procedures
- Indicate to other States that there has not been any child support payments collected from the non-custodial parent in order for the state to take appropriate action, such as suspension of Driver's Licenses
- Indicate collection of Back Payments from the non-custodial parent to assure the other States that proper collections have been made
- Indicate payments taken from IRS refunds and credited to the non-custodial parent's account.

Information Requirements for the Target System

Information collected from the Child Support Database and the out-of-State Payment Database for the Non-Custodial Parent:

- Social Security Number
- Case Worker
- Home Address
- Work Address
- Non-Custodial Child Social Security Number
- Account Status
- Payment Type
- Payment Amount

- Bank Account
- Transit Routing Number
- Bank Account Number
- Payment Due Date
- Court Case Number
- Last Court Date
- Duration Remaining (in years and months) for Child Support
- County (in State)
- Out-of-State Code
- State Number
- EDI Standards Transaction Numbers

This should require approximately 60 days to complete a preliminary Solution Set. The major Risk within this time frame is the EDI requirement of out-of-State. Can the State accept EDI or have the transactions submitted to our local bank for processing by the Automated Clearing House? The development times are dependent on the number of EDI transactions that are to be created or perhaps the purchase of an off the shelf system to produce EDI transactions. This decision will need to be made early in this project. It is estimated that our State collects approximately $800,000 to $1,000,000 in out-of-State payments each year.

Solution Set Scope

DEFINITION	
Name	Child Support Payments to Other States (ACH) – Solution Set Scope
Description	Currently the State receives child support payments that are destined for other States. Initially these payments are captured in the State's payment database, then subsequently transferred to an out-of-State payment database. A balance listing is prepared by the State and forwarded to the Office of Child Support, Department of Human Services for distribution to the destination States. This office requests payment in the amount of the total due other States and the check, along with the printed check register, is mailed to the destination State for credit to the non-custodian parent's account. This requires several days to complete and in numerous cases the payments are late. By taking the child support payments from the payments database and building an EDI or Automated Clearing House transaction, the receipt of the child support payment should result in a reduction of labor by the Child Support, Department of Human Services office. Additionally the payments should be more accurate, and the State's total payment amount can be broken down by non-custodial parent to be directly posted to the non-custodian parent's account.
Rationale	To be certified by the Federal Government, a system must be in place to EDI the payments to the destination states or utilize the Automated Clearing House to route the payments.
Benefits	The following advantages should be gained by implementation of this change to the existing system: • Faster procession of the out-of-State payments • Non-custodial accounts in other States will be updated more quickly and accurately • Payments to other States will be generated automatically by the system and required accounting and audit reports will be produced • Reduction in cost by introduction of Business Process Improvements resulting in reduced processing steps • Reduction in errors as each non-custodial parent's payment will be created in a transaction with the proper account number and other personal data • Compliance with Federal Requirements to retain the certification and funding by the Federal Government • Reduction in errors of processing and better audit controls
BOUNDARY	
Boundary Scope Statement	This applies to all non-custodial out-of-State child support payment recipients. The initial scope will focus on those States leveraging automated clearing house functions through normal banking environments. At this time, it will not focus on states that accept EDI transactions.

ASSOCIATED IMPLEMENTATION PLAN ITEMS			
Implementation Plan Project Identifier	05DHS007; Child Support Payments to Other State – ACH		
Plan Items Solution Set is Dependant Upon	04DHS018; Child Support Payments Database – Portal		
Plan Items Dependant Upon Solution Set	N/A		
Related Migration Strategies	Child Support Payments to Other States – EDI		
Selected Solution Set Conceptual Model	Child Support Payments to Other States – ACH: Conceptual Model.doc within EA Repository		
Solution Set Types	☐ *Business* ☒ *Application* ☐ *IT Infrastructure*		
KEYWORDS			
List All Keywords	Child Support Payments; Non-custodial, Custodial Parent; Out-Of-State, ADC		
CONTACT INFORMATION			
Project Sponsor	John A. Smith, Director of Child Support Operations		
Implementation Plan Coordinator	Mary E. Locking, Director of Plans & Administration		
Solution Set Architect	Yi Chang, Solutions Architecture, Solutions Development		
Solution Set Contributors	Fred Jones 555-1212 ext. 999, Senior Child Support Case Worker Marcus Rodriguez 555-1212 ext. 1003, Financial Management Maribeth Wayand 555-1212 ext. 7007, Database Management Janice Taylor 555-1212 ext. 111, Administrative Staff Jonathan Lloyd 555-1212 ext. 404, Legal Counsel Sara Chambers 555-1212 ext. 999, Child Support Case Worker Betty Lewis 555-1212 ext. 1003, Help Desk		
CONTRACT INFORMATION			
Name	Federal Funding Assistance for Child Support Development		
Reference Number	FDH3456785		
Contact Information	Barbara Cummings, Federal Oversight Coordinator 555-555-1212		
Implications	Failure to implement will incur loss of Federal funding.		
CURRENT STATUS			
Solution Set Status	☒ *In Development* ☐ *Under Review* ☐ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	07/30/2004	*Date Accepted / Rejected*	
Created By	Judy Bell, Business Systems Analyst, Customer Relations		
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Updated By			
Reason for Update			

Solution Set Requirements

Definition			
Name	Child Support Payments to Other States (ACH) – Solution Set Requirements		
Keywords			
Keywords / Aliases	Child Support Payments; Non-custodial Parent; Custodial Parent; Out-of-State, ADC		
Solution Set Type			
Type of Solution	☐ *Business* ☒ *Application* ☐ *IT Infrastructure*		
Requirements View			
Requirement View Name	Application		
Category Name	Functionality		
Requirement Statement		*Requirement Owner*	*Related EA Component*
Create out-of-State transaction (with transaction detail) for sending to other States.		John A. Smith, Director of Child Support Operations	IA Process Component (Target) - Batch Processing for out-of-State transactions
Create transmission file in proper format for bank.		Freda Welch, Child Support Payment Processing	Process Component (Target) -Batch Processing for Out of States
Category Name	Data Accuracy		
Requirement Statement		*Requirement Owner*	*Related EA Component*
Validate transmission file data prior to sending to external State.		Freda Welch, Child Support Payment Processing	Business Architecture Component (Target) – Business Rule: Validate Data for Proper State
Requirements View			
Requirement View Name	Usability		
Category Name	GUI		
Requirement Statement		*Requirement Owner*	*Related EA Component*
Case Worker data available for display and review on their workstation via standard browser interface.		Ted Webb 555-1212 ext. 999, Child Support Case Worker Chris North 555-1212 ext. 1003, Help Desk	GAP Component – Child Support Portal Requirements

Category Name	Queries		
Requirement Statement		*Requirement Owner*	*Related EA Component*
Query information based on individual case worker ID number		Ted Webb 555-1212 ext. 999, Child Support Case Worker	GAP Component - Child Support Query Enhancements
REQUIREMENTS VIEW			
Requirement View Name	Business		
Category Name	Business Cycle		
Requirement Statement		*Requirement Owner*	*Related EA Component*
Received payments need to be available to Case Workers after end of month processing		John A. Smith, Director of Child Support Operations	IA Process Component (Target) - Monthly Processing Updates
REQUIREMENTS VIEW			
Requirement View Name	Security		
Category Name	Technical		
Requirement Statement		*Requirement Owner*	*Related EA Component*
All files transmitted to automated clearing house must be encrypted.		Jurgen Schmidt, Systems Security	Solution Set Requirements Component - Child Support Payments to Other States – ACH
REQUIREMENTS VIEW			
Requirement View Name	Integration		
Category Name	Technical – Accuracy		
Requirement Statement		*Requirement Owner*	*Related EA Component*
Send only payments that are still in effect per the custodial parent Court orders.		Ted Webb 555-1212 ext. 999, Child Support Case Worker	IA Process Component (Target) - Monthly Batch Update
Update system upon successful receipt of payments from out-of-State agency.		Ted Webb 555-1212 ext. 999, Child Support Case Worker	IA Process Component (Target) - Business Rule: Review Payment Posting
Category Name	Technical – Capacity		
Requirement Statement		*Requirement Owner*	*Related EA Component*
Need Disk Space to accommodate 20,000 daily payments. Transaction records need to be retained for 7 years. Approximately 5 million records per year will result in 36 million records stored in 7 years.		Robert Large, System Capacity Planner	* Operational Impact - Planning of DASD Space

Category Name	Managerial - Training		
Requirement Statement		*Requirement Owner*	*Related EA Component*
Provide new business process training for register checking to ensure payments have been made and transferred to the proper State.		John A. Smith, Director of Child Support Operations; Ted Webb 555-1212 ext. 999, Child Support Case Worker	Business Architecture Component (Baseline) - Process Improvement Training
CURRENT STATUS			
Solution Set Requirement Status	☒ *In Development* ☐ *Under Review* ☐ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	08/06/2004	*Date Accepted / Rejected*	
Created By	Yi Chang, Solutions Architecture, Solutions Development		
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Updated By			
Reason for Update			

Solution Set Design

DEFINITION	
Name	Child Support Payments to Other States (ACH) – Solution Set Design
KEYWORDS	
Keywords / Aliases	Child Support Payments; Non-custodial Parent; Custodial Parent; Out-of-State, ADC
SOLUTION SET TYPE	
Type of Solution	☐ *Business* ☒ *Application* ☐ *IT Infrastructure*
DESIGN VIEW	
Design View Name	Application
Category Name	Functionality

Design Specification	*Related EA Component*
Create transaction database table with appropriate record detail.	TA Compliance Component – Database Standards-Batch Record Update
Related Requirements	***Relationship***
Create out-of-State transaction (with transaction detail) for sending to other States.	Satisfies Requirement
Create transmission file in proper format for bank.	Satisfies Requirement
Data in transmission file are 100% accurate (Note: Transmission is delivered in format and content as originators specified. Accuracy of data cannot be controlled)	Technically Satisfied; However, cannot control data accuracy.

DESIGN VIEW	
Design View Name	Usability
Category Name	GUI

Design Specifications	*Related EA Component*
Assemble payments by Case Worker ID and display for review on their workstation.	EA Component Needed.
Adhoc query by caseworker number will produce information to be displayed by browser.	TA Product Component-Crystal Reports
Related Requirements	***Relationship***
Viewing of specific caseworker payments viewable via standard browser interface.	Satisfies Requirement
Query information based on individual case worker ID number	Satisfies Requirement

DESIGN VIEW	
Design View Name	Business
Category	Business Cycle
Design Specifications	*Related EA Component*
Received payments need to be available to Case Workers after end of month processing	IA Process Component-Batch Processing
Related Requirements	*Relationship*
Submit out-Of-State transaction database update job after completion of month-end payment processing batch job.	Satisfies Requirement - Business Rule

DESIGN VIEW	
Design View Name	Security
Category	Technical
Design Specifications	*Related EA Component*
Transmission file data must be sent with 128 encryption standards.	TA Compliance Component - SSL Encryption Standards
Related Requirements	*Relationship*
SSL Encryption Standards	Satisfies Requirement

DESIGN VIEW	
Design View Name	Integration
Category	Technical - Accuracy
Design Specification	*Related EA Component*
Query Family Court related database to determine status of Court order.	TA Compliance Component — Database Queries
Related Requirements	*Relationship*
Transmit only payments that are still in effect per the custodial parent Court orders.	Satisfies Requirement
Update system upon successful receipt of payments from out-of-State agency.	Satisfies Requirement

DESIGN VIEW	
Design View Name	Integration
Category	Technical - Capacity
Design Specification	*Related EA Component*
Impact Statement---Coordinate with Capacity Planning team to ensure adequate space is available	* Operational Impact - Planning of DASD Space

Related Requirements		*Relationship*
Need disk space to accommodate 20,000 daily payments to be retained for 7 years.		Satisfies Requirement as long as this is considered in Capacity Planning in the future.
Category	Managerial – Training	
Design Specification		*Related EA Component*
Provide training on new business processes for checking registers to ensure payments have been made and transferred to the proper State		Business Component-Process Improvement Training
Related Requirements		*Relationship*
Development Training Material to support the change in Business process		BA Business Architecture Component - Training Materials

CURRENT STATUS			
Solution Design Status	☒ *In Development* ☐ *Under Review* ☐ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	07/27/04	*Date Accepted / Rejected*	
Created By	Yi Chang, Solution Architecture, Solutions Development		
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Updated by			
Reason for Update			

A Solution Project: Enterprise GIS Clearinghouse

Solution Set Scope

DEFINITION	
Name	Enterprise GIS Clearinghouse – Solution Set Scope
Description	Currently GIS systems exist in several State agencies and numerous local government entities. These are usually very specialized databases and applications for the agencies and entities that use them. At no time in the past has there been a collection of GeoSpatial data in one database that covers many GIS layers. The Enterprise GIS Clearinghouse will be such a collection of data. The Clearinghouse will reside in the State Data Center and will host, at a minimum, the Mississippi Digital Earth Model (MDEM) which includes the following core data layers of a digital land base computer model of the State of Mississippi on a Statewide basis: ▪ Geodetic Control ▪ Elevation and Bathymetry ▪ Orthoimagery ▪ Hydrography ▪ Transportation ▪ Government Boundaries ▪ Cadastral In addition, the clearinghouse will contain other geospatial data and applications to access data as determined by the GIS Council, Policy Advisory Committee, Technical Users' Committee and Clearinghouse staff.
Rationale	During the 2003 legislative session, legislation was passed that created a Council on Remote Sensing and GIS. That legislation directed that the Department of Information Technology Services would host an Enterprise GIS Clearinghouse that contains the MDEM and other data of interest to citizens, businesses, and State and local governments.
Benefits	Provides a single source for accessing and retrieving Geospatial data that is available to all along with applications that will supply users with various ways of looking at the data.
BOUNDARY	
Boundary Scope Statement	Provides a single source for accessing and retrieving Geospatial data that is available to all users in addition to applications that will supply users with various ways of looking at the data. All Clearinghouse applications and data will be accessed through the GIS Portal.

ASSOCIATED IMPLEMENTATION PLAN ITEMS			
Implementation Plan Project Identifier	05ITS001; Planning and Implementation of a Enterprise GIS Clearinghouse		
Plan Items Upon Which the Solution Set is Dependant	05DEQ01; Funding for, Purchasing, and QA of initial clearinghouse data 05ITS02; Funding for ITS GIS Infrastructure		
Plan Items Dependant Upon Solution Set	N/A		
Related Migration Strategies	Strategy for Determining Effect of GIS Clearinghouse on Statewide Network		
Selected Solution Set Conceptual Model	Enterprise GIS Clearinghouse: Conceptual Model.doc within EA		
Solution Set Types	☐ *Business* ☒ *Application* ☐ *IT Infrastructure*		
KEYWORDS			
Keywords / Aliases	GIS; Geographic Information Systems; Geospatial; Clearinghouse; Warehouse; Data;		
CONTACT INFORMATION			
Project Sponsor	David Litchliter, CIO, Mississippi Department of Information Technology Services; Charles Chism, CEO, Mississippi Department of Environmental Quality		
Implementation Plan Coordinator	Claude Johnson, Strategic Services Director, Mississippi Department of Information Technology Services		
Solution Set Architect	Craig Orgeron, Architect, Mississippi Department of Information Technology Services		
Solution Set Contributors	Cragin Knox 555-1212, Department of Environmental Quality Jim Steil 555-1212, MARIS David Rankin, 555-1212, Warren County Terry Bergin, 555-1212, Department of Information Technology Services		
CONTRACT INFORMATION			
Name	There are no additional contractual requirements for this project		
Reference Number			
Contact Information			
Implications			
CURRENT STATUS			
Solution Set Scope Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	08/17/2004	*Date Accepted / Rejected*	
Created By	Claude Johnson, Director Strategic Services		
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Updated By			
Reason for Update			

Solution Set Requirements

DEFINITION	
Name	Enterprise GIS Clearinghouse and Portal – Solution Set Requirements
Description	Currently GIS systems exist in several State agencies and numerous local government entities. These are usually very specialized databases and applications for the agencies and entities that use them. At no time in the past has there been a collection of GeoSpatial data in one database that covers many GIS layers. The Enterprise GIS Clearinghouse will be such a collection of data. The Clearinghouse will reside in the State Data Center and will host, at a minimum, the Mississippi Digital Earth Model (MDEM) which includes the following core data layers of a digital land base computer model of the State of Mississippi on a Statewide basis: ▪ Geodetic Control ▪ Elevation and Bathymetry ▪ Orthoimagery ▪ Hydrography ▪ Transportation ▪ Government Boundaries ▪ Cadastral In addition, the clearinghouse will contain other geospatial data and applications to access data as determined by the GIS Council, Policy Advisory Committee, Technical Users' Committee and Clearinghouse staff.
Rationale	During the 2003 legislative session, legislation was passed that create a Council on Remote Sensing and GIS. That legislation directed that the Department of Information Technology Services would host an Enterprise GIS Clearinghouse that contains the MDEM and other data of interest to citizens, businesses, and State and local governments.
Benefits	Provides a single source for accessing and retrieving Geospatial data that is available to all, along with applications that will supply users with various ways of looking at the data.
BOUNDARY	
Boundary Limit Statement	Provides a single source for accessing and retrieving Geospatial data that is available to all users in addition to applications that will supply users with various ways of looking at the data. All Clearinghouse applications and data will be accessed through the GIS Portal.
KEYWORDS	
Keywords / Aliases	GIS; Geographic Information Systems; Geospatial; Clearinghouse; Warehouse; Data;
SOLUTION SET TYPE	
Type of Solution	☐ *Business* ☒ *Application* ☐ *IT Infrastructure*
REQUIREMENTS VIEW	
Requirements View Name	Enterprise GIS Clearinghouse and Portal
View Category	Infrastructure; Information

Requirement Statement	*Requirement Owner*	*Related EA Component*

Infrastructure must reside on Unix servers in the State Data Center.		Dennis Bledsoe, ITS Infrastructure Coordinator	Infrastructure Domain – Product Component - Unix
Clearinghouse/Portal must use the Statewide backbone network		Jimmy Webster, ITS Network Manager	Infrastructure Domain Compliance Component – Statewide Network Standards
View Category	Database/Data		
Requirement Statement		*Requirement Owner*	*Related EA Component*
Database must be a relational database with spatial extensions and must contain the following data types: ▪ Geodetic Control ▪ Elevation and Bathymetry ▪ Orthoimagery ▪ Hydrography ▪ Transportation ▪ Government Boundaries ▪ Cadastral		Bruce Lightsey, ITS Database Administrator	Information Domain – Compliance Component – Database Standards, Data Types
The clearinghouse must be able to operate in a distributed environment; meaning that data will be hosted at the clearinghouse site but the clearinghouse will also provide an index which will point to data available at other sites.		Dennis Bledsoe, ITS Infrastructure Coordinator; Bruce Lightsey, ITS Database Administrator	Infrastructure Domain – Compliance Component – Distributed Access; Information Domain - Compliance Component – Distributed Database Standards; Platform Domain – Compliance Component – Platform Standards
View Category	Applications		
Requirement Statement		*Requirement Owner*	*Related EA Component*
There must be a GIS Portal application that serves as the entryway for all GIS Clearinghouse data and associated applications; including linkages to all GIS information on the State, Federal, and private sector levels.		Claude Johnson, ITS Clearinghouse/Portal Project Manager	Application Domain – Compliance Component – GIS Portal Configuration
There must be GIS applications that are developed specifically for accessing, displaying, and reporting on GIS data stored on the Clearinghouse.		Claude Johnson, ITS Clearinghouse/Portal Project Manager	Application Domain – Compliance Component – GIS Portal Configuration

CURRENT STATUS			
Solution Set Requirement Status	☒ *In Development* ☐ *Under Review* ☐ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	8/24/04	*Date Accepted / Rejected*	
Created By	Claude Johnson, ITS		
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Updated By			
Reason for Update			

Solution Set Design

Definition	
Name	Enterprise GIS Clearinghouse – Solution Set Design
Keywords	
Keywords / Aliases	GIS; Geographic Information Systems; Geospatial; Clearinghouse; Warehouse; Data;
Solution Set Type	
Type of Solution	☐ *Business* ☒ *Application* ☐ *IT Infrastructure*
Design View	
Design View Name	Enterprise GIS Clearinghouse and Portal
Category Name	Infrastructure; Information

Design Specification Statements	*Related EA Component*
Design of database and sizing estimates for all data.	Information Domain – Compliance Component – Database Standards, Data Capacity
Based on sizing activities, a model of the GIS infrastructure within the State Data Center depicting all necessary GIS database servers, web servers and application servers.	Infrastructure Domain – Compliance Component – Distributed Access
▪ Network Analysis Report of potential bandwidth requirements of transporting large amounts of GIS data over the Statewide backbone network. ▪ Plan for upgrading of network capacity capabilities.	Infrastructure Technology Scan Infrastructure Domain – Compliance Component – Capacity Planning
Related Requirements	*Relationship*
Test plan for ensuring that upgrades to the network were effective in dealing with additional network traffic brought on by GIS.	Satisfies Requirement

Category Name	Database/Data

Design Specification Statements	*Related EA Component*
Design of mandated types/levels of GIS data, but also including other types/levels as deemed necessary by the GIS Council.	Information Domain – Compliance Component – Database Standards, Data Types

Related Requirements	*Relationship*
GIS Council approval of database/data design.	Satisfies Requirement
Department of Environmental Quality must have produced and QA'd the data prior to implementation of data on the Clearinghouse.	Satisfies Mandate
Category Name	Applications
Design Specification Statement	*Related EA Component*
Design of the GIS Portal must fit Web design standards.	Application Domain – Compliance Component – Web Portal Design Standards
Design of GIS Clearinghouse applications must meet Web application design standards.	Application Domain – Compliance Component – Web Application Design Standards
Related Requirements	*Relationship*
GIS Council approval of GIS Portal	Satisfies Requirement
GIS Council approval of GIS Clearinghouse applications	Satisfies Requirement

SOLUTION SET LOGICAL MODEL			
Source Document	GIS Clearinghouse and Portal Logical Design (not yet completed) Refer to the Enterprise GIS Clearinghouse: Conceptual Model.doc within EA		
CURRENT STATUS			
Solution Set Design Status	☒ *In Development* ☐ *Under Review* ☐ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	8/24/04	*Date Accepted / Rejected*	
Created By	Claude Johnson, ITS		
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Updated by			
Reason for Update			

Project: e-Forms

Solution Set Scope

Definition	
Name	E-Forms - Solution Set Scope
Description	Currently, the majority of State forms are available on the State's Website in a non-enterable format. They have to be printed, filled in, and either faxed or mailed in to the appropriate agency. This is true both for forms used by the public and for forms used internally. The capability to be able to fill out and submit a form on-line would have tremendous value.
Rationale	This solution directly supports the State's efforts to make it easier to do business with all agencies of the State and to become more efficient and effective with our internal processes.
Benefits	For the public, the information on any e-form is sent directly to the agency without faxing or mailing, resulting in a more efficient and speedy process. In addition, all required information and appropriate formats are assured at the time the form is filled resulting in a decrease of issues related incomplete or incorrect forms being submitted. This can result in fewer delays in service delivery and an increase in customer satisfaction. The State will benefit by having information collected within the form available directly after its entry.
Boundary	
Boundary Scope Statement	This solution will not initially integrate with the existing digital signature capability. The information gathered on the form will be available to be directly entered into existing processes and databases without any re-entry of data or editing. Solution will need to allow the State Commission on Public Records to approve every new form that is made available on the State Website
Associated Implementation Plan Items	
Implementation Plan Project Identifier	ITOC 010; e-Forms
Plan Items Upon Which the Solution Set is Dependant	ITOC 011; e-Forms Routing
Plan Items Dependant Upon Solution Set	N/A
Related Migration Strategies	N/A
Selected Solution Set Conceptual Model	e-Forms flow diagram(Visio); shared drive under IT Architecture Models

Solution Set Type	Application Solution		
KEYWORDS			
Keywords / Aliases	Fill-able PDF; on-line forms; (Form Titles i.e. Request for Birth Certificate, etc)		
CONTACT INFORMATION			
Project Sponsor	Sean Fahey, Director, INTELENET		
Implementation Plan Coordinator	Andy Miller, Director, accessIndiana		
Solution Set Architect	Randy Grimes, Architect, accessIndiana		
Solution Set Contributors	Connie Hume, Commission on Public Records, 317/232-5555 Chris Pichereau, Director, DoIT; 317/232-5556 Jake Moelk, Systems Consultant, ITOC; 317/232-5557 Paul Tex, Manager, DoIT; 317/232-5558 Jim Hussey, Business Consultant, DoIT; 317/232-5559		
CONTRACT INFORMATION			
Name	Forms Fill-in Vendor		
Reference Number	FF-2367A		
Contact Information	Connie Hume, Commission on Public Records, 317/232-5555; Forms Fill-in Vendor Representative, 317/555-1212		
Implications	Failure will mean we do not make our efficiency and effectiveness goals		
CURRENT STATUS			
Solution Set Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	1/2/02	*Date Accepted / Rejected*	6/1/04
Created By	Jake Moelk, Systems Consultant, ITOC; 317/232-5557		
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Updated By			
Reason for Update			

Solution Set Requirements

Definition			
Name	e-Forms – Solution Set Requirements		
Keywords			
Keywords / Aliases	Enterable PDF; on-line forms		
Solution Set Type			
Type of Solution	☐ *Business* ☒ *Application* ☐ *IT Infrastructure*		
Requirements View			
Requirements View Name	Application		
Category Name	Technical		
Requirement Statement		*Requirement Owner*	*Related EA Component*
Form needs to be enterable from a browser. No "foot-print" is wanted		Laura Larimer, ITOC	Access Domain – Compliance Component – Web Design Configuration
Requirements View			
Requirements View Name	Integration		
View Category	Managerial		
Requirement Statement		*Requirement Owner*	*Related EA Component*
Both direct and "train-the-trainers" training is required		Laura Larimer, ITOC	General Government
Requirements View			
Requirements View Name	Usability		
View Category	Other		
Requirement Statement		*Requirement Owner*	*Related EA Component*
E-mail capability to send user ID and password back to an end user when they have "subscribed" to the site		Laura Larimer, ITOC	Application Domain – Compliance Component – e-Mail Configuration Standards
Need on-line storage to be able to save partially completed forms		Laura Larimer, ITOC	Information Domain – Compliance Component – Data Storage Standards
Current Status			
Solution Set Requirement Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
Audit Trail			

Creation Date	1/2/04	*Date Accepted / Rejected*	6/1/04
Created By	Jake Moelk, Systems Consultant, ITOC		
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Updated By			
Reason for Update			

Solution Set Design

Definition			
Name	E-Forms - Solution Set Design		
Keywords			
Keywords / Aliases	Enterable PDF; on-line form; (Form Names i.e. Birth Certificate Copy Request, etc…)		
Solution Set Type			
Type of Solution	☐ *Business* ☒ *Application* ☐ *IT Infrastructure*		
Design View			
Design View Name	Usability		
Category Name	Other		
Design Specification Statements			*Related EA Component*
Utility to provide authentication is needed. This is to allow the end user to disconnect from a session when they have not finished a form and to come back to it within a pre-described period of time.			Technical Architecture-Security Compliance Component - User Authentication
Related Requirements			*Relationship*
E-Mail capability to send user ID and password back to an end user when they have "subscribed" to the site.			Satisfies Requirement
Need on-line storage to be able to save partially completed forms			Satisfies Requirement
Solution Set Logical Model			
Source Document	Utility Forms Fill-In Model -- Reference Number FF-3478		
Current Status			
Solution Set Design Status	☒ *In Development* ☐ *Under Review* ☐ *Approved* ☐ *Rejected*		
Audit Trail			
Creation Date	6/1/04	*Date Accepted / Rejected*	7/1/04
Created By	Andy Miller, Director, access Indiana		
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Updated by			
Reason for Update			

Sample Requirements/Design Specifications

The following chart provides few examples of Security Requirements and their associated Design Specifications

Requirement	*Design Specification*
Users are required to authenticate their ID within the Solution Set. Users require a single log-in	Authenticate only once and be able to access a wide variety of applications and data available on local and remote systems. Also referred to as single sign-on (SSO).
Provide access to, or restrict access from, authentication data	Authentication data should be protected, or allowed, with access control and one-way encryption. This allows access to those who need it while preventing unauthorized individuals, including system administrators or hackers from obtaining the data.
Secure transmission of authentication data	Protect authentication data transmitted over public or shared data networks.
Limit log-on attempts	Limit the number of attempts by configuring the system to lock the user ID.
Secure authentication data as it is entered	Suppressing the display of the password or key as it is entered
Monitor authentication data	Monitor authentication data and token via procedures to disable lost or stolen passwords or tokens; implement monitoring systems to look for stolen or shared accounts

SUMMARY/CONCLUSION

The Solution Architecture provides a framework for capturing requirements and design specifications that are necessary for developing integrated enterprise solutions. Solution Architecture establishes a critical link between Business Architecture, Information Architecture, and Technology Architecture. Solution Architecture brings all these components together and enables the solution architect to leverage all the architecture artifacts to design integrated, enterprise-wide, reusable solutions.

It is through the pursuit of a formal Solution Architecture that the following are provided:

- A demonstrable, repeatable approach to assuring solutions are designed from an integrated perspective and based on the stated future architectural direction of the enterprise
- Identification of opportunities to leverage linkage across government-wide entities and increase collaboration and sharing of systems and solutions
- A means to increase architecture re-use and reduce the development of point solutions throughout the enterprise.

State and local government entities use Solution Architecture to provide clarity and direction for designing an integrated set of solutions, based on the overall business, information, and technology goals of the organization.

NASCIO Online
Visit NASCIO on the web for the latest information on the Architecture Program or to download the current version of the Enterprise Architecture Development Tool-Kit.

www.nascio.org

NASCIO EA Development Tool-Kit
Technology Architecture

Version 3.0

October 2004

TABLE OF CONTENTS

TECHNOLOGY ARCHITECTURE

Technology Architecture is a disciplined approach for documenting the enterprise's current, emerging and retiring technologies in order to leverage the investment in those resources and maximize their potential as solutions to business problems. Technology Architecture examines the underlying technologies that are required to run the enterprise and develops a unified vision of the target model of the enterprise's infrastructure and technology platforms.

Documentation of the Technology Architecture facilitates design of flexible, reliable, scalable, and secure systems that will support both known and unforeseen future requirements. Technology Architecture allows the enterprise to add systems and manage the lifecycle of current systems while guiding investment and design decisions. Balancing technology agility with technology efficiency is a challenge for all organizations. The Technology Architecture provides the tools for an organization to achieve the best balance for their state or local governmental body.

Figure 1 shows how Technology Architecture fits within the overall Enterprise Architecture Framework. The Technology Architecture is designed to support the strategic and operational requirements of the enterprise. It aligns with the Business and Information Architectures and supports Implementation Planning and Solution Architecture.

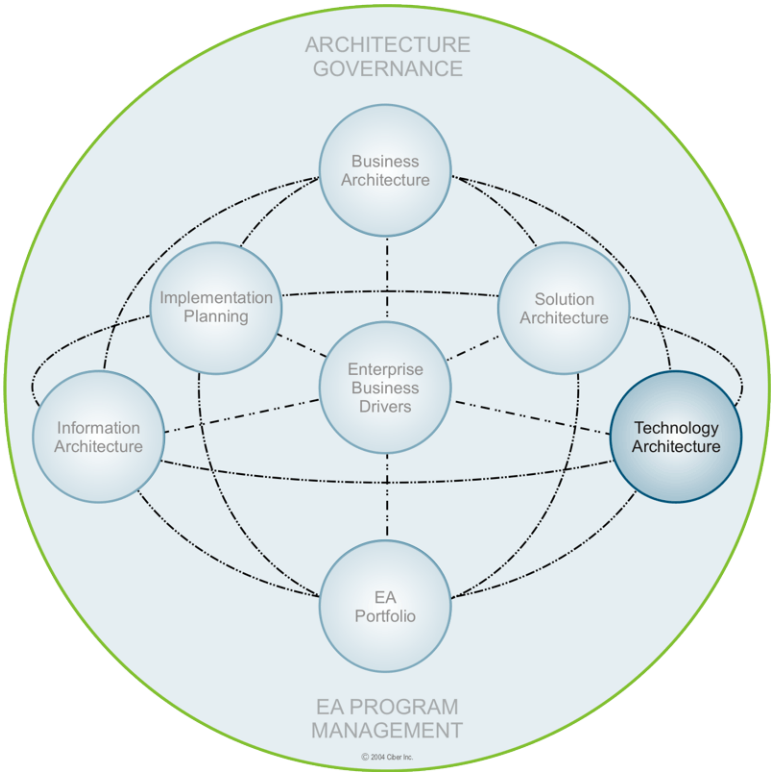


Figure 1. Technology Architecture Touch-points

State and local governments continually face mandates for inter-agency Information Technology system interoperability. Technology Architecture provides an adaptable framework for developing solutions that operate across agencies and within the lines of business of state and local governments. The pursuit of formal Enterprise Architecture Programs within organizations contributes to interoperability across enterprises. This is depicted in Figure 2.

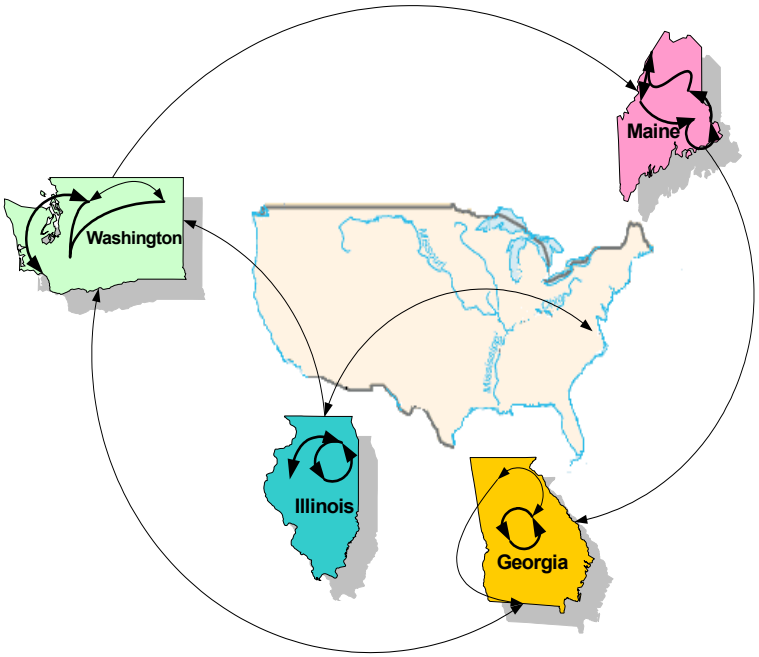


Figure 2. EA enhances interoperability between all government bodies.

Definitions

When discussing Technology Architecture and related topics, the terminology varies, including a variety of terms with the same or similar meanings, as well as varied meanings for the same term. To minimize any confusion in terminology, a glossary, which provides definitions of terms used throughout the Tool-Kit, is provided in Appendix A. A brief list of the terms and definitions used within this Technology Architecture section are provided here:

- *Adaptive:* Able to support a wide variety of applications and evolve as technology changes.
- *Agency:* A governmental unit; in the narrowest sense, a governmental unit of the executive branch.
- *Best Practices:* Trends and approaches that have successfully provided services and information over time.
- *Blueprint:* The dynamic, detailed information about a specific enterprise that is captured using standardized, structured processes and templates (the framework). The Technology Architecture Blueprint records the present direction of the enterprise and the direction the enterprise intends to pursue from a perspective of technology products and standards.
- *Business Drivers:* Global influences on business and technology that are captured within the architecture to show their acceptance and adoptability into the environment.

- *Component:* Within this Tool-Kit, component refers to a level of architectural detail. Within each of the constituent architectures, the component level detail is captured utilizing a respective template. Technology Architecture addresses Product Components and Compliance Components.
- *Current Technologies:* Technologies that are the current standard for use within the enterprise, and tested and generally accepted as standard within the industry. These items comply with or support the principles listed for the discipline.
- *Discipline:* Logical functional areas to address when building the architecture blueprint. The descriptions of the disciplines used in this document are found in Appendix D.
- *Domain:* High-level logical groupings of functional or topical operations that form the main building blocks within the architectural framework.
- *Emerging Technologies:* Technologies that, while possibly accepted and well utilized throughout the industry, are new to the enterprise. It is generally understood that emerging technologies be considered carefully before implementing in an enterprise-wide architecture. It is therefore recommended that, for initial implementation, emerging technologies be limited to smaller, non-mission-critical projects until it is proven that they can be integrated successfully into the existing enterprise architecture.
- *Framework:* The combination of the structure, processes, and templates that facilitate the documentation of the architecture in a systematic and disciplined manner. Use of the framework guides the documentation of the enterprise detail, which becomes the architecture blueprint.
- *Gap:* The difference between the "baseline" business environment and the "target" environment.
- *Infrastructure:* The basic, fundamental architecture of the system that supports the flow and processing of information, and that determines how the system functions and how flexible it is to meet future requirements.
- *Integration:* The ability to access and exchange critical information electronically at key decision points throughout the enterprise.
- *Interoperability:* The ability of a system or a product to work with other systems or products without special effort on the part of the customer, either by adhering to published interface standards or by making use of a "broker" of services that can convert one product's interface into another product's interface "on the fly"[1]
- *Legacy systems* An automated system built with older technology that may be unstructured and lacking in modularity, documentation and even source code.
- *Migration:* The evolution from the baseline to the target state.
- *Principle:* A statement of preferred direction or practice. Principles constitute the rules, constraints and behaviors that a bureau, agency or organization will abide by in its daily activities over a long period of time. Principles are business practices and approaches that the organization chooses to institutionalize to better provide services and information.
- *Repository:* An information system used to store and access architectural information, relationships among the information elements, and work products[2].
- *Scalability:* The ability to use the same applications and application systems on all classes of computers from personal computers to supercomputers.
- *Sunset Technologies:* Technologies that have been phased out and cannot be used within the organization past a specified date.

[1] http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci212372,00.html
[2] A Practical Guide to Federal Enterprise Architecture v1.0, CIO Council, February 2001

- *System:* A set of different elements so connected or related as to perform a unique function not performable by the elements alone (Rechtin 1991).
- *Target:* The desired future or "to be" state of the environment, captured in a set of target models.
- *Technology:* Tools or tool systems by which we transform parts of our environment and extend our human capabilities (Tornatzky and Fleischer 1990).
- *Technology Architecture Framework:* the combination of structures, templates and structured processes that facilitates the documentation of the enterprise's technology artifacts (e.g., products, standards) in a systematic and disciplined manner.
- *Template*: The empty form that serves as a guide for documenting the architecture detail. The resulting dynamic content captured using the template is referred to as the "blueprint" and ultimately resides in an Enterprise Architecture repository.
- *Trends:* Emerging patterns of operation within the business world that are impacting how services and information will be provided. Trends include governmental trends as well as architecture specific tends, i.e. technology trends, information management trends, etc.
- *Twilight Technologies:* Technologies being phased out by the enterprise but not yet having an established end date.

A sound Technology Architecture Framework is needed to support implementation of the architecture blueprint. The Technology Architecture Framework shows the relationship of the business drivers to the IT portfolio. The technology model must be flexible enough to provide the processes and templates to document any number of technology solutions to address business needs and problems.

This section of the Tool-Kit supports NASCIO's architecture program by providing government entities a method of establishing effective architecture technology models. It effectively supports the gap analysis of existing technology documentation, identifying methods to improve technology documentation performance, as well as the development of a Technology Architecture Blueprint in its entirety.

Technology Architecture Framework

The Technology Architecture Framework includes the templates and processes of the Enterprise Architecture Framework that will structure technology direction and existing IT services (Figure 3). This portion of the Tool-Kit documents the semi-static information, i.e. information that changes only when a major shift in the business or technology occurs. The following resources are available:

- Description of the Business Drivers that are a result of the business and IT strategies. These Business Drivers are mapped to the IT portfolio in the Architecture Blueprint.
- Processes for documentation of the Technology Architecture Blueprint levels
- Templates for the capturing information discovered during the Technology Architecture Processes

Business Drivers

The identification and development of Business Drivers is an important part of developing Enterprise Architecture. Business Drivers refer to the global influences on business that drive government and are captured within the architecture to show their acceptance and adoptability into the environment. Though these global influences can be of numerous types, three common categories of Business Drivers are Principles, Best Practices and Trends.

Principles: Principles are statements of preferred direction or practice. Principles constitute the rules, constraints and behaviors that a bureau, agency or organization will abide by in its daily activities over a long period of time. Principles are business practices and approaches that the organization chooses to institutionalize to better all provided services and information.

Best Practices: Best practices are behaviors and approaches that have proven successful at providing services and information over time.

Trends: Trends are emerging influences within the business world that are impacting how services and information will be provided. Trends include governmental trends, as well as architecture specific trends, i.e. technology trends, information management trends, etc.

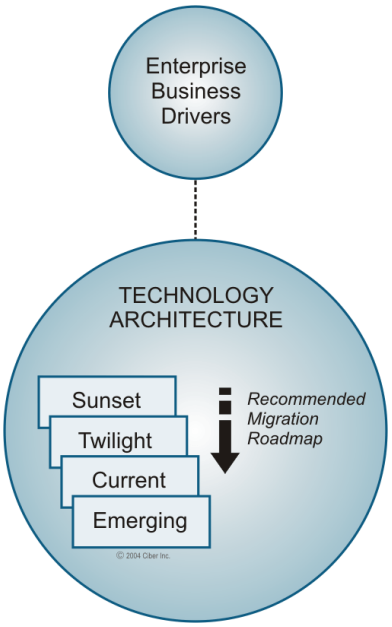


Figure 3. Technology Architecture Flow

TECHNOLOGY ARCHITECTURE BLUEPRINT STRUCTURE

The Technology Architecture Blueprint Framework consists of:

- The Technology Architecture Blueprint Documentation Processes
- The Technology Architecture Blueprint Templates

In order to discuss the Technology Architecture Blueprint Documentation Process, it is first necessary to become familiar with the various levels of the Technology Architecture Blueprint and get an overall picture of how the pieces fit together.

There are five technology architecture blueprint levels:

- Domains
- Disciplines
- Technology Areas
- Product Components
- Compliance Component

As can be seen from the graphic in Figure 4, these pieces work together to ensure the complete documentation of the Domains that form the Technology Architecture Blueprint.

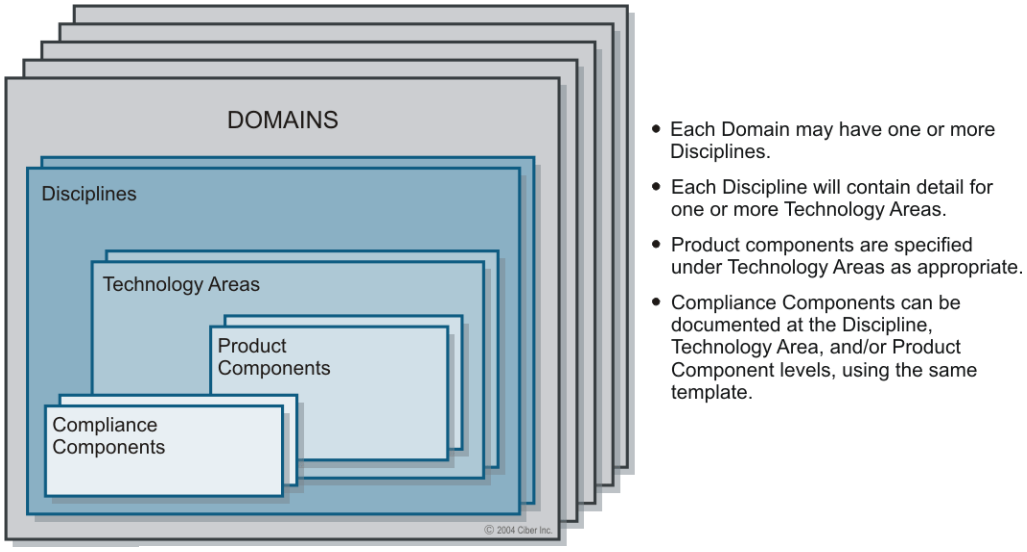


Figure 4. Blueprint Structure

Domains are the natural divisions of the technology architecture and, as seen in Figure 5, form the main building blocks of the technology architecture blueprint.

A Domain is simply a category that is used to group related topics, similar to the way a library groups related topics (Biographies, Art, History, etc.). Each Domain identified will be developed and documented by a team made up of subject matter experts who are familiar with the organization's IT environment.

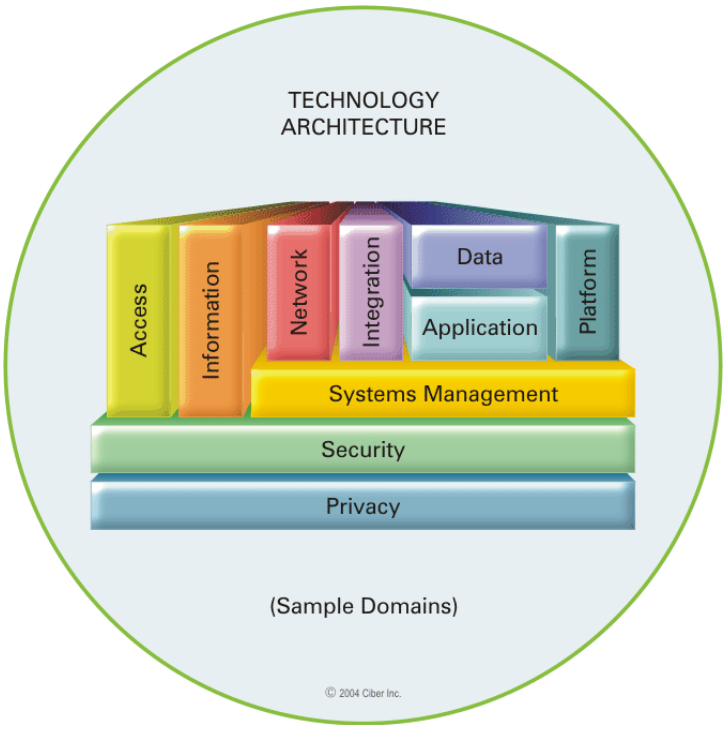


Figure 5. Sample Technology Architecture Domains

The logical functional subsets of a Domain are called **Disciplines**. Disciplines allow further breakdown of the Domain into manageable pieces, especially for Domains that cover large and/or diverse topics. Each Discipline is a cohesive unit with regard to its subject areas and stakeholders.

The Systems Management Domain provides a good example of a Domain with multiple Disciplines:

Domain	*Disciplines*
Systems Management	• Asset Management • Change Management • Console/Event Management • Help Desk/Problem Management • Business Continuity

Each Domain will have one or more Disciplines. As with Domains, additional Disciplines may be identified during the development or evolution of the enterprise architecture

Technology Areas are those technical topics that support the technology functional areas of the architecture blueprint.

A few examples of technology areas from within the Database Management Discipline of the Information Domain are:

- Relational Database
- Flat File Systems
- Desktop Database
- Data Models

Each of these technology areas will have products, protocols or configurations associated with it. These are documented at the Product Component level.

Technology Areas are identified and addressed within each Discipline. At this level, the technical details of the Technology Architecture Blueprint start to form.

Product Components include the protocols, products (families) and configurations that are specific to a technology area. Examples of Product Components identified within the technology area of Data Models include ERWin, Visio, Rational Rose, System Architect and Designer 2000.

The documentation of each Product Component includes the evaluation criteria used by the Documenter to determine the component's acceptance as part of the technology architecture blueprint.

Compliance Components identify guidelines, standards and legislative mandates associated with a Discipline, Technology Areas, and/or Product Components as appropriate.

Compliance Components provide the basis for making important decisions about new products, protocols, configurations, etc. The same template for evaluation, classification, and documentation may be used for Compliance Components at all three levels. Guidelines, standards and legislative mandates differ primarily in the degree of compliance prescribed by each.

Domain	*Discipline*	*Technology Area*	*Product Component*	*Compliance Component*
Information	Data Management	• Relational Database • Flat File Systems • Desktop Database • Data Models	• Oracle • Sybase • DB2 • ERWin • Designer 2000	• Data Model Denotations- Crows Feet • Normalization • Column Naming Standards

Each sub-process in the Technology Architecture Documentation Process describes the documentation of one level of the Blueprint, with one additional sub-process to cover the evaluation and classification of the Product and Compliance Components.

Each sub-process will have a process model and narrative section. Where a template is introduced within a process model, the template and its detail follow the process narrative. The Technology Architecture Documentation Process includes the following Sub-processes and Templates.

- Document/Update Domain Blueprint Process
- Domain Blueprint Template
- Document/Update Discipline Blueprint Process
- Discipline Blueprint Template
- Document/Update Technology Area Blueprint Process
- Technology Area Blueprint Template
- Document/Update Product Component Blueprint Process
- Product Component Blueprint Template
- Document/Update Compliance Component Blueprint Process
- Compliance Component Blueprint Template
- Evaluate Compliance/Product Components

TECHNOLOGY ARCHITECTURE DEVELOPMENT

The process of developing the Technology Architecture begins with initiating the Technology Architecture Documentation Process. This documentation process allows the architecture teams to capture, analyze, and document details about the products and standards, which will be included in the Technology Architecture Blueprint.

Figure 6 provides a graphical representation of the workflow path for the architecture team as it moves through the processes and sub-processes of the Technology Architecture Documentation Process.

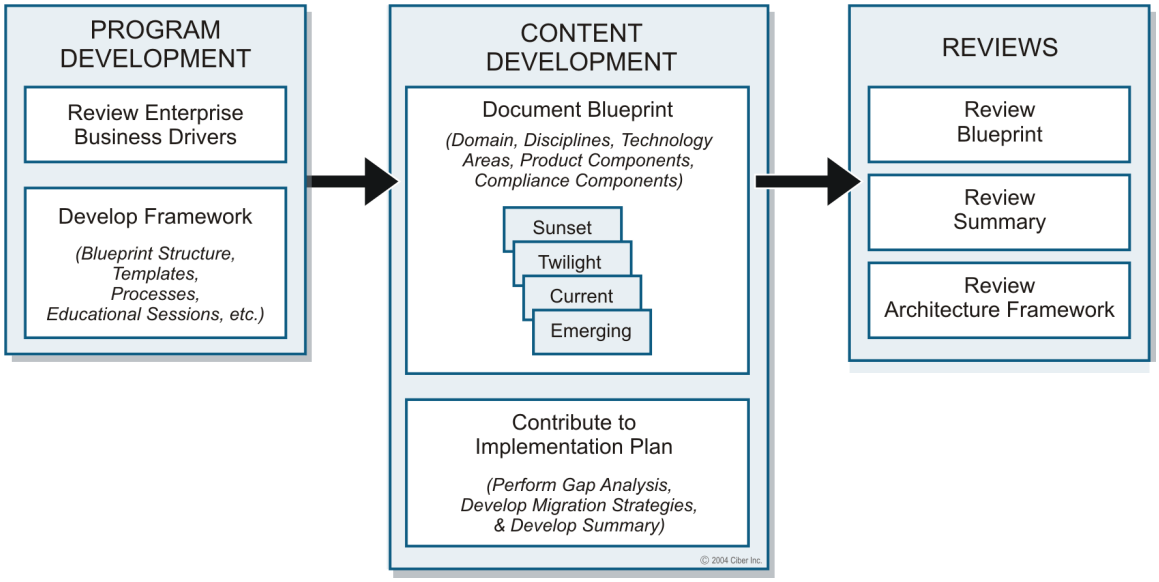


Figure 6. Technology Architecture Development Work Flow

The Technology Architecture Documentation Process describes the systematic process for developing and maintaining the Technology Architecture Blueprint. The Technology Architecture Documentation Process consists of several sub-processes, including:

- Initiate Technology Architecture Documentation Process
- Develop Enterprise Drivers
- Develop Technology Architecture Framework
- Conduct Technology Architecture Work Sessions
- Create/Update Technology Architecture Blueprint Items
- Complete/Update Domain Blueprint
- Complete/Update Discipline Blueprint
- Complete/Update Technology Area Blueprint
- Complete/Update Product Component Blueprint
- Complete/Update Compliance Component Blueprint
- Evaluate Product/ Compliance Component

The structure for each sub-process of this Technology Architecture Documentation Process follows the same format:

- Introductory material (where applicable)
- Process model
- Narrative description of the process
- Template for capturing Blueprint detail (where applicable)
- Narrative description of the detail to be captured utilizing the template

Initiate Technology Architecture Documentation Process

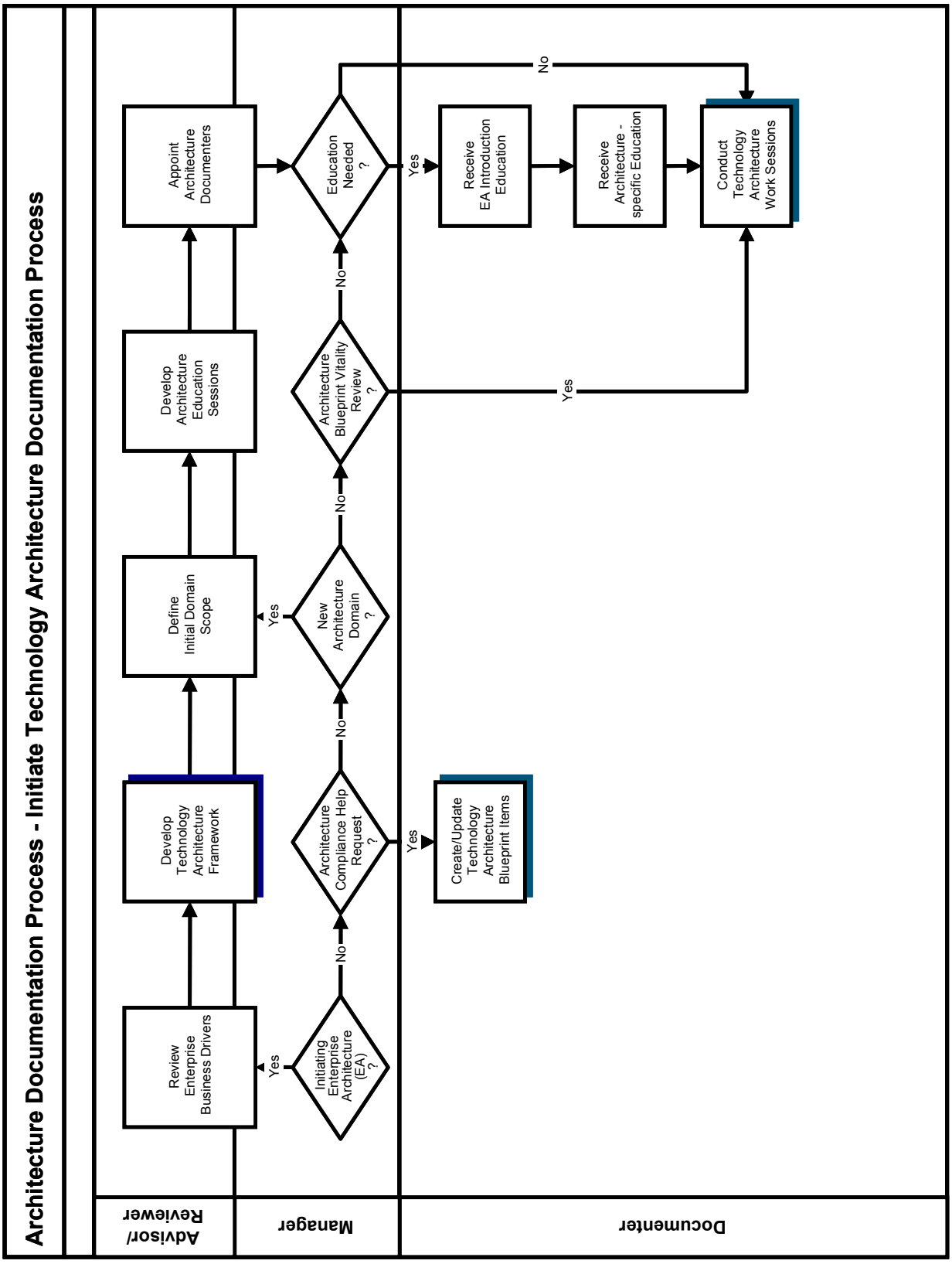
PROCESS OVERVIEW

The architecture documentation process may be initiated based on three events:

- The initial development of the adaptive enterprise architecture
- Following the Architecture Blueprint Vitality Process
- Following the Compliance Process (Architecture Help Request)

The starting point depends on the event that triggered the documentation process. The following explains the starting points and rationales:

- *Enterprise Architecture Initiation Trigger* – The first time the Architecture Blueprint is documented, the Documenters are supplied with basic information for each of the Domains and Disciplines, such as definition, rationale, benefits, boundary statements and an initial set of technology areas to be covered within each. Also, the Documenters are trained on the various enterprise architecture processes and templates. The Documenters are then prepared to develop the detail that will become the EA Blueprint.
- *Architecture Blueprint Vitality Process Trigger* – This periodic process verifies that the Architecture Blueprint is staying current with the changes in the business and in the technology world. Vitality can impact the Architecture Blueprint from the Domain level down.
- *Compliance Process Trigger* – The Compliance Process is the point where IT groups outside of the Architecture group interact with the various Architecture processes and blueprints. This process is initiated from an Architecture Help Request. Compliance can impact the Architecture Blueprint from the Technology Area down


Architecture Documentation Process - Initiate Technology Architecture Documentation Process
Advisor/ Reviewer
Manager
Documenter
Review Enterprise Business Drivers
Initiating Enterprise Architecture (EA) ?
Yes
No
Develop Technology Architecture Framework
Architecture Compliance Help Request ?
Yes
No
Create/Update Technology Architecture Blueprint Items
Define Initial Domain Scope
New Architecture Domain ?
Yes
No
Develop Architecture Education Sessions
Architecture Blueprint Vitality Review ?
No
Yes
Appoint Architecture Documenters
Education Needed ?
Yes
No
Receive EA Introduction Education
Receive Architecture - specific Education
Conduct Technology Architecture Work Sessions

PROCESS DETAIL

Review Enterprise Business Drivers – It is important for the Technology Architecture teams to understand and become familiar with the Enterprise Business Drivers. While the development of the Enterprise Business Drivers is typically an overarching activity of Business, the Technology Architecture teams may become aware of circumstances or shifts from documented drivers and can contribute to the vitality of the Enterprise Business Drivers.

Develop Technology Architecture Framework – The information documented within the Technology Architecture Framework will play an important role in the development of the Technology Architecture Blueprints. The NASCIO Technology Architecture Framework provides structured processes and templates for capturing this information in a consistent and systematic manner. An enterprise may decide to use the framework elements as described in the NASCIO Tool-Kit, or may choose to develop modified versions, or may use processes, templates and governance structures other than the examples provided in this Tool-Kit.

Define Initial Domain Scope – Develop the definition of the Technology Domains and add any detail that will be helpful in identifying the documentation team members. Also, add any information that will help the team develop the appropriate level of documentation for these domains.

Develop Architecture Education Sessions– The Architecture Education Sessions provide a high-level overview of the Enterprise Architecture Program and prepare Documenters for their role in the Technology Architecture effort. Developers of education materials should consider inclusion of the following materials:

- Purpose
- Presenters
- Intended audience
- Session structure
- Prerequisites
- Syllabus
- Objectives
- Class materials for both instructors and attendees

Appoint Architecture Documenters – At this point, the Documenters are appointed from subject matter experts familiar with the business, information or technology of the enterprise, depending on the architecture to be documented. The team will be responsible for steering, shaping, and developing the Architecture Blueprints.

The educational sessions described below are progressive in nature. The sessions will be conducted after the architecture team is identified:

Receive EA Introduction Education – Documenters should receive initial training that covers the overview of enterprise architecture and architecture governance.

Receive Architecture-specific Education – After receiving initial enterprise architecture training, the Documenters will receive specialized instruction addressing the business, information or technology

architecture documentation templates and respective architecture documentation processes that they will use to document the Architecture Blueprint.

Conduct Technology Architecture Work Sessions – Applying knowledge gained in the first two sessions, Documenters will begin development of the Architecture Blueprint documentation. The detail pertaining to architecture-specific work sessions is presented as a separate process (see *Conduct Documenter Work Sessions*).

Create/Update Technology Architecture Blueprint Items – If architecture compliance help is requested, the various Blueprint items should be updated. The process model and details pertaining to updating the Blueprint items is presented in a separate process. (See *Create/Update Technology Architecture Blueprint Items*).

Develop Technology Architecture Framework

PROCESS OVERVIEW

Framework refers to the combination of the structure, processes, and templates that facilitate the documentation of the architecture in a systematic and well-disciplined manner. In this Tool-Kit, the term Technology Architecture Framework is used to refer to the combination of the structural elements of the Technology Architecture, including the templates and the structured processes for documenting, reviewing communicating, implementing and maintaining the Technology Architecture.

Each organization should develop a Technology Architecture Framework based on their individual circumstances. The NASCIO Tool-Kit is designed to provide a jumpstart for organizations as they develop their architectures, not to provide a methodology. The framework elements provided in this Tool-Kit represent a sampling of the structural elements an organization should consider as they build their Technology Architecture, and are by no means exhaustive, nor are they intended to be prescriptive There are many methodologies for developing architectures. Regardless of the methodology selected, the structure for capturing Technology Architecture Blueprint detail should be consistent and concise to ensure uniform documentation and communication across the enterprise.

Architecture Documentation Process - Develop Technology Architecture Framework
Advisor/Reviewer
Manager
Documenter
Develop Technology Architecture Processes/ Templates
Identify/Define Domains
Identify/Define Disciplines
Select Initial Technology Domains for Documentation

PROCESS DETAIL

Develop Technology Architecture Processes/Templates – Developing the processes and templates for capturing pertinent architecture detail, as well as defining and documenting the governance structure to support the architecture activity, is a step that is critical when initiating EA or any of the underlying architectures. Each enterprise must decide upon the methodology that best suits their organization. The best methodology for an organization is one that addresses the resource and time constraints of that enterprise.

The development of the Technology Architecture processes and templates is a good time to consider the use of a repository or automated tool for the capture and storage of the architecture documentation. The use and maintenance of the Enterprise Architecture is greatly simplified when the information and models are readily available to all stakeholders. There is a large amount of information collected and documented within an EA with many interrelations between the parts of the EA. It is best if all the EA information, models and products are placed in a robust EA repository to maximize the potential for reuse.

Identify/Define Domains, Identify/Define Disciplines - Technology Domains provide the natural divisions of the Technology Architecture based on scope and are the main building blocks of the Technology Architecture blueprint. The further breakdown of the Domains into manageable sub-sets, referred to in this Tool-Kit as Disciplines, should also be done as part of the framework development process. Each organization must identify its own Technology Domains and respective Disciplines. Examples of typical Domains and Disciplines with brief descriptions as used in this Tool-Kit can be found in *Appendix D: Sample Domain-Discipline Descriptions*.

Select Initial Technology Domains for Documentation – It will not be feasible to attempt to document every Domain at one time. Care should be taken to select a reasonable number of Domains, based on criticality and resources.

Each organization must identify its own priorities regarding which Domains should be the focus for further development. IT and Business strategic elements and cross-functional goals provide vital information for determining the prioritization. Specific circumstances of each enterprise such as legislative mandates, federal regulation, budgetary constraints, competing resources, organizational readiness, pain points, and delivery timeframes will all be additional considerations as Advisors/Reviewers work to define a manageable number of Technology Domains for their enterprise.

Conduct Technology Architecture Work Sessions

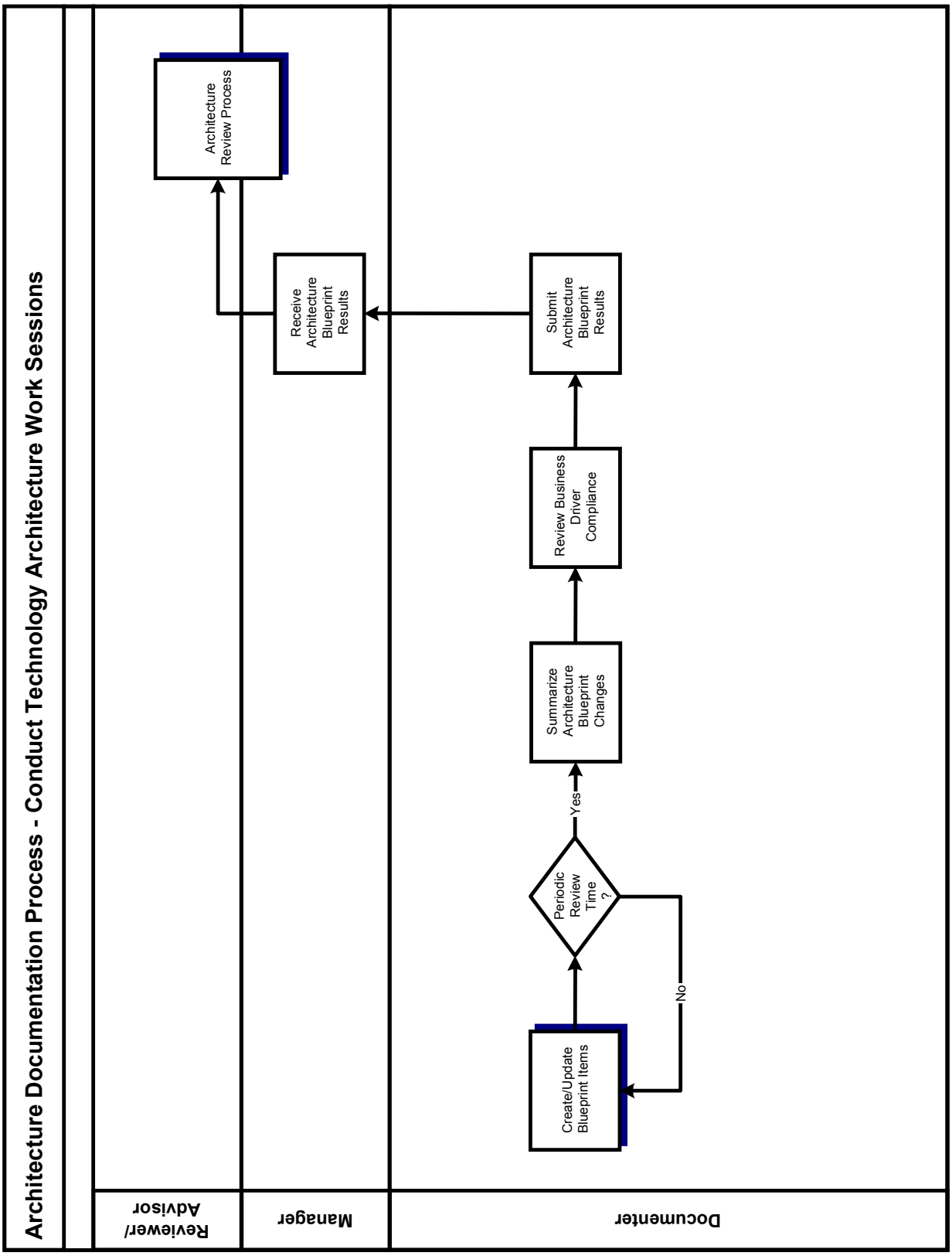
PROCESS OVERVIEW

The Technology Architecture work sessions are intended to produce the documentation that initially populates the Architecture Blueprint. Ongoing Documenter meetings are required to maintain the vitality of the Domain's architecture blueprint. The first session will include:

- Defining roles and responsibilities
- Reviewing architecture blueprint documentation requirements
- Determining expectations of on-going meetings.

After the first meeting, on-going working sessions are triggered from Architecture Lifecycle Processes including:

- Architecture Review Process
- Architecture Compliance Process
- Architecture Blueprint Vitality Process.


Architecture Documentation Process - Conduct Technology Architecture Work Sessions
Reviewer/ Advisor
Manager
Documenter
Architecture Review Process
Receive Architecture Blueprint Results
Submit Architecture Blueprint Results
Review Business Driver Compliance
Summarize Architecture Blueprint Changes
Yes
Periodic Review Time ?
No
Create/Update Blueprint Items

PROCESS DETAIL

Create/Update Blueprint Items - The primary purpose of the working sessions is to document the Technology Architecture, therefore creating and/or updating the Technology Blueprint items will be on the agenda for most working sessions. The process steps for documentation of the Blueprint items are covered in a separate process step later in this section. (See sub-process - *Create/Update Blueprint Items*)

Summarize Architecture Blueprint Changes - Based on changes occurring since the last periodic review, the Documenter will create a summary listing all changes to the Architecture Blueprint for that Domain throughout the five levels.

Review Business Driver Compliance - The submitted changes for a specific Domain may cause a conflict with one of the Business Drivers. This process step assures that the Documenter takes a high-level review of the Domain's architecture blueprint to verify that no conflicts exist. Where conflicts exist, the Documenter will provide the proper documentation to the Architecture Manager.

Submit Architecture Blueprint Results - Based on time or completion of a documentation process, the Documenter will gather and submit the available Domain blueprint results to the Architecture Manager.

Review Architecture Blueprint Results - The Architecture Manager will receive, review, and summarize the Domain results.

Architecture Review Process - The prepared Domain Results will be presented and reviewed at the next Architecture Review Meeting.

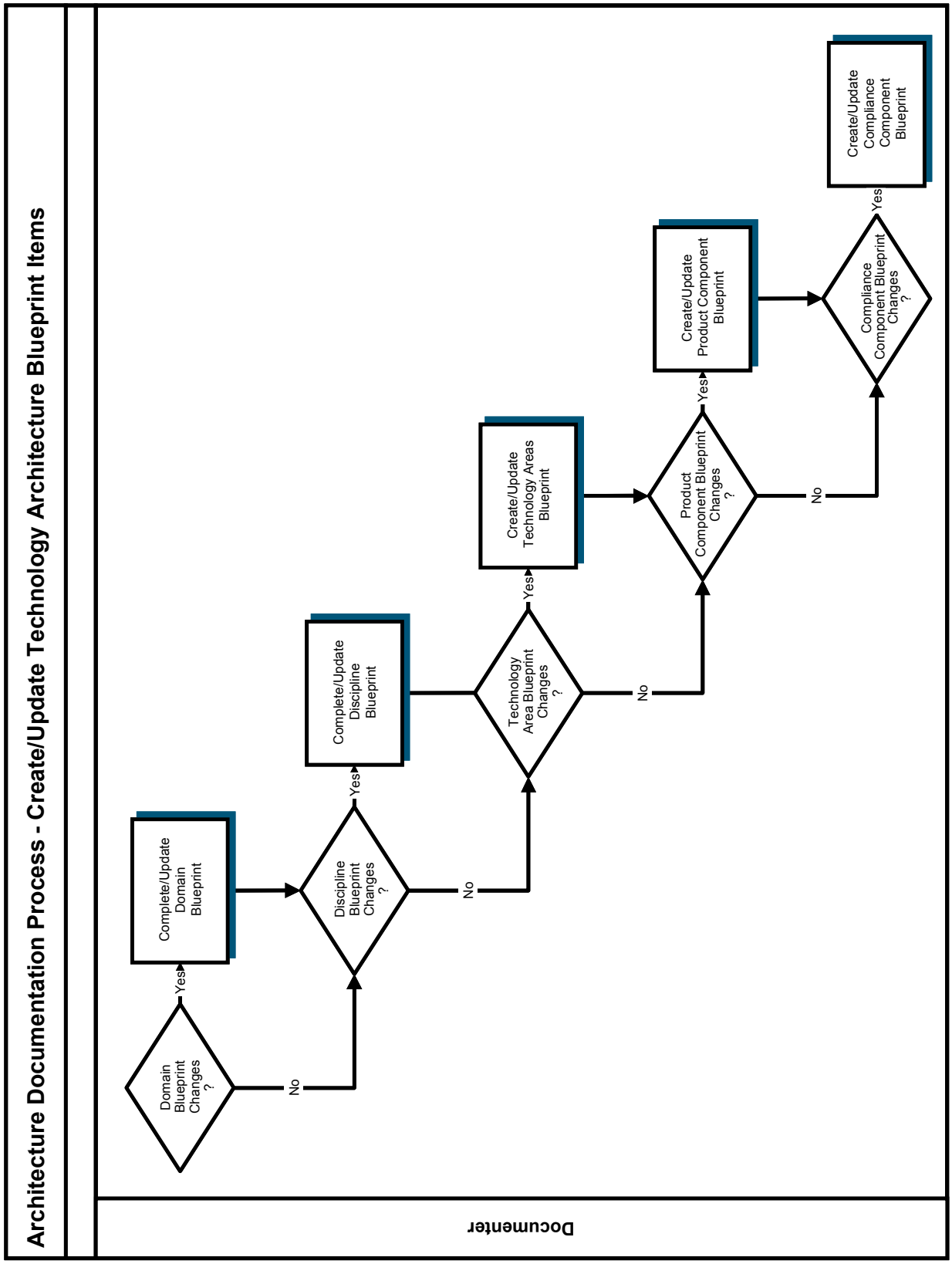
Create/Update Technology Architecture Blueprint Items

PROCESS OVERVIEW

Various architecture processes trigger the update of the Technology Architecture Blueprint, including:

- Conduct Technology Work Sessions
- Architecture Review Process
- Architecture Compliance Process
- Architecture Blueprint Vitality Process

The appropriate Technology Architecture Blueprint levels will be updated, based on what triggered the Create/Update Technology Architecture Blueprint Items process.


Architecture Documentation Process - Create/Update Technology Architecture Blueprint Items
Documenter
Domain Blueprint Changes ?
Yes
No
Complete/Update Domain Blueprint
Discipline Blueprint Changes ?
Yes
No
Complete/Update Discipline Blueprint
Technology Area Blueprint Changes ?
Yes
No
Create/Update Technology Areas Blueprint
Product Component Blueprint Changes ?
Yes
No
Create/Update Product Component Blueprint
Compliance Component Blueprint Changes ?
Yes
Create/Update Compliance Component Blueprint

PROCESS DETAIL

NOTE: The following processes are sub-processes of the Architecture Documentation Process and are used for updating the Architecture Blueprints. Details for each of these sub-processes are provided later in this section.

Complete/Update Domain Blueprint - If the accepted change identified a new Domain, the new Domain should be fully documented, including all subordinate levels.

If the change being sought identified changes to an existing Domain, the blueprint for the Domain and the other affected Domains should be updated to reflect the accepted or rejected change.

For documentation requirements, see Architecture Blueprint Templates – Domain Template.

Complete/Update Discipline Blueprint - If the accepted change identified a new Discipline, fully document the new Discipline, including all subordinate levels. If the requested change identified changes to an existing Discipline, update the blueprint for the Discipline and other affected Disciplines to reflect the accepted or rejected change.

For documentation requirements, see Architecture Blueprint Templates – Discipline Template.

Create/Update Technology Areas Blueprint - If the accepted change identifies a new Technology Area, fully document the new Technology Area, including all subordinate levels. If the requested change identified changes to an existing Technology Area, update the blueprint for the area to reflect the accepted or rejected change.

For documentation requirements, see Architecture Blueprint Templates – Technology Area Template.

Create/Update Product Component Blueprint - If the accepted change identified a new Product Component, fully document the new Product Component, including all subordinate levels. If the requested change identified changes to an existing Product Component, update the blueprint for the product to reflect the accepted or rejected change.

Conditional use should be documented as well, if it applies.

For documentation requirements, see Architecture Blueprint Templates – Product Component Template.

Create/Update Compliance Component Blueprint - If the accepted change identified a new Compliance Component, fully document the new Compliance Component. If the requested change identified changes to an existing Compliance Component, update the blueprint for the Compliance Component to reflect the accepted or rejected change.

Conditional use should be documented as well, if it applies.

For documentation requirements, see Architecture Blueprint Templates – Compliance Component Template.

Complete/Update Domain Blueprint

PROCESS OVERVIEW

The Domain is the highest level of the Technology Architecture Blueprint levels. The definition and development of each Domain is a process that will evolve and change as information is gathered and documented. A domain template is provided to ensure consistent documentation of each Domain.

The NASCIO working group has been involved in a high-level review process to define and document a sample set of Domains. This sample set of Domains includes:

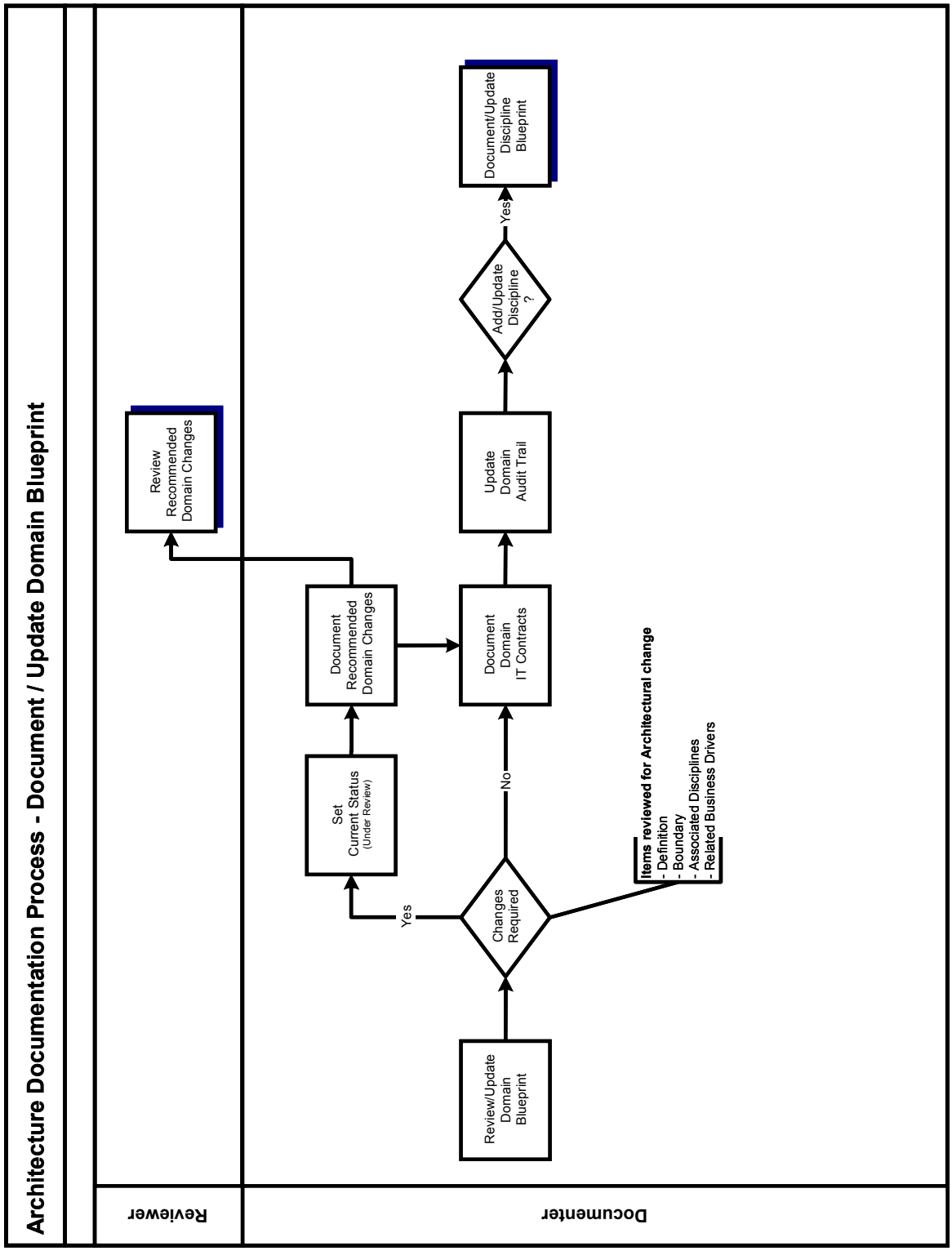
- Access
- Platform
- Network
- Application
- Information
- Integration
- Systems Management
- Security
- Privacy

Each governmental entity must determine the Domain structure that works best for their own organization. Many government entities may identify or define Domains differently during the development or evolution of their own enterprise architecture.

Important items to keep in mind when determining the breakout of Domains are:

- A committee of subject area experts should be established to handle the development and maintenance of each Domain.
- Domains should not be too broad. The scope of each Domain should be reasonable for a committee to handle.
- Domains should not be too narrow. Having Domains that are narrow in scope will cause the creation of many Domains, which in turn results in numerous committees.
- It is best to keep the number of Domains between 5 and 10.

The following information is provided to assist organizations in their efforts to document the items essential to Domain development.


Architecture Documentation Process - Document / Update Domain Blueprint
Reviewer
Documenter
Review/Update Domain Blueprint
Changes Required
Yes
No
Set Current Status (Under Review)
Document Recommended Domain Changes
Review Recommended Domain Changes
Document Domain IT Contracts
Items reviewed for Architectural change
- Definition
- Boundary
- Associated Disciplines
- Related Business Drivers
Update Domain Audit Trail
Add/Update Discipline ?
Yes
Document/Update Discipline Blueprint

PROCESS DETAIL

The Domain Architecture Blueprint will be completed/updated using the Domain Template as a guide. The following process steps will aid in this documentation:

Review/Update Domain Blueprint - The definition of the Domain and the primary Disciplines are provided to the Documenter during the facilitated workshop training. The Documenter will have the responsibility of reviewing:

- Domain definition and Domain boundary
- Associated Disciplines

An Architecture change request should be submitted if additional Disciplines are required.
This request is submitted to the Architecture Manager for validation prior to any further work on that topic.

Conduct a review of the Business Drivers to ensure that the development of the Domain does not conflict with the established Principles, Best Practices and Trends (Industry or Technology). The Documenters should identify the Business Drivers that apply most directly to their Domain and elaborate on (and document) the relationship between their Domain and the Drivers.

Set Current Status - Set the Current Status as appropriate. It is important to understand where a given Domain is in the architecture documentation process. Initial statuses identified include:

- *In Development* – The architecture team is currently crafting and/or reviewing the Domain content.
- *Under Review* – The architecture team has completed the Domain content and it is under review by an EA governing body.
- *Accepted* – Indicates the Domain has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Domain was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

Document Recommended Domain Changes; Review Recommended Domain Changes - Document and submit to the Architecture Manager any changes to the definition, boundary, or Business Drivers prior to proceeding with the Domain documentation. These types of changes can affect more than just the Documenter requesting the modification.

Document Domain IT Contracts - Identify existing or planned state contracts that address the specific Domain technologies. This part of the Domain template should be completed after documenting the Technology Areas, Product Components, and Compliance Components under the Domain.

Update Domain Audit Trail - Maintain audit trails for the information provided in the template. During this initial development of the Domain, only information about the creation, accepted/rejected, and date last updated need to be maintained.

Document/ Update Discipline Blueprint - If additions or updates to any of the Disciplines are needed, continue with the sub-process Document/ Update Discipline Blueprint, which is described in detail later in this chapter.

Domain Template

TEMPLATE OVERVIEW

The Domain Template provides a checklist for documenting the Domain details. A detailed description of each of the content areas follows the visual representation of the Domain Template provided here.

The Domain Template will include the following sections:

- Definition
- Boundary
- Associated Disciplines
- Related Principles
- Related Best Practices
- Related Trends
- State Contracts
- Current Status
- Audit Trail

Domain

Definition	
Name	
Description	
Rationale	
Benefits	

Boundary	
Boundary Limit Statement	

Associated Disciplines	
Disciplines under this Domain	

Related Principles		
Reference #s, Statements or Links	*Conflict*	*Relationship*
	☐	
	☐	

Related Best Practices		
Reference #s, Statements or Links	*Conflict*	*Relationship*
	☐	
	☐	

Related Trends		
Reference #s, Statements or Links	*Conflict*	*Relationship*
	☐	
	☐	

State Contracts	
Planned Contracts	
Existing Contracts	

Current Status				
Domain Status	☐ *In Development*	☐ *Under Review*	☐ *Rejected*	☐ *Accepted*

Audit Trail			
Creation Date		*Date Accepted/Rejected*	
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

TEMPLATE DETAIL

Definition

Name - Determine an appropriately descriptive name for the Domain.

Description - Supply a description of the Domain in a paragraph or two that provides sufficient clarity to reader about the Domain and what it covers.

Rationale - Provide a paragraph or two containing the reason or basis for inclusion of this Domain in the technology architecture.

Benefits - Provide a paragraph or bulleted statements that supply the benefits associated with the Domain.

Boundary

Boundary Limit Statement - The Boundary Limit Statement provides parameters for identifying the boundaries for the Domain. This section should contain statements about what is included, as well as items that are related to, but excluded from, the Domain. If excluded items are identified, it is beneficial to include a reference to the Domain where that information can be found.

Associated Disciplines

Disciplines under this Domain - Provide a list of the Disciplines that are covered within this Domain. This provides an index for these Disciplines. The detailed documentation for each Discipline listed will be completed using the Discipline Template.

Related Principles

References #s, Statements or Links - Principles identify the overarching general rules that hold true across the enterprise architecture. The principles are developed and documented as Business Drivers at the most global level of the enterprise architecture.

Conflict - Verify that the development of the Domain does not conflict with the established Business and Technology Driver Principles. This is a yes/no answer.

Relationship - The relationship should be documented for those principles that apply most directly to the Domain. Principles with the relationship left blank will indicate that the principle does not apply to this Domain.

Related Best Practices

References #s, Statements or Links – Best practices identify industry processes related to the implementation of the enterprise architecture that will assist in the maintenance and expansion of an adaptive enterprise technology architecture. They are based on experience and proven results. The best practices are documented as Business Drivers, which apply to the enterprise-wide concept of architecture.

Conflict - Verify that the development of the Domain does not conflict with the established Business and Technology Driver Best Practices. This is a yes/no answer.

Relationship - The relationship should be documented for those best practices that apply most directly to the Domain. Best practices with the relationship left blank will indicate that the best practice does not apply to this Domain.

NOTE: Best Practices that are identified as specific to the Domain will be defined and documented as Compliance Components (guidelines or standards) at the Discipline level.

Related Trends

References #s, Statements or Links - Industry and technology trends have an effect on the deployment of information technology. Identifying these trends and having an awareness of their impact will allow IT decision makers to develop more informed, effective decisions. The trends are documented as Business Drivers, which apply to the enterprise-wide concept of architecture.

Conflict - Verify that the development of the Domain does not conflict with the established Industry and Technology Trends. This is a yes/no answer.

Relationship - The relationship should be documented for those trends that apply most directly to the Domain. Trends with the relationships left blank will indicate that the trend does not apply to this Domain.

NOTE: Business and Technology Trends that are identified as specific to the Domain will be further defined and documented at the Discipline level. This will allow the trends to be defined within the Discipline where they most appropriately apply.

State Contracts

Planned Contracts - Provide a list of planned future contracts associated with this Domain.

Existing Contracts - Provide a list of existing contracts associated with this Domain

Current Status

Domain Status - Document the status of Domain, indicating whether the Domain is in development, under review, rejected, or accepted.

- *In Development* – The architecture team is currently crafting and/or reviewing the Domain content.
- *Under Review* – The architecture team has completed the Domain content and it is under review by an EA governing body.
- *Accepted* – Indicates the Domain has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Domain was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

Audit Trail

The Audit Trail is included at each level of the Architecture Blueprint. It provides the means to track changes made to each of the levels, identifies the date the level was last reviewed to assist in the Vitality Process, and identifies roles and/or individuals involved in the introduction or modification of the Blueprint information for historical purposes.

This information is extremely helpful for the vitality of the Blueprints, as well as invaluable to Project /IT Services Teams in their research when requesting a variance, and to Documenters conducting research on related items across Domains.

Creation Date - Provide the date the Domain was created.

Created By – List all individuals and their titles that helped in the creation of this Domain.

Date Accepted/Rejected - Provide the date the Domain was accepted into the architecture blueprint or rejected.

Reason for Rejection - If the Domain was rejected, document the reason for the rejection.

Last Date Reviewed - Document the most recent date the Domain was taken through the Architecture Blueprint Vitality Process.

Last Date Updated - Document the most recent date that any item in the Domain template was changed.

Reason for Update - Document the reason for the update to the Domain. This information should be a detailed description of the change, for future reference.

Updated By - Provide the names of the persons responsible for the update to the Domain. This will be helpful information for future reference.

Complete/Update Discipline Blueprint

Process Overview

Disciplines are the second level of the Technology Architecture Blueprint. Disciplines are the technology functional areas within a Domain. The overall structure of the architecture blueprint begins to form at the Discipline level. Each Domain will contain one or more Disciplines. A Discipline template is provided to ensure consistent documentation of each Discipline.

The NASCIO workgroup has been involved in a high-level review process to define and document a sample set of Domains and associated Disciplines for this Tool-Kit. This sample set is intended to provide an example of one way to set up the Domain/Discipline relationships, but is not prescriptive. Descriptions of the sample Domains and Disciplines, as used in this Tool-Kit, can be found in Appendix D.

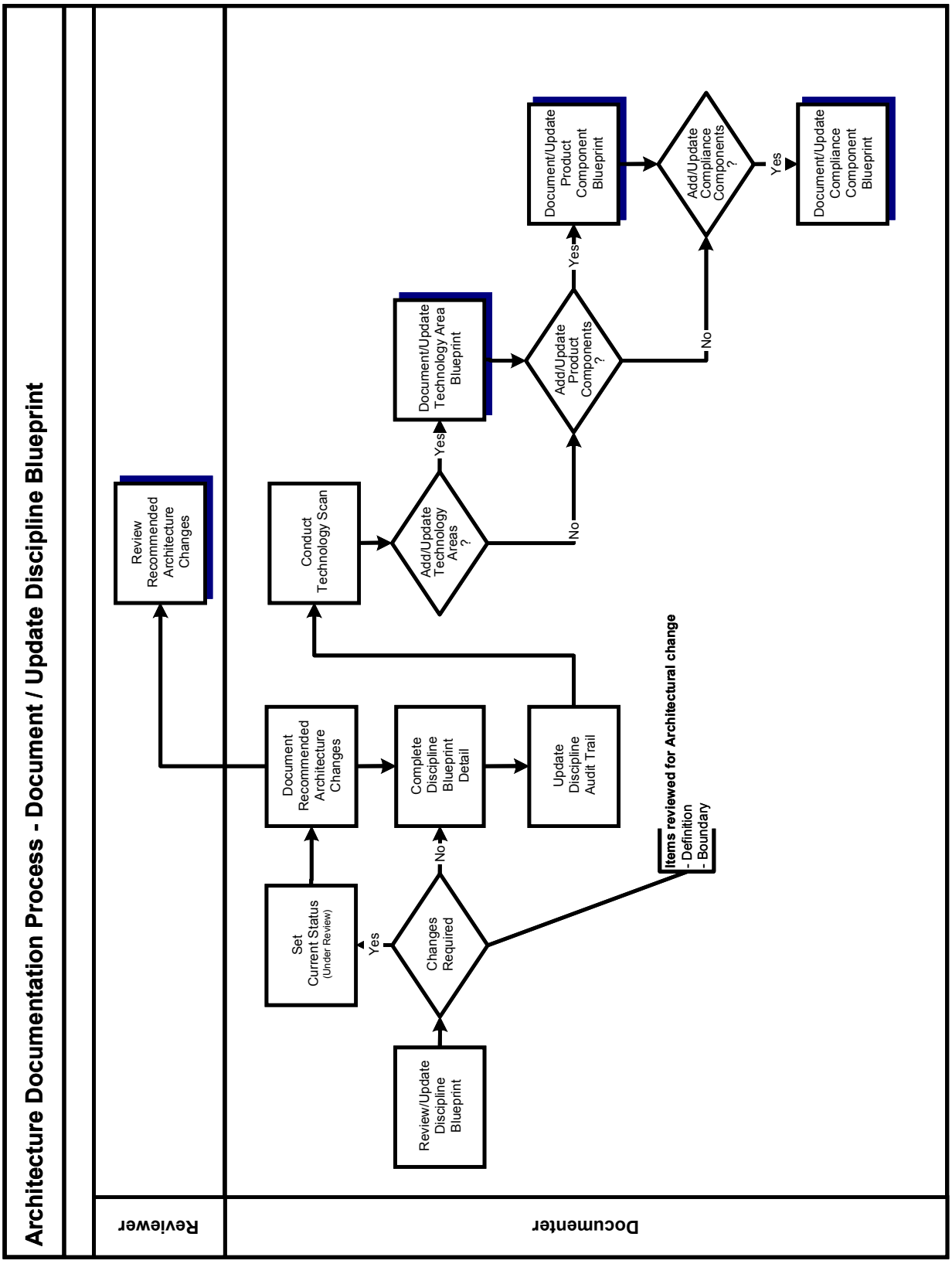
The development of Disciplines within each Domain is the responsibility of the Documenters. This process will evolve and change as information is gathered and documented.

It is anticipated that Documenters may uncover additional information that should be included as part of the Architecture Blueprint and/or Enterprise Architecture Framework. The committees and other enterprise architecture stakeholders are encouraged to provide feedback to the Architecture Manager whenever it is apparent that the feedback will enhance the enterprise architecture.

Important items to keep in mind when determining the creation of Disciplines include:

- Establish Disciplines that include categories of products and services having similar compliances or requiring similar expertise for implementation. This will allow Documenters to document the disciplines in a consistent manner.
- Set up Disciplines based on what will best support your organization's installation base of products and services.
- Avoid spending excessive time determining terminology issues. Just as in metadata documentation, fine-tuning terminology can occupy a majority of the time. Utilize the keywords and boundary statements to assist in identifying various terms that are covered by the discipline.

The first layout of the Disciplines under the Domains may not be the permanent arrangement. The best Discipline/Domain combinations will surface naturally over time during implementation of the Architecture Blueprint within your organization.


Architecture Documentation Process - Document / Update Discipline Blueprint
Reviewer
Documenter
Review Recommended Architecture Changes
Document Recommended Architecture Changes
Complete Discipline Blueprint Detail
Update Discipline Audit Trail
Conduct Technology Scan
Add/Update Technology Areas ?
Yes
No
Document/Update Technology Area Blueprint
Add/Update Product Components ?
Yes
No
Document/Update Product Component Blueprint
Add/Update Compliance Components ?
Yes
Document/Update Compliance Component Blueprint
Set Current Status (Under Review)
Yes
Changes Required
No
Review/Update Discipline Blueprint
Items reviewed for Architectural change
- Definition
- Boundary

PROCESS DETAIL

The Discipline Blueprint will be completed/updated using the Discipline Template as a guide. The following process steps will aid in this documentation:

Review/Update Discipline Blueprint – The Documenter will have the responsibility of reviewing the Discipline definition and Discipline boundary.

An Architecture change request should be submitted if:

- Additional Technology Areas are required
- Changes to the Discipline Definition are made
- Changes to the Discipline Boundary are made.

This request is submitted to the Architecture Manager for validation prior to any further work on that topic and the current status will be set to "Under Review".

Set Current Status – Set the Current Status as appropriate. It is important to understand where a given Domain is in the architecture documentation process. Initial statuses identified include:

- *In Development* – The architecture team is currently crafting and/or reviewing the Discipline content.
- *Under Review* – The architecture team has completed the Discipline content and it is under review by an EA governing body.
- *Accepted* – Indicates the Discipline has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Discipline was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

Document Recommended Architecture Changes; Review Recommended Architecture Changes – Document and submit to the Architecture Manager any changes to the definition or boundary limit statement prior to proceeding with the Discipline documentation. These types of changes can affect more than just the Documenter requesting the modification.

Complete Discipline Blueprint Detail – Critical References can aid in identifying the Technology Areas, Product Components, and/or Compliance Components. The references that are specific for the Discipline include:

- Documentation of Related Disciplines
- Identification of the various Standards Organizations and Government Bodies
- Identification of the Stakeholders/Roles
- Documentation of Discipline-specific Technology Trends

Compliances that are more Discipline-related should be listed at the Discipline level. Each Documenter should evaluate and select Compliance Components that apply to the Discipline. These would include:

- *Guidelines* – General statements of direction or desired future state for this Discipline. These will not be mandated.

- *Standards* – Items set by any generally accepted standards organization appropriate for the Discipline. More than one standard may exist. Variances must be sought if not following one of the existing standards.
- *Legislated* – Items required by law. Only a change in the mandate can allow variances.

The Compliance Component Blueprint details will be captured, using the Compliance Component Template, as described in the sub-process Document/Update Compliance Component Blueprint covered later in this chapter.

Methodologies followed while developing or supporting this Discipline should be documented. This is another place to verify that the deliverables of the methodology do not conflict with the components of the enterprise architecture. Implementation of the selected Technology Areas should be aided by the methodology deliverables.

Technology Areas covered under the Discipline should be listed at this time. The process for deriving and capturing all the remaining levels of the architecture blueprint begins at the Technology Area level, which aids in defining and finding the various products and compliances under a technology. The process steps for documenting the Technology Areas will be covered in detail in Document/Update Technology Area Blueprint process model.

Documentation requirements for the Discipline must be specified, assuring that the quality and level of the documentation intended by the Documenter is maintained. Various subject matter experts will work as Documenters as the architecture blueprint continues to mature. The documentation will preserve the history of the decision-making processes throughout the architecture maturity process. The Documenters can express expectations for how the Discipline is to be maintained within the documentation.

Set the Current Status as appropriate. It is important to understand where a given Discipline is in the architecture documentation process. Initial statuses identified include:

- *In Development* – The architecture team is currently crafting and/or reviewing the Discipline content.
- *Under Review* – The architecture team has completed the Discipline content and it is under review by an EA governing body.
- *Accepted* – Indicates the Discipline has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Discipline was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

Update Discipline Audit Trail - Audit trails for the information provided in the template must be maintained. During the initial development of the Discipline, only the information regarding creation, accepted/rejected, and date last updated must be maintained.

Conduct Technology Scan - At this level, a technology scan of the enterprise should be conducted to determine the existing or proposed products and compliance components used throughout the state as related to this discipline. Based on the technology found, one of the following levels will be documented and/or updated:

- Technology Area Blueprint
- Product Component Blueprint
- Compliance Component Blueprint

One question that arises during the documentation process is how to incorporate the documentation of the existing baseline products and compliance components in the most efficient and effective manner. In reviewing the product and compliance components, select those attributes that provide the most valuable information for your categorization and create a smaller checklist. Send this checklist out to the various subject matter experts in the organization, requesting that they complete the portion that pertains to their area of expertise and return the results within an agreed amount of time (3 – 4 weeks should suffice for most organizations).

Recommended checklist items would include:

Definition (Name and Description)

- Keywords
- Vendor Information (Name)
- Required Component
- Audit Trail (Creation Date)

Document/Update Technology Area Blueprint, Document/Update Product Component Blueprint, and Document/Update Compliance Component Blueprint - Each of these processes will be executed as needed, based on the results of the technology scan. These processes are covered as independent processes in the remainder of this section.

Discipline Template

TEMPLATE OVERVIEW

The Discipline Template provides a checklist for documenting the Discipline details. A detailed description of each of the content areas follows the visual representation of the Discipline Template provided here.

The Discipline Template will include the following sections:

- Definition
- Boundary
- Associated Domain
- Critical References
- Methodologies
- Associated Compliance Components
- Associated Technology Areas
- Discipline Documentation Requirements
- Current Status
- Audit Trail

Discipline Template

Definition	
Name	
Description	
Rationale	
Benefits	

Boundary	
Boundary Limit Statement	

Associated Domain	
Domain Name	

Critical References

Related Domains/Disciplines

	Domain - Disciplines		*Domain - Disciplines*		*Domain - Disciplines*
☐		☐		☐	
☐		☐		☐	
☐		☐		☐	
☐		☐		☐	
☐		☐		☐	
☐		☐		☐	
☐		☐		☐	

Standards Organizations

Name		*Web Address*	
Contact Information			

Government Bodies

Name		*Web Address*	
Contact Information			

Stakeholders/Roles

Stakeholders	
Roles (if stakeholder titles are not known)	

Discipline-Specific Trends

Trend Statement	
Trend Source	

Methodologies	
Methodologies Followed	

ASSOCIATED COMPLIANCE COMPONENTS			
Compliance Component Names			
ASSOCIATED TECHNOLOGY AREAS			
Technology Areas			
DISCIPLINE DOCUMENTATION REQUIREMENTS			
Documentation requirements for this Discipline			
CURRENT STATUS			
Discipline Status	☐ *In Development* ☐ *Under Review* ☐ *Rejected* ☐ *Accepted*		
AUDIT TRAIL			
Creation Date		*Date Accepted/Rejected*	
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

TEMPLATE DETAIL

Definition

Name - Determine an appropriately descriptive name for the Discipline.

Description - Supply a description of the Discipline in a paragraph or two that provides sufficient clarity about the Discipline and what it covers.

Rationale - Provide a paragraph or two containing the reason or basis for inclusion of this Discipline in the architecture blueprint.

Benefits - Provide a paragraph or bulleted statements that supply the benefits associated with the Discipline.

Boundary

Boundary Limit Statement - The Boundary Limit Statement provides parameters for identifying the boundaries for the Discipline. This section includes statements about what is included, as well as items that are related to—but excluded from—the Discipline. If excluded items are identified, it is beneficial to include a reference to the Domain and Discipline where that information can be found.

Associated Domain

Domain Name - Provide the name of the Domain with which this Discipline is associated. This provides the appropriate mapping between Domains and Disciplines.

Critical References

Related Domains/Disciplines - Provide a list of the Domains and underlying Disciplines that will have an affect on, or be affected by, changes within this Discipline. These references provide coordination points for critical decisions. The Domain-Discipline Intersection Matrix, provided in the Technology Samples section of this Tool-Kit, can be a helpful tool to easily identify these coordination points. If your organization chooses to use such a tool, it should be updated with the new information as well.

In the Discipline template provided, the names of the related Domains/Disciplines have been omitted. Please note that once you have determined the Domains and Disciplines for your organization, the template can be customized to include your information.

Standards Organizations/Government Bodies - Provide a list of the various standards organizations and/or government bodies that affect this Discipline. Provide URLs for reference whenever possible. These organizations can affect the Discipline in various ways. Some will have authority to dictate certain decisions, while others may only provide an influence on decisions within the Discipline.

Stakeholders/ Roles - Provide a list of Stakeholders for this Discipline. Stakeholders are those who are affected by, or will affect, the Discipline.

If a stakeholder title is not known, provide a description of the role the person or group performs in the roles section. Roles ensure the accountability of all IT components, ensure IT efforts support the needs of the business, and increase quality of IT solutions within the Discipline.

Discipline-Specific Trends - Add any Discipline-specific Industry or Technology Trends. Industry and technology trends have an effect on the deployment of information technology. IT decision makers will develop more informed, effective decisions if they are aware of the impact of the trends related to both business and technology.

Some key questions that should be considered when identifying the trends include:

- What trends and events will drive new business investment in IT?
- What technology advances or changes will impact IT deployment decisions?
- How can the organization exploit IT, while facing a complex and volatile environment?

In addition to the trends, provide the source of each trend for reference/historical purposes. This section can include references to organizations like Gartner Group, or they can include the name of the person who proposed the trend. URLs may also be included if applicable.

Methodologies

Methodologies Followed - Provide a list of methodologies followed in developing or supporting this Discipline, as appropriate.

Associated Compliance Components

Compliance Component Names - Provide a list of Compliance Components that are specific to the Discipline level. The detailed documentation for each component listed will be completed using the Compliance Component Template.

Associated Technology Areas

Technology Areas - Provide a list of the Technology Areas that are covered within this Discipline. This provides an index for these Technology Areas. The detailed documentation for each Technology Area listed will be completed using the Technology Area Template.

Discipline Documentation Requirements

Documentation requirements for this Discipline - As the enterprise architecture continues to mature, a variety of subject matter experts will serve as Documenters. The transfer of knowledge and the reasoning behind previous additions and modifications can be invaluable to these Documenters, but may not always be obvious.

The Documenters should use this section to specify the quality assurance criteria for the Discipline and express their expectations for how the Discipline is to be maintained.

Current Status

Discipline Status - Document the status of Discipline, indicating whether it is in development, under review, rejected, or accepted.

- *In Development* – The architecture team is currently crafting and/or reviewing the Discipline content.
- *Under Review* – The architecture team has completed the Discipline content and it is under review by an EA governing body.
- *Accepted* – Indicates the Discipline has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Discipline was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

Audit Trail

Creation Date - Provide the date the Discipline was created.

Created By – List all individuals and their titles that helped in the creation of this Discipline.

Date Accepted/Rejected - Provide the date the Discipline was accepted into the architecture blueprint or rejected.

Reason for Rejection - If the Discipline was rejected, document the reason for the rejection.

Last Date Reviewed - Document the most recent date the Discipline was taken through the Architecture Blueprint Vitality Process.

Last Date Updated - Document the most recent date that any item in the Discipline template was changed.

Reason for Update - Document the reason for the update to the Discipline.

Updated By - Provide the names of the persons responsible for the update to the Discipline. This will be helpful information for future reference.

Document/Update Technology Area Blueprint

PROCESS OVERVIEW

Technology Areas are the third level of the Architecture Blueprint. Technology Areas are those technical categories that support the technology functional areas (Disciplines) of the architecture blueprint. Each Discipline will contain one or more Technology Areas. A Technology Area template is provided to ensure consistent documentation of each Technology Area.

Technology Areas allow products for each Discipline to be categorized for:

- Documentation of Compliances
- Research of Architecture Blueprint
- Communication of Architecture Blueprint
- Defining the Discipline Boundaries.

A majority of the Documenters' work will focus on the Technology Areas, Product Components, and Compliance Components including such activities as:

- Documentation
- Vitality of Architecture Blueprint
- Compliance Reviews
- Architecture Help Requests.

Important items to keep in mind when determining the Technology Areas within a Discipline include:

- Technology scans are helpful in capturing information regarding existing products within the organization.
- There is more than one way to determine Technology Areas. Documenters preferring bottom-up analysis will capture the list of products and then categorize these products to determine the Technology Areas. Those preferring top-down analysis will determine and document the Technology Areas first and then proceed to document the products that fall under each of the Technology Areas.
- Create a Technology Area where compliances exist that span products.

- Documentation of products within a Technology Area for a specific Discipline can become an area for boundary debate. A question can arise as to which group is responsible for documenting which products. When certain products span functional areas, a review of the best way to document the product should be discussed. A decision should be made as to whether the product should be documented under multiple Technology Areas, or whether all subject matter experts should come together to document the product once under a specific Technology Area.

Architecture Documentation Process - Document / Update Technology Area Blueprint
Reviewer
Documenter
Complete Technology Area Blueprint Details
Update Technology Area Audit Trail
Add/Update Product Components ?
Yes
No
Document/Update Product Component Blueprint
Add/Update Compliance Components ?
Yes
Document/Update Compliance Component Blueprint

PROCESS DETAIL

The Technology Area Blueprint should be completed/updated using the Technology Area template as a guide. The following process steps will aid in this documentation:

Complete Technology Area Blueprint Details - Review/Document the Technology Areas definition and rationale.

Keywords/nomenclature commonly associated with the Technology Area should be documented to aid in finding various Technology Areas in the architecture blueprint.

Set the Current Status as appropriate. Since so many different Technology Areas go through the Architecture Documentation Process at one time, it is important to understand where a given Technology Area is in the process. Initial statuses identified include:

- *In Development* – The architecture team is currently crafting and/or reviewing the Technology Area content.
- *Under Review* – The architecture team has completed the Technology Area content and it is under review by an EA governing body.
- *Accepted* – Indicates the Technology Area has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Technology Area was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

List the Product and Compliance Components that are associated with this Technology Area. After the technology scan is complete, the Product and Compliance Components can be documented and assigned their classification within the architecture blueprint. The details for documenting the Product and Compliance Components are described in the sub-processes Document/Update Product Component Blueprint and Document/Update Compliance Component Blueprint, which are covered later in this chapter.

If the Technology Area requires a single product solution, the date the determination was made should be documented, along with the rationale for the decision.

Update Technology Area Audit Trail - Audit trails for the information provided in the template must be maintained. During the initial development of the Technology Area, only the creation, accepted/rejected, and date last updated will be provided.

Document/Update Product Component Blueprint - The details for documenting the Product Components are covered in the sub-process Document/Update Product Components later in this chapter.

Document/Update Compliance Component Blueprint - The details for documenting the Compliance Components are covered in the sub-process Document/Update Compliance Components later in this chapter.

Technology Area Template

TEMPLATE OVERVIEW

The Technology Area Template provides a checklist for documenting the Technology Area details. A detailed description of each of the content areas follows the visual representation of the Technology Area Template provided here.

The Technology Area Template will include the following sections:

- Definition
- Associated Discipline
- Keywords
- Associated Compliance Components
- Single Product Solution
- Associated Product Components
- Current Status
- Audit Trail

Technology Area Template

Definition	
Name	
Description	
Rationale	
Benefits	
Associated Discipline	
Discipline Name	
Keywords	
Keywords/Aliases	
Associated Compliance Components	
Compliance Component Names	
Single Product Solution	
Date of Single Product Solution Determination	
Rationale for Decision	
Associated Product Components	
Product Component Names	
Current Status	
Technology Area Status	☐ *In Development* ☐ *Under Review* ☐ *Rejected* ☐ *Accepted*

Audit Trail			
Creation Date		*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

TEMPLATE DETAIL

Definition

Name - Determine an appropriately descriptive name for the Technology Area.

Description - Supply a description of the Technology Area in a paragraph or two that provides sufficient clarity about the Technology Area and what it covers.

Rationale - Provide a paragraph or two containing the reason or basis for inclusion of this Technology Area in the architecture blueprint.

Benefits - Provide a paragraph or bulleted statements that supply the benefits associated with the Technology Area.

Associated Discipline

Discipline Name - Provide the name of the Discipline with which this Technology Area is associated. This provides the appropriate mapping between Technology Areas and Disciplines.

Keywords

Keywords/Aliases - List any keywords/nomenclature and /or aliases that can be used to assist in searching for these Technology Areas. This information will be helpful for anyone looking for information on similar technologies.

Associated Compliance Components

Compliance Component Names - List the Compliance Components associated with this Technology Area. The detailed documentation for each component listed will be completed using the Compliance Component Template.

Single Product Solution

For certain Technology Areas, it is essential for an organization to make a determination of a single product solution. E-mail is a good example of a Technology Area that would be a candidate for a single product solution.

Date of Single Product Solution Determination; Rationale for Decision - For Technology Areas that require single product solutions, provide the date of the determination, as well as the rationale for the decision.

Associated Product Components

Product Component Names - List the Product Components associated with this Technology Area. The detailed documentation for each component listed will be completed using the Product Component Template.

Current Status

Technology Area Status - Document the status of Technology Area, indicating whether it is in development, under review, rejected, or accepted.

- *In Development* – The architecture team is currently crafting and/or reviewing the Technology Area content.

- *Under Review* – The architecture team has completed the Technology Area content and it is under review by an EA governing body.
- *Accepted* – Indicates the Technology Area has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Technology Area was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

Audit Trail

Creation Date - Provide the date the Technology Area was created.

Created By – List all individuals and their titles that helped in the creation of this Technology Area.

Date Accepted/Rejected - Provide the date the Technology Area was accepted into the architecture blueprint or rejected.

Reason for Rejection - If the Technology Area was rejected, document the reason for the rejection.

Last Date Reviewed - Document the most recent date the Technology Area was taken through the Architecture Blueprint Vitality Process.

Last Date Updated - Document the most recent date that any item in the Technology Area template was changed.

Reason for Update - Document the reason for the update to the Technology Area.

Updated By - Provide the names of the persons responsible for the update to the Technology Area. This will be helpful information for future reference.

Document/Update Product Components

PROCESS OVERVIEW

The Product Component is the fourth level of the Architecture Blueprint. Product Components include the protocols, products and services that are specific to a Technology Area. Each Technology Area will contain one or more Product Components. A Product Component template is provided to ensure consistent documentation of each Product Component.

The Documenter will evaluate each Product Component identified to determine its applicability. Document each Product Component reviewed in a Product Component Template, whether accepted or rejected.

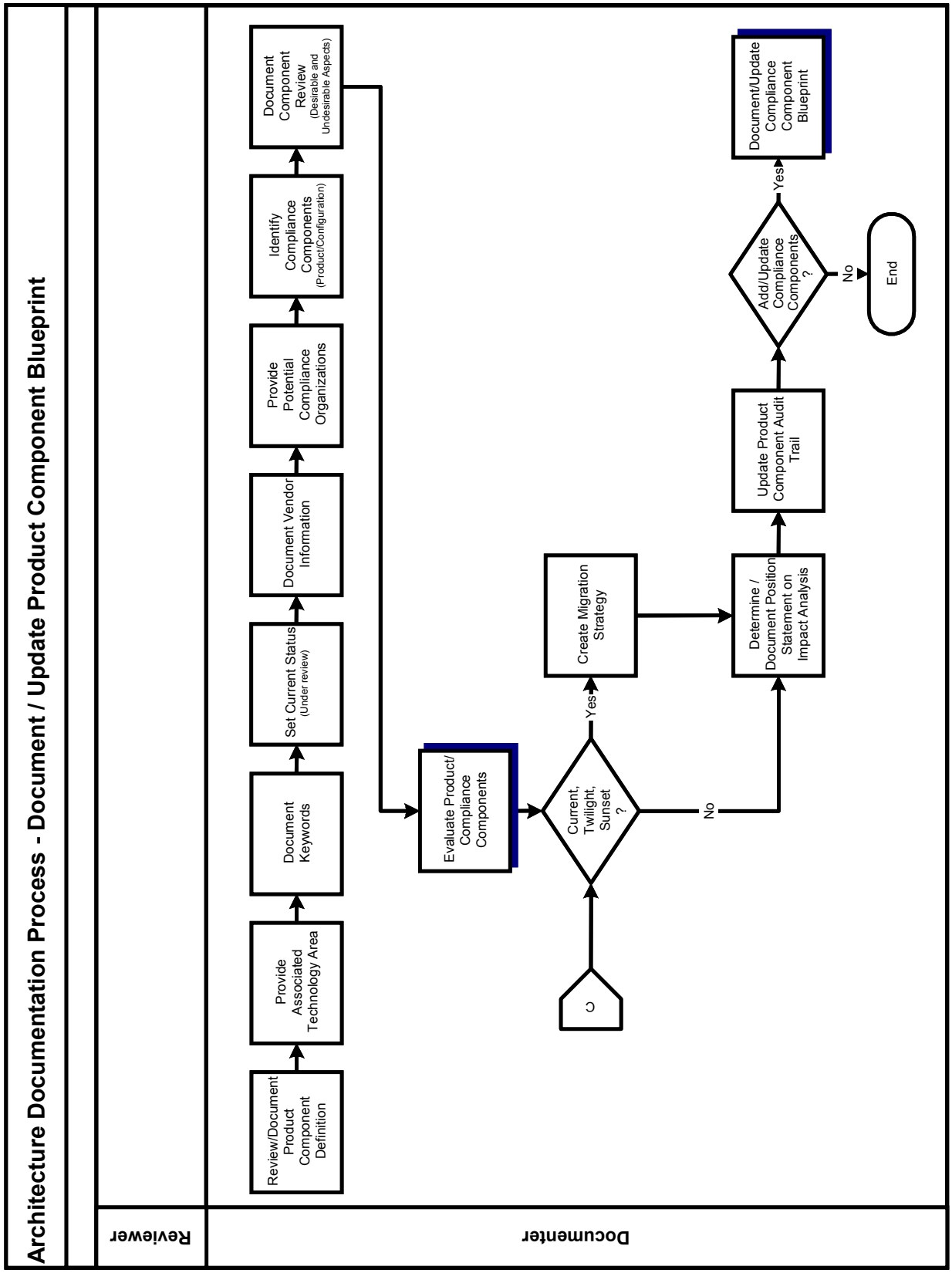
Important items to keep in mind when determining the various product components to document include:

- Is this product in the existing IT portfolio?
- Is this product needed in the next *x* time period to aid in business strategies?
- Is there a request from a project or support team to help find a product to answer a specific business need?
- Has the product already been documented in the Architecture Blueprint under another Domain/Discipline?

  - If this product has been documented elsewhere, did the evaluation of the product include the type of fit criteria needed for classification for your Domain/Discipline?
  - If this product has not been documented previously, is it possible that this product could fall under another Domain/Discipline's boundary?
- Will the product version be captured at the Product Component or the Compliance Component level? The documentation of this information needs to be consistent across the Discipline. (Note: The Discipline template contains a section entitled "Discipline Documentation Requirements" for capturing this type of information.) Examples of this include:
  - Versions captured at the Compliance Component Level:
    - Technology Area: Application Languages
    - Product: Visual Basic
    - Compliance Component: Version 5
    - Compliance Component: Version 6
    - Compliance Component: Visual Basic Standards (regardless of version)
  - Versions captured at the Product Level:
    - Technology Area: Application Languages
    - Product: Visual Basic Version 5
    - Product: Visual Basic Version 6
    - Compliance Components: Visual Basic Standards for Version 5
    - Compliance Components: Visual Basic Standards for Version 6

The Product Components, documented in this sub-process, and the Compliance Components, documented in the Document Compliance Component sub-process, become the essence of the technology architecture for the Architecture Blueprint.

They specifically identify what products, compliances, and recommendations will be used for implementation of the Architecture Blueprint. The levels of the Architecture Blueprint covered to this point are included to aid in bringing subject matter experts together, categorizing products and standards in logical sets, and aiding in concise communication of the Architecture Blueprint.


Architecture Documentation Process - Document / Update Product Component Blueprint
Reviewer
Documenter
Review/Document Product Component Definition
Provide Associated Technology Area
Document Keywords
Set Current Status (Under review)
Document Vendor Information
Provide Potential Compliance Organizations
Identify Compliance Components (Product/Configuration)
Document Component Review (Desirable and Undesirable Aspects)
Evaluate Product/ Compliance Components
Current, Twilight, Sunset ?
Yes
No
Create Migration Strategy
C
Determine / Document Position Statement on Impact Analysis
Update Product Component Audit Trail
Add/Update Compliance Components ?
Yes
No
End
Document/Update Compliance Component Blueprint

PROCESS DETAIL

The Product Component Blueprint should be completed/updated using the Product Component Template as a guide. The following process steps aid in this documentation:

Review/Document Product Component Definition - Review the product component's definition and rationale. Provide updates as necessary.

Provide Associated Technology Area - The associated Technology Area should be listed in order to provide the appropriate mapping between Products and Technology Areas.

Document Keywords - To aid in finding various products documented in the architecture blueprint, keywords/nomenclature commonly associated with the product will be documented.

Set Current Status - Set the Current Status as appropriate. Since so many different Product Components go through the Architecture Documentation Process at one time, it is important to understand where a given Product Component is in the process. Initial statuses identified include:

- *In Development* – The architecture team is currently crafting and/or reviewing the Product Component content.
- *Under Review* – The architecture team has completed the Product Component content and it is under review by an EA governing body.
- *Accepted* – Indicates the Product Component has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Product Component was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

Document Vendor Information - Information about the vendor providing the product will be documented, including the name, contact information, and Web site for the vendor. In addition, any evaluation conducted on the vendor should also be documented to aid in future evaluations conducted on the vendor.

Provide Potential Compliance Organizations - To assist in the identification of potential Compliance Components for the product, a list of standards organizations and/or government bodies associated with the product will be documented. This list should include:

- Name
- Contact information
- Web site

Identify Compliance Components - Compliances that are more product-related should be listed at this level. These might include:

- Guidelines – General statements of direction or desired future states for the product. These will not be mandated.
- Standards – Product releases/versions currently used within the enterprise or proposed for use. More than one standard may exist. A variance must be granted to excuse compliance with an existing standard.

- Legislation – Items required by law. Only a change in the legislation can allow variances to be granted.

The details for documenting the Compliance Components are covered in the sub-process Document/Update Compliance Components covered later in this chapter.

Document Component Review - Document both desirable and undesirable aspects of the product. If the undesirable aspects have been discussed with the vendor, summarize the discussion showing the likelihood of vendor redress.

Evaluate Product/ Compliance Components - An evaluation of the Product Component is necessary to determine its classification. This will be discussed in detail in the Evaluate Product/Compliance Components sub-process.

Create Migration Strategy - For products classified as current, twilight or sunset, a migration strategy must be formulated. This will be done for products migrating from:

- Product Components classified as emerging that are moving to the classification of current.
- Product Components classified as current that are moving to either twilight or sunset.

Migration strategies will identify:

- Impacts on existing components
- Considerations for conversion
- Recommendations for:
  - New development
  - Modifications to existing components (corrections & enhancements)
  - Possibilities for user-base expansion (reuse).

Determine/Document Position Statement on Impact Analysis - An impact analysis must be conducted to determine the impact the classification of the product will have on the existing architecture blueprint. Examples of impacts can include:

- Is a product classified as current that is moving to twilight going to cause a software component to go through a release update that may take months to accomplish?
- Support levels may be impacted when choosing not to move a product from current to twilight when a vendor has chosen to no longer support the product.

These are examples of the type of impacts that need a Position Statement on impact.

Update Product Component Audit Trail - Audit trails for the information provided in the template must be maintained. During the initial development of the Product Component, only the creation, accepted/rejected, and date last updated must be maintained.

Document/Update Compliance Component Blueprint - If new Compliance Components were listed or if updates are needed to existing Compliance Components, the sub-process Document/Update Compliance Component Blueprint will be executed.

Product Component Template

TEMPLATE OVERVIEW

The Product Component Template provides a checklist for documenting the Product Component details. A detailed description of each of the content areas follows the visual representation of the Product Component Template provided here.

The Product Component Template will include the following sections:

- Definition
- Component Classification
- Associated Technology Area
- Keywords
- Vendor Information
- Potential Compliance Organizations
- Associated Compliance Components
- Component Review
- Required Component
- Conditional Use Restrictions
- Migration Strategy
- Impact Position Statement
- Current Status
- Audit Trail

Product Component Template

Definition				
Name				
Description				
Rationale				
Benefits				
Component Classification				
Classification	☐ *Emerging*	☐ *Current*	☐ *Twilight*	☐ *Sunset*
Sunset Date				
Rationale for Classification				
Associated Technology Area				
Technology Area Name				
Keywords				
Keywords/Aliases				
Vendor Information				
Vendor Name		*Web Address*		
Contact Information				
Potential Compliance Organizations				
Standards Organizations				
Name		*Web Address*		
Contact Information				
Government Bodies				
Name		*Web Address*		
Contact Information				
Associated Compliance Components				
Product				
Product-specific Compliance Components				
Configurations				
Configuration-specific Compliance Components				
Component Review				
Desirable aspects				
Undesirable aspects				

REQUIRED COMPONENT			
Business Area, Department or Application Name			
CONDITIONAL USE RESTRICTIONS			
Restrictions			
MIGRATION STRATEGY			
Strategy/Source Document			
IMPACT POSITION STATEMENT			
Impact Statement			
CURRENT STATUS			
Product Component Status	☐ *In Development* ☐ *Under Review* ☐ *Rejected* ☐ *Accepted*		
AUDIT TRAIL			
Creation Date		*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

TEMPLATE DETAIL

Definition

Name - Determine an appropriately descriptive name for the Product Component.

Description - Supply a description of the Product Component in a paragraph or two that provides sufficient clarity about the Product Component and what it covers.

Rationale - Provide a paragraph or two containing the reason or basis for inclusion of this Product Component in the architecture blueprint.

Benefits - Provide a paragraph or bulleted statements that supply the benefits associated with the Product Component.

Component Classification

Classification - Provide the classification for this Product Component.
(The process for determination is covered under Evaluate Product/Compliance Component Process.)

Classifications include:

- *Emerging:* New technology that has the potential to become current.
- *Current:* Recommended technology that meets the requirements of the enterprise architecture.
- *Twilight:* Items that do not conform to the Technology Drivers and/or Business Drivers.
- *Sunset:* Items that do not conform to the Technology Drivers and/or Business Drivers and have a set discontinuation date.

Sunset Date - Document the date for discontinuation of the Product Component.

Rationale for Classification - Provide a rationale statement for the chosen classification based on the review of:

- Technology Architecture Blueprint Conformance
- Business Functionality Fit
- Technical Fit
- Operational Fit
- Vendor Evaluation
- Cost of Ownership

Associated Technology Area

Technology Area Name - Provide the name of the Technology Area with which this Product Component is associated. This will ensure the appropriate mapping of Product Component to Technology Area.

Keywords

Keywords/Aliases - List any keywords/nomenclatures and/or aliases that can be used to assist in searching for these Product Components. This information will be helpful for anyone looking for information on similar technologies.

Vendor Information

Provide the following vendor information for the vendor that supplies and or supports the Product Component being documented.

- **Vendor Name**
- **Contact Information**, such as phone number, address, and email address.
- Company **Web Address**, URL, and associated links.

Potential Compliance Organizations

Standards Organizations - List all standards organizations that supply standards associated with this Product Component. Provide contact information for each organization, as well as URLs, if available.

Government Bodies - List all government bodies that provide policies and/or mandates associated with this Product Component. Provide contact information for each government body, as well as URLs, if available.

These are research references only and are used in identifying standards that may need to be escalated to Compliance Components.

All standards are addressed using the Compliance Component template.

Associated Compliance Components

Product - List the product-specific Compliance Components associated with this product. The detailed documentation for each component listed will be completed using the Compliance Component Template.

Configurations - List the configuration-specific Compliance Components associated with this product. The detailed documentation for each component listed will be completed using the Compliance Component Template.

Component Review

Desirable Aspects - Document the desirable aspects of this Product Component.

Un-desirable Aspects - Document the un-desirable aspects of this Product Component.
This information is used to justify recommendations for future use of the component.

Required Component

Business Area, Department or Application Name - If this Product Component is specifically required, specify the Business Area, Department or Application for which the product is a requirement.

Conditional Use Restriction

Restrictions - Document any specialized circumstances and requirements associated with the use of this Product Component.

Migration Strategy

Strategy/Source Document - Document Migration Strategy for:

- Product Components classified as emerging that are moving to the classification of current.
- Product Components classified as current that are moving to either twilight or sunset.

These strategies should identify the following items, as applicable:

- Existing user base and technical staff
- Training for existing user base
- Training for existing technical staff
- Impacts on existing Technology Areas
- Considerations for conversion
- Recommendations for the Technology Area in:
  - New development
  - Modifications (corrections & enhancements)
  - Possibilities for user-base expansion (reuse).

Note: A link to the source document should be provided if the Migration Strategy is documented as a stand-alone document.

Impact Position Statement

Impact Statement - Provide a position statement on the impact of this product on the organization. Consider the follow items when developing the impact position statement:

- The impact on the overall Technology Architecture Blueprint
- The impact on the physical technical environment
- The impact on the business community.

Current Status

Product Component Status - Document the status of Product Component, indicating whether the Product Component is in development, under review, rejected, or accepted.

- *In Development* – The architecture team is currently crafting and/or reviewing the Product Component content.
- *Under Review* – The architecture team has completed the Product Component content and it is under review by an EA governing body.
- *Accepted* – Indicates the Product Component has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Product Component was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

Audit Trail

Creation Date - Provide the date the Product Component was created.

Created By – List all individuals and their titles that helped in the creation of this Product Component

Date Accepted/Rejected - Provide the date the Product Component was accepted into the architecture blueprint or rejected.

Reason for Rejection - If the Product Component was rejected, document the reason for the rejection.

Last Date Reviewed - Document the most recent date the Product Component was taken through the Architecture Blueprint Vitality Process.

Last Date Updated - Document the most recent date that any item in the Product Component template was changed.

Reason for Update - Document the reason for the update to the Product Component.

Updated By - Provide the names of the persons responsible for the update to the Product Component. This will be helpful information for future reference.

Document/Update Compliance Components

PROCESS OVERVIEW

Compliance Components are the fifth level of the Architecture Blueprint. Compliance Components are the guidelines, standards and legislative mandates associated with a Discipline, Technology Area, or Product Component, as appropriate. Each Discipline, Technology Area, and/or Product Component will contain one or more Compliance Components. A Compliance Component template is provided to ensure consistent documentation of each Compliance Component.

There are three different types of Compliance Components:

- ***Guidelines*** – General statements of direction or desired future state. Guidelines are highly recommended, but they are not mandated.
- ***Standards*** – Mandated statements. A variance must be granted to excuse compliance with an existing standard. (More than one standard may exist to allow flexibility in the architecture blueprint.)
- ***Legislation*** – Compliance criteria legislated that can be changed only by changing the law. There are numerous types of legislation including, but not limited to, policy, executive order, code of state, federal regulation, or statute.

Compliance Components (guidelines, standards and mandates) documented at the Discipline level provide the basis for making important decisions about new products, protocols, configurations, etc. Compliance Components documented at the Technology Area or Product Component level provide the basis for decisions on which configuration, implementation, or product to utilize. The documentation of Compliance Components provides the information most critical for interoperability.

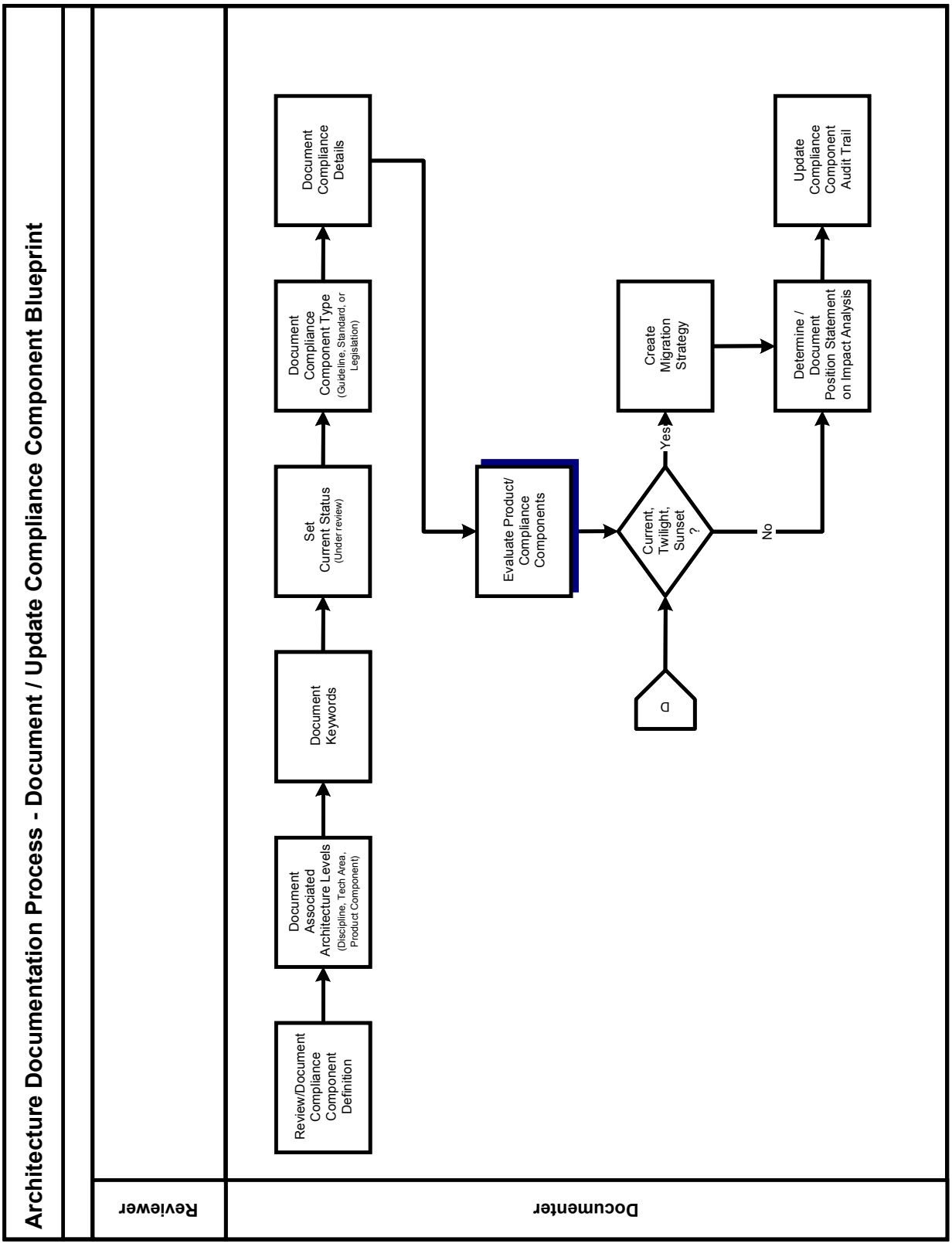
The template for Compliance Components, as well as the process for evaluation and classification, is very similar to that for Product Components. The separation between Product and Compliance Components is necessary for clarity and because the Compliance Components (guidelines, standards and mandates) can be documented at the three levels: Discipline, Technology Area and Product Component level.

Important items to keep in mind when determining the various Compliance Components to document:

- Information captured must be maintainable.
- Overly generic Compliance Components are difficult to enforce.
- Verbose compliance documentation is difficult to understand.
- Utilize standards created in the various standards groups or industry providers.
- When referencing existing compliance documentation from various standards organizations or departments within your organization, be aware of the following:

- Links can become invalid if the original documentation is moved.
- Copies of compliance documentation may no longer be valid if updates are made to the original.

Compliance Components may be guidelines, standards and legislative mandates. The primary difference between the types of Compliance Components lies in the degree of authority as described in the Template Overview. Compliance Components may be associated with a Discipline, Technology Area, and/or a Product Component.


Architecture Documentation Process - Document / Update Compliance Component Blueprint
Reviewer
Documenter
Review/Document Compliance Component Definition
Document Associated Architecture Levels (Discipline, Tech Area, Product Component)
Document Keywords
Set Current Status (Under review)
Document Compliance Component Type (Guideline, Standard, or Legislation)
Document Compliance Details
Evaluate Product/ Compliance Components
Current, Twilight, Sunset ?
Yes
No
Create Migration Strategy
Determine / Document Position Statement on Impact Analysis
Update Compliance Component Audit Trail
D

PROCESS DETAIL

The Compliance Component Blueprint should be completed/updated using the Compliance Component Template as a guide. The following process steps aid in this documentation:

Review /Document Compliance Component Definition - Review the compliance component's definition, rationale, and benefits. Rationale and benefits will be included when the information will aid in the understanding of the compliance component being documented.

Document Associated Architecture Levels - Compliances must be defined and associated with the correct levels in the architecture blueprint (Discipline, Technology Area, and/or Product Component).

Document Keywords - Keywords or nomenclatures that aid in locating a Compliance Component should be listed. These help identify existing Compliance Components that may already exist for a specific keyword.

Set Current Status - Since there will be so many different Compliance Components moving through the Architecture Documentation Process at one time, it is important to understand where a given Compliance Component resides in the process. Initial statuses identified include:

- *In Development* – The architecture team is currently crafting and/or reviewing the Compliance Component content.
- *Under Review* – The architecture team has completed the Compliance Component content and it is under review by an EA governing body.
- *Accepted* – Indicates the Compliance Component has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Compliance Component was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

Document Compliance Component Type - Compliances are of three types that describe the level of compliance expected. They include:

- Guidelines – General statements of direction or desired future state for this level of the architecture blueprint (Discipline, Technology Area, or Product Component). These will not be mandated.
- Standards – Specific protocols, product or version statements. More than one standard may exist. Variance must be sought not to follow one of the standards that exist.
- Legislation – Items required by law. Only a change in the legislation will allow variances.

If further clarification of the Component type is needed, the Compliance Component Sub-type is available.

Document Compliance Details - The Compliance Component details should be articulated. These include:

- Compliance Statement
- Compliance Referenced Source
  - Standards Organization/Government Body
  - Actual Statue or Standards Document Version

Evaluate Product/ Compliance Components - An evaluation of the Compliance Component is necessary to determine its classification. This will be discussed in detail in the Evaluate Product/Compliance Components sub-process.

Create Migration Strategy - For a Compliance Component classified as current, twilight, or sunset, a migration strategy must be formulated. This must be done for compliances migrating from:

- Compliance Components classified as emerging that are moving to current.
- Compliance Components classified as current that are moving to either twilight or sunset.

These strategies will identify:

- Impacts on existing components
- Considerations for conversion
- Recommendations for:
  - New development
  - Modifications to existing components (corrections & enhancements)
  - Potential for user-base expansion (reuse).

Determine/Document Position Statement on Impact Analysis - An impact analysis must be conducted to determine what impact the most recently determined classification of this Compliance Component will have on the existing architecture blueprint. The analysis must be documented in a Position Statement on impact.

Update Compliance Component Audit Trail - Audit trails for the information provided in the template must be maintained. During the initial development of the Compliance Component, only the creation, accepted/rejected, and date last updated must be maintained.

Compliance Component Template

TEMPLATE OVERVIEW

The Compliance Component Template provides a checklist for documenting the Compliance Component details. A detailed description of each of the content areas follows the visual representation of the Compliance Component Template provided here.

The Compliance Template will include the following sections:

- Definition
- Component Classification
- Associated Technology Architecture Blueprint Level
- Keywords
- Compliance Component Type
- Compliance Detail
- Conditional Use Restrictions

- Migration Strategy
- Impact Position Statement
- Current Status
- Audit Trail

Compliance Component

Definition	
Name	
Description	
Rationale	
Benefits	

Component Classification				
Classification	☐ *Emerging*	☐ *Current*	☐ *Twilight*	☐ *Sunset*
Sunset Date				
Rationale for Classification				

Associated Technology Architecture Blueprint Level	
Discipline Name	
Technology Area Name	
Product Component Name	

Keywords	
Keywords/Aliases	

Compliance Component Type			
Component Type	☐ *Guideline*	☐ *Standard*	☐ *Legislation*
Compliance Sub-type			

Compliance Detail	
Statement	
Source Reference	

Standards Organization			
Name		*Web Address*	
Contact Information			

Government Body			
Name		*Web Address*	
Contact Information			

Conditional Use Restrictions	
Restrictions	

Migration Strategy	
Strategy/Source Document	

IMPACT POSITION STATEMENT				
Impact Statement				
CURRENT STATUS				
Compliance Component Status	☐ *In Development*	☐ *Under Review*	☐ *Rejected*	☐ *Accepted*
AUDIT TRAIL				
Creation Date		*Date Accepted / Rejected*		
Created By				
Reason for Rejection				
Last Date Updated		*Last Date Reviewed*		
Reason for Update				
Updated By				

TEMPLATE DETAIL

Definition

Name - Determine an appropriately descriptive name for the Compliance Component.

Description - Supply a description of the Compliance Component in a paragraph or two that provides sufficient clarity about the Compliance Component and what it covers.

Rationale - Provide a paragraph or two about the reason or basis for inclusion of this Compliance Component in the architecture blueprint.

Benefits - Provide a paragraph or bulleted statements that supply the benefits associated with the Compliance Component.

Component Classification

Classification - Provide the classification for this Compliance Component.

(The process for determination is covered under Evaluate Product/Compliance Component Process.) Classifications include:

- *Emerging:* New technology, which has the potential to become current
- *Current:* Recommended technology (technology that meets the requirements of the enterprise architecture.*)*
- *Twilight:* Items that do not conform to the Business/Technology Drivers
- *Sunset:* Items that do not conform to the Business/Technology Drivers and have a set discontinuation date

Sunset Date - Document the date for discontinuation of the Compliance Component.

Rationale for Classification - Provide a rationale statement for the chosen classification based on the review of:

- Technology Architecture Blueprint Conformance
- Business Functionality Fit
- Technical Fit
- Operational Fit
- Vendor Evaluation
- Cost of Ownership

Associated Technology Architecture Blueprint Level

Discipline Name - Provide the name of the Discipline with which this Compliance Component is associated. This will ensure the appropriate mapping of Compliance Component to Discipline.

Technology Area Name- Provide the name of the Technology Area with which this Compliance Component is associated. This will ensure the appropriate mapping of Compliance Component to Technology Area.

Product Component Name - Provide the name of the Product Component with which this Compliance Component is associated. This will ensure the appropriate mapping of Compliance Component to Product Component.

Keywords

Keywords/Aliases - List any keywords/nomenclature and/or aliases that can be used to assist in searching for these Compliance Components. This information will be helpful for anyone looking for information on similar technologies.

Compliance Component Type

Component Type - Denote whether the Compliance Component being considered or documented is a guideline, standard or legislation.

Compliance Sub-type - If the component is legislated, provide the type of legislation. Examples include items such as policy, executive order, code of state, federal regulation, or statute. For guidelines or standards, this area is available for instances where a sub-type may need to be included.

Compliance Detail

Statement - Provide the compliance statement.

Source Reference - Provide source reference for the compliance statement. This will include any reference numbers used for standards and mandates. URLs to web page that contain the full standard or mandate would also be useful.

Standards Organization - List the standards organization that supplies the standard. Provide contact information for each organization, as well as URLs, if available.

Government Body - List the government body that provides the mandate associated with this Compliance Component. Provide contact information for the government body, as well as URLs, if available.

Conditional Use Restrictions

Restrictions - Document any specialized circumstances and/or requirements associated with the use of this Compliance Component.

Migration Strategy

Strategy/Source Document - Document Migration Strategy for:

- Compliance Components classified as emerging that are moving to current.
- Compliance Components classified as current that are moving to either twilight or sunset.

These strategies should identify the following items, as applicable:

- Existing user base and technical staff
- Training for existing user base
- Training for existing technical staff
- Impacts on existing Technology Areas, Product and Compliance Components
- Considerations for conversion
- Recommendations for the Compliance Component as it applies to:
  - New development
  - Modifications (corrections & enhancements)
  - Possibilities for user-base expansion (reuse).

Note: A link to the source document should be provided if the Migration Strategy is documented as a stand-alone document.

Impact Position Statement

Impact Statement - Document position statement about the impact of this Compliance Component on the Organization. Consider the follow items when developing the impact position statement:

- The impact on the Technology Architecture Blueprint
- Physical implementation requirements
- The impact on installed applications or services
- The impact on existing installation standards.

Current Status

Compliance Component Status - Document the status of Compliance Component, indicating whether the Compliance Component is in development, under review, rejected, or accepted.

- *In Development* – The architecture team is currently crafting and/or reviewing the Compliance Component content.
- *Under Review* – The architecture team has completed the Compliance Component content and it is under review by an EA governing body.
- *Accepted* – Indicates the Compliance Component has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Compliance Component was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

Audit Trail

Creation Date - Provide the date the Compliance Component was created.

Created By – List all individuals and their titles that helped in the creation of this Compliance Component.

Date Accepted/Rejected - Provide the date the Compliance Component was accepted into the architecture blueprint or rejected.

Reason for Rejection - If the Compliance Component was rejected, document the reason for the rejection.

Last Date Reviewed - Document the most recent date the Compliance Component was taken through the Architecture Blueprint Vitality Process.

Last Date Updated - Document the most recent date that any item in the Compliance Component template was changed.

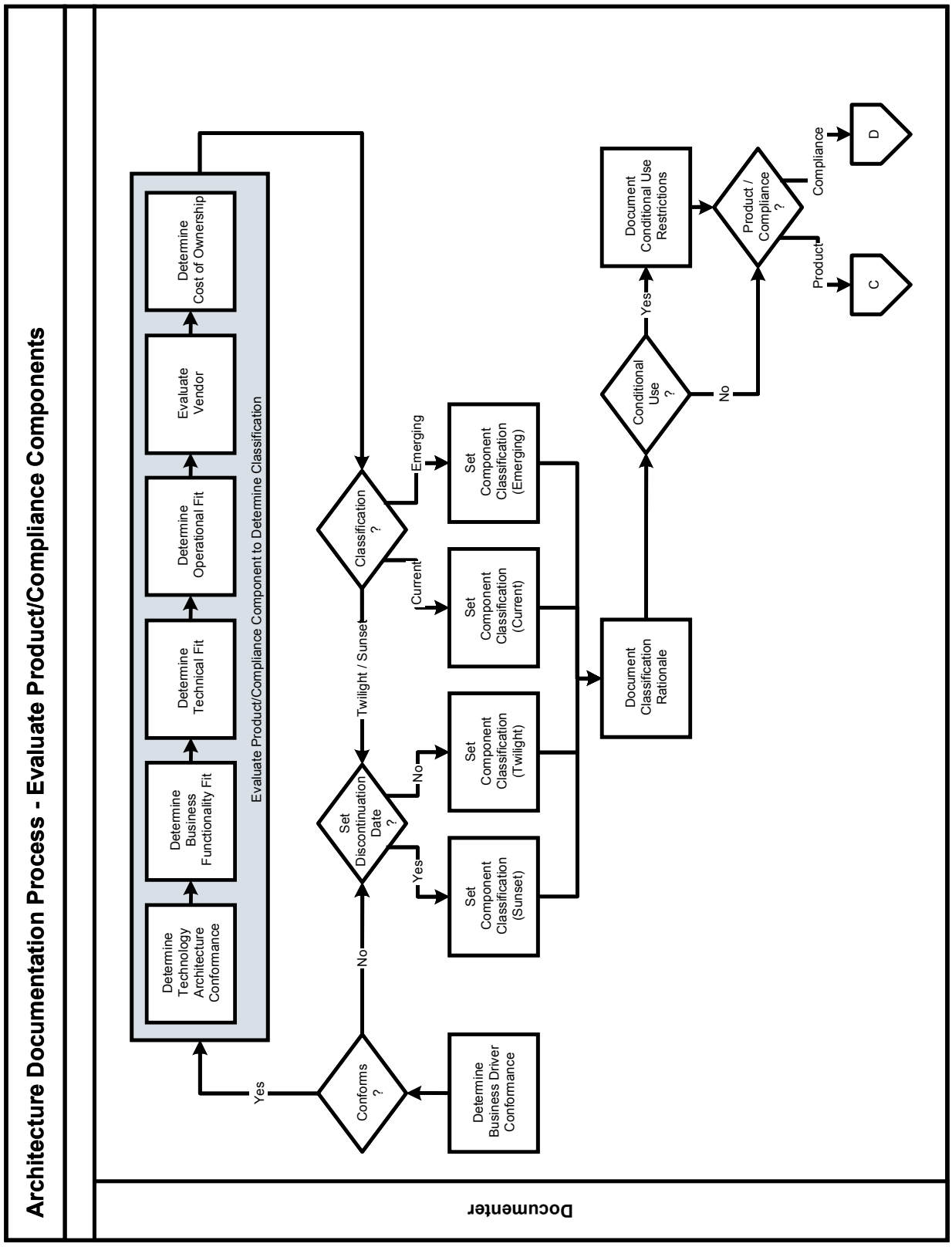
Reason for Update - Document the reason for the update to the Compliance Component.

Updated By - Provide the names of the persons responsible for the update to the Compliance Component. This will be helpful information for future reference.

Evaluate Product/Compliance Components

PROCESS OVERVIEW

In order to develop consistent evaluation of Products and Compliance Components associated with the Technology Architecture Blueprint, there must be objective selection and evaluation criteria.


Architecture Documentation Process - Evaluate Product/Compliance Components
Documenter
Determine Business Driver Conformance
Conforms ?
No
Yes
Evaluate Product/Compliance Component to Determine Classification
Determine Technology Architecture Conformance
Determine Business Functionality Fit
Determine Technical Fit
Determine Operational Fit
Evaluate Vendor
Determine Cost of Ownership
Set Discontinuation Date ?
Twilight / Sunset
No
Yes
Classification ?
Current
Emerging
Set Component Classification (Sunset)
Set Component Classification (Twilight)
Set Component Classification (Current)
Set Component Classification (Emerging)
Document Classification Rationale
Conditional Use ?
Yes
No
Document Conditional Use Restrictions
Product / Compliance ?
Product
Compliance
C
D

PROCESS DETAIL

Determine Business Driver Conformance - Components that do not conform to Business Drivers should be classified as either "Twilight" or "Sunset". See further detail for these under Classifications below.

Evaluate Product/Compliance Component to Determine Classification - For Components that do conform to the Business Drivers, the following additional evaluation must be performed:

- *Determine Technology Architecture Conformance* – The Component must align with the architecture blueprint. How well does the product comply with the IT principles and standards selected?
- *Determine Business Functionality Fit* – The Component being evaluated must address the functional business requirements. This part of the evaluation should include information on current and pending release levels. Families of products should also be considered when relevant.
- *Determine Technical Fit* – The Component being evaluated must be consistent with the current and planned technical environment.
- *Determine Operational Fit* – The Component being evaluated must meet the systems and other management requirements for operating and supporting the service level agreements in a specific environment.
- *Evaluate Vendor* – The vendor should be evaluated to determine its ability to support the offering, survive in the marketplace, and keep up with changing technology. Market share may be a consideration in determining product viability.
- *Determine Cost of Ownership* – The total cost of ownership must be considered, including acquisition, maintenance, support, integration services, skills, infrastructure, and de-acquisition costs. This should take into account the current organization user base.

Set Component Classification - Based on results of the evaluation, classify the Component using the following classifications:

- *Sunset* components are those that are in use but do not conform to the stated Business or Technology Architecture Blueprints. The sunset component will have a date of discontinuance identified, indicating the date that the component will no longer be acceptable for use within the architecture.
- *Twilight* components are those that are in use but do not conform to the stated Business Drivers or Technology Architecture Blueprints. The components have no date of discontinuance identified. These Components should not be used to develop new applications. Extensive modifications to these systems should be reviewed to determine if the system should be redeployed completely using newer technology.
- *Current* components are defined as those having met the requirements of the enterprise architecture. These represent the recommended Components that should be used in deployment of technology solutions.
- *Emerging* products are those that have potential to become current architecture blueprint components. While identified as Emerging, these Components should be used only in pilot or test environments and under highly controlled regulations. After sufficient testing, these Components may become current or may be identified non-compliant or non-functional in the organization's environment. Use of these components requires a variance that must be documented and approved through the compliance process.

Document Classification Rationale - Once the classification is known, the rationale for the classification must be documented.

Document Conditional Use Restrictions - Occasionally, a component has some characteristic that would limit its usefulness as an enterprise product. For example, some desktop database products may be well suited for a personal desktop application but should never be used for storing, accessing, or maintaining enterprise data.

Document the additional classification of "Conditional" for Components with limited usefulness.

SAMPLES

Technology Architecture Samples

This section contains three sets of Blueprint samples, one set of samples from the Application domain and two separate sets of samples from different Security domains. The second set of samples from the Security domain is provided to illustrate that there are many ways to name and group the architectural elements, all of which are correct.

It should be noted that some of the samples were completed using earlier versions of the templates and, while the information that was gathered is the same, it may be presented in a slightly different order or have a slightly different heading or topic title than the latest template versions.

APPLICATION BLUEPRINT SAMPLES

Samples are provided as models to help articulate the Tool-Kit concepts – not as the solution.

The five levels of the Application Domain are represented starting at the domain level and following a single path throughout the levels as follows:

- Domain – Application
- Discipline – Application Development Management
- Technology Area – Programming Language/Environment
- Product Component - Visual Basic
- Compliance Component - Prefix all constants with c_ and a scope designator

A second example of a Discipline from within the Application Domain includes:

- Discipline – Electronic Collaboration

Domain	*Discipline*	*Technology Area*	*Product Component*	*Compliance Component*
Application	Application Development Management	Programming Language / Environment	Visual Basic	Prefix all constants with a c_ and a scope designator
	Electronic Collaboration			

Domain Blueprint

DEFINITION	
Name	Domain – Application Architecture
Description	Defines the roles, policies, standards, and application development methodologies required to bring support the various custom and purchased applications throughout the organization. Disciplines for this domain cover the automation of the workforce, promote group productivity, and provide a set of reusable application components.
Rationale	The domain of applications has been a stand-alone set of technology experts, tools, and disciplines from the invention of the computer. It is from this base domain that other domains have come in existence and will continue to come as skills and tools become more specialized. Good application architecture enables a high level of system integration, reuse of components, and rapid deployment of applications in response to changing business requirements.
Benefits	The Application Architecture standardizes the approach to application development and electronic collaboration. This standardization provides a cost effective approach to application development/deployment and minimizes training and retraining requirements. The capability to retain staff will be increased by the simplification of staff retraining and a more effective investment of available project funding.

BOUNDARY	
Boundary Limit Statement	Includes the applications that are developed or deployed to support the business functionality. Subject Areas include: • Business Rules • Development Tools • Coding Standards • Component Object Repositories • Custom Systems • Enterprise wide applications (ex: Electronic Payment Applications, Electronic Benefits Applications, etc.) • Commercial Products • N-Tiered Architecture Electronic Collaboration applications are also included: • Email • Calendar • Messenger services • Workgroup • Messaging Boards • Chat rooms

ASSOCIATED DISCIPLINES	
Disciplines under this Domain	Application Development Management Electronic Collaboration

RELATED PRINCIPLES		
Reference #s, Statements or Links	*Conflict*	*Relationship*
Business case and metrics for effectiveness of application should accompany automation efforts. (MA-Claudia)	☐	Used to verify effectiveness of application pre and post implementation.
A business process analysis and review must always accompany automation efforts. Before automating business processes, a demonstrated attempt must be made to eliminate unnecessary processes and to simplify those remaining.	☐	Used to verify that automation is done for only critical business functions/processes.
Applications should address a business need and requirements for the application should be carefully documented and traced throughout the application development process.	☐	Requirements become the basis for the design and testing of the applications. Vital deliverable for making sure the users' needs are met.
The order of preference for solution delivery will be to reuse existing, purchase new and tailor, and then build.	☐	Use this principle when reviewing new initiatives.
Application programs, whether purchased or developed internally, will be deployed with separation of presentation logic, business logic and data access in order to provide modular, reusable functionality.	☐	Bases for design and technical fit reviews.
New applications will be modular and independent (“atomic”) in nature. They will access common data, use common services and have only inherently essential dependence on other applications (e.g. for provision of up-to-date data).	☐	Bases for design and technical fit reviews.
New applications will use defined and documented standards-based programming interfaces.	☐	Bases for design and code reviews.
Long-term plans will be considered when implementing new systems to avoid obsolescence. Agency IT plans need to develop strategies for the removal of non-strategic or retired technologies.	☐	IT Portfolio Lifecycle requirements.
Vendor neutral standards should be applied to reduce effort required for system integration. Exceptions should be negotiated and mitigated.	☐	Architecture Documenters need to adhere to this principle. Exceptions should be noted with rationale.
Application configuration decisions should be based on N-tiered and browser-based technologies where appropriate.	☐	Bases for design and technical fit reviews.

Hardware and software should comply with industry standards for remote control and monitoring.	☐	Bases for design and technical fit reviews.
Applications should present a consistent user interface that is adaptable to a particular user's requirement.	☐	Bases for design and technical fit reviews.
All applications will be built to accessibility standards. (MA-Claudia	☐	Bases for design and technical fit reviews.

Related Best Practices

Reference #s, Statements or Links	*Conflict*	Relationship
Business Environment and Organizational Support	☐	Include in part of methodologies for projects and IT Services, and implementation plan.
Project Preparation	☐	Consistent project steps from a business, IT, procurement and architecture view must be created.
Project Sequence and Outputs	☐	Consistent project steps from a business, IT, procurement and architecture view must be created.
Project Tools and Disciplines	☐	Education in tools and project roles must be conducted. Their relationship with the Architecture Roles must be specified.
Project Organization and Leadership	☐	Education of project organization and leadership on Architecture must be conducted prior to project. Project Management Office on large projects should look to having an Architecture representation as part of the project organization.
Personnel Management	☐	Must work with this management to assure the Architecture Documenters and Subject Matter Experts will be available to aid in documenting the architecture.
Interagency Coordination	☐	Must be spear headed not only by IT Management but also by the Architecture groups so show benefit of coordination.
Operations	☐	All groups within IT need to be consulted when creating the Architecture. This group represents the day in and day out activity of supporting the IT operations. This perspective cannot be down played.

Related Trends

Reference #s, Statements or Links	*Conflict*	*Relationship*
	☐	
	☐	

State Contracts

Planned Contracts	None identified
Existing Contracts	None identified

Current Status

Domain Status	☐ *In Development* ☐ *Under Review* ☐ *Rejected* ☐ *Accepted*

AUDIT TRAIL			
Creation Date	03/01/02	*Date Accepted/Rejected*	
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	03/06/02
Reason for Update			
Updated By			

Click on this link to return to Application Blueprint Samples.

Discipline Blueprint

DEFINITION	
Name	Discipline – Application Development Management
Description	Defines roles, development methodologies, technology standards, and technologies that define how applications are designed and how they cooperate. It defines how those applications are documented and maintained. The Application Development Management discipline provides criteria, approved methodologies, and technologies that optimize the use and reuse of application components. The discipline includes strategies for the retention of legacy knowledge and the phase out or upgrade of legacy systems.
Rationale	The Application Development & Management discipline standardizes the methodology, approach, standards and technology components used in application development. The discipline has relationships with but does **not** include database applications and middleware or their associated platforms and operating systems. The Application Development & Management discipline does not include the security and privacy aspects associated with deployment of these technologies. The Middleware Architecture, Platform Architecture, Data Management Architecture, Security Architecture and Privacy disciplines need to be referenced for guidance on those aspects associated with implementation of these technologies. The Application Development & Management discipline promotes common presentation and interface standards to facilitate rapid training and implementation of new applications and functions. Good application architecture enables a high level of system integration, reuse of components and rapid deployment of applications in response to changing business requirements.
Benefits	The Application Development & Management discipline standardizes the approach to application development and maintenance. This standardization provides a cost effective approach to application development and minimizes training and retraining requirements. The capability to retain staff will be increased by the simplification of staff retraining and a more effective investment of available project funding. Deploy applications systems that are (business) event-driven. Application systems should be engineered or re-engineered to be “highly granular” and “loosely coupled”. Applications systems employ reusable components using a browser-based model. Application systems should share reusable components across the enterprise Consider the complete Lifecycle costs of the application.

BOUNDARY	
Boundary Limit Statement	Includes the applications that are developed or deployed to support the business functionality. Subject Areas include: • Business Rules • Development Tools • Coding Standards • Component Object Repositories • Custom Systems • Enterprise wide applications (ex: Electronic Payment Applications, Electronic Benefits Applications, etc.) • Commercial Products • N-Tiered Architecture

ASSOCIATED DOMAIN	
Domain Name	Application Architecture

CRITICAL REFERENCES					
Related Domains/Disciplines					
	Domain – Disciplines		*Domain - Disciplines*		*Domain - Disciplines*
☒	Access: Internet /Intranet	☒	Integration: Functional Integration	☒	System Management: Help Desk / Problem Management
☒	Access: Branding	☒	Integration: Middleware	☒	System Management: Business Continuity
☒	Access: Accessibility	☒	Application: Application Development Management	☒	Security: Enterprise Security
☒	Information: Data Management	☒	Application: Electronic Collaboration	☒	Security: Network Security
☒	Information: Knowledge Management	☒	Platform: Platform	☒	Security: Host Security
☒	Information: GIS	☒	Platform: Configuration Management	☒	Privacy: Profiling
☒	Information: Data Storage	☐	Systems Management: Asset Management	☒	Privacy: Personalization
☒	Network: Physical Network	☒	System Management: Change Management	☒	Privacy: Privacy
☐	Network: Network Management	☒	System Management: Console / Event Management	☐	

Standards Organizations			
Name	International Organization for Standardization	*Web Address*	http://www.iso.ch/iso/en/ISOOnline.frontpage
Contact Information	**ISO Central Secretariat:** International Organization for Standardization (ISO) 1, rue de Varembé, Case postale 56 CH-1211 Geneva 20, Switzerland Telephone + 41 22 749 01 11; Telefax + 41 22 733 34 30; E-mail: central@iso.org; Web: http://www.iso.org		

Government Bodies			
Name	None Identified	*Web Address*	
Contact Information			

Stakeholders/Roles	
Stakeholders	Business Analyst, Systems Analyst, Business Functional Users, Quality Assurance Testers, IT Operations Staff, Developers, Software Vendors, Outsource Development Vendors, Data Analyst, etc…
Roles (if stakeholder titles are not known)	

Discipline-specific Trends	
Trend Statement	Utilizing XML for API calls. Standardize the data types used in the XML. See: XML Schema Part 2: Data types
Trend Source	http://www.w3.org/TR/xmlschema-2/

METHODOLOGIES			
Methodologies followed	Rapid Application Development (RAD) Joint Application Development (JAD)		
ASSOCIATED COMPLIANCE COMPONENTS			
Compliance Component Names	ANSI/IEEE 1016-1987 (Recommended Practice for Software Design Description) Software design ANSI/IEEE 1016.1 –1993 (Guide for Software Design Descriptions) Software design		
ASSOCIATED TECHNOLOGY AREAS			
Technology Areas	Application Development Languages Case Tools Source code repositories		
DISCIPLINE DOCUMENTATION REQUIREMENTS			
Documentation requirements for this Discipline	This discipline will be documented to the product level and the compliance components associated with the product version, family etc…)		
CURRENT STATUS			
Discipline Status	☐ *In Development* ☐ *Under Review* ☐ *Rejected* ☐ *Accepted*		
AUDIT TRAIL			
Creation Date	03/01/02	*Date Accepted/Rejected*	
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	03/01/02
Reason for Update			
Updated By			

Click on this link to return to Application Blueprint Samples.

Technology Area Blueprint

Definition	
Name	Technology Area – Programming Language / Environment
Description	Programming Language / Environment includes all the various coding languages and IDE (Integrated Development Environments) utilized within the organization to deliver software applications, components, and objects.
Rationale	Having a single technology area for all of these allows compliance components that may be applied across all languages to be associated at the Technology Area.
Benefits	Compliance components will be maintained once for all languages that they apply for thus saving time. This time may be spent in furthering other areas of the architecture blueprint.

Associated Discipline	
Discipline Name	Application Development

Keywords	
Keywords/Aliases	Coding Studios, Programming, Coding Standards, Code Sets, Application Languages

Associated Compliance Components	
Compliance Component Names	Overall Programming Standards

Single Product Solution	
Date of Single Product Solution Determination	
Provide Rationale for Decision	

Associated Product Components		
Product Component Names	JAVA, COBOL II (MF, AS) C C++	COBOL (MF, AS) RPG (AS) Pascal Microsoft Visual Basic

Current Status				
Technology Area Status	☐ *In development*	☐ *Under Review*	☐ *Rejected*	☒ *Accepted*

Audit Trail			
Creation Date	03/02/02	*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	03/02/02
Reason for Update			
Updated By			

Click on this link to return to Application Blueprint Samples.

Product Component Blueprint

Definition			
Name	Product Component – Visual Basic		
Description	Visual Basic programming language.		
Rationale			
Benefits			
Component Classification			
Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Sunset Date			
Rationale for Classification	Current application language in use in nth architecture for the organization.		
Associated Technology Area			
Technology Area Name	Application Languages		
Keywords			
Keywords/Aliases	VB, Visual Studio, Client Server language, VBA,		
Vendor Information			
Vendor Name	Microsoft	*Web Address*	www.microsoft.com
Contact Information	**(800) 936-5800** Developers		
Potential Compliance Organizations			
Standards Organizations			
Name	ISO	*Web Address*	http://www.iso.ch
Contact Information	**ISO Central Secretariat:** International Organization for Standardization (ISO) 1, rue de Varembé, Case postale 56 CH-1211 Geneva 20, Switzerland Telephone + 41 22 749 01 11; Telefax + 41 22 733 34 30; E-mail: central@iso.org; Web: http://www.iso.org		
Government Bodies			
Name		*Web Address*	
Contact Information			
Associated Compliance Components			
Product			
Product-specific Compliance Components	Practical Standards for Microsoft® Visual Basic® Author James D. Foxall Pages 400 Disk 1 CD Level Int/Adv Published 01/26/2000 ISBN 0-7356-0733-8		

Configurations			
Configuration-specific Compliance Components	Visual Basic 5 Visual Basic .nt		
COMPONENT REVIEW			
Desirable aspects			
Undesirable aspects			
REQUIRED COMPONENT			
Business Area, Department or Application Name			
CONDITIONAL USE RESTRICTIONS			
Restrictions			
MIGRATION STRATEGY			
Strategy/Source Document			
IMPACT POSITION STATEMENT			
Impact Statement			
CURRENT STATUS			
Product Component Status	☐ *In development* ☐ *Under Review* ☐ *Rejected* ☒ *Accepted*		
AUDIT TRAIL			
Creation Date	03/02/02	*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	03/02/02
Reason for Update			
Updated By			

Click on this link to return to the Application Blueprint Samples.

Compliance Component Blueprint

Definition	
Name	Compliance Component – Prefix all constants with c_ and a scope designator
Description	Naming standard for constants. Includes scope of constant in the name.
Rationale	Ease of code maintenance and code reviews.
Benefits	Coding errors are minimized because of consistent naming standards.
Component Classification	
Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*
Sunset Date	
Rationale for Classification	Visual Basic 5 is current application language used in the organization for client server and nth tier application development.
Associated Technology Architecture Blueprint Level	
Discipline Name	Application Development
Technology Area Name	Application Languages
Product Component Name	Visual Basic
Keywords	
Keywords/Aliases	Constance, Variable, naming,
Compliance Component Type	
Component Type	☐ *Guideline* ☒ *Standard* ☐ *Legislation*
Compliance Sub- Type	Coding
Compliance Detail	
Statement	**5.1 Prefix all constants with c_ and a scope designator**. In the past, one convention for denoting a constant was to use all uppercase letters for the constant's name. For instance, when you created a constant to store a column index in a grid, you would use a statement like this: **Const** COLUMN_INDEX = 7 Typing anything in code in all uppercase letters is now considered antiquated and undesirable. Mixed-case text is much easier to read. However, since variable and procedure names are also entered in mixed case, it's important to denote when an item is a constant. A better convention is to prefix the constant name with *c_*. For example, the constant shown above would be declared like this: **Const** c_Column_Index = 7 This constant name is a bit easier to read, and you can still immediately tell that you're looking at a constant as opposed to a variable. The second underscore is optional. Some developers (including me) prefer not to use an underscore in this way. This is fine, as long as your approach is consistent. The same constant declaration without the second underscore would look like the following line of code. (Remember that you'll always have an underscore

in the constant prefix.)

Const c_ColumnIndex = 7

Note Labels for use with *GoTo* are one of the few exceptions to using mixed-case letters. Such labels, which should be used sparingly, appear in all uppercase letters. Refer to Chapter 11, "Controlling Code Flow," for more information on using these labels.

Another identifying characteristic of a constant as opposed to a variable is the lack of a data type prefix. For instance, if you were storing the column indicator in a variable, you would probably declare the variable by using a statement like this:

Dim intColumnIndex **As Integer**

Note Some external libraries still use uppercase constants. For instance, if you use the API viewer to locate and copy API-related constants, you'll often see these constants in uppercase letters. In such cases, leave the constants, as they are to promote cross-application consistency.

Many developers don't realize that you can actually create a constant of a specific data type. For instance, the following statement is completely legal:

Const c_InterestRate **As Single** = 7.5

You can specify a data type for a constant, but it adds complexity. If a data type is used for a constant, use the variable-naming prefixes discussed in Chapter 4, "Naming Conventions." The previous declaration, for instance, is not correct—according to the directives presented in this book—because the data type prefix is omitted. The proper declaration would be as follows:

Const c_sngInterestRate **As Single** = 7.5

Although the prefix for constants is different from the prefixes for variables, you should still use the same prefix scheme for indicating the scope of constants that you use for variables. For constants declared locally (within a procedure), no scope indicator is necessary. For constants declared as *Private* in the Declarations section of a module, you should use the prefix *m*. For global constants (constants declared as *Public* within a standard module), you should use the prefix *g*. The following are declarations of the same constant at different levels of scope:

Procedure: Const c_InterestRate = 7.5
Module (private): Private Const mc_InterestRate = 7.5
Global: Public Const gc_InterestRate = 7.5

Note Constants are declared *Private* by default if you don't explicitly declare them with the *Public* keyword. As with procedures and variables, constants should always have a clearly defined scope. If you want to create a private constant, explicitly declare the constant using the *Private* keyword.

By consistently specifying the scope of a constant in addition to denoting the constant with *c_*, you'll make your code easier to read and to debug. If you're ever unsure where a constant is declared, simply place the cursor anywhere within the name of the constant and press Shift+F2. Visual Basic will take you directly to the constant's declaration.

Practical Applications

When you uniquely identify constants and denote their scope, you create code that is more readable.

	5.1.1 Declare constants using mixed-case characters, prefixing each constant with *c_*. Remember that identifying constants by using all uppercase letters is out. **Incorrect:** **Const** USDATE = "mm/dd/yyyy" **Const** KEYCONTROL = 17 **Correct:** **Const** c_USDate = "mm/dd/yyyy" **Const** c_KeyControl = 17 **Also correct:** **Const** c_US_Date = "mm/dd/yyyy" **Const** c_Key_Control = 17 **5.1.2 Denote a constant's scope using a scope designator prefix.** Knowing a constant's scope is extremely important for debugging. All constants declared in the Declarations section of any type of module need a *g* or an *m* designator. **Incorrect (module level or global level):** **Private Const** c_US_DATE = "mm/dd/yyyy" **Public Const** c_KeyControl = 17 **Correct:** **Private Const** mc_US_Date = "mm/dd/yyyy" **Public Const** gc_KeyControl = 17
Source Reference	Practical Standards for MS Visual Basic - Chapter 5 by James D. Foxall ISBN 0-7356-0733-8
Standards Organization	
Name	*Web Address*
Contact Information	
Government Body	
Name	*Web Address*
Contact Information	
CONDITIONAL USE RESTRICTIONS	
Restrictions	
MIGRATION STRATEGY	
Strategy/Source Document	
IMPACT POSITION STATEMENT	
Impact Statement	

CURRENT STATUS					
Compliance Component Status	☐ *In development*	☐ *Under Review*	☐ *Rejected*	☒ *Accepted*	
AUDIT TRAIL					
Creation Date	03/02/02		*Date Accepted / Rejected*		
Created By					
Reason for Rejection					
Last Date Updated			*Last Date Reviewed*	03/02/02	
Reason for Update					
Updated By					

Click on this link to return to the Application Blueprint Samples.

Discipline Blueprint

DEFINITION	
Name	Discipline - Electronic Collaboration
Description	The Electronic Collaboration discipline defines the standards and infrastructure components that facilitate the interaction of the workforce and promote group productivity. These include e-mail, directory services and other person-to-person or group collaboration tools. The market-driven complexity and integration capability of Workgroup Services products will create increasing demands on system resources: processing power (speed and memory), operating system features and network bandwidth. A network-centric/thin client design, the option that requires the least impact on user desktop machines, is critically dependent on high-speed, highly reliable, very secure network connections. Changing from a paper-based organization to a "digitally-based" organization will require significant investment in infrastructure capacity, reliability and security. Within government, the necessary investment in Workgroup Services will receive requisite support only when it is clearly cost-justified in terms of service to the citizens.
Rationale	The Electronic Collaboration discipline describes Workgroup Services: practices, typically software related, that allow for data to easily be shared between different agencies, bureaus and departments. Other disciplines such as Application Development and Management and Asset Management describe the process of developing and tracking COTS software licenses, etc. Office automation is an inherent aspect of the office environment and is key to enabling employees to carry out the day-to-day business of the agency. Increasingly, the use of office automation will support the need of the public to receive information in electronic format.
Benefits	The Electronic Collaboration discipline standardizes the approach to automating the correspondence, scheduling of personnel and resources, documentation creation, and desktop data analysis tools. . This standardization provides a cost effective approach to electronic collaboration and minimizes training and retraining requirements. The capability to retain staff will be increased by the simplification of staff retraining and a more effective investment of available project funding.
BOUNDARY	
Boundary Limit Statement	Office automation software provides administrative support for completing daily business functions. This element is defined as including, but not limited to, the following: • Spreadsheets • Business Graphics • Presentation Packages • Personal Data Bases • Word Processing • Time Management and Scheduling • Calendars • Desktop Publishing • Multi-media • Document Imaging • Mail

ASSOCIATED DOMAIN	
Domain Name	Application Architecture

CRITICAL REFERENCES

Related Domains/Disciplines

Domain – Disciplines		*Domain - Disciplines*		*Domain - Disciplines*	
☐	*Access: Internet /Intranet*	☒	*Integration: Functional Integration*	☐	*System Management: Help Desk / Problem Management*
☐	*Access: Branding*	☐	*Integration: Middleware*	☒	*System Management: Business Continuity*
☒	*Access: Accessibility*	☒	*Application: Application Development Management*	☒	*Security: Enterprise Security*
☐	*Information: Data Management*	☒	*Application: Electronic Collaboration*	☒	*Security: Network Security*
☐	*Information: Knowledge Management*	☐	*Platform: Platform*	☒	*Security: Host Security*
☐	*Information: GIS*	☒	*Platform: Configuration Management*	☐	*Privacy: Profiling*
☐	*Information: Data Storage*	☐	*Systems Management: Asset Management*	☐	*Privacy: Personalization*
☒	*Network: Physical Network*	☒	*System Management: Change Management*	☒	*Privacy: Privacy*
☐	*Network: Network Management*	☐	*System Management: Console / Event Management*		

Standards Organizations

Name	International Organization for Standardization	*Web Address*	http://www.iso.ch/iso/en/ISOOnline.frontpage
Contact Information	**ISO Central Secretariat:** International Organization for Standardization (ISO) 1, rue de Varembé, Case postale 56 CH-1211 Geneva 20, Switzerland Telephone + 41 22 749 01 11; Telefax + 41 22 733 34 30; E-mail: central@iso.org; Web: http://www.iso.org		

Government Bodies

Name	None Identified	*Web Address*	
Contact Information			

Stakeholders/Roles

Stakeholders	Business Analyst, Systems Analyst, Business Functional Users, Software Vendors, and, Data Analyst, etc…
Roles (if stakeholder titles are not known)	

Discipline-specific Trends

Trend Statement	None identified
Trend Source	

METHODOLOGIES			
Methodologies followed			
ASSOCIATED COMPLIANCE COMPONENTS			
Compliance Component Names	None identified		
ASSOCIATED TECHNOLOGY AREAS			
Technology Areas	e-Mail Calendaring		
DISCIPLINE DOCUMENTATION REQUIREMENTS			
Documentation requirements for this Discipline	This discipline will be documented to the product level and the compliance components associated with the product version, family etc…)		
CURRENT STATUS			
Discipline Status	☐ *In development* ☐ *Under Review* ☐ *Rejected* ☒ *Accepted*		
AUDIT TRAIL			
Creation Date	03/01/02	*Date Accepted/Rejected*	
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	03/01/02
Reason for Update			
Updated By			

Click on this link to return to Application Blueprint Samples.

SECURITY BLUEPRINT SAMPLES – SET ONE

The five levels of the first Security Domain sample are represented starting at the domain level and following a single line throughout the levels as follows:

- Domain – Security
- Discipline – Host Security
- Technology Area – Directory Services
- Product Component - OpenLDAP
- Compliance Component – OpenLDAP 2.0 Administrator's Guide

Additional examples of Disciplines and a Discipline-level Compliance Component from within the first sample Security Domain include:

- Discipline – Enterprise Security
- Compliance Component – Workstation Security
- Discipline – Network Security

Domain	*Discipline*	*Technology Area*	*Product Component*	*Compliance Component*
Security	Host Security	Directory Services	OpenLDAP	OpenLDAP 2.0 Administrator's Guide
	Enterprise Security			Workstation Security
	Network Security			

Domain Blueprint

DEFINITION	
Name	Domain – Security
Description	The Security Domain defines the roles, technologies, standards, and policies necessary to protect the information assets of states and their citizenry from vandalism, theft, and any other form of unauthorized access. The Security Domain defines the security and access management principles that are applied to ensure the appropriate level of protection for states' information assets. This Domain facilitates identification, authentication, authorization, administration, audit, and naming services. Security involves many issues and requires a systematic approach to ensure all aspects are addressed and that they all function together as a total system. This document provides the user a basic outline of the areas of review. A systematic approach is very necessary and involves analysis of at least the following major categories: Physical Security Physical security is the security of the physical devices that provide access, storage, and/or permit modification of an agency's data resources. This includes the ability to control access to such hardware whether electronic (i.e., computers) or mechanical (i.e., file cabinets). The control of inventory, including the protection from casual loss and theft as well as the proper disposition of obsolete equipment and records, would be included as part of this category. User Security The ability to ensure that users accessing data and systems are in fact who they say they are and that they have access only to those resources to which they are authorized is critical to the success of any security plan. Functions that are involved in analysis of this issue include identification, authentication, and authorization of the individual. The need for audit procedures and mechanisms also requires evaluation. Application Security This aspect of security is aimed at ensuring that an application that accesses another application or data is secure. Knowing the linkages to which an application has access and the security requirements of the distant data source or program is essential. The impact of distributed traffic, proxy accesses and middleware must be evaluated. System Security Analysis of the systems supporting data access is required, regardless of whether the system is a mainframe computer, file/application server or other host server. Consideration must be given to the need for access security as well as issues such as encryption of data on a server. Links to the server from the remote client or directly connected console must be evaluated. The "system" encompasses the user operating a client, data transmission, and the host server. Evaluation as a unit is required to ensure all aspects have been considered.

	Data Security Data security encompasses both physically protecting the data from unauthorized access as well as loss of data through mechanical/electrical failure or viruses. As such, consideration of backup and archive procedures, off-site storage, and audit procedures must be given. Information classification is also included in data security. Classification of data is necessary to ensure protection and recovery policies are adequate. Network Security Network security includes the physical/electrical links between the desktop client and the host computer. This responsibility is generally split between agencies with the user agency and DISC performing part of the functions. In view of this, close cooperation between these groups must be maintained. The LAN and WAN links must be reviewed and evaluated for security needs. The use of the Internet and dial-up connections to facilitate traveling staff places an additional burden on this analysis; since those links can not be controlled and therefore carry a greater risk of being compromised. Security Administration A significant and often omitted part of any security plan is the administration of the plan. This includes the setting and periodic review of policies and the design and analysis of the proposed or existing systems. This function also includes the periodic testing of the existing security plans, including both Business Recovery Plans and protection against unauthorized intrusion. Security administration is broken into two job functions: the ISA (Information Security Administrator) who focuses attention on individual systems and the ISO (Information Security Officer) who pays attention to the larger enterprise. Social Engineering/Human Factors All computer networks and applications are susceptible to compromise by malicious or unauthorized persons. Many techniques employ the use of deceptive practices aimed at individual users or employees. Staff members at all levels must be constantly aware of the potential to be used as a resource to enable illegitimate access to computer-based systems or network infrastructure. All employees should exercise caution to prevent the release of sensitive infrastructure details to unauthorized sources. Organizations are encouraged to develop procedures to positively identify requesters of information and their legitimate purposes.
Rationale	The Security discipline standardizes the methodology, approach, and technology components utilized in the implementation of information resource protection measures. Government, industry, and the public are realizing numerous benefits from the emergence of new information technologies and the increased availability of the Internet. This technology boom has also increased the security risk to the state's information resources. With the ever-increasing percentage of the public that is Internet capable, there has also been an increase in the number of Internet users with malicious intent as well as an increase in the availability of malicious tools and viruses. Decision-making criteria are required in order to ensure that security requirements are identified and security components are incorporated to provide the appropriate level of protection for the government entity's information resources. Security policies need to provide consistency across the enterprise, and appropriate

	measures need to be in place to support authorized exchange of information between systems of different security levels. Security involves many aspects, such as providing: • Physical security of the data and resources used to produce the data. • Protection against unauthorized and inappropriate use that could potentially impede authorized and appropriate use of the resource. • Identification and validation of the person who is requesting the information • Control of access involves the ability to read, write, delete or otherwise acquire access to information. • Data Privacy or confidentiality includes protection of information from unauthorized disclosure and interception. • Data integrity or protecting the data from unauthorized modification, including unintentional modifications caused by disk errors, system problems, etc. • Audit trails for accountability. • Non-repudiation involves proving either the validity of the data and/or the occurrence of actions with respect to the origin of data (or transaction) and the delivery (or receipt) of the data.
Benefits	• Security supports secure distribution and integrity of information. • Security protects the computing infrastructure from unauthorized access. • A functional, yet non-intrusive, secure architecture ensures enterprise-wide interoperability, as well as connectivity with external stakeholders. • Security, designed into all architectural elements balances accessibility and ease-of-use with protection of data. • Security, based on accepted standards allows the architecture to focus on open systems.
BOUNDARY	
Boundary Limit Statement	The Security Domain is associated with virtually all other domains because security needs must be assessed and applied where necessary in all phases of information resource development and management. The Security Domain does not include the privacy aspects associated with deployment of information technologies.
ASSOCIATED DISCIPLINES	
Disciplines under this Domain	Enterprise Security Network Security Host Security

RELATED PRINCIPLES		
Reference #s, Statements or Links	*Conflict*	*Relationship*
The principles contained under the first seven categories in this section were compiled during the NASCIO Forum on Security and Critical Infrastructure Protection, held November 13th and 14th. The principles under the seven categories (Architecture through Legislation) were developed from a security perspective.		
Architecture		
Architecture is a recognized framework of principles and standards that enable information sharing and interoperability.	☐	The protection of resources and data is critical to information sharing and interoperability.
Business initiatives drive architecture.	☐	Security of IT systems requires the protection of systems and information, and the assurance that the systems do exactly what they are supposed to do and nothing more.
Architecture is an on-going program—not a one-time project.	☐	Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.
Privacy and security are fundamental attributes of technology.	☐	IT security requires management controls to ensure authorized access to the information in the systems and proper handling of input, processing, and output. The confidentiality of information must be assured whether on-site or off-site. Risk assessment, contingency planning, and physical security are also essential to implementing effective security policies.
Architecture requires definition and education. It is NOT an initiative.	☐	Education on the Security aspects of architecture will be contained in the communications processes.
Assessment		
States should adopt a common methodology for identification and assessment of critical assets (e.g. project matrix). The methodology should: focus on mission critical business processes, identify interdependencies between systems, and identify risks and vulnerabilities.	☐	Security policies need to provide consistency across the enterprise, and appropriate measures need to be in place to support authorized exchange of information between systems of different security levels. Without a properly crafted policy, the resulting design and deployment of the technology to enforce the policy will be faulty.
Assessments should be performed on a periodic basis to keep information current.	☐	Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.
Assessment of IT critical assets should align with state and federal government Homeland Security efforts.	☐	System security measures should be tailored to meet organizational security goals.
Business Alignment		
Public safety and health, education, human services, financial and other critical services are the critical business of government.	☐	Identify the systems that must be protected for business to continue or trust to be maintained.
Multiple levels of government are involved in providing these essential government services (seamless).	☐	Security policies need to provide consistency across the enterprise, and appropriate measures need to be in place to support authorized exchange of information between systems of different security levels.

Government leaders are responsible for the continuity of these essential services that affect the citizens of every state.	☐	
The delivery of these services is dependent on reliable and secure computing and communication systems. These IT systems are susceptible to physical and electronic attacks.	☐	
Education and Communication		
Information security education and information sharing are critical, and should be targeted to specific audiences in order to promote their intrinsic value to the organization and foster partnerships for action at private, city, county, state, regional and federal levels.	☐	The security officer shall communicate the security policies to all agency personnel. Administrators shall conduct periodic training in security awareness so that all personnel understand the security threats and their part in enforcing the policies. Implement a program and related security awareness education to help users know what to do in case they encounter a potential security breach, and how users can avoid unsafe computing.
Funding		
Security is a fundamental element of Information Technology, and funding must reflect its importance to the services government provides to our citizens.	☐	Without sufficient financial resources for staffing, training and security assets, the security of the enterprise systems cannot be adequately protected from vulnerability.
Governance		
Security is a fundamental function of government.	☐	
As such, a formal, permanent, executive level governance structure is required.	☐	
Governance structure should encourage an intergovernmental approach.	☐	
Legislation		
State statutes should identify an entity with compliance and enforcement authority over IT management.	☐	
Governors and CIOs should support the passage of HB2435 (Davis-VA)—which would exempt state cybersecurity communications with the federal government and ISACs from FOIA/Open access laws—and encourage states to pass similar legislation for internal purposes and sharing with private partners regarding critical infrastructure.	☐	
Keep all cyber security legislation broad, not limited to “cyber-terrorism”.	☐	
CIOs and their leadership should champion legislation that creates real penalties for cyber-crimes.	☐	

Security Specific		
Security measures should be appropriate to the value and relative vulnerability of the assets.	☐	Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.
System security should be an essential part of every agency's annual IT plan.	☐	Establish a sound security policy as the "foundation" for design. Protect information while being processed, in transit, and in storage.
Each agency should develop, implement and maintain written enterprise security policies and document exceptions to those policies.	☐	Security policies need to provide consistency across the enterprise, and appropriate measures need to be in place to support authorized exchange of information between systems of different security levels. Without a properly crafted policy, the resulting design and deployment of the technology to enforce the policy will be faulty. System security measures should be tailored to meet organizational security goals. Unnecessary security mechanisms should not be implemented.
Agencies should follow the principle of "separation of duties" with regards to security functions.	☐	To maintain separation of duties, security administrators should not be allowed to have application or systems programming duties. If such separation of duties isn't feasible, then compensating controls must be in place to ensure adequate crosschecking of functions occurs (e.g., supervisory reviews, independent audits).
Access to and transmission of data or resources should be secured, audited and monitored at a level consistent with their sensitivity.	☐	Reduce risk to an acceptable level.
Each agency should conduct and document periodic security audits and update security practices accordingly.	☐	Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.
The recipient of sensitive data is responsible for maintaining the security of the data.	☐	Each agency or department must have security measures in place, consistent with the sensitivity of the data.
Any individual or service accessing sensitive data or resource(s) should be identified.	☐	Design and implement audit mechanisms to detect unauthorized use and to support incident investigations. Use unique identities to ensure accountability.
Financial resources must be dedicated for adequate staffing and security assets.	☐	Without sufficient financial resources for staffing, training and security assets, the security of the enterprise systems cannot be adequately protected from vulnerability.
Each agency should develop Incident Response plans/procedures.	☐	Provide assurance that the system is, and continues to be, resilient in the face of expected threats. Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.
Each agency should provide ongoing security awareness training to all agency employees.	☐	The security officer shall communicate the security policies to all agency personnel. Administrators shall conduct periodic training in security awareness so that all personnel understand the security threats and their part in enforcing the policies. Implement a program and related security awareness education to help users know what to do in case they encounter a potential security breach, and how users can avoid unsafe computing.

Information security should be administered in a responsible and ethical manner.	☐	Security policies will be administered in conjunction with all laws and regulations.
Develop redundancy in critical resources.	☐	Identify the systems that must be protected for business to continue or trust to be maintained. Develop systems with redundancy built in to protect resources critical to these business functions.
Management should ensure that security is incorporated in all stages of the system development life cycle.	☐	Establish a sound security policy as the "foundation" for design. Treat security as an integral part of the overall system design.
Encryption, with appropriate key management, should be used where appropriate.	☐	Implement audited access using one or more forms of encryption, certificates, or tokens. Encryption should be considered for all data that are sensitive, have high value, or represent a high value if they are vulnerable to unauthorized disclosure or modification during transmission or while in storage.

Related Best Practices

Reference #s, Statements or Links	*Conflict*	*Relationship*
Physical Security	☐	Employees should be made aware of physical security issues and the importance of adhering to published security policies and procedures.
Physical Security - Access Control	☐	State entities should ensure that all desktop equipment, servers, data centers, telecommunication rooms, wiring closets, off-site storage, and alternative work sites are appropriately secured and controls are in place to restrict the access/entry of personnel to only authorized individuals. Wiring should be installed in conformance with industry standards.
Physical Security - Loss prevention, theft protection	☐	Equipment should be located in environmentally appropriate facilities, and environmental controls such as water detection, smoke detection, fire prevention, and un-interruptible power supplies should be utilized. Intrusion detection systems should signal an alarm when unauthorized entry is attempted. Portable equipment should never be left unattended in unsecured areas.
Physical Security - Inventory control	☐	A full physical inventory of all State-owned equipment, software, and materials should be maintained and accountability assigned to appropriate individuals. Appropriate physical identification tags should be utilized. Software licenses should be maintained, linking software to specific devices.
User Security - Identification	☐	State entities should utilize some method of ensuring that only authorized individual users are permitted access to information systems. The user must be required to provide some unique identification (e.g. User ID), to provide a claimed identity to the system. These means of identification should be administered by an appropriate source, independent of the users, and inactive User IDs should be removed in a timely manner.
User Security - Authentication	☐	State entities should validate a user's claim to who he/she is. This should be based on something the individual knows (e.g., a password), something the individual possesses (e.g., a smart card), or by something the individual is (a biometric). Responsible password management should be employed whenever authentication is based on passwords (e.g., password aging, minimum length, mixed characters, etc.).

		If non-repudiation is a requirement, PKI technology can provide the assurance that the information received has not been altered and also that the reputed sender of the information is indeed who sent it. This may be a requirement for transmission of legally binding documents
User Security - Authorization	☐	State entities should determine the appropriate levels of access for all users for all systems, based on need to know, specific job responsibilities, and sensitivity of the data. Appropriate controls such as segregation of duties should be maintained.
User Security - Audit	☐	State entities should maintain automated records to enable reconstruction and/or review of operations performed on systems. Audit trails should be protected in such a way that a user cannot change them. Individuals in a supervisory or security capacity should review them regularly.
Application Security	☐	Many vendor-supplied applications have built-in security features. These features should be used to best conform to the existing security polices. In-house-developed applications should be designed and implemented with information protection in mind.
System Security	☐	In addition to making every effort to secure the local network, each system on that network should be made as secure as possible. This will be a function of the operating system technicians. This work will include: research of known vulnerabilities, incorporating vendor-supplied upgrades and patches, removing or disabling any service not required, and acquiring additional security software to reside on the system. Vulnerability scans can be useful in determining the weaknesses of the system.
Data Security	☐	Every effort should be made to ensure the security of data and protect it from loss or misuse. There should be policies, procedures, and products in place to ensure the security of the data. When storage media (for example, hard drives or tapes) are no longer usable, all data on the media should be erased before disposal. When storage media are being sent off-site for repair, the data may need to be removed or made inaccessible by encryption or password protection, as appropriate. CMOS passwords and file encryption should be employed on portable devices when they contain sensitive information. Security of Access (Alternative to above bullet: Authentication should be used at all times when accessing or making changes to data. Auditing should be activated, and all access to data should be logged.)
Data Backups	☐	All data backups should be made on a frequent basis. The frequency of the backups may depend on the sensitivity, criticality, and value of the data. There should be locations available for off-site storage of the backups. Encryption of backups should be considered when highly sensitive data is involved.

Data Media Security	☐	The data storage media should also be used to protect the data. Encrypting data on servers will help prevent unauthorized access of the data. Protect all OS and application media.
LAN Security Technology	☐	The LAN should be isolated from any network-connected device that does not have a valid business relationship with resources on the LAN. Internal dial connections in general are difficult to secure, and if possible, should be avoided. When this type of connection is unavoidable due to business requirements, policy should be clearly written about how it is to be secured. Router connectivity should be secured by means of a firewall type device to control any access from outside the LAN, consistent with agency policy. If public access to a server in the internal LAN is required, it is best to put that server on a separate LAN segment behind the firewall device. It is typically referred to as the DMZ. Public access should never be allowed into the secured private LAN.
Enterprise Network Security	☐	If communications are to be confined to specific users or sites, an encrypted VPN should be considered.
WAN Security	☐	An agency should always assume a network outside its control is unsecured, especially a WAN.
Security Administration	☐	Security professionals should be encouraged to work toward a professional certification such as the Information Systems Security Professional (ISSP) administered by the International Information Systems Security Certification Consortium. They should also be encouraged to be active in professional organizations such as the Information Systems Security Association. The first and most critical function of security administration is to create the agency comprehensive security policy for each of the contexts outlined in this architecture. Representatives of all areas of the agency should be involved in developing the policy. Without a properly crafted policy, the resulting design and deployment of the technology to enforce the policy will be faulty. The effectiveness of agency information protection is proportionate to how well the agency's Security Policy is crafted. Management at all levels should make every effort to supply the support and resources necessary to assure the best Security Policy possible is used and enforced. The security policy should consider whether to allow and how to gain access to resources where passwords are no longer known (e.g., an employee leaves). The security officer should ensure that the security policies reflect the agency's mission and are based on the value of the confidentiality, availability and integrity of the agency's resources. The security officer should communicate the security policies to all agency personnel. Administrators should conduct periodic training in security awareness so that all personnel understand the security threats and their part in enforcing the policies.

Security Personnel - Information Security Administrator (ISA)	☐	ISAs make the computing environment less vulnerable by ensuring proper access by users. ISAs are responsible for presenting and disseminating the security policy to users and vendors and answer any questions users may have regarding the policies or security. ISAs have the responsibility of monitoring security on systems. Common functions of the ISA include: Implement on-line warnings to inform each user of the rules for access to the organization's systems. Without such warnings, internal and external attackers can often avoid prosecution even if they are caught. Enable logging for important system level events and for services and proxies, and set up a log archiving facility. Review the logs. Perform system audits to learn who is using the system, to assess the existence of open ports for outsiders to use, and to review several other security-related factors about the system. Run password-cracking software to identify easy-to-guess passwords. Weak passwords allow attackers to appear as "authorized" users allowing them to test for weaknesses until they find ways to take control of those systems. Scan the network to create and maintain a complete map of systems to which the agency is connected. Select an incident response team and establish the procedures to be used to respond to various types of attacks.
Security Personnel - Information Security Officer (ISO)	☐	ISOs focus their attention from individual systems to the enterprise and raise the barriers to attackers even further, paying special attention to intrusion detection, finding and fixing unprotected "back doors" and ensuring that remote access points are well secured. ISOs focus on threats from insiders, on improving monitoring on systems that contain the most critical information, and support the most important business functions. Common functions of the ISO include: Use network-based vulnerability scanners. Implement the latest applicable patches, remove or tighten unnecessary services, and tighten system settings on each host operating system. Establish a host-based perimeter. Implement a file integrity (cryptographic fingerprinting) system to ensure that you can tell which files were changed in an attack. Identify the systems that must be protected for business to continue or trust to be maintained. These are identified as critical servers. Implement instrumentation (such as host-based intrusion detection and cryptographic file fingerprinting) for critical servers to enable immediate response to unauthorized access. Conduct a physical security assessment and correct insecure access and other physical security weaknesses. Implement intrusion detection sensors and analysis stations. Implement audited access using one or more forms of encryption, certificates, or tokens. Assess and strengthen dial-in service configuration.

		Conduct a modem sweep to search for back doors. Search for and eradicate sniffer programs. Conduct a vulnerability scan, searching for additional vulnerabilities that have been exploited but are more rare and sophisticated. Implement configuration management controls for the introduction of new systems to the network. Implement a program and related security awareness education to help users know what to do in case they encounter a potential security breach, and how users can avoid unsafe computing. Implement encryption, possibly as a virtual private network, to avoid disclosure of sensitive information traveling over the network. Tighten security of the web server. Implement more sophisticated log file analysis.
Security Personnel - General	☐	While the security technicians should have a minimal presence in crafting the Security Policy, during this step they should be allowed to take the lead in designing the technology that will enforce the Policy. Upper management should be readily available to support the technicians with guidance in interpreting the intent of the policy statement, as needed, and to provide resources required by the technical staff. To maintain separation of duties, security administrators should not be allowed to have application or systems programming duties. If such separation of duties isn't feasible, then compensating controls must be in place to ensure adequate crosschecking of functions occurs (e.g., supervisory reviews, independent audits). Security administrators should see that agencies' security implementations are audited on a regular basis. The audit should test compliance with the policies and measure the effectiveness of the policy and its implementation. Administrators should consider using available tools to test such things as the strength of passwords. The security policy should also be reviewed and updated on a regular basis. As part of the Security Policy, provisions for recovery should be in place to ensure continued business function if some facet of the protection fails.
Social Engineering/Human Factors	☐	Prohibit the release of passwords via telephone or unsecured electronic mail. Maintain a list of technical support personnel authorized to request information. Encourage users to have vendors, outside technical support or contractors contact the organization's IT staff support for information pertaining to the network or information access.
RELATED TRENDS		
Reference #s, Statements or Links	*Conflict*	*Relationship*
	☐	
	☐	

IT CONTRACTS			
Planned Contracts			
Existing Contracts			
CURRENT STATUS			
Domain Status	☐ *In development* ☐ *Under Review* ☐ *Rejected* ☒ *Accepted*		
AUDIT TRAIL			
Creation Date	4/15/2002	*Date Accepted/Rejected*	
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

Click on this link to return to the Security Blueprint Samples – Set One.

Discipline Blueprint

DEFINITION	
Name	Discipline - Host Security
Description	Defines the roles, standards, policies, and tools for monitoring and ensuring the security across the organization's platform infrastructure. The Host Security discipline defines the security and access management principles that are applied to ensure the appropriate level of protection for information assets.
Rationale	Security of IT systems requires the protection of systems and information, and the assurance that the systems do exactly what they are supposed to do and nothing more. IT security requires management controls to ensure authorized access to the information in the systems and proper handling of input, processing, and output. The confidentiality of information must be assured whether on-site or off-site. Key elements of a successful security approach include an appropriate balance of data access and data protection, user buy-in, training and continued awareness.
Benefits	

BOUNDARY	
Boundary Limit Statement	Host Security covers the following areas: User Security – identification, authentication, and authorization of user, including audit procedures and mechanisms. Application Security – security between applications, including impact of distributed traffic, proxy accesses and middleware. System Security – analysis of the systems supporting data access, links to the server from the remote client or directly connected console, including access and encryption. ("System" encompasses the user operating a client and the host server) Data Security – encompasses both physically protecting the data from unauthorized access as well as loss of data through mechanical/electrical failure or viruses, includes information classification, backup and archive procedures, off-site storage, and audit procedures.

ASSOCIATED DOMAIN	
Domain Name	Security

CRITICAL REFERENCES

Related Domains/Disciplines

Domain-Disciplines		*Domain-Disciplines*		*Domain-Disciplines*	
☐	*Interface – Branding*	☐	*Integration – Functional Integration*	☐	*Systems Mgt – Business Continuity*
☒	*Interface – Access*	☒	*Integration – Middleware*	☐	*Security – Enterprise Security*
☐	*Interface – Accessibility*	☐	*Application – Application Engineering*	☒	*Security – Network Security*
☐	*Information – Knowledge Mgt*	☐	*Application – Electronic Collaboration*	☒	*Security – Host Security*
☐	*Information – Data Mgt*	☐	*Systems Mgt – Asset Mgt*	☐	*Privacy – Profiling*
☐	*Information- GIS*	☐	*Systems Mgt – Change Mgt*	☐	*Privacy – Personification*
☐	*Infrastructure - Network*	☐	*Systems Mgt – Console/Event Mgt*	☐	*Privacy – Privacy*
☐	*Infrastructure - Platform*	☒	*Systems Mgt – Help Desk/Problem Mgt*		

Standards Organizations

Name	National Institute of Standards and Technology (NIST)	*Web Address*	http://www.nist.gov/ - NIST Homepage
Contact Information	**NIST** 100 Bureau Drive, Stop 3460 Gaithersburg, MD 20899-3460 Email: inquiries@nist.gov Telephone: 301. 975.NIST (6478) or TTY 301.975.8295		
Name	American National Standards Institute	*Web Address*	http://web.ansi.org/default.asp - ANSI Online
Contact Information	**American National Standards Institute** Washington, DC Headquarters 1819 L Street, NW, 6th Fl. Washington, DC, 20036 Email: info@ansi.org Telephone: 202.293.8020 Fax: 202.293.9287		

Government Bodies

Name	None Identified	*Web Address*	
Contact Information			

Stakeholders/Roles

Stakeholders	
Roles (if stakeholder titles are not known)	

Discipline-specific Trends

Trend Statement	
Trend Source	

METHODOLOGIES			
Methodologies followed			
ASSOCIATED COMPLIANCE COMPONENTS			
Compliance Component Names	IEEE Std 1363-2000, IEEE Standard Specifications for Public-Key Cryptography FIPS 46-3 October 1999, Data Encryption Standard (DES); specifies the use of Triple DES FIPS 140-2 June 2001, Security requirements for Cryptographic Modules FIPS 186-2 January 2000, Digital Signature Standard (DSS)		
ASSOCIATED TECHNOLOGY AREAS			
Technology Areas	User Security Directory Services Application Security System Security Data Security		
DISCIPLINE DOCUMENTATION REQUIREMENTS			
Documentation requirements for this Discipline			
CURRENT STATUS			
Discipline Status	☐ *In development* ☐ *Under Review* ☐ *Rejected* ☒ *Accepted*		
AUDIT TRAIL			
Creation Date	4/16/2002	*Date Accepted/Rejected*	
Created By			
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			
Updated By			

Click on this link to return to the Security Blueprint Samples – Set One.

Technology Area Blueprint

Definition	
Name	Technology Area – Directory Services
Description	A means for managing access to computer resources and keeping track of the users of a network, such as a company's intranet. Directories are repositories of network name knowledge, essential for navigating loosely structured data like the Web. One type of directory common on TCP/IP networks is the Domain Name System (DNS), which is a globally accessible table of domain names and their corresponding IP addresses.
Rationale	A directory is specialized database optimized for reading, browsing and searching. Directories contain descriptive, attribute-based information and support sophisticated filtering capabilities. Directories are tuned to give quick-response to high-volume lookup or search operations. They may have the ability to replicate information widely in order to increase availability and reliability, while reducing response time.
Benefits	Applications like e-mail and network management can benefit from more natural directory entries that include, for instance, people's names, type of service, or geographic locale. This is particularly true on the global Internet, where the address space is growing exponentially; but it's increasingly true on wide-area intranets, as well.
Associated Discipline	
Discipline Name	Host Security
Keywords	
Keywords/Aliases	Authentication, Directory Services
Associated Compliance Components	
Compliance Component Names	N/A
Single Product Solution	
Date of Single Product Solution Determination	N/A
Rationale for Decision	N/A
Associated Product Components	
Product Component Names	OpenLDAP NDS (Novell Directory Services)
Current Status	
Technology Area Status	☐ *In development* ☐ *Under Review* ☐ *Rejected* ☒ *Accepted*

AUDIT TRAIL			
Creation Date	5/12/2002	*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

Click on this link to return to the Security Blueprint Samples – Set One.

Product Component Blueprint

DEFINITION	
Name	Product Component – OpenLDAP
Description	OpenLDAP Software is an open source implementation of the Lightweight Directory Access Protocol (LDAP). The suite includes: • slapd - stand-alone LDAP server • slurpd - stand-alone LDAP replication server • Libraries implementing the LDAP protocol, and • Utilities, tools, and sample clients. Lightweight Directory Access Protocol (LDAP) is an open-standard protocol for accessing information services. The protocol runs over Internet transport protocols, such as TCP, and can be used to access stand-alone directory servers or X.500 directories. Key aspects of LDAP are: • Protocol elements are carried directly over TCP or other transport, bypassing much of the session/presentation overhead. • Many protocol data elements are encoding as ordinary strings (e.g., Distinguished Names). • A lightweight BER encoding is used to encode all protocol elements.
Rationale	LDAP has been endorsed as the directory protocol of choice by many organizations, including the University of Michigan and Netscape Communications.
Benefits	LDAP is a lightweight alternative to the X.500 Directory Access Protocol (DAP) for use on the Internet. It uses TCP/IP stack verses the overly complex OSI stack. It also has other simplifications, such as the representing most attribute values and many protocol items as textual strings, which are designed to make clients easier to implement.

COMPONENT CLASSIFICATION				
Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*
Sunset Date				
Rationale for Classification	OpenLDAP is currently in use within the organization.			

ASSOCIATED TECHNOLOGY AREA	
Technology Area	Directory Services

KEYWORDS	
Keywords/Aliases	LDAP, OpenLDAP, Directory Access, sldap

VENDOR INFORMATION			
Vendor Name	OpenSource	*Web Address*	http://www.openldap.org/
Contact Information	Foundation@OpenLDAP.org The OpenLDAP Foundation 270 Redwood Shores Pkwy, PMB#107 Redwood City, California 94065 USA		
POTENTIAL COMPLIANCE ORGANIZATIONS			
Standards Organizations			
Name	Internet Engineering Task Force (IETF)	*Web Address*	http://www.ietf.org/
Contact Information	Contact information is provided per workgroup. See information contained on web site.		
Government Bodies			
Name		*Web Address*	
Contact Information			
ASSOCIATED COMPLIANCE COMPONENTS			
Product			
Product-specific Compliance Components	OpenLDAP Admin Guide		
Configurations			
Configuration-specific Compliance Components	OpenLDAP Admin Guide – 5. The slapd Configuration File		
COMPONENT REVIEW			
Desirable aspects	slapd is an LDAP directory server that runs on many different platforms. Some of slapd's features and capabilities include: LDAPv2 and LDAPv3: slapd supports both versions 2 and 3 of the Lightweight Directory Access Protocol. slapd provides support for the latest features while maintaining interoperability with existing clients. slapd supports both IPv4 and IPv6. Simple Authentication and Security Layer: slapd supports strong authentication services through the use of SASL. slapd's SASL implementation utilizes Cyrus SASL software, which supports a number of mechanisms including DIGEST-MD5, EXTERNAL, and GSSAPI. Transport Layer Security: slapd provides privacy and integrity protections through the use of TLS (or SSL). slapd's TLS implementation utilizes OpenSSL software. Access control: slapd provides a rich and powerful access control facility, allowing controlled access to the information in database(s). Access can be controlled to entries based on LDAP authorization information, IP address, domain name and other criteria. slapd supports both static and dynamic access control information. Internationalization: slapd supports Unicode and language tags.		

	Choice of databases: slapd comes with a variety of different backend databases. They include LDBM, a high-performance disk-based embedded database; SHELL, a database interface to arbitrary shell scripts; and PASSWD, a simple password file database. LDBM utilizes either BerkeleyDB or GDBM. Multiple database instances: slapd can be configured to serve multiple databases at the same time. A single slapd server can respond to requests for many logically different portions of the LDAP tree, using the same or different backend databases. Generic modules API: Allows for customization, slapd allows for easy writing of customized modules. slapd consists of two distinct parts: a front end that handles protocol communication with LDAP clients; and modules which handle specific tasks such as database operations. Because these two pieces communicate via a well-defined C API, customized modules can be easily written, which extend slapd in numerous ways. In addition, a number of programmable database modules are provided. These allow exposure of external data sources to slapd using popular programming languages (Perl, Shell, SQL, and TCL). Threads: slapd is threaded for high performance. A single multi-threaded slapd process handles all incoming requests, reducing the amount of system overhead required. Replication: slapd can be configured to maintain replica copies of its database. This single-master/multiple-slave replication scheme is vital in high-volume environments where a single slapd just doesn't provide the necessary availability or reliability. slapd also includes experimental support for multi-master replication. Configuration: slapd is highly configurable through a single configuration file, which allows a wide range of change. Configuration options have reasonable defaults, which also makes configuration easier.
Undesirable aspects	Limitations – The main LDBM database backend does not handle range queries or negation queries very well. These features and more will be coming in a future release.
REQUIRED COMPONENT	
Business Area, Department or Application Name	N/A
CONDITIONAL USE RESTRICTIONS	
Restrictions	N/A
MIGRATION STRATEGY	
Strategy/Source Document	

IMPACT POSITION STATEMENT			
Impact Statement			
CURRENT STATUS			
Product Component Status	☐ *In development* ☐ *Under Review* ☐ *Rejected* ☒ *Accepted*		
AUDIT TRAIL			
Creation Date	5/21/2002	*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

Click on this link to return to the Security Blueprint Samples – Set One.

Compliance Component Blueprint

Definition	
Name	Compliance Component – OpenLDAP Administrator's Guide
Description	This document describes how to build, configure, and operate OpenLDAP software to provide directory services.
Rationale	This includes details on how to configure and run the stand-alone LDAP daemon, slapd(8) and the stand-alone LDAP update replication daemon, slurpd(8).
Benefits	Provides information including, but not limited to: Configuration Choices Building and Installing OpenLDAP Software slapd Configuration Database Creation and Maintenance Tools Schema Specification

Component Classification				
Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*
Sunset Date				
Rationale for Classification	Configurations as documented within the Administrator's Guide are currently in use within the organization.			

Associated Technology Architecture Blueprint Levels	
Discipline Name	
Technology Area Name	
Product Component Name	OpenLDAP

Keywords	
Keywords/Aliases	LDAP, OpenLDAP, sldap

Compliance Component Type			
Component Type	☒ *Guideline*	☐ *Standard*	☐ *Legislation*
Compliance Sub-type			

Compliance Detail			
Statement	OpenLDAP 2.0 Administrator's Guide		
Source Reference	http://www.openldap.org/doc/admin/index.html		
Standards Organization			
Name	Internet Engineering Task Force (IETF)	*Web Address*	http://www.ietf.org/
Contact Information	Contact information is provided per workgroup. See information contain ed on web site.		
Government Body			
Name		*Web Address*	
Contact Information			

CONDITIONAL USE RESTRICTIONS			
Restrictions	N/A		
MIGRATION STRATEGY			
Strategy/Source Document			
IMPACT POSITION STATEMENT			
Impact Statement			
CURRENT STATUS			
Compliance Component Status	☐ *In development* ☐ *Under Review* ☐ *Rejected* ☒ *Accepted*		
AUDIT TRAIL			
Creation Date	5/20/2002	*Date Accepted / Rejected*	
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

Click on this link to return to the Security Blueprint Samples – Set One.

Discipline Blueprint

DEFINITION	
Name	Discipline – Enterprise Security
Description	Defines the roles, standards, policies, audits, and business process reviews for monitoring and ensuring the security across the organization's enterprise. Includes securing the physical assets from theft and vandalism.
Rationale	Enterprise security can be an issue with State agencies. Due to lack of proper office space, sensitive equipment is often located outside secured areas. Some of the smaller computer rooms are left unlocked and untended. Take steps to place business critical equipment in secure areas. The installation of unauthorized software or authorized software from unverified sources onto state systems is a problem and a violation of fundamental security procedures. This includes software obtained from the Internet and from individuals' homes. Such software is a significant source of viruses and can create major problems within State systems as well as potentially create a liability to the State for licensing issues.
Benefits	

BOUNDARY	
Boundary Limit Statement	Enterprise security covers the security of the physical devices that provide access, storage, and/or permit modification of an agency's data resources. This includes the ability to control access to such hardware whether electronic (i.e., computers) or mechanical (i.e., file cabinets). The control of inventory, including the protection from casual loss and theft as well as the proper disposition of obsolete equipment and records, would be included as part of this category. Enterprise Security also covers: • Security Administration – setting, periodic review and testing of policies and the design and analysis of the proposed or existing security systems • Social Engineering/Human Factors – prevent the release of sensitive infrastructure details by employees to unauthorized sources.

ASSOCIATED DOMAIN	
Domain Name	Security Domain

CRITICAL REFERENCES					
Related Domains/Disciplines					
Domain-Disciplines		*Domain-Disciplines*		*Domain-Disciplines*	
☐	*Interface – Branding*	☐	*Integration – Functional Integration*	☒	*Systems Mgt – Business Continuity*
☐	*Interface – Access*	☐	*Integration – Middleware*	☒	*Security – Enterprise Security*
☐	*Interface – Accessibility*	☐	*Application – Application Engineering*	☐	*Security – Network Security*
☐	*Information – Knowledge Mgt*	☐	*Application – Electronic Collaboration*	☐	*Security – Host Security*
☐	*Information – Data Mgt*	☒	*Systems Mgt – Asset Mgt*	☐	*Privacy – Profiling*
☐	*Information- GIS*	☐	*Systems Mgt – Change Mgt*	☐	*Privacy – Personification*
☐	*Infrastructure - Network*	☐	*Systems Mgt – Console/Event Mgt*	☐	*Privacy – Privacy*
☐	*Infrastructure - Platform*	☒	*Systems Mgt – Help Desk/Problem Mgt*		

Standards Organizations	
Name	
Contact Information	
Government Bodies	
Name	
Contact Information	
Stakeholders/Roles	
Stakeholders	Security Personnel Help Desk Personnel Operations Staff Users
Roles (if stakeholder titles are not known)	
Discipline-specific Trends	
Trend Statement	
Trend Source	
METHODOLOGIES	
Methodologies followed	
ASSOCIATED COMPLIANCE COMPONENTS	
Compliance Component Names	
ASSOCIATED TECHNOLOGY AREAS	
Technology Areas	Physical Security Security Administration Social Engineering/Human Factors
DISCIPLINE DOCUMENTATION REQUIREMENTS	
Documentation requirements for this Discipline	

CURRENT STATUS			
Discipline Status	☐ *In development* ☐ *Under Review* ☐ *Rejected* ☒ *Accepted*		
AUDIT TRAIL			
Creation Date	4/15/2002	*Date Accepted/Rejected*	
Created By			
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

Click on this link to return to the Security Blueprint Samples – Set One.

Compliance Component Blueprint

Definition	
Name	Work Station Security Policy
Description	Policies regarding work station security
Rationale	Guidelines are provided in order to maintain enterprise wide security related to work stations and work station use.
Benefits	Increased security awareness, protection of enterprise assets include intellectual capital
Associated Architecture Levels	
Domain Name	Security
Discipline Name	Enterprise Security
Technology Area Name	
Product Component Name	
Compliance Component Type	
Component Type	Policy
Component Sub-type	
Compliance Detail	
Policy, Guideline, Standard or Legislation	1.0 Overview All programmable workstations equipped with fixed storage devices, e.g., hard disks, shall have security policies established and implemented to restrict unauthorized individuals and programs from accessing information and software stored in the workstation and associated peripherals. 2.0 Mandatory Protection for all Workstations All workstations must have adequate controls to provide continued confidentiality, integrity, and availability of data stored on the system. Critical business functions must not reside on workstations unless specifically authorized for that environment. All workstations must employ an approved access control mechanism (e.g., software or hardware) to restrict access to authorized users. Workstations must be configured with screen savers to blank the screen and require a password to resume operation whenever the workstations are unattended. GOT employees and contractors must not leave their workstation unattended without first shutting down the workstation, logging out, or invoking a password-protected screen saver. Unless otherwise notified by systems administrators or the Division of Security Services, GOT employees and contractors are required to shut down and power off their workstation at the end of the workday. The owner of the workstation has ultimate responsibility for the security of the information on their workstation. 2.1 Protection for Sensitive Workstations In addition to the protection required for all workstations, workstations that access sensitive data must use password protection which prevents the rebooting or powering on of the workstation without authentication. Furthermore, workstation equipment must be physically protected to lessen the risks of theft, destruction, and unauthorized access to data.

	2.2 Resident Protection from Malicious Software Workstations must employ approved virus screening programs at all times. If the screening program detects a virus, the users must immediately notify the LAN administrator. Users will NOT attempt to eradicate a virus or use the affected machine until trained personnel have been notified so they may document and address the problem. 2.3 Erasure of Restricted/Confidential Information Sensitive data must be electronically erased from media or overwritten with approved software before the media leaves the business environment. This does not apply to confidential data written to media as part of scheduled backup processes. Due to the wide availability of programs to restore files that were "accidentally" deleted, the erasure of sensitive data must be accomplished by means other than "deleting" the file and as authorized by the Director, Division of Security Services. 2.4 Workstation/Server/Device Equipped with Modems Workstations/servers/devices with modems are not permitted unless approved by the Director, Division of Security Services. For those workstations authorized to have modems, the modem and telecommunication line must be configured to permit outbound dialing only. An auto-answering modem attached to a workstation is an easy target and method to subvert perimeter security (modem banks, Firewalls, etc.) and gain unauthorized access to internal networks. 2.5 Unattended Workstation Processing If workstations are connected to a network and are not performing specialized approved background functions such as monitoring or logging, when unattended, they must always be logged out. Workstation must be shut down and powered off at the end of the day. For specialized workstations that cannot be logged off, measures such as screensavers or physical security access to keyboards must be employed. 2.6 Supplemental Encryption Data that has been identified to be sensitive in nature by the data owner must be encrypted with the aid of approved encryption programs when stored on disks, tapes, or other media. Potential standards and tools are currently under review. 2.7 Authorized Applications Only GOT authorized applications and utilities may be loaded on user workstations. Installing unauthorized applications can impact the performance of the workstation and potentially circumvent security controls implemented by GOT. Unauthorized applications will be removed and the user will be subject to possible disciplinary actions. 2.8 Workstations that Employ Password Controls For workstations that employ operating systems software that have the capability to enact password restrictions, such as Microsoft Windows NT, those capabilities must be configured and enabled.

Source Reference	http://csrc.nist.gov/fasp/FASPDocs/security-ate/ISSO-participant-book.doc		
Standards Organizations			
Name	National Institute of Standards and Technology (NIST) http://csrc.nist.gov/	*Website*	csrc.nist.gov
Contact Information	cert@cert.org		
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
KEYWORDS			
Keywords/Aliases	Workstation, security, policy,		
COMPONENT CLASSIFICATION			
Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Rationale for Component Classification			
Conditional Use Restrictions			
Restrictions			
Migration Strategy			
Migration Strategy			
Impact Position Statement			
Position Statement on Impact			
CURRENT STATUS			
Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	5/19/2004	*Date Accepted / Rejected*	5/19/2004
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

Click on this link to return to the Security Blueprint Samples – Set One.

Discipline Blueprint

DEFINITION	
Name	Discipline – Network Security
Description	Defines the roles, standards, policies, and tools for monitoring and ensuring the security across the organization's network.
Rationale	As enterprise information systems become increasingly decentralized, the responsibility for security becomes distributed across the various operating locations. Therefore, it is essential that all aspects of security, including security policies, procedures, information-system-based controls and network security be coordinated, monitored, audited and enforced.
Benefits	

BOUNDARY	
Boundary Limit Statement	Network security includes the physical/electrical links between the desktop client and the host computer. This responsibility is generally split between agencies with the user agency and DISC performing part of the functions. In view of this, maintain close cooperation between these groups. The LAN and WAN links must be reviewed and evaluated for security needs. The use of the Internet and dial-up connections to facilitate traveling staff places an additional burden on this analysis; since those links can not be controlled and therefore carry a greater risk of being compromised. The following areas are also covered under Network Security: • Web security – covers firewalls, DMZs, etc. • Electronic Transaction Security- the transmissions into and out of the State's host computers. Includes all types of information sharing: e-mail, file transfer, electronic data interchange, etc.

ASSOCIATED DOMAIN	
Domain Name	Security

CRITICAL REFERENCES

Related Domains/Disciplines

Domain-Disciplines		*Domain-Disciplines*		*Domain-Disciplines*	
☐	*Interface – Branding*	☒	*Integration – Functional Integration*	☒	*Systems Mgt – Business Continuity*
☒	*Interface – Access*	☒	*Integration – Middleware*	☐	*Security – Enterprise Security*
☐	*Interface – Accessibility*	☐	*Application – Application Engineering*	☒	*Security – Network Security*
☒	*Information – Knowledge Mgt*	☐	*Application – Electronic Collaboration*	☒	*Security – Host Security*
☒	*Information – Data Mgt*	☐	*Systems Mgt – Asset Mgt*	☐	*Privacy – Profiling*
☒	*Information- GIS*	☒	*Systems Mgt – Change Mgt*	☐	*Privacy – Personification*
☒	*Infrastructure - Network*	☒	*Systems Mgt – Console/Event Mgt*	☐	*Privacy – Privacy*
☐	*Infrastructure - Platform*	☒	*Systems Mgt – Help Desk/Problem Mgt*		

Standards Organizations			
Name	International Organization for Standardization	*Web Address*	http://www.iso.ch/iso/en/ISOOnline.frontpage
Contact Information	**ISO Central Secretariat:** International Organization for Standardization (ISO) 1, rue de Varembé, Case postale 56 CH-1211 Geneva 20, Switzerland Email: central@iso.org Telephone + 41 22 749 01 11; Telefax + 41 22 733 34 30;		
Name	National Institute of Standards and Technology (NIST)	*Web Address*	http://www.nist.gov/ - NIST Homepage
Contact Information	**NIST** 100 Bureau Drive, Stop 3460 Gaithersburg, MD 20899-3460 Email: inquiries@nist.gov Phone: (301) 975-NIST (6478) or TTY (301) 975-8295		
Name	Institute of Electrical and Electronics Engineers, Inc (IEEE)	*Web Address*	http://www.ieee.org/ - IEEE Home Page
Contact Information	**IEEE-USA** 1828 L Street, N.W., Suite 1202 Washington, D.C. 20036-5104 Email: ieeeusa@ieee.org Tel: +1 202 785 0017 Fax: +1 202 785 0835		
Government Bodies			
Name	None Identified	*Web Address*	
Contact Information			
Stakeholders/Roles			
Stakeholders	Systems Analysts, Network Personnel, Applications Developer, Applications Testing Team, Third-Party Network Vendors, System Administrators, Security Personnel, Configuration Management Team, Help Desk Personnel		
Roles (if stakeholder title is not known)			
Discipline-specific Trends			
Trend Statement			
Trend Source			
METHODOLOGIES			
Methodologies Followed			
ASSOCIATED COMPLIANCE COMPONENTS			
Compliance Component Names	Secure Sockets Layer (SSL) Electronic Communications Privacy Act of 1986 (Public Law 99-508) IEEE 802.10-1998, IEEE Standard for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS) IEEE 802.10a-1999, Supplement to 802.10-1998, Standard for Interoperable LAN/MAN Security (SILS) - Security Architecture Framework IEEE 802.10c-1998, Supplement to 802.10-1998, Key management (Clause 3) FIPS 146-2, TCP/IP for wide-area network transmission. RFC 791 as the definition of IP for wide area network transmission. Open Systems Interconnection (OSI) Reference Model (ISO/DIS 7498) Telecommunications Security: Electronic Signature Standardization Report European Telecommunications Standards Institute		

ASSOCIATED TECHNOLOGY AREAS			
Technology Areas	Network Security Web security Electronic Transaction Security		
DISCIPLINE DOCUMENTATION REQUIREMENTS			
Documentation requirements for this Discipline	(This discipline will be documented to the product level and the compliance components associated with the product version, family etc…)		
CURRENT STATUS			
Discipline Status	☐ *In development* ☐ *Under Review* ☐ *Rejected* ☒ *Accepted*		
AUDIT TRAIL			
Creation Date	4/16/2002	*Date Accepted/Rejected*	
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

Click on this link to return to the Security Blueprint Samples – Set One.

SECURITY BLUEPRINT SAMPLES – SET TWO

The second set of sample Blueprints from a Security Domain represent an additional set of Discipline, Technology Areas and Compliance Components. This sample addresses the Disciplines of Management, Operational and Technical Controls. The Security Domain Blueprint has not been repeated.

- Discipline – Management Controls
- Discipline – Operational Controls
- Technology Area – Incident Response
- Compliance Component – Incident Response Reporting
- Compliance Component – Risk Level Awareness & Countermeasures
- Discipline – Technical Controls
- Technology Area – Identification/Authentication
- Compliance Component – Password Controls
- Technology Area – Virus Detection & Elimination
- Compliance Component – Criteria for E-Mail
- Compliance Component – Criteria for Gateways
- Compliance Component – Criteria for Server
- Compliance Component – Criteria for Workstation
- Compliance Component – Criteria for Wireless
- Technology Area – Intrusion Detection Systems
- Compliance Component – Network Based IDS
- Compliance Component – Host Based IDS
- Compliance Component – Application Based IDS
- Technology Area – Logical Access Controls
- Compliance Component – Date/Time Controls
- Compliance Component – Inactivity Controls
- Compliance Component – Logon Banners

Domain	*Discipline*	*Technology Area*	*Product Component*	*Compliance Component*
Security	Management Controls			
	Operational Controls	Incident Response		• Incident Response Reporting • Risk Level Awareness & Countermeasures
	Technical Controls	Identification / Authentication		• Password Controls
		Virus Detection & Elimination		• Criteria for E-Mail • Criteria for Gateways • Criteria for Server • Criteria for Workstation • Criteria for Wireless
		Intrusion Detection Systems		• Network Based IDS • Host Based IDS • Application Based IDS
		Logical Access Controls		• Date/Time Controls • Inactivity Controls • Logon Banners

Again, a reminder that some of the sample Blueprints were completed using earlier versions of the templates and, while the information that was gathered is the same, it may be presented in a slightly different order or have a slightly different heading or topic title than the latest template versions, which were presented earlier within this document.

Discipline Blueprint

Definition	
Name	Discipline – Management Controls
Description	Management Controls are techniques and concerns, normally addressed by management, regarding the organization's computer security strategy. It includes the mitigation of risk within the organization.
Rationale	Addresses security within a business context and provides implementation authority.
Benefits	Promotes trust, maintains continuous business flow, provides guidance
Boundary	
Boundary Limit Statement	Security controls that focus on the management of the enterprise security programs and managing security risks.
Boundary Topics	Life Cycle Management; Risk Management; Review of Security Controls; System Certification and Accreditation; System Security Planning; Personnel Security
Associated Domain	
Domain Name	Security

Critical References

Related Domains/Disciplines

☐	*Interface – Branding*	☐	*Integration – Functional Integration*	☐	*Systems Mgt – Business Continuity*
☐	*Interface – Access*	☐	*Integration – Middleware*	☒	*Security – Management Controls*
☐	*Interface – Accessibility*	☐	*Application – Application Engineering*	☒	*Security – Operational Controls*
☐	*Information – Knowledge Mgt*	☐	*Application – Electronic Collaboration*	☒	*Security – Enterprise Security*
☐	*Information – Data Mgt*	☐	*Systems Mgt – Asset Mgt*	☒	*Security – Network Security*
☐	*Information- GIS*	☐	*Systems Mgt – Change Mgt*	☒	*Security – Host*
☐	*Infrastructure - Network*	☐	*Systems Mgt – Console/Event Mgt*	☐	*Privacy – Profiling*
☐	*Infrastructure - Platform*	☐	*Systems Mgt – Help Desk/Problem Mgt*	☐	*Privacy – Personification*
				☐	*Privacy – Privacy*

Standards Organizations/Government Bodies

Standards Organizations	National Institute of Standards & Technology (NIST) Computer Security Resource Center International Organization for Standardization (ISO)	*Web Address*	http://csrc.nist.gov/ http://www.iso.ch/iso/en/ISOOnline.frontpage
Government Bodies	NSA, FBI, Department of Homeland Security		

Stakeholders/Roles			
Stakeholders	Executive Management – Department Director, Department CIO, Department CFO, etc.		
Roles	Decision makers; administrative authority		
Discipline-specific Trends			
Trend Statement			
Trend Source			
METHODOLOGIES			
Methodologies followed	National Institute of Standards and Technologies (NIST), Computer Security Resource Center		
ASSOCIATED COMPLIANCE COMPONENTS			
Compliance Component Names			
ASSOCIATED TECHNOLOGY AREAS			
Technology Areas	Information Classification; Personnel Security; Security Risk Management; Vulnerability Testing		
DISCIPLINE DOCUMENTATION REQUIREMENTS			
Documentation requirements for this Discipline			
CURRENT STATUS			
Discipline Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	12-19-2002	*Date Accepted / Rejected*	01-21-2003
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

Click on this link to return to the Security Blueprint Samples – Set Two.

Discipline Blueprint

DEFINITION	
Name	Discipline – Operational Controls
Description	Operational Controls are procedures implemented and executed by people, as opposed to systems, to improve the security of a system or group of systems. They often require technical or specialized expertise and may rely upon management activities as well as technical controls.
Rationale	Provides consistent controls to secure the enterprise.
Benefits	Promotes standardization, structure, and consistent behavior; Defines responsibilities related to security operations.
BOUNDARY	
Boundary Limit Statement	Controls implemented and executed by people, including policies and procedures
Boundary Topics	Physical Security; Production, Input/Output Controls; Contingency Planning; Hardware & Systems Security Software Maintenance; Data Verification; Security Documentation; Security Awareness, Training & Education; Incident Response Capability
ASSOCIATED DOMAIN	
Domain Name	Security

CRITICAL REFERENCES

Related Domains/Disciplines

☐	*Interface – Branding*	☐	*Integration – Functional Integration*	☐	*Systems Mgt – Business Continuity*
☐	*Interface – Access*	☐	*Integration – Middleware*	☒	*Security – Management Controls*
☐	*Interface – Accessibility*	☐	*Application – Application Engineering*	☒	*Security – Operational Controls*
☐	*Information – Knowledge Mgt*	☐	*Application – Electronic Collaboration*	☒	*Security – Enterprise Security*
☐	*Information – Data Mgt*	☐	*Systems Mgt – Asset Mgt*	☒	*Security – Network Security*
☐	*Information- GIS*	☐	*Systems Mgt – Change Mgt*	☐	*Security – Host*
☐	*Infrastructure – Network*	☐	*Systems Mgt – Console/Event Mgt*	☐	*Privacy – Profiling*
☐	*Infrastructure – Platform*	☐	*Systems Mgt – Help Desk/Problem Mgt*	☐	*Privacy – Personification*
				☐	*Privacy – Privacy*

Standarda Organizations

Name	National Institute of Standards & Technology (NIST) Computer Security	*Web Address*	http://csrc.nist.gov/

	Resource Center		
Name	International Organization for Standardization (ISO)	*Web Address*	http://www.iso.ch/iso/en/ISOOnline.frontpage
Name	SysAdmin, Audit, Network, Security (SANS)	*Web Address*	http://www.sans.org/newlook/home.php
Government Bodies			
Government Bodies	HIPPA, DOT, local government		
Stakeholders/Roles			
Stakeholders	System Administrators; security officers; facility managers		
Roles	Implementers		
Discipline-specific Trends			
Trend Statement			
Trend Source			
METHODOLOGIES			
Methodologies followed	National Institute of Standards & Technology (NIST), Computer Security Resource Center		
ASSOCIATED COMPLIANCE COMPONENTS			
Compliance Component Names			
ASSOCIATED TECHNOLOGY AREAS			
Technology Areas	Authorization; Data Verification; Event Monitoring/Analysis; Fire/Safety Factors / Supporting Utilities; Incident Response; Message Authentication; Password Policy Controls; Penetration Testing; Physical Access Control; Portable System Controls (Phys Access); Security Awareness; Security Education; Security Skills Training / Certification; Virus Detection & Elimination		
DISCIPLINE DOCUMENTATION REQUIREMENTS			
Documentation requirements for this Discipline			
CURRENT STATUS			
Discipline Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		

AUDIT TRAIL			
Creation Date	12-19-2002	*Date Accepted / Rejected*	01-21-2003
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

Click on this link to return to the Security Blueprint Samples – Set Two.

Technology Area Blueprint

Definition			
Name	Technology Area - Incident Response		
Description	Incident Response capability is a combination of technically skilled people, policies, procedures, and techniques that constitute a proactive approach to handling computer security incidents.		
Rationale	Provides a consistent approach to handling security incidents.		
Benefits	Consistent method of evaluation and associate metrics; decrease spread; minimize damage; fulfills risk mitigation; limits impacts; promotes awareness; proactively improves network assurance; increases communication		
Associated Dicipline			
Discipline Name	Operational Controls		
Keywords			
Keywords/Aliases	Incident reporting; intrusion detection; exposure; vulnerability; INFOCON; attack; incident impacts; defense; threat; risk; alerts; countermeasure; communication; denial of service		
Associated Compliance Components			
Compliance Component Names	❑ Incident Reporting Procedures ❑ Incident Risk Level Assessment and Countermeasures		
Associated Product Components			
Product Component Names			
Technology Area Detail			
Supporting Documentation	NIST Special Publication: SP-800-3 Establishing a Computer Security Incident Response Capability (CSIRC) – November 1991		
Source Reference	http://csrc.nist.gov/publications/nistpubs/800-3/800-3.pdf		
Standards Organization / Government Body			
Name	NIST	*Website*	http://www.nist.gov/
Contact Information	National Institute of Standards and Technology (301) 975-NIST		
Current Status			
Technology Area Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
Audit Trail			
Creation Date	12-19-2002	*Date Accepted / Rejected*	01-21-2003
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

Click on this link to return to the Security Blueprint Samples – Set Two.

Compliance Component Blueprint

Definition	
Name	Compliance Component - Incident Response Reporting
Description	Plan and procedures to help ensure the State's IT community is aware of information security threats and concerns. Plan and Procedures should record and document the following: • Attempts (failed or successful) to gain unauthorized access to systems or data; • Unwanted disruption or denial of service; • The unauthorized use of a system for the transmission, processing or storage of data; • Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction or consent.
Rationale	Minimizes the damage from security incidents and facilitates communication throughout State agencies.
Benefits	Promotes awareness of incidents; allows for monitoring; builds knowledge base – collecting the right information enables the creation of useful reports (big picture/patterns); standardization

Associated Architecture Levels	
Domain Name	Security
Discipline Name	Operational Controls
Technology Area Name	Incident Response
Product Component Name	

Compliance Component Type	
Component Type	Guideline
Component Sub-type	

Compliance Detail	
Guideline, Standard or Legislation	State Incident Response Plan and Procedures
Source Reference	

Standards Organization			
Name	OA Information Security Management Office (ISMO)	*Website*	
Contact Information			

Government Body			
Name	Information Technology Advisory Board (ITAB)	*Website*	
Contact Information	Security Committee		

Keywords	
Keywords/Aliases	INFOCON; intrusion detection; exposure; vulnerability; attack; incident impacts; defense; threat; risk; alerts; communication; denial of service

Component Classification				
Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*

Rationale for Component Classification			
Rationale for Component Classification	Currently the active plan and procedures authorized by Information Technology Advisory Board.		
Conditional Use Restrictions			
Restrictions			
Migration Strategy			
Migration Strategy			
Impact Position Statement			
Position Statement on Impact			
CURRENT STATUS			
Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	12-19-2002	*Date Accepted / Rejected*	01-21-2003
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

Click on this link to return to the Security Blueprint Samples – Set Two.

Compliance Component Blueprint

Definition	
Name	Compliance Component - Incident Risk Level Awareness, Assessment and Countermeasures
Description	Actions to uniformly heighten or reduce defensive posture, to defend against computer network attacks, and to mitigate sustained damage to the State information infrastructure, including computer and telecommunications networks and systems. This is a comprehensive defense posture and protocol based on the status of information systems, sustaining operations, and intelligence assessments of adversary capabilities and intent.
Rationale	Incidents impact all personnel who use State information systems. Awareness, assessment, and countermeasures protect systems while supporting mission accomplishment, and coordinate the overall effort through adherence to guidelines.
Benefits	The State gains standard processes for assessing threats to the information infrastructure, and prescribes predictable responsive actions. When implemented consistently, each member of the State's enterprise will have reasonable assurance that other members of the network present no greater vulnerability than the defined baseline standards. Provides an opportunity for the technology community to make senior management aware there is a constant battle to maintain network security, and that the entire State government is moving proactively to improve network assurance.

Associated Architecture Levels			
Domain Name	Security		
Discipline Name	Operational Controls		
Technology Area Name	Incident Response		
Product Component Name			
Compliance Component Type			
Component Type	Standard		
Component Sub-type			
Compliance Detail			
Guideline, Standard or Legislation	INFOCON (INFormation Operations CONdition) System for State Agencies -- Nov 19, 2002		
Source Reference			
Standards Organization			
Name	Information Technology Advisory Board (ITAB)	*Website*	
Contact Information	Security Committee		
Government Body			
Name		*Website*	
Contact Information			
Keywords			
Keywords/Aliases	INFOCON; countermeasure; incident reporting; intrusion detection; exposure; vulnerability; attack; incident impacts; defense; threat; risk; alerts; risk level		

COMPONENT CLASSIFICATION			
Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Rationale for Component Classification	Established by the State Office of Information Technology (OIT), with the consensus of the Office of Homeland Security (OHS), at the recommendation of the Information Technology Advisory Board (ITAB).		
Conditional Use Restrictions			
Restrictions	N/A		
Migration Strategy			
Migration Strategy	N/A		
Impact Position Statement			
Position Statement on Impact			
CURRENT STATUS			
Current Status)	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	12-19-2002	*Date Accepted / Rejected*	01-21-2003
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

Click on this link to return to the Security Blueprint Samples – Set Two.

Discipline Blueprint

DEFINITION	
Name	Discipline - Technical Controls
Description	Technical Controls are security controls executed by computer systems, as opposed to people. The implementation of technical controls requires significant operational consideration and should be consistent with the management of security within the organization.
Rationale	Identifies automated controls that improve system security.
Benefits	Promotes standardization, trust, interoperability, connectivity, automation, and increased efficiency.
BOUNDARY	
Boundary Limit Statement	Security controls implemented and executed by systems and/or machines.
Boundary Topics	Identification and Authentication; Logical Access Controls; Audit Trails
ASSOCIATED DOMAIN	
Domain Name	Security

CRITICAL REFERENCES

Related Domains/Disciplines

☐	*Interface – Branding*	☐	*Integration – Functional Integration*	☐	*Systems Mgt – Business Continuity*
☐	*Interface – Access*	☐	*Integration – Middleware*	☒	*Security – Management Controls*
☐	*Interface – Accessibility*	☐	*Application – Application Engineering*	☒	*Security – Operational Controls*
☐	*Information – Knowledge Mgt*	☐	*Application – Electronic Collaboration*	☒	*Security – Technical Controls*
☐	*Information – Data Mgt*	☐	*Systems Mgt – Asset Mgt*	☐	*Privacy – Profiling*
☐	*Information- GIS*	☐	*Systems Mgt – Change Mgt*	☐	*Privacy – Personification*
☐	*Infrastructure - Network*	☐	*Systems Mgt – Console/Event Mgt*	☐	*Privacy – Privacy*
☐	*Infrastructure - Platform*	☐	*Systems Mgt – Help Desk/Problem Mgt*		

Standards Organizations/Government Bodies	
Standards Organizations	National Institute of Standards & Technology (NIST) Computer Security Resource Center http://csrc.nist.gov/ International Organization for Standardization (ISO) http://www.iso.ch/iso/en/ISOOnline.frontpage SysAdmin, Audit, Network, Security (SANS) http://www.sans.org/newlook/home.php
Government Bodies	
Stakeholders/Roles	
Stakeholders	Network Administrators, CIT, CIS, etc.
Roles	Technical personnel

Discipline-specific Trends			
Trend Statement			
Trend Source			
METHODOLOGIES			
Methodologies followed	National Institute of Standards & Technology (NIST), Computer Security Resource Center		
ASSOCIATED COMPLIANCE COMPONENTS			
Compliance Component Names			
ASSOCIATED TECHNOLOGY AREAS			
Technology Areas	Access Controls; Cryptography; Date / Time Controls; Entity Authentication; Intrusion Detection Systems; Inactivity Controls; Log-on Banners; Remote Access; Secure Gateways / Firewalls		
DISCIPLINE DOCUMENTATION REQUIREMENTS			
Documentation requirements for this Discipline			
CURRENT STATUS			
Discipline Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	12-19-2002	*Date Accepted / Rejected*	01-21-2003
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

Click on this link to return to the Security Blueprint Samples – Set Two.

DEFINITION	
Name	Technology Area - Identification and Authentication
Description	Identification and Authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Identification is a unique way of identifying each individual (e.g., a unique user name or ID). Authentication is the mechanism that verifies that an individual is who they claim to be. Verification is based on one or more of the following: • Something known (e.g., a password or pin); • Something carried (e.g., a smart card or a token); • Something the individual is (e.g., biometrics – like a fingerprint).
Rationale	Hardware platforms, operating systems, application-specific constraints, and overall financial or confidentiality risk are factors that influence the need for identification and authentication controls. System and application developers are responsible for designing strong authentication into the systems they build, and individual users are responsible for assisting in the protection of the systems they use. Identification and Authentication are the first lines of defense to protect enterprise system assets from unauthorized access, destruction or theft.
Benefits	• If identification and authentication are not handled correctly, they are the weakest link in the protection of enterprise systems and data. • Identification and authentication provides user accountability and auditable trails of user access. • Identification and authentication helps prevent unauthorized persons from entering enterprise IT systems.
ASSOCIATED DISCIPLINE	
Discipline Name	Technical Controls
KEYWORDS	
Keywords/Aliases	Passwords, password controls, digital signatures, access cards, smart cards, tokens, biometrics, user name, user ID, PIN, logon ID
ASSOCIATED COMPLIANCE COMPONENTS	
Compliance Component Names	• Password Controls
ASSOCIATED PRODUCT COMPONENTS	
Product Component Names	
TECHNOLOGY AREA DETAIL	
Supporting Documentation	NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems
Source Reference	www.csrc.nist.gov/publications/nistpubs
Standards Organization / Government Body	

Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
Name	National Security Agency (NSA), Security Recommendation Guides	*Website*	http://nsa2.www.conxion.com/index.html
Contact Information	W2KGuides@nsa.gov		
CURRENT STATUS			
Technology Area Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	02/13/2003	*Date Accepted / Rejected*	03/24/2003
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

Click on this link to return to the Security Blueprint Samples – Set Two.

Compliance Component Blueprint

Definition	
Name	Compliance Component - Password Controls
Description	Password Controls apply to information technology systems and processes that create, modify, or use information that is private/confidential or of significant value to the organization. All such systems shall adhere to the minimum acceptable standards for system authentication by means of a password. A password is a sequence of characters obtained by a selection or generation process from a set of acceptable controls.
Rationale	A login ID with a secret password is the most common method of authenticating users to a computer system or application, and often the only technical control employed. For systems that rely upon password protection, system administrators shall institute strong password controls, and users shall be responsible for creating strong passwords and keeping them secret.
Benefits	• Password controls provide a method to authenticate users. • Passwords represent a first line of defense, and if not handled correctly, they can be the weakest link in the enterprise. • Strong password controls reduce the threat of password compromise as an avenue of attack on computer resources. • Password controls help prevent unauthorized persons from entering IT systems. • Password Controls provide user accountability.

Associated Architecture Levels	
Domain Name	Security
Discipline Name	Technical Controls
Technology Area Name	Identification and Authentication
Product Component Name	

Compliance Component Type	
Compliance Component Type	Guideline
Component Sub-type	

Compliance Detail	
Guideline, Standard or Legislation	**Password Control Guidelines** Systems that do not support external identification and authentication via an application-programming interface, or do not natively support the minimum password controls outlined in these guidelines, shall be considered candidates for upgrade or replacement. **General Password Requirements** • All enterprise systems and applications shall utilize, as a minimum form of security, a unique user identifier and a secret password as a means of authentication. • Internal network devices (routers, firewalls, access control servers, etc.) shall be password protected. • Default system or device passwords must be changed. • Passwords shall not be hard coded into software unless they are encrypted.

- All enterprise systems should provide automated support of password controls.
- Passwords issued initially or reset by systems or administrators shall be uniquely defined for each user.
- Proof of identity shall be presented to the administrator for user password resets, such as photo ID, supervisor verification, or knowledge of a shared secret.
- If intervention is required, only administrators are authorized to reset, change or disable user passwords.
- Password resets or changes shall be promptly confirmed with the user. The confirmation method is at the discretion of each agency (e.g., phone, e-mail, registered mail, etc.).
- Passwords shall be changed after a system compromise or after the threat of a system compromise, such as the termination of a system administrator, security level change, etc.
- Users shall promptly change all passwords if they suspect or know unauthorized parties received the passwords or they have shared it in the course of getting help with a problem.
- Passwords shall be different for State (internal) and non-State (external) networks and systems, such as local ISP.
- Restricted public access systems or machines that have no access to critical State systems or data are exemptions to State password controls.

Password Composition Requirements

Passwords are made up of various characters, which can be broken down into four character groups. These are uppercase alphabetic, lowercase alphabetic, numeric, and special characters. Requiring complex passwords also increases the time necessary to crack passwords exponentially.

- Passwords for all systems are subject to the following password composition rules:
  - Password shall contain characters from at least three of the following four categories:
    - English Uppercase Alphabetic (A - Z)
    - English Lowercase Alphabetic (a - z)
    - Numeric Base-ten digits (0 – 9)
    - Special characters (e.g., exclamation point [!], dollar sign [$], pound sign [#], percent sign [%], asterisk [*], etc.)
    - Passwords are not to be your name, address, date of birth, username, nickname, or any term that could be easily guessed by someone who is familiar with you.
    - Passwords are not to be related to the job or personal life, e.g., not a license plate number, spouse's name, telephone number, etc.
    - Passwords are not to be dictionary words or proper names, places or slang.
    - Passwords may not contain all or part (3 or more sequential characters) of the user's account or login name.
    - Passwords shall not contain characters that do not change combined with characters that predictably change when changing passwords upon expiration. For example, users may not choose passwords like "x345JAN" in January, "x345FEB" in February, etc., or identical or substantially similar to passwords the user previously chose.

Password Lifetime Requirements

The purpose for requiring password lifetime restrictions is to prevent users from using their favorite password until it expires, and changing their password more

	times than the system remembers, and cycling back to their favorite password, thus circumventing the system. • Passwords for all systems are subject to the following password aging and history rules: – Password age shall not exceed 90 days. However, passwords should be changed on a more frequent basis commensurate with the sensitivity, criticality and value of the information it protects. – Administrator password age shall not exceed 60 days. – Any default or initial password issued by a security administrator shall be valid only for the user's first logon session. – Systems shall maintain an encrypted history of previously used passwords per logon ID. – Password history files should contain, at a minimum, the last 24 passwords particular to a logon ID to ensure that users do not cycle through regular passwords. – The minimum password age is 1 day (24 hours). **Password Length Requirements** *A 7-character password made up of only lowercase characters has 26^7 possible passwords. A 7 character password made up of uppercase, lowercase, and special characters (on a standard 104 key keyboard) has 95 possible keys (excluding control characters) that make for 95^7 possible password combinations. That's nearly the "simple" set of passwords to the power of four!* • All passwords shall be at least 7 characters in length. • Passwords that do not comply with the frequency portion of the Password Lifetime Requirements above, such as system service passwords, shall be at least 14 characters in length. **Password Source Requirements** • Only end-users or automated processes shall generate passwords. **Password Ownership Requirements** • Passwords for all systems are subject to the following password ownership rules: – Users shall not disclose their password to anyone. – No passwords are to be spoken, written, e-mailed, hinted at, shared, or in any way known to anyone other than the user involved. – User-initiated password changes shall be supported on enterprise networks and systems. **Password Storage Requirements** • Passwords for all State IT systems are subject to the following password storage rules: – Personnel shall not record their passwords unless they have a secure method of storing them, such as saving them in an encrypted file or storing them in a locked safe. – Passwords area not to be displayed or concealed at the user's workspace. – Passwords shall not be stored in dial-up communications programs or Internet browsers. – Passwords stored and transmitted over open networks shall be encrypted. **Password Entry Requirements** *One method of gaining access to a computer system is to continuously access systems, using common account names, and different passwords until one works.*

	Dictionary attacks use lists of common words as passwords in attempts to logon to a system. They are often successful against weak passwords. Brute force attacks attempt to use every possible character combination as a password, and will always be successful given enough time. *In order to combat these attacks, password entry requirements are established to disable an account after a specified number of failed logins occurs during a defined period of time. That account will remain locked out for a defined period of time. Enabling lockout policies make these attacks mathematically infeasible.* • After a maximum of five invalid password or unsuccessful access attempts, one of the following actions shall be enforced: – Disable or revoke the account until intervention by a system administrator. – Suspend the account for at least 30 minutes. – Disconnect if dial-up or other external network connection. **Password Auditing Requirements** • An authorized system administrator shall audit all passwords to ensure compliance with password guidelines.		
Source Reference	N/A		
Standards Organizations			
Name		*Website*	
Contact Information			
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
Name	National Security Agency (NSA), Security Recommendation Guides	*Website*	http://nsa2.www.conxion.com/index.html
Contact Information	W2KGuides@nsa.gov		
KEYWORDS			
Keywords/Aliases	Passwords, password controls, digital signatures, access cards, smart cards, tokens, biometrics, user name, user ID, PIN, logon ID, dial-up, lost, forgotten		
COMPONENT CLASSIFICATION			
Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Rationale for Component Classification			
Conditional Use Restrictions			
Restrictions			
Migration Strategy			
Migration Strategy			
Impact Position Statement			

Position Statement on Impact			
CURRENT STATUS			
Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	02-13-2003	*Date Accepted / Rejected*	03-24-2003
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

Click on this link to return to the Security Blueprint Samples – Set Two.

DEFINITION	
Name	Technology Area - Virus Detection and Elimination
Description	Virus Detection and Elimination addresses those policies, methods and tools associated with detecting, combating, reporting and eradicating malicious program code (e.g., worms, Trojan horse, malware). A virus usually has a destructive or disruptive effect on the executable program or system component that it affects.
Rationale	Provide a scalable multi-tiered defense to fend off virus threats and prevent loss of time and money.
Benefits	Protect assets (i.e., data and resources) from corruption, disruption, destruction, and unavailability. Can assist in the system quarantine, repair and clean-up virus damage.
ASSOCIATED DISCIPLINE	
Discipline Name	Technical Controls
KEYWORDS	
Keywords/Aliases	virus, zoo, trojan horse, backdoor, worm, stealth, blended threat, boot sector infector, companion, denial of service, dropper, file infector, logic bomb, malware, multi-partite, overwriting, parasitic, polymorphic, tunneling, variant, terminate and stay resident (tsr), management; boot sector infector
ASSOCIATED COMPLIANCE COMPONENTS	
Compliance Component Names	• Virus Detection and Elimination Policies and Best Practices • Virus Detection and Elimination Criteria for Anti-Virus Management Tools • Virus Detection and Elimination Criteria for Gateways • Virus Detection and Elimination Criteria for E-mail/Groupware • Virus Detection and Elimination Criteria for Servers • Virus Detection and Elimination Criteria for Workstations • Virus Detection and Elimination Criteria for Wireless
ASSOCIATED PRODUCT COMPONENTS	
Product Component Names	• McAfee – VirusScan (workstation) – NetShield (server) – Groupshield (e-mail) – WebShield Appliances(gateway) – EPolicy Orchestrator (management tool) – VirusScan Wireless Devices (wireless) • Symantec – AntiVirus Corporate Edition (workstation) – AntiVirus Corporate Edition (server) – AntiVirus Corporate Edition (e-mail) – AntiVirus Corporate Edition (gateway) – AntiVirus Corporate Edition (management tool) • Sybari Software Inc. – Antigen for Microsoft Exchange (e-mail) – Antigen for Lotus Notes/Domino (e-mail) ○ Antigen for Microsoft Exchange (gateway) • Computer Associates – InoculateIT (workstation)

	- InoculateIT (server) - InoculateIT (management tool)		
TECHNOLOGY AREA DETAIL			
Supporting Documentation	• NIST 800-5 and 500-1166 • Gartner Research Group – Enterprise Anti-Virus product evaluation. Release Note 22 May 2002		
Source Reference			
Standards Organizations / Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
Name	ICSA Labs	*Website*	www.icsalabs.com
Contact Information	ICSA Labs is a division of TruSecure Corporation and can be reached at 1-888-396-8348 (info@trusecure.com)		
CURRENT STATUS			
Technology Area Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	02-06-03	*Date Accepted / Rejected*	02-27-2003
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

Click on this link to return to the Security Blueprint Samples – Set Two.

DEFINITION	
Name	Compliance Component - Virus Detection and Elimination Criteria for E-Mail
Description	To make available to the State Enterprise a set of minimum criteria for the selection of anti-virus software and products for security protection of E-mail and Groupware applications.
Rationale	All E-mail and Groupware applications within the State computer environment shall execute an anti-virus security product that conforms to a minimum set of compliance criteria. These criteria shall serve as a checklist to help administrators choose the appropriate anti-virus solution for their environment.
Benefits	To significantly improve E-mail and Groupware trust and security through a set of criteria for the following security services: 1. Protection to E-mail and Groupware application systems from computer virus intrusion. 2. Detection of computer viruses on an infected E-mail or Groupware applications. 3. E-mail and Groupware application recovery from a computer virus infection.

ASSOCIATED ARCHITECTURE LEVELS	
Domain Name	Security
Discipline Name	Technical Controls
Technology Area Name	Virus Detection and Elimination
Product Component Name	

COMPLIANCE COMPONENT TYPE	
Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	
Guideline, Standard or Legislation	**Virus Detection and Elimination Criteria for E-Mail and Groupware Applications** State E-mail and Groupware applications shall be protected with anti-virus software and procedures that meet the checklist of criteria detailed in the following service areas. <u>General E-mail and Groupware Anti-Virus Criteria</u> • Virus scanner software shall be run on all E-mail and Groupware applications even if the networks perimeter devices are scanning for viruses. • Anti-virus software shall use a separate and configurable agent specifically designed to protect E-mail and Groupware applications. • All E-mail and Groupware applications shall be scanned for viruses at least once a day. • E-mail and Groupware anti-virus software shall provide integration capabilities with an enterprise anti-virus policy management suite. • All State E-mail and Groupware applications shall execute a virus scan product certified by the ICSA Labs (http://www.icsalabs.com). ICSA Labs certification requires anti-virus products to detect 100% of all viruses "in the wild" as captured by the WildList Organization International (http://www.wildlist.org).

	Virus Detection/Scanning Capabilities • Anti-virus software shall be capable of detecting malicious software before it is executed. • Shall support both On-Access (real-time) and On-Demand (flexible) scanning capabilities. • Shall provide detection for all "in the wild" virus types (boot viruses, file viruses, macro viruses, and script viruses). • Shall provide detection for Zoo type viruses (file viruses, macro viruses, script viruses, polymorphic viruses, other malware, false positives). • Shall provide detection for archived and compressed file types (ZIP, TAR, LZH, recursive and self-extracting archives, runtime-compressed files). • Shall provide scanning capabilities for all standard office file formats (including embedded OLE objects and password protected files). • Shall provide for flexible configuration to include/exclude file types, drives and directories from scans. • Shall support both Inbound and Outbound real-time scan protection of E-mail. • Shall support customizable e-mail message and attachment scanning, blocking and quarantine. • Shall provide Heuristic-scanning capabilities (intelligent analysis of unknown or suspicious sections of messages, attachments and code). • Shall support multi-mode scanning (Windows platforms only) to protect Windows API, ESE, and MAPI. E-mail Content Filtering • E-Mail and Groupware anti-virus products shall support the filtering of e-mail messages for tailored anti-viral support including filtering on items such as: – E-mail file size – Sender name (virus@malicious.com) – DNS extension name (@dns.com) – Subject line – Message body context – Attachment name – Multiple criteria Virus Reporting Capabilities • Anti-virus software shall provide the ability for detection notification via both audio and visual alerts. • Anti-Virus software must provide remote notification of administrative alerts via the following methods: – SMTP/E-Mail – SNMP Alerts – Log to a file – Log to an Enterprise Repository Post-Detection Anti-Virus Action Capabilities • It is highly desirable that anti-virus software be able to eradicate malicious software and viruses detected through the following means: – Quarantine – moving the infected file into an area where it cannot cause more harm. – Virus Removal – allows for repair of the damage caused by the virus. – Deny Access – prohibits the file from being accessed once infected. – Delete – complete removal of the infected file from the system. Anti-Virus Scan Engine Update Capabilities • Anti-virus signatures need to be updated continuously, either through a manual

	or automated process. • Shall provide a secure procedure for keeping the detection engine up-to-date with the latest detection signatures & scan engine techniques (new viruses are discovered daily) • Shall provide for automated updates of both scan engine and signatures on a scheduled interval or as needed. • Virus scan engine shall have the ability to stay up-to-date with the latest developments in malicious software detection. Anti-Virus Installation Criteria • Anti-Virus software shall be capable of automatic deployment and installation via the following: – Installation via image – anti-virus software shall be able to be included in the standard E-mail or Groupware application image deployed within the enterprise. – Remote installation – Anti-virus software shall support deployment to remote systems (dial-up, VPN, etc.) providing the same level of protection to these devices. • Anti-virus software deployment (and updates) shall be transparent to end-users. • Anti-virus software shall provide "Wizard-enabled" installation routines to automate and expedite installation. Service and Support • State virus protection products shall be backed by vendors who offer 24 x 7, 365 days a year phone support. • Anti-virus vendors shall provide a comprehensive documentation and assistance package, including a facility for pro-active timely warnings of new malicious software and virus events. • Anti-virus vendors shall provide "Virus Catalog Support" including: – A lexicon of known viruses detailing descriptions, how they are spread, what they do, how they are recognized and how to remove them. – Downloads or links to disinfection tools. – A clear and concise description of the anti-virus tools functionality, including procedures for updating the product with new detection signatures. – General advice to end-users on attacks and avoidance measures.
Source Reference	N/A

Standards Organizations			
Name	ISCA Labs	*Website*	www.iscalabs.com
Contact Information	ISCA Labs is a division of TruSecure Corporation and can be reached at 1-888-396-8348 (info@trusecure.com)		

Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
KEYWORDS			
Keywords/Aliases	Virus, virus detection, malicious code, virus products, virus reporting, anti-virus vendors, anti-virus engine, zoo, trojan horse, backdoor, worm, stealth, blended threat, boot sector infector, companion, denial of service, dropper, file infector, logic bomb, malware, multi-partite, overwriting, parasitic, polymorphic, tunneling, variant, terminate and stay resident (tsr), management, content filtering		
COMPONENT CLASSIFICATION			
Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Rationale for Component Classification			
Conditional Use Restrictions			
Restrictions			
Migration Strategy			
Migration Strategy			
Impact Position Statement			
Position Statement on Impact			
CURRENT STATUS			
Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	02-06-2003	*Date Accepted / Rejected*	02-27-2003
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

Click on this link to return to the Security Blueprint Samples – Set Two.

Compliance Component Blueprint

DEFINITION	
Name	Compliance Component - Virus Detection and Elimination Criteria for Gateways
Description	To make available to the State Enterprise a set of minimum criteria for the selection of anti-virus software and products for security protection of Gateways.
Rationale	All Gateways within the State computer environment shall execute an anti-virus security product that conforms to a minimum set of compliance criteria. These criteria shall serve as a checklist to help administrators choose the appropriate anti-virus solution for their environment.
Benefits	To significantly improve Gateway trust and security through a set of criteria for the following security services: 4. Multi-tiered virus protection. 5. Offload virus scan processing to a dedicated system. 6. Protection to Gateways from computer virus intrusion. 7. Detection of computer viruses on an infected Gateway. 8. Gateway recovery from a computer virus infection.

ASSOCIATED ARCHITECTURE LEVELS	
Domain Name	Security
Discipline Name	Technical Controls
Technology Area Name	Virus Detection and Elimination
Product Component Name	

COMPLIANCE COMPONENT TYPE	
Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	
Guideline, Standard or Legislation	**Virus Detection and Elimination Criteria for Gateways** State computer Gateways shall run anti-virus software and procedures that meet the checklist of criteria detailed in the following service areas. <u>General Gateway Anti-Virus Criteria</u> • Gateways shall be scanning for viruses continuously. • Gateway anti-virus software shall provide integration capabilities with an enterprise anti-virus policy management suite. • All State Gateways shall execute a virus scan product certified by the ICSA Labs (http://www.icsalabs.com). ICSA Labs certification requires anti-virus products to detect 100% of all viruses “in the wild” as captured by the WildList Organization International (http://www.wildlist.org). <u>Virus Detection/Scanning Capabilities</u> • Anti-virus software shall be capable of detecting malicious software before it is executed. • Shall support continuous real-time scanning capabilities.

	• Shall provide detection for all “in the wild” virus types (boot viruses, file viruses, macro viruses, and script viruses).
	• Shall provide detection for Zoo type viruses (file viruses, macro viruses, script viruses, polymorphic viruses, other malware, false positives).
	• Shall provide detection for archived and compressed file types (.ZIP, TAR, LZH, recursive and self-extracting archives, runtime-compressed files).
	• Shall provide scanning capabilities for all standard office file formats (including embedded OLE objects and password protected files).
	• Shall provide for flexible configuration to include/exclude file types, drives and directories from scans.
	• Shall support both Inbound and Outbound real-time scan protection.
	• Shall provide Internet Download and Content scanning for protection from suspicious web content, including:
	  - ActiveX filtering and scanning
	  - JavaScript filtering and scanning
	• Shall provide Heuristic-scanning capabilities (intelligent analysis of unknown or suspicious sections of code).
	• Gateway anti-virus software shall have the capability to scan all major message protocols including:
	  - SMTP
	  - POP3
	  - HTTP
	  - FTP
	• Gateway anti-virus software shall support SPAM detection and anti-relay (DNS based black hole lists and administrative defined anti-relay).
	
	<u>Internet Content Filtering</u>
	• Gateway anti-virus products shall support the filtering of web content (including POP3 email) for tailored anti-viral support including filtering on items such as:
	  - File size
	  - DNS extensions (dns.com)
	  - Web page content
	  - File extensions
	  - Multiple criteria
	
	<u>Virus Reporting Capabilities</u>
	• Anti-virus software shall provide remote notification of administrative alerts via the following methods:
	  - SMTP/E-Mail
	  - SNMP Alerts
	  - Log to a file
	  - Log to an Enterprise Repository
	
	<u>Post-Detection Virus Action Capabilities</u>
	• It is highly desirable that anti-virus software be able to eradicate malicious software and viruses detected through the following means:
	  - Quarantine – moving the infected file into an area where it cannot cause more harm.
	  - Virus Removal – allows for repair of the damage caused by the virus.
	  - Deny Access – prohibits the file from being accessed once infected.
	  - Delete – complete removal of the infected file from the system.
	
	<u>Virus Scan Engine Update Capabilities</u>
	• Anti-virus signatures need to be updated continuously, either through a manual or automated process.

	• Shall provide a secure procedure for keeping the detection engine up-to-date with the latest detection signatures & scan engine techniques (new viruses are discovered daily) • Shall provide for automated updates of both scan engine and signatures on a scheduled interval or as needed. • Virus scan engine shall have the ability to stay up-to-date with the latest developments in malicious software detection. <u>Anti-Virus Installation Criteria for Sever-based Gateways</u> • Anti-virus software shall be capable of automatic deployment and installation via the following: – Installation via image – anti-virus software shall be able to be included in the standard Gateway server image deployed within the enterprise. – Remote installation – Anti-virus software shall support deployment to remote systems (not locally-connected) providing the same level of protection to these devices. • Anti-virus software shall provide "Wizard-enabled" installation routines to automate and expedite installation. <u>Service and Support</u> • State virus protection products shall be backed by vendors who offer 24 x 7, 365 days a year phone support. • Anti-virus vendors shall provide a comprehensive documentation and assistance package, including a facility for pro-active timely warnings of new malicious software and virus events. • Anti-virus vendors shall provide "Virus Catalog Support" including: – A lexicon of known viruses detailing descriptions, how they are spread, what they do, how they are recognized and how to remove them. – Downloads or links to disinfection tools. – A clear and concise description of the anti-virus tools functionality, including procedures for updating the product with new detection signatures. – General advice to end-users on attacks and avoidance measures.		
Source Reference	N/A		
Standards Organizations			
Name	ISCA Labs	*Website*	www.iscalabs.com
Contact Information	ISCA Labs is a division of TruSecure Corporation and can be reached at 1-888-396-8348 (info@trusecure.com)		
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		

KEYWORDS			
Keywords/Aliases	Virus, virus detection, malicious code, virus products, virus reporting, anti-virus vendors, anti-virus engine, zoo, trojan horse, backdoor, worm, stealth, blended threat, boot sector infector, companion, denial of service, dropper, file infector, logic bomb, malware, multi-partite, overwriting, parasitic, polymorphic, tunneling, variant, terminate and stay resident (tsr), management		
COMPONENT CLASSIFICATION			
Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Rationale for Component Classification			
Conditional Use Restrictions			
Restrictions			
Migration Strategy			
Migration Strategy			
Impact Position Statement			
Position Statement on Impact			
CURRENT STATUS			
Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	02-06-2003	*Date Accepted / Rejected*	02-27-2003
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

Click on this link to return to the Security Blueprint Samples – Set Two.

DEFINITION	
Name	Compliance Component - Virus Detection and Elimination Criteria for Servers
Description	To make available to the State Enterprise a set of minimum criteria for the selection of anti-virus software and products for security protection of servers.
Rationale	All servers within the State computer environment shall execute an anti-virus security product that conforms to a minimum set of compliance criteria. These criteria shall serve as a checklist to help administrators choose the appropriate anti-virus solution for their environment.
Benefits	To significantly improve server trust and security through a set of criteria for the following security services: 9. Protection to servers and media from computer virus intrusion. 10. Detection of computer viruses on an infected server system or media. 11. Server recovery from a computer virus infection.

ASSOCIATED ARCHITECTURE LEVELS	
Domain Name	Security
Discipline Name	Technical Controls
Technology Area Name	Virus Detection and Elimination
Product Component Name	

COMPLIANCE COMPONENT TYPE	
Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	
Guideline, Standard or Legislation	**Virus Detection and Elimination Criteria for Servers** State servers shall be protected with anti-virus software and procedures that meet the checklist of criteria detailed in the following service areas. <u>General Server Anti-Virus Criteria</u> • Anti-virus scanner software shall be run on all servers even if the networks perimeter devices are scanning for viruses. • All servers shall be scanned for viruses at least once a day. • Server anti-virus software shall provide integration capabilities with an enterprise anti-virus policy management suite. • All State servers shall execute a virus scan product certified by the ICSA Labs (http://www.icsalabs.com). ICSA Labs certification requires anti-virus products to detect 100% of all viruses "in the wild" as captured by the WildList Organization International (http://www.wildlist.org). <u>Virus Detection/Scanning Capabilities</u> • Anti-virus software shall be capable of detecting malicious software before it is executed. • Shall support both On-Access (real-time) and On-Demand (flexible) scanning capabilities. • Shall provide detection for all "in the wild" virus types (boot viruses, file viruses,

	macro viruses, and script viruses). • Shall provide detection for Zoo type viruses (file viruses, macro viruses, script viruses, polymorphic viruses, other malware, false positives). • Shall provide detection for archived and compressed file types (.ZIP, TAR, LZH, recursive and self-extracting archives, runtime-compressed files). • Shall provide scanning capabilities for all standard office file formats (including embedded OLE objects and password protected files). • Shall provide for flexible configuration to include/exclude file types, drives and directories from scans. • Shall support both Inbound and Outbound real-time scan protection. • Shall provide Internet Download and Content scanning for protection from suspicious web content, including: – ActiveX filtering and scanning – JavaScript filtering and scanning • Shall provide Heuristic-scanning capabilities (intelligent analysis of unknown or suspicious sections of code). <u>Virus Reporting Capabilities</u> • Anti-virus software shall provide the ability for detection notification via both audio and visual alerts. • Anti-virus software shall provide remote notification of administrative alerts via the following methods: – SMTP/E-Mail – SNMP Alerts – Log to a file – Log to an Enterprise Repository <u>Post-Detection Virus Action Capabilities</u> • It is highly desirable that Anti-virus software be able to eradicate malicious software and viruses detected through the following means: – Quarantine – moving the infected file into an area where it cannot cause more harm. – Virus Removal – allows for repair of the damage caused by the virus. – Deny Access – prohibits the file from being accessed once infected. – Delete – complete removal of the infected file from the system. <u>Virus Scan Engine Update Capabilities</u> • Anti-virus signatures need to be updated continuously, either through a manual or automated process. • Shall provide a secure procedure for keeping the detection engine up-to-date with the latest detection signatures & scan engine techniques (new viruses are discovered daily) • Shall provide for automated updates of both scan engine and signatures on a scheduled interval or as needed. • Virus scan engine shall have the ability to stay up-to-date with the latest developments in malicious software detection. <u>Anti-Virus Software Configuration Security</u> • Anti-virus product configurations and settings shall be able to be password protected to prevent misuse and disablement. • Anti-virus software shall support multiple & customizable definitions of security rights to various levels of the software configuration settings. <u>Anti-Virus Installation Criteria</u> • Anti-virus software shall be capable of installation on clustered servers.

	• Anti-virus software shall be capable of automatic deployment and installation via the following:
	  – Installation via image – anti-virus software shall be able to be included in the standard file server images deployed within the enterprise.
	  – Remote installation – anti-virus software shall support deployment to remote systems (not locally-connected) providing the same level of protection to these devices.
	• Anti-virus software shall provide "Wizard-enabled" installation routines to automate and expedite installation.
	
	<u>Service and Support</u>
	• Virus protection for servers shall support full virus protection in clustered server environments.
	• State virus protection products shall be backed by vendors who offer 24 x 7, 365 days a year phone support.
	• Anti-virus vendors shall provide a comprehensive documentation and assistance package, including a facility for pro-active timely warnings of new malicious software and virus events.
	• Anti-virus vendors shall provide "Virus Catalog Support" including:
	  – A lexicon of known viruses detailing descriptions, how they are spread, what they do, how they are recognized and how to remove them.
	  – Downloads or links to disinfection tools.
	  – A clear and concise description of the anti-virus tools functionality, including procedures for updating the product with new detection signatures.
	  – General advice to end-users on attacks and avoidance measures.		

Source Reference	N/A		
Standards Organizations			
Name	ICSA Labs	*Website*	www.icsalabs.com
Contact Information	ICSA Labs is a division of TruSecure Corporation and can be reached at 1-888-396-8348 (info@trusecure.com)		
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
KEYWORDS			
Keywords/Aliases	Virus, virus detection, malicious code, virus products, virus reporting, anti-virus vendors, anti-virus engine, zoo, trojan horse, backdoor, worm, stealth, blended threat, boot sector infector, companion, denial of service, dropper, file infector, logic bomb, malware, multi-partite, overwriting, parasitic, polymorphic, tunneling, variant, terminate and stay resident (tsr), management, server		
COMPONENT CLASSIFICATION			
Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Rationale for Component Classification			

Conditional Use Restrictions			
Restrictions			
Migration Strategy			
Migration Strategy			
Impact Position Statement			
Position Statement on Impact			
CURRENT STATUS			
Current Status	☐ In Development ☐ Under Review ☒ Approved ☐ Rejected		
AUDIT TRAIL			
Creation Date	02-06-2003	Date Accepted / Rejected	02-27-2003
Reason for Rejection			
Last Date Reviewed		Last Date Updated	
Reason for Update			

Click on this link to return to the Security Blueprint Samples – Set Two.

Compliance Component Blueprint

DEFINITION	
Name	Compliance Component - Virus Detection and Elimination Criteria for Workstations
Description	To make available to the State Enterprise a set of minimum criteria for the selection of anti-virus software and products for security protection of workstations.
Rationale	All workstations within the State computer environment shall execute an anti-virus security product that conforms to a minimum set of compliance criteria. These criteria shall serve as a checklist to help administrators choose the appropriate anti-virus solution for their environment.
Benefits	To significantly improve workstation trust and security through a set of criteria for the following security services: 12. Protection to workstation computer systems and media from computer virus intrusion. 13. Detection of computer viruses on an infected workstation system or media. 14. Workstation recovery from a computer virus infection.
ASSOCIATED ARCHITECTURE LEVELS	
Domain Name	Security
Discipline Name	Technical Controls
Technology Area Name	Virus Detection and Elimination
Product Component Name	
COMPLIANCE COMPONENT TYPE	
Component Type	Guideline
Component Sub-type	
COMPLIANCE DETAIL	
Guideline, Standard or Legislation	**Virus Detection and Elimination Criteria for Workstations** State computer workstations shall be protected with anti-virus software and procedures that meet the checklist of criteria detailed in the following service areas. <u>General Workstation Anti-Virus Criteria</u> • Virus scanner software shall be run on all workstations even if the networks perimeter devices are scanning for viruses. • All workstations shall be scanned for viruses at least once a day. • Workstation anti-virus software shall provide integration capabilities with an enterprise anti-virus policy management suite. • All State workstations shall execute a virus scan product certified by the ICSA Labs (http://www.icsalabs.com). ICSA Labs certification requires anti-virus products to detect 100% of all viruses “in the wild” as captured by the WildList Organization International (http://www.wildlist.org). <u>Virus Detection/Scanning Capabilities</u> • Anti-virus software shall be capable of detecting malicious software before it is executed. • Shall support both On-Access (real-time) and On-Demand (flexible) scanning

	capabilities. • Shall provide detection for all “in the wild” virus types (boot viruses, file viruses, macro viruses, and script viruses). • Shall provide detection for Zoo type viruses (file viruses, macro viruses, script viruses, polymorphic viruses, other malware, false positives). • Shall provide detection for archived and compressed file types (.ZIP, TAR, LZH, recursive and self-extracting archives, runtime-compressed files). • Shall provide scanning capabilities for all standard office file formats (including embedded OLE objects and password protected files). • Shall provide for flexible configuration to include/exclude file types, drives and directories from scans. • Shall support both Inbound and Outbound real-time scan protection. • Shall provide Internet Download and Content scanning for protection from suspicious web content, including: - ActiveX filtering and scanning - JavaScript filtering and scanning • Shall provide Heuristic-scanning capabilities (intelligent analysis of unknown or suspicious sections of code). <u>Virus Reporting Capabilities</u> • Anti-virus software shall provide the ability for detection notification via both audio and visual alerts. • Anti-virus software shall provide remote notification of administrative alerts via the following methods: - SMTP/E-Mail - SNMP Alerts - Log to a file - Log to an Enterprise Repository <u>Post-Detection Anti-Virus Action Capabilities</u> • It is highly desirable that anti-virus software be able to eradicate malicious software and viruses detected through the following means: - Quarantine – moving the infected file into an area where it cannot cause more harm. - Virus Removal – allows for repair of the damage caused by the virus. - Deny Access – prohibits the file from being accessed once infected. - Delete – complete removal of the infected file from the system. <u>Virus Scan Engine Update Capabilities</u> • Anti-virus signatures need to be updated continuously, either through a manual or automated process. • Shall provide a secure procedure for keeping the detection engine up-to-date with the latest detection signatures & scan engine techniques. • Shall provide for automated updates of both scan engine and signatures on a scheduled interval or as needed. • Virus scan engine shall have the ability to stay up-to-date with the latest developments in malicious software detection. <u>Anti-Virus Software Configuration Security</u> • Anti-virus product configurations and settings shall be able to be password protected to prevent misuse and disablement. • Anti-virus software shall support multiple & customizable definitions of security and rights to various levels of the software configuration settings. <u>Anti-Virus Installation Criteria</u>

	• Anti-virus software shall be capable of automatic deployment and installation via the following:
	  - Installation via image – anti-virus software shall be able to be included in the standard workstation image deployed within the enterprise.
	  - Remote installation – Anti-virus software shall support deployment to remote systems (not locally-connected) providing the same level of protection to these devices.
	• Anti-virus software deployment (and updates) shall be transparent to end-users.
	• Anti-virus software shall provide "Wizard-enabled" installation routines to automate and expedite installation.
	
	<u>Service and Support</u>
	• State anti-virus protection products shall be backed by vendors who offer 24 x 7, 365 days a year phone support.
	• Anti-virus vendors shall provide a comprehensive documentation and assistance package, including a facility for pro-active timely warnings of new malicious software and virus events.
	• Anti-virus vendors shall provide "Virus Catalog Support" including:
	  - A lexicon of known viruses detailing descriptions, how they are spread, what they do, how they are recognized and how to remove them.
	  - Downloads or links to disinfection tools.
	  - A clear and concise description of the anti-virus tools functionality, including procedures for updating the product with new detection signatures.
	  - General advice to end-users on attacks and avoidance measures.		

Source Reference	N/A		
Standards Organizations			
Name	ICSA Labs	*Website*	www.icsalabs.com
Contact Information	ICSA Labs is a division of TruSecure Corporation and can be reached at 1-888-396-8348 (info@trusecure.com)		
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
KEYWORDS			
Keywords/Aliases	Virus, virus detection, malicious code, virus products, virus reporting, anti-virus vendors, anti-virus engine, zoo, trojan horse, backdoor, worm, stealth, blended threat, boot sector infector, companion, denial of service, dropper, file infector, logic bomb, malware, multi-partite, overwriting, parasitic, polymorphic, tunneling, variant, terminate and stay resident (tsr), management, PC		
COMPONENT CLASSIFICATION			
Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Rationale for Component Classification			

Conditional Use Restrictions			
Restrictions			
Migration Strategy			
Migration Strategy			
Impact Position Statement			
Position Statement on Impact			
CURRENT STATUS			
Current Status	☐ In Development ☐ Under Review ☒ Approved ☐ Rejected		
AUDIT TRAIL			
Creation Date	02-06-2003	Date Accepted / Rejected	02-27-2003
Reason for Rejection			
Last Date Reviewed		Last Date Updated	
Reason for Update			

Click on this link to return to the Security Blueprint Samples – Set Two.

Compliance Component Blueprint

DEFINITION	
Name	Compliance Component - Virus Detection and Elimination Criteria for Wireless Devices
Description	To make available to the State Enterprise a set of minimum criteria for the selection of anti-virus software and products for security protection of Wireless Devices (e.g. PDAs) which connect directly (via a wireless adapter) or connect indirectly (via a cradle) to it's computer networks. All Wireless Devices used within the State computer environments that are directly or indirectly connected to enterprise networks or computers shall execute an anti-virus security product that conforms to a minimum set of compliance criteria. These criteria shall serve as a checklist to help administrators choose the appropriate anti-virus solution for their environment.
Rationale	When using wireless devices there is a major security gap, as server and workstation anti-virus applications can't protect from a virus being introduced during a sync operation with the wireless device.
Benefits	To significantly improve wireless device trust and security through a set of criteria for the following security services: 15. Protection to workstation computer systems and servers from computer virus intrusion transmitted via wireless devices. 16. Detection and protection computer viruses on an wireless handheld system. 17. Wireless handheld device recovery from a computer virus infection.

ASSOCIATED ARCHITECTURE LEVELS	
Domain Name	Security
Discipline Name	Technical Controls
Technology Area Name	Virus Detection and Elimination
Product Component Name	

COMPLIANCE COMPONENT TYPE	
Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	
Guideline, Standard or Legislation	**Virus Detection and Elimination Criteria for Wireless Devices** Wireless devices, which connect to State systems or networks, shall be protected with anti-virus software and procedures that meet the checklist of criteria detailed in the following service areas. <u>General Wireless Handheld Anti-Virus Criteria</u> • Wireless anti-virus software shall protect the sync operation and/or the wireless device, even if the workstation and network perimeter devices are scanning for viruses. • Wireless handheld anti-virus software shall protect against malicious data as transferred via: – Sync operations with a workstation or network – Infrared transfer with another handheld device, laptop, or workstation – Wireless network or Internet connections

	• Wireless virus protection shall cover all major palm top operating systems including:
	  - Palm OS
	  - Pocket PC
	  - Windows CE
	  - Symbian EPOC
	
	<u>Virus Detection/Scanning Capabilities</u>
	• Wireless device anti-virus software shall be capable of detecting malicious software before it is transferred to workstations or networks.
	• Shall provide detection for all “in the wild” virus types (boot viruses, file viruses, macro viruses, and script viruses).
	• Shall provide detection for Zoo type viruses (file viruses, macro viruses, script viruses, polymorphic viruses, other malware, false positives).
	• Shall provide detection for archived and compressed file types (.ZIP, TAR, LZH, recursive and self-extracting archives, runtime-compressed files).
	• Shall provide scanning capabilities for all standard office file formats (including embedded OLE objects and password protected files).
	• Shall provide for flexible configuration to include/exclude file types, drives and directories from scans.
	• Shall provide Internet Download and Content scanning for protection from suspicious web content, including:
	  - ActiveX filtering and scanning
	  - JavaScript filtering and scanning
	• Shall provide Heuristic-scanning capabilities (intelligent analysis of unknown or suspicious sections of code).
	
	<u>Post-Detection Anti-Virus Action Capabilities</u>
	• If a virus is discovered, all synchronization between the wireless device and the workstation or network shall be disabled until the destructive code can be removed from the device.
	• It is highly desirable that anti-virus software be able to eradicate malicious software and viruses detected through the following means:
	  - Quarantine – moving the infected file into an area where it cannot cause more harm.
	  - Virus Removal – allows for repair of the damage caused by the virus.
	  - Deny Access – prohibits the file from being accessed once infected.
	  - Delete – complete removal of the infected file from the system.
	
	<u>Virus Scan Engine Update Capabilities</u>
	• Anti-virus signatures need to be updated, either through a manual or automated process.
	• Shall provide a secure procedure for keeping the detection engine up-to-date with the latest detection signatures & scan engine techniques (new viruses are discovered daily).
	• Shall provide for automated updates of both scan engine and signatures during synchronization processes.
	• Virus scan engine shall have the ability to stay up-to-date with the latest developments in malicious software detection.
	
	<u>Anti-Virus Installation Criteria</u>
	• Anti-virus software shall be capable of flexible deployment techniques.
	• Anti-virus software deployment (and updates) shall be transparent to end-users.
	• Anti-virus software shall provide “Wizard-enabled” installation routines to automate and expedite installation.

	Service and Support • State virus protection products shall be backed by vendors who offer 24 x 7, 365 days a year phone support. • Anti-virus vendors shall provide a comprehensive documentation and assistance package, including a facility for pro-active timely warnings of new malicious software and virus events. • Anti-virus vendors shall provide "Virus Catalog Support" including: – A lexicon of known viruses detailing descriptions, how they are spread, what they do, how they are recognized and how to remove them. – Downloads or links to disinfection tools. – A clear and concise description of the anti-virus tools functionality, including procedures for updating the product with new detection signatures. – General advice to end-users on attacks and avoidance measures.		
Source Reference	N/A		
Standards Organizations			
Name	ICSA Labs	*Website*	www.icsalabs.com
Contact Information	ICSA Labs is a division of TruSecure Corporation and can be reached at 1-888-396-8348 (info@trusecure.com)		
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
KEYWORDS			
Keywords/Aliases	Virus, virus detection, malicious code, virus products, virus reporting, anti-virus vendors, anti-virus engine, zoo, trojan horse, backdoor, worm, stealth, blended threat, boot sector infector, companion, denial of service, dropper, file infector, logic bomb, malware, multi-partite, overwriting, parasitic, polymorphic, tunneling, variant, terminate and stay resident (tsr), management, palm top, palm pilot, handheld, PDA		
COMPONENT CLASSIFICATION			
Classification	☒ *Emerging* ☐ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Rationale for Component Classification			
Conditional Use Restrictions			
Restrictions			
Migration Strategy			
Migration Strategy			
Impact Position Statement			
Position Statement on Impact			

CURRENT STATUS			
Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	02-06-2003	*Date Accepted / Rejected*	02-27-2003
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

Click on this link to return to the Security Blueprint Samples – Set Two.

Definition	
Name	Technology Area - Intrusion Detection Systems (IDS)
Description	Intrusion Detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network. Intrusion Detection Systems (IDS) are software or hardware products that automate this monitoring and analysis process.
Rationale	Intrusion detection allows State organizations to protect their systems from the threats that come with increasing network connectivity and reliance on information systems. Given the level and nature of modern network security threats, the question for security professionals should not be *whether* to use IDS, but which IDS features and capabilities to use.
Benefits	• IDS prevents problem behaviors by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse a system. • IDS detects attacks and other security violations that are not prevented by other security measures. • An IDS can act as a quality control for security design and administration. • IDS provides useful information about intrusions that do take place, allowing improved diagnosis, recovery, correction of causative factors, and data for potential prosecution.
Associated Discipline	
Discipline Name	Technical Controls
Keywords	
Keywords/Aliases	Honey Pot, intrusion, cracker, buffer overflows, passwords, sniffing, exploit, denial-of-service, Java, ActiveX, SMURF, DNS, probes, logging, auditing, monitoring, anomaly, patterns, exploits, misuse
Associated Compliance Components	
Compliance Component Names	• Host-Based IDS • Network-Based IDS • Application-Based IDS
Associated Product Components	
Product Component Names	
Technology Area Detail	
Supporting Documentation	NIST SP 800-31 Intrusion Detection Systems (IDS)
Source Reference	www.csrc.nist.gov/publications/nistpubs

Standards Organizations / Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
CURRENT STATUS			
Technology Area Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	3/27/2003	*Date Accepted / Rejected*	05/14/2003
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Updated By			
Reason for Update			

Click on this link to return to the Security Blueprint Samples – Set Two.

Compliance Component Blueprint

Definition	
Name	Compliance Component - Network-Based Intrusion Detection Systems (NIDS)
Description	Network-Based Intrusion Detection Systems (NIDS) detect attacks by capturing and analyzing network traffic. NIDS are dedicated software or hardware systems that "sit" on a network and analyze network packets. NIDS often consist of a set of single-purpose sensors placed at various points in a network. These sensors monitor network traffic, performing local analysis of that traffic and reporting attacks to a centralized console.
Rationale	The first step in delivering an efficient and secure network intrusion protection strategy is accurately detecting all possible threats. To achieve this goal, multiple detection methods should be employed to ensure comprehensive coverage. The failure to secure State networks with NIDS puts agencies at a much greater risk of loss. A single attack can cost millions of dollars in time spent recovering from the attack and liability for compromised data and hardware. The damage from an attack to State services can also include inconvenience to citizens and the loss of public confidence.
Benefits	• NIDS identify and prevent security threats from compromising secure networks. • The deployment of NIDS has little impact on network performance. NIDS are usually passive devices that listen on a network without interfering with the normal operation of a network. • NIDS can be made very secure against attack and even made invisible to many attackers.
Associated Architecture Levels	
Domain Name	Security
Discipline Name	Technical Controls
Technology Area Name	Intrusion Detection Systems
Product Component Name	
Compliance Component Type	
Component Type	Guideline
Component Sub-type	
Compliance Detail	
Guideline, Standard or Legislation	**General NIDS Requirements** • Administrators shall be trained on the IDS before implementation. Despite vendor claims of ease of use, training and/or experience are necessary to manage any IDS. • It is preferred to have the NIDS controlled directly from a central location(s). However, the NIDS may be agent-based where response decisions are made at the agent. • IDS administrators shall be able to create or change policies easily. **NIDS Deployment Requirements** • NIDS shall be deployed in conjunction with Host-Based IDS to fully protect the system.

- It is recommended that organizations install the NIDS first on critical networks. Once administrators are familiar with the NIDS, it may be installed on the remainder of the organization's networks.
- NIDS shall be installed on any Network where sensitive or critical information is transmitted.
- It is preferred to install IDS Management software on a dedicated system in the target networks being monitored.
- It is preferred to have the NIDS use an agent-manager (server) architecture, where policy is created and modified on the manager and automatically distributed to all agents.
- It is preferred that Server agents poll the manager at periodic intervals for policy changes or new software updates.

NIDS Analysis Requirements

- NIDS shall utilize information from operating system audit trails and system logs.
- NIDS shall have easy-to-use tools to analyze the logs.
- NIDS shall detect, and preferably prevent, the following:
- System scanning (probing the target with different kinds of packets to garner information about the system, such as topology, active systems, operating systems and software in use),
- Denial of Service (DoS) (slow or shut down targeted systems or hosts), and
- Penetration (unauthorized acquisition and/or alteration of system privileges, resources, or data).
- NIDS shall use Misuse Detection methods (matching a predefined pattern of events describing an attack) and may include Anomaly Detection (abnormal, unusual behavior) components.
- Administrators shall follow a schedule for checking the results of the NIDS to ensure attackers have not modified the system.

NIDS Response Requirements

- NIDS shall respond in real-time.
- It is preferred that IDS provide active responses to intrusions by:
  - Collecting additional information:
- Turning up the number of events logged, or
- Capturing all packets, not just those targeting a particular port or system.
  - Changing the environment:
- Terminating the connection, or
- Reconfiguring routers and firewalls to:
  - Block packets from the intruder's IP address,
  - Block network ports, protocols or services, or
  - Sever all connections that use certain network interfaces.
- NIDS administrators shall work closely with router and firewall administrators when creating rules for routers and firewalls to ensure intruders cannot abuse the feature to deny access to legitimate users.
- NIDS may provide passive responses requiring subsequent human action to intrusions by:
  - Generating alarms and notifications with popup windows, cellular phones, pagers and email, or
  - Reporting alarms and alerts using SNMP traps and plug-ins to central network management consoles.
  - All NIDS communications shall be secure and use encrypted tunnels or other cryptographic measures.

	- NIDS shall create output with the following information for each intrusion detected: - Time/date - Sensor IP address - Specific attack name - Source and destination IP addresses - Source and destination port numbers - Network protocol used - Description of the attack type - Attack severity level - Type of loss expected - Type of vulnerability exploited - Input validation (buffer overflow or boundary condition) - Access validation (faulty access control mechanism) - Exceptional condition • Environmental (unexpected interaction with an application and the operating system or between two applications) • Server Configuration • Race (delay between the time a system checks to see if an operation is allowed and the time it performs the operation) • Design • Software types and versions vulnerable • Patch information to counter the attack • References to advisories about the attack or vulnerability - It is preferred that NIDS reports combine redundant attack entries and make attacks of highest importance stand out.
Source Reference	NIST SP 800-31 (www.csrc.nist.gov/publications/nistpubs) Intrusion Detection Systems (IDS), NIST SP 800-18 (www.csrc.nist.gov/publications/nistpubs) CERT Guide to System and Network Security Practices (www.cert.org/security-improvement/)

Standards Organizations			
Name		*Website*	
Contact Information			

Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		

KEYWORDS	
Keywords/Aliases	Honey Pot, intrusion, cracker, buffer overflows, passwords, sniffing, exploit, denial-of-service, Java, ActiveX, SMURF, DNS, probes

COMPONENT CLASSIFICATION				
Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*
Rationale for Component Classification				

Rationale for Component Classification			
Conditional Use Restrictions			
Restrictions			
Migration Strategy			
Migration Strategy			
Impact Position Statement			
Position Statement on Impact			
CURRENT STATUS			
Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	04/03/2003	*Date Accepted / Rejected*	5/14/2003
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

Click on this link to return to the Security Blueprint Samples – Set Two.

Compliance Component Blueprint

DEFINITION	
Name	Compliance Component - Host-Based Intrusion Detection Systems (HIDS)
Description	Host-Based Intrusion Detection Systems (HIDS) operate on information collected from within an individual computer system. This vantage point allows HIDS to analyze activities to determine exactly which processes and users are involved in an attack on a particular system or host. HIDS can see the outcome of an attempted attack, as they can directly access and monitor the data files and operating system processes targeted by the attack.
Rationale	The first step in delivering an efficient and secure intrusion protection strategy is accurately detecting all possible threats. To achieve this goal, multiple detection methods including HIDS should be employed to ensure comprehensive coverage. The failure to secure any State host system with HIDS puts agencies at a much greater risk of loss. A single attack can cost millions of dollars in time spent recovering from the attack and liability for compromised data and hardware. The damage from an attack to State services can also include inconvenience to citizens and the loss of public confidence.
Benefits	• HIDS can detect attacks that cannot be seen by a Network-Based IDS since they monitor events local to a host. • HIDS can often operate in an environment where network traffic is encrypted. • HIDS are unaffected by switched networks. • HIDS can detect, and in some cases prevent, attacks that involve software integrity breaches, such as Trojan Horses. • HIDS have the ability to monitor local files for any changes or modifications. • HIDS can see the outcome of an attempted attack since they can directly access and monitor the data files and operating system processes targeted by the attack.
ASSOCIATED ARCHITECTURE LEVELS	
Domain Name	Security
Discipline Name	Technical Controls
Technology Area Name	Intrusion Detection Systems
Product Component Name	
COMPLIANCE COMPONENT TYPE	
Component Type	Guideline
Component Sub-type	
COMPLIANCE DETAIL	
Guideline, Standard or Legislation	**General HIDS Requirements** • Administrators shall be trained on the IDS before implementation. Despite vendor claims of ease of use, training and/or experience are absolutely necessary to manage any IDS. • It is preferred to have the HIDS controlled directly from a central location(s). However, the HIDS may be agent-based where response decisions are made at the host. • IDS administrators shall be able to create or change policies easily. **HIDS Deployment Requirements** • HIDS shall be deployed in conjunction with Network-Based IDS to fully protect

the system.
- It is recommended that organizations install the Network-Based IDS first, followed by the HIDS installation on critical servers. Once administrators are familiar with the HIDS, it may be installed on the remainder of the organization's hosts.
- HIDS shall be installed on any host where sensitive or critical information is stored.
- It is preferred to install IDS Management software on a separate system from the target host being monitored.
- It is preferred to have the HIDS use an agent-manager (server) architecture, where policy is created and modified on the manager and automatically distributed to all agents.
- It is preferred that host agents poll the manager at periodic intervals for policy changes or new software updates.

HIDS Analysis Requirements

- HIDS shall utilize information from operating system audit trails and system logs.
- HIDS shall have easy-to-use tools to analyze the logs.
- HIDS shall detect, and preferably prevent, the following:
  - System scanning (probing the target with different kinds of packets to garner information about the system, such as topology, active hosts, operating systems and software in use),
  - Denial of Service (DoS) (slow or shut down targeted systems or hosts), and
  - Penetration (unauthorized acquisition and/or alteration of system privileges, resources, or data).
- HIDS shall use Misuse Detection methods (matching a predefined pattern of events describing an attack) and may also include Anomaly Detection (abnormal, unusual behavior) components.
- Administrators shall follow a schedule for checking the results of the HIDS to ensure attackers have not modified the system.

HIDS Response Requirements

- HIDS shall respond in real-time.
  - It is preferred that HIDS provide active responses to intrusions by:
    - Collecting additional information:
      - Turning up the number of events logged, or
      - Capturing all packets, not just those targeting a particular port or system.
      - Changing the environment:
      - Terminating the connection, or
      - Reconfiguring routers and firewalls to:
      - Block packets from the intruder's IP address,
      - Block network ports, protocols or services, or
      - Sever all connections that use certain network interfaces.
      - HIDS administrators shall work closely with router and firewall administrators when creating rules for routers and firewalls to ensure intruders cannot abuse the feature to deny access to legitimate users.
      - HIDS may provide passive responses requiring subsequent human action to intrusions by:
      - Generating alarms and notifications with popup windows, cellular phones, pagers and email, or
      - Reporting alarms and alerts using SNMP traps and plug-ins to

	central network management consoles. - All HIDS communications shall be secure and use encrypted tunnels or other cryptographic measures - HIDS shall create output with the following information for each intrusion detected: - Time/date - Sensor IP address - Specific attack name - Source and destination IP addresses - Source and destination port numbers - Network protocol used - Description of the attack type - Attack severity level - Type of loss expected - Type of vulnerability exploited - Input validation (buffer overflow or boundary condition) - Access validation (faulty access control mechanism) - Exceptional condition - Environmental (unexpected interaction with an application and the operating system or between two applications) - Host Configuration - Race (delay between the time a system checks to see if an operation is allowed and the time it performs the operation) - Design - Software types and versions vulnerable - Patch information to counter the attack - References to advisories about the attack or vulnerability - It is preferred that HIDS reports combine redundant attack entries and make attacks of highest importance stand out.
Source Reference	NIST SP 800-31 (www.csrc.nist.gov/publications/nistpubs) Intrusion Detection Systems (IDS), NIST SP 800-18 (www.csrc.nist.gov/publications/nistpubs) CERT Guide to System and Network Security Practices (www.cert.org/security-improvement/)

Standards Organizations			
Name		*Website*	
Contact Information			

Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) CVE Vulnerability Search on ICAT Metabase	*Website*	http://csrc.nist.gov/ http://icat.nist.gov/
Contact Information	inquiries@nist.gov		

KEYWORDS	
Keywords/Aliases	Honey Pot, intrusion, cracker, buffer overflows, passwords, sniffing, exploit, denial-of-service, Java, ActiveX, SMURF, DNS, probes

COMPONENT CLASSIFICATION				
Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*
Rationale for Component Classification				
Rationale for Component Classification				
Conditional Use Restrictions				
Restrictions				
Migration Strategy				
Migration Strategy				
Impact Position Statement				
Position Statement on Impact				
CURRENT STATUS				
Current Status	☐ *In Development*	☐ *Under Review*	☒ *Approved*	☐ *Rejected*
AUDIT TRAIL				
Creation Date	04/03/2003	*Date Accepted / Rejected*	05/14/2003	
Reason for Rejection				
Last Date Reviewed		*Last Date Updated*		
Reason for Update				

Click on this link to return to the Security Blueprint Samples – Set Two.

DEFINITION	
Name	Compliance Component - Application-Based Intrusion Detection Systems (IDS)
Description	Application-Based IDS is a special subset of Host-Based IDS (HIDS) that analyzes the events transpiring within a software application. The most common information source for Application-Based IDS is the application's transaction log file.
Rationale	The ability to interface with applications directly allows Application-Based IDS to detect suspicious behavior such as users exceeding their security authorization.
Benefits	• Application-Based IDS monitors the interaction between user and application, which traces activity to individual users. • Application-Based IDS works with applications that access encrypted data since it interfaces with the application at transaction endpoints where information is presented to users in unencrypted form.
ASSOCIATED ARCHITECTURE LEVELS	
Domain Name	Security
Discipline Name	Technical Controls
Technology Area Name	Intrusion Detection Systems
Product Component Name	
COMPLIANCE COMPONENT TYPE	
Component Type	Guideline
Component Sub-type	
COMPLIANCE DETAIL	
Guideline, Standard or Legislation	**General Application-Based IDS Requirements** • Administrators shall be trained on the Application-Based IDS before implementation. Despite vendor claims of ease of use, training and/or experience are absolutely necessary to manage any IDS. • It is preferred to have the Application-Based IDS controlled directly from a central location(s). However, the Application-Based IDS may be agent-based where response decisions are made at the agent. • Application-Based IDS administrators shall be able to create or change policies easily. **Application-Based IDS Deployment Requirements** • Application-Based IDS shall be deployed in conjunction with Network-Based IDS (NIDS) and/or HIDS to fully protect the system. • It is recommended that organizations install the NIDS first, followed by the HIDS, and then the Application-Based IDS installation on critical servers. • Application-Based IDS shall be enabled on hosts that have critical applications. • Application transaction logs shall be enabled. • It is preferred to install Application-Based IDS Management software on a separate system from the application being monitored. • It is preferred to have the Application–Based IDS use an agent-Manager (server) architecture, where policy is created and modified on the manager and automatically distributed to all agents.

- It is preferred that application agents poll the manager at periodic intervals for policy changes or new software updates.

Application-Based IDS Analysis Requirements

- Application-Based IDS shall utilize, at a minimum, information from an application's transaction log files.
- Application-Based IDS shall have easy-to-use tools to analyze the logs.
- Application-Based IDS shall use Misuse Detection methods (matching a predefined pattern of events describing an attack) and may also include Anomaly Detection (abnormal, unusual behavior) components.
- Application-Based IDS may be configured to intercept the following types of requests and use them in combinations and sequences to constitute an application's normal behavior:
- File System (file read or write)
- Network (packet events at the driver (NDIS) or transport (TDI) level)
- Configuration (read or write to the registry on Windows)
- Execution Space (write to memory not owned by the requesting application. For example, attempts to inject a shared library DLL into another process)
- Operators shall follow a schedule for checking the results of the Application-Based IDS to ensure attackers have not modified the system.

Application-Based IDS Response Requirements

- Application-Based IDS shall respond in real-time.
- It is preferred that Application-Based IDS provide active responses to intrusions by:
- Collecting additional information by turning up the number of events logged, or
- Terminating the user's access.
- Operators shall be extremely careful when creating rules to ensure intruders cannot abuse the feature to deny access to legitimate users.
- Application-Based IDS may provide passive responses requiring subsequent human action to intrusions by:
- Generating alarms and notifications with popup windows, cellular phones, pagers and email, or
- Reporting alarms and alerts using SNMP traps and plug-ins to central network management consoles.
  - All Application-Based IDS communications shall be secure and use encrypted tunnels or other cryptographic measures.
  - Application-Based IDS shall create output with the following information for each intrusion detected:
  - Time/date
  - Sensor IP address
  - Specific attack name
  - Source and destination IP addresses
  - Network protocol used
  - Description of the attack type
  - Attack severity level
  - Type of loss expected
  - Type of vulnerability exploited
  - Access validation
  - Exceptional condition
  - Environmental (unexpected interaction with the operating system or between two applications)
  - Host Configuration
  - Race (delay between the time a system checks to see if an operation is

	allowed and the time it performs the operation) - Design - Software types and versions vulnerable - Patch information to counter the attack - References to advisories about the attack or vulnerability - It is preferred that Application-Based IDS reports combine redundant attack entries and make attacks of highest importance stand out.		
Source Reference	NIST SP 800-18 (www.csrc.nist.gov/publications/nistpubs) CERT Guide to System and Network Security Practices (www.cert.org/security-improvement/)		
Standards Organizations			
Name		*Website*	
Contact Information			
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) CVE Vulnerability Search on ICAT Metabase	*Website*	http://csrc.nist.gov/ http://icat.nist.gov/
Contact Information	inquiries@nist.gov		
KEYWORDS			
Keywords/Aliases	Honey Pot, intrusion, cracker, buffer overflows, passwords, sniffing, exploit, denial-of-service, Java, ActiveX, SMURF, DNS, probes, logging, auditing, monitoring, anomaly, patterns, exploits, misuse		
COMPONENT CLASSIFICATION			
Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Rationale for Component Classification			
Conditional Use Restrictions			
Restrictions			
Migration Strategy			
Migration Strategy			
Impact Position Statement			
Position Statement on Impact			
CURRENT STATUS			
Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	04/03/2003	*Date Accepted / Rejected*	05/14/2003

Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

Click on this link to return to the Security Blueprint Samples – Set Two.

Technology Area Blueprint

Definition			
Name	Technology Area - Logical Access Controls		
Description	Logical access controls are protection mechanisms that limit users' access to information and restrict their forms of access on the system to only what is appropriate for them. Logical access controls are typically a system of measures and procedures, both within an organization and in the software products used, aimed at protecting computer resources (data, programs and terminals) against unauthorized access attempts.		
Rationale	Logical Access Control policies and procedures provide assurance that access to operating systems, programs, and data is limited to properly authorized individuals.		
Benefits	• Preventing intruders from entering state systems • Constraining the authorized users to their legitimate purposes		
Associated Discipline			
Discipline Name	Technical Controls		
Keywords			
Keywords/Aliases	Misuse, entry, least privilege, create, read, write, update, delete		
Associated Compliance Components			
Compliance Component Names	• Logon Banners • Date/Time Controls • Inactivity Controls		
Associated Product Components			
Product Component Names			
Technology Area Detail			
Supporting Documentation	NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems		
Source Reference	www.csrc.nist.gov/publications/nistpubs		
Standards Organizations / Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
Name	National Security Agency (NSA), Security Recommendation Guides	*Website*	http://nsa2.www.conxion.com/index.html
Contact Information	W2KGuides@nsa.gov		
Current Status			
Technology Area Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		

AUDIT TRAIL			
Creation Date	3/6/2003	*Date Accepted / Rejected*	03/24/2003
Created By			
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

Click on this link to return to the Security Blueprint Samples – Set Two.

Compliance Component Blueprint

Definition	
Name	Compliance Component - Date/Time Controls
Description	Restrictions based on time and day bolsters the control environment. The intent is to require more than simple access controls, normally based on user-IDs and passwords.
Rationale	Hackers are most active at night, just when systems are sparsely staffed, if staffed at all. If users stay logged on, hackers can attack their network assets and use them to attack other systems.
Benefits	Reduces the amount of time the account is open to unauthorized access.

Associated Architecture Levels	
Domain Name	Security
Discipline Name	Technical Controls
Technology Area Name	Logical Access Controls
Product Component Name	

Compliance Component Type	
Component Type	Guideline
Component Sub-type	

Compliance Detail	
Guideline, Standard or Legislation	• Whenever possible access control should constrain the user to use of the system within a limited working day and only on normal working days of the week (some systems even make allowances for denying access on public holidays). Such a restriction helps prevent misuse of the system out of hours by an employee (a cleaner, perhaps) or by a hacker (who often rely on out-of-hours access to avoid detection by legitimate users). • Similarly, restrictions should be placed on the workstations the user can employ and on the applications that can be run on a particular workstation. This measure is particularly useful in limiting very privileged activities (system support, security administration, for example) to certain workstations and thus putting a physical barrier in the way of a would-be attacker.
Source Reference	NIST SP 800-18 (www.csrc.nist.gov/publications/nistpubs) CERT Guide to System and Network Security Practices (www.cert.org/security-improvement/)

Standards Organizations			
Name	Carnegie Mellon University, CERT/Coordination Center (CERT/CC)	*Website*	www.cert.org
Contact Information	cert@cert.org		

Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		

KEYWORDS			
Keywords/Aliases	Access, times, work schedule, hours, system availability, after hours		
COMPONENT CLASSIFICATION			
Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Rationale for Component Classification			
Conditional Use Restrictions			
Restrictions			
Migration Strategy			
Migration Strategy			
Impact Position Statement			
Position Statement on Impact			
CURRENT STATUS			
Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	3/6/2003	*Date Accepted / Rejected*	03/24/2003
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

Click on this link to return to the Security Blueprint Samples – Set Two.

DEFINITION	
Name	Compliance Component - Inactivity Controls
Description	Inactivity controls prevent unauthorized disclosure of information and unauthorized system usage by terminating an electronic session after a pre-determined time of inactivity.
Rationale	Appropriate inactivity safeguards must be used to prevent unauthorized access to or use of information, data, and software resident on computers, peripheral devices, and storage media, or transmitted over communication lines or networks. Inactivity controls are particularly necessary in open offices where there are no walls and many people leave their computers on and available for anyone who happens to walk by.
Benefits	• Prevent unauthorized disclosure • Prevent unauthorized system usage
ASSOCIATED ARCHITECTURE LEVELS	
Domain Name	Security
Discipline Name	Technical Controls
Technology Area Name	Logical Access Controls
Product Component Name	
COMPLIANCE COMPONENT TYPE	
Component Type	Guideline
Component Sub-type	
COMPLIANCE DETAIL	
Guideline, Standard or Legislation	• If the computer system contains sensitive information, users shall log-out or invoke a password-protected screen saver before leaving their computer unattended. • If there has been no activity on a computer terminal, workstation, or microcomputer (PC) for a maximum of thirty (30) minutes, the system shall be electronically locked. Re-establishment of the session shall take place only after the user has renewed access via the proper authentication, such as a password. • During computing sessions, user ids are locked out or disabled after specified period of inactivity. – For normal users, screen lockout will occur after a maximum of 30 minutes of inactivity. – For users with administrative or system-level privileges, screen lockout will occur after a maximum of 15 minutes of inactivity. – Users will be required to re-enter their password to continue their sessions after screen lockout due to inactivity. – Prior to screen lockout, the user may receive a display on the screen warning the user of a pending screen lockout. • User IDs that are inactive on the system for a specific period of time (e.g., three months) should be disabled. • User id inactivity results in suspension of access authorization and requires renewal of privileges. – 4 consecutive days of inactivity following notification of new user id setup. – 120 consecutive days of inactivity of existing user ids.

Source Reference	NIST SP 800-18 (www.csrc.nist.gov/publications/nistpubs) CERT Guide to System and Network Security Practices (www.cert.org/security-improvement/)		
Standards Organizations			
Name	Carnegie Mellon University, CERT/Coordination Center (CERT/CC)	*Website*	www.cert.org
Contact Information	cert@cert.org		
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
KEYWORDS			
Keywords/Aliases	Idle, time out, login, screen saver, lockout		
COMPONENT CLASSIFICATION			
Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Rationale for Component Classification			
Conditional Use Restrictions			
Restrictions			
Migration Strategy			
Migration Strategy			
Impact Position Statement			
Position Statement on Impact			
CURRENT STATUS			
Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	3/6/2003	*Date Accepted / Rejected*	03/24/2003
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			

Click on this link to return to the Security Blueprint Samples – Set Two.

Compliance Component Blueprint

Definition	
Name	Compliance Component - Logon Banners
Description	A Logon Banner is verbiage that an end-user sees at the point of access to a system which sets the right expectations for users regarding authorized and acceptable use of a computer system and its resources, data, and network access capabilities. These expectations include notice of authorized monitoring of users' activities while they are using the system, and warnings of legal sanctions should the authorized monitoring reveal evidence of illegal activities or a violation of security policy.
Rationale	Failure to include a logon banner regarding authorized and acceptable use of a computer system can make it difficult to prosecute violations when they occur. Legal cases exist in which defendants have been acquitted of charges for tampering with computer systems because no explicit notice was given prohibiting unauthorized use of the computer systems involved. In other cases, organizations have been taken to court for alleged violations of individual privacy because no notice was given and acknowledged regarding authorized monitoring of users' activities on computer systems.
Benefits	• Logon Banners are particularly important in cases that consider whether government employees enjoy a reasonable expectation of privacy in government computers. • Pre-logon warning messages can deter unauthorized use, increase IT security awareness, and provide a legal basis for prosecuting unauthorized access. • A key to establishing that a user has no right to privacy when using State networks and/or computer systems is the implementation of a logon banner.

Associated Architecture Levels	
Domain Name	Security
Discipline Name	Technical Controls
Technology Area Name	Logical Access Controls
Product Component Name	

Compliance Component Type	
Component Type	Guideline
Component Sub-type	

Compliance Detail	
Guideline, Standard or Legislation	Logon banners are required on all State Information Technology access points. Such a banner shall warn authorized and unauthorized users: • What is considered the proper use of the system. • Only authorized users are to proceed beyond the banner. • Users who login represent that they are authorized to do so. • Unauthorized system usage or abuse is subject to disciplinary action and/or civil and criminal action. • Use of the system constitutes consent to monitoring. • Use of the system constitutes consent to the retrieval and disclosure of information stored on the network. • Users of the system shall have no reasonable expectation of privacy in the network. • Contains express or implied limitations or authorizations relating to the purpose of any monitoring, who may conduct the monitoring, and what will be done with the fruits of any monitoring.

	• Require users to "click through" or otherwise acknowledge the banner before using the system. Logon banners should not identify sensitive information about the organization, the data systems, network, hardware, operating system, system configuration, or other internal matters. • The following is an example logon banner that could be used for users connecting to internal computer systems: NOTICE TO USERS This is a State computer system and is the property of the same. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized State and law enforcement personnel, as well as authorized officials of other agencies. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized personnel. Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. Do not continue to use this system if you do not agree to the conditions stated in this warning. • Each Agency should tailor its logon banners to their precise needs. • Any questions should be directed to your organization's legal counsel.		
Source Reference	NIST SP 800-18 (www.csrc.nist.gov/publications/nistpubs) CERT Guide to System and Network Security Practices (www.cert.org/security-improvement/)		
Standards Organizations			
Name	Carnegie Mellon University, CERT/Coordination Center (CERT/CC)	*Website*	www.cert.org
Contact Information	cert@cert.org		
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
KEYWORDS			
Keywords/Aliases	Logon, username, welcome screen		
COMPONENT CLASSIFICATION			
Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		

Rationale for Component Classification			
Rationale for Component Classification			
Conditional Use Restrictions			
Restrictions			
Migration Strategy			
Migration Strategy			
Impact Position Statement			
Position Statement on Impact			
CURRENT STATUS			
Current Status	☐ In Development ☐ Under Review ☒ Approved ☐ Rejected		
AUDIT TRAIL			
Creation Date	3/6/2003	Date Accepted / Rejected	3/24/2003
Reason for Rejection			
Last Date Reviewed		Last Date Updated	
Reason for Update			

Click on this link to return to the Security Blueprint Samples – Set Two.

TECHNOLOGY ARCHITECTURE COMMUNICATIONS DOCUMENT SAMPLES

APPLICATION DEVELOPMENT CLASSIFICATION REPORT

The following is an example of a communications document that Team Leaders or Managers might request. Once the Architecture Blueprints are documented, the range of communications documents is limited only by the requirements of the Audience and the criteria set forth by the architecture governance groups.

The Architecture Blueprint Vitality Process ensures the up-to-date data that is essential to the communication of useful information.

Domain: Application Architecture *Discipline:* Application Development Management

Technology Area	*Emerging Technologies*	*Current Technologies*	*Twilight Technologies*	*Sunset Technologies*
Analysis/Design Environment	• Object Oriented Analysis and Design • UML • CDIF	• Information Engineering	• Structured Analysis and Design	
Programming Language / Environment	• Java	• Visual Basic • COBOL II (MF, AS) • C • C++	• COBOL (MF, AS) • RPG (AS) • Pascal	
Code / Screen Generation	• Advantage Joe	• Advantage Plex	• Power Builder • Knowledgeware ADW	
Documentation	• 9 Standard Products	• JCIT reporting requirements		
Commercial Products	• CRM	• ERP • MRP	• General Ledger Software	

ELECTRONIC COLLABORATION CLASSIFICATION REPORT

Domain: Application Architecture | *Discipline:* Electronic Collaboration

Technology Area	*Emerging Technologies*	*Current Technologies*	*Twilight Technologies*	*Sunset Technologies*
E-mail		• SMTP • MIME • IMAP4 • POP3	• OV/VM • IMAP3 • POP2	
Document Format	• XML	• .rtf • .txt • .pdf		
Spreadsheet		• MS Excel	• SYLK	
Images	• JPEG 2000 • SVG	• .bmp • TIFF • GIF • JPEG • MPEG	• Proprietary	
Document Digitizing		• TWAIN • ISIS		
Character Recognition				
Document Endorsement and Authentication	• Digitized signature • Digitized signature with biometric data • PKI digital signature (X.509v3) • Biometric imprint	• Physical signature		
Calendaring	• ICAP • iCalendar	• MS Outlook		
Electronic Forms	• XHTML Extended Forms • XFA	• XFDL	• OFDL • OFML	
Multimedia	• MP3			

SECURITY CLASSIFICATION REPORT

Domain: Application Architecture | *Discipline:* Electronic Collaboration

Technology Area	*Emerging Technologies*	*Current Technologies*	*Twilight Technologies*	*Sunset Technologies*
Physical Security	• Smart Cards • Biometrics	• Cypher lock • Key card • Bar code	• Property stickers • Key locks	
User Security				
- Authentication	• Smart cards • Kerberos • Biometrics	• Token-based-2-factor • Certificates (x.509) • Passwords • RADIUS/TACACS	• Address-based	
- Authorization		• Directory-based services • LDAP	• Access-control-lists • X.500 • Password protected directories • OS-based systems	
- Audit		• Vendor specific • OS Specific	• SYSLOG	
Application Security	• Transport Layer Security (TSL)	• S/MIME • PGP • SSL • Middle-ware • Signed JAVA	• Privilege mode (root user) • Embedded Application specific security	
Hardware / System Security		• NT Domains • TOPSECRET/ RACF/TACACS • Virus control • Intrusion detection	• ACF2	
Data Security	• Advanced Encryption Standard (AES)	• CORBA • Virus control • PGP	• Embedded passwords	
Network Security	• AES (encryption)	• Firewalls/router ACL • IPSEC • Encryption (3 DES/RSA) • Encrypted VPN • Intrusion Detection • Vulnerability Scanners	• Dedicated lines	

Domain: Application Architecture | *Discipline:* Electronic Collaboration

Technology Area	*Emerging Technologies*	*Current Technologies*	*Twilight Technologies*	*Sunset Technologies*
Security Administration	• Directory-based services	• Product specific	• Product specific	

DOMAIN/DISCIPLINE – COMBINATIONS

The nine Domains used as the example for the Tool-Kit are compiled from information gathered from states and counties that are already working with their enterprise architecture. As the architecture sample models evolve, the domains may change.

The Domains are further broken out into 26 technical functional areas, described in this document as Disciplines. Table 1depicts the 26 disciplines and the domains as used in this document.

Descriptions of the type of information contained in the disciplines used in this document are located in Appendix D.
Each government entity should define the disciplines as appropriate for its enterprise. The descriptions provided in Appendix D are provided as basic information only. They are not meant to be prescriptive or to constrain the government entity in any way. However, there are implications to changing the number of domains. Carefully choose to collapse or expand the domains.

Typically, organizations define a group, such as a task force, working group, or committee the responsibility for developing/maintaining documentation, expertise relative to the domain, an updated architecture blueprint, etc. The number of domains should determine the number of groups defined. Coordination is required when documenting updates addressing disciplines that have relationships to several domains.

Domains	*Disciplines*
Information	• Data Management • Knowledge Management • GIS • Data Storage
Application	• Application Development Management • Electronic Collaboration
Integration	• Functional Integration • Middleware
Access	• Access • Branding • Accessibility
Network	• Physical Network • Network Management
Platform	• Platform • Configuration Management
Systems Management	• Asset Management • Change Management • Console/Event Management • Help Desk/Problem Management • Business Continuity
Privacy	• Profiling • Personalization • Privacy
Security	• Enterprise Security • Network Security • Host Security

Table 1. Domains & Disciplines

On the other hand, minimizing the number of domains may present the risk of once again dealing with a piece that becomes too huge to manage. It is best to keep the number of domains to a minimum of five and a maximum of 10.

The disciplines within each domain have been grouped logically, based on the close relationship between the discipline and the domain, as well as the relationships to other disciplines within the domain. Table 1 shows the disciplines and how they are grouped within the nine domains.
Figure 7 provides a pictorial view of the sample Domains that make up the Technology Architecture in this Tool-Kit.

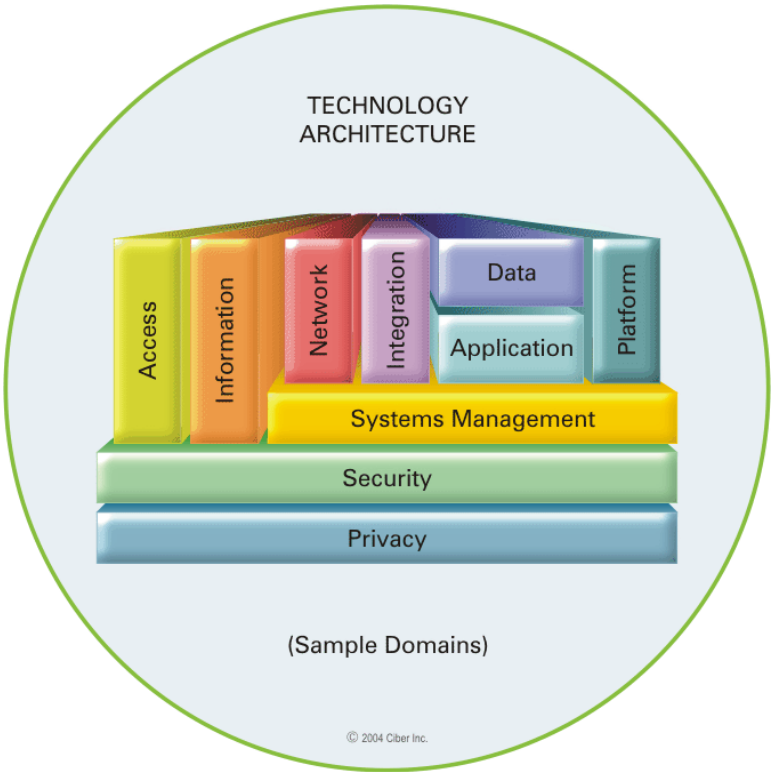


Figure 7. Sample Technology Architecture Domains

DOMAIN/DISCIPLINE – INTERSECTIONS

Be aware that disciplines can also intersect with disciplines in other domains. Note all intersections so that changes made in one discipline will not be overlooked in another related discipline.

The matrix in Table 2 portrays an example of the relationships between disciplines. As with the choice of domains and disciplines, your ideas of how the relationships match up may differ from the example here. This is merely the example of the tool that was used to assist in determining the organization of the disciplines and domains for this project.

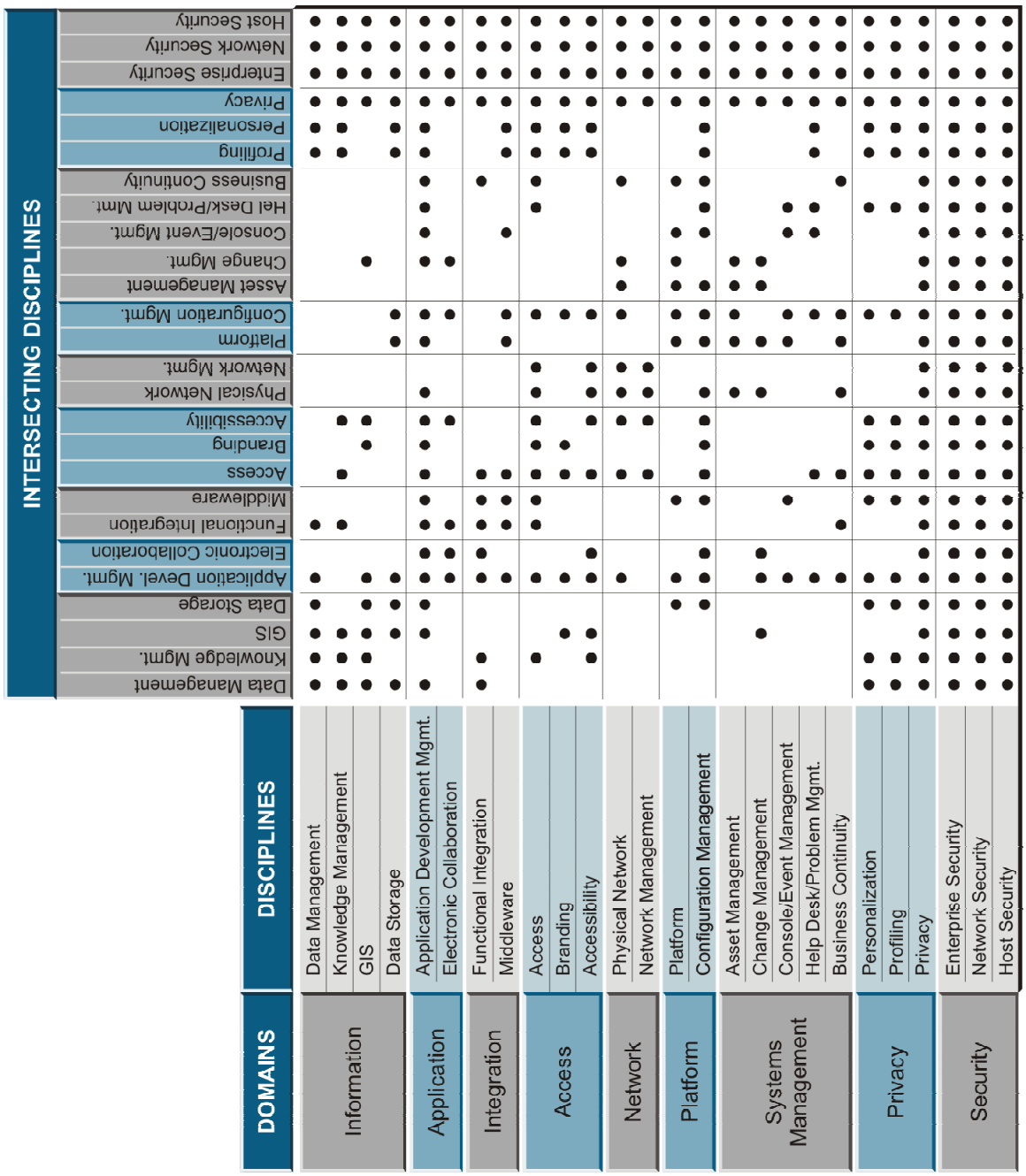
A tool such as this may be used within the organization to identify relationships and coordination efforts that must occur when decisions are made or changes are mandated. It is used for quickly identifying the points of coordination that are essential between the disciplines.

As mentioned earlier, when building a home we can rely on the experience of those who have previously built homes to provide plans and logical groupings of functions, such as plumbing, electrical, etc. By separating disciplines into logical categories, we can also utilize IT Subject Matter Experts in the various fields to perform the work or advise concerning items of importance.

Though the basic elements of every home built may follow a similar pattern, it is not necessary that every home be the same. In most cases, each home will have individual characteristics particular to the requirements of the owner, based on the environment, available funding, or personal preferences.

Likewise, while developing the enterprise architecture within the organization, be aware of required items and components particular to the organization and address them accordingly.

Table 2. Domain-Discipline Intersection Matrix



SUMMARY/CONCLUSION

The Technology Architecture provides a framework, based on business needs that are aligned with technology, for developing technology solutions that operate across agencies and align with the business needs of state and local governments.

It is through the pursuit of a formal Technology Architecture that the following are provided:

- A demonstrable, repeatable approach to assuring critical technology standards are documented and shared throughout the enterprise
- A clear understanding of the enterprise's emerging, current, twilight and sunset technology products and/or compliance standards.
- Identification of opportunities to leverage linkage across government-wide entities and increase collaboration and sharing of technology and information
- A means to increase re-use of technology, systems, application or configurations and reduce redundancy throughout the enterprise.

The Technology Architecture identifies and inter-relates the technology assets of the enterprise to enable sharing and exchange of critical information. Though enterprise typically refers to the organization as a whole, the development of Technology Architecture can also be accomplished at an agency level. For example, in North Carolina, compliance standards are determined at the enterprise (statewide) level, and the products are determined at the agency level, based on the enterprise standards.

NASCIO Online
Visit NASCIO on the web for the latest information on the Architecture Program or to download the current version of the Enterprise Architecture Development Tool-Kit.

www.nascio.org

Enterprise Architecture Facilitation Guides

July 2005

FACILITATION GUIDES

Introduction

This supplement is intended to be a library of facilitation guides used within the NASCIO community for facilitating the delivery of enterprise programs and projects.

NASCIO is interested in providing tools that will assist the wider government community launch and mature their enterprise architecture programs. The Architecture Working Group identified the need for tools to assist in ***facilitating*** the delivery process of enterprise architecture. That delivery process will require attention to governance, framework(s), methodology, training, facilitating, and many other dimensions for insuring the successful initiation and vitality of an enterprise architecture program. If there is a primary dimension that requires more attention and careful planning than the others it is organization – ***i.e., the people side of enterprise architecture***. It is critical to the success of any enterprise architecture program that people are drawn into the activities of enterprise architecture delivery through effective communication and collaboration.

This supplement of the NASCIO Enterprise Architecture Tool-Kit is intended to collect and share a variety of facilitation guides from members of the NASCIO community. NASCIO members have addressed various aspects of program implementation and architecture development depending upon their unique circumstances and priorities. The aspects presented include the following subjects:

- *guidance on facilitation of meetings and workshops;*
- *establishing teams and team membership;*
- *gaining participation from team members;*
- *resolving conflict;*
- *record keeping of decisions and action items;*
- *keeping the team spirit alive;*
- *maintaining productive working relationships;*
- *keeping the team on track;*
- *approaches for productively exercising an established methodology;*
- *researching new technologies;*
- *gap analysis; and*
- *conducting compliance reviews*

As enterprise architecture is a program, the continued vitality of such a program is dependent on continued effective planning and execution in delivering enterprise architecture elements. For example, it can be expected that teams and committees will be required to deal with issues where there is a diversity of opinion. The creativity inherent in a team must be fully leveraged, while maintaining a course of action that delivers the intended results within the constraints of budget and schedules. Effective use of facilitation tools can expedite establishing consensus on the issues while maintaining a positive team spirit. This approach recognizes that the team will have many more mountains to climb after the current issues are identified, discussed, and resolved. The project team must be good at solving problems in an effective, productive manner. Conflict must be recognized as inevitable, and must be faced with objectivity and a strategic perspective – an enterprise perspective.

The following guides are presented with the understanding that there is also a diversity in the level of skill and experience among facilitators. The guides presented are pragmatic and can assist individuals at all

levels of skill and experience. It is expected that everyone will find the varied aspects of these materials useful in continuing to develop skills and expertise in the broad discipline of facilitation.

State of Connecticut
Enterprise Architecture Planning
Domain Team Guidebook

Developed for Domain Team Leaders
and Team Members

Single Document Version 2.0
June 2005

Department of Information Technology
Enterprise Architecture Program Office

Table of Contents

Section 1. Introduction to the Domain Team Operations Manual

As an active participant in the State of Connecticut Enterprise Architecture Program, you are aware that an Enterprise-wide Technical Architecture (EWTA) is never completed. For that reason, the Department of Information Technology (DOIT) felt it necessary to create a guidebook to be utilized as a reference when progressing through the processes involved in maintaining the EWTA. This document will guide domain team leaders, team members and subcommittee members through the various technical and governance processes that have been defined to make EWTA a self-sustaining program.

Background and Goals

DOIT embarked on a project in April 2000 to create a statewide technical architecture to provide the framework for making strategic technology investment decisions on a cost effective, enterprise basis. These IT decisions must also meet the diverse business needs of the agencies in the executive branch, the constitutional officers, higher education institutions, and the other branches of state government. It was determined from the beginning of the project that to be successful, the State of Connecticut's technical architecture would have to:

- Be based on the strategic business direction of the state as an enterprise.
- Be based on a planning process that supports strategic business planning as well as ongoing tactical decisions made when implementing systems.
- Involve agency business managers as well as IT staff throughout the process.
- Provide strategic direction for making technology decisions without requiring wholesale and major changes to the current IT environment.
- Allow agencies to share many IT infrastructure components without sacrificing responsiveness to the changing business needs of individual agencies.
- Reduce the time it takes IT to satisfy ever shorter agency business change cycles by making the IT environment adaptable to change.
- Reduce the cost of IT over the lifecycle of each system.
- Have a governance process that supports the ongoing evolution of the architecture as well as its enforcement.
- Evolve in synch with changing business strategies.
- Be implemented in a short amount of time to avoid analysis paralysis.

In May 2000, an Architecture Team, made up of six DOIT managers and six senior agency managers, was established to discover and articulate the enterprise business requirements of the State for use within the EWTA process. These business requirements were documented in two essential documents: the Common Requirements Vision and the Conceptual Architecture Principles.

The Common Requirements Vision represents the environmental trends, major business drivers, business information requirements and requirements for technical architecture that tie the IT architecture to the business needs of the agencies

The nine original technical architecture domains:

1. Platforms
2. Networks
3. Security
4. Enterprise Systems Management
5. Middleware
6. Data Management and Data Warehouses
7. Application Development
8. Collaboration and Directory Services
9. Web / E-Government

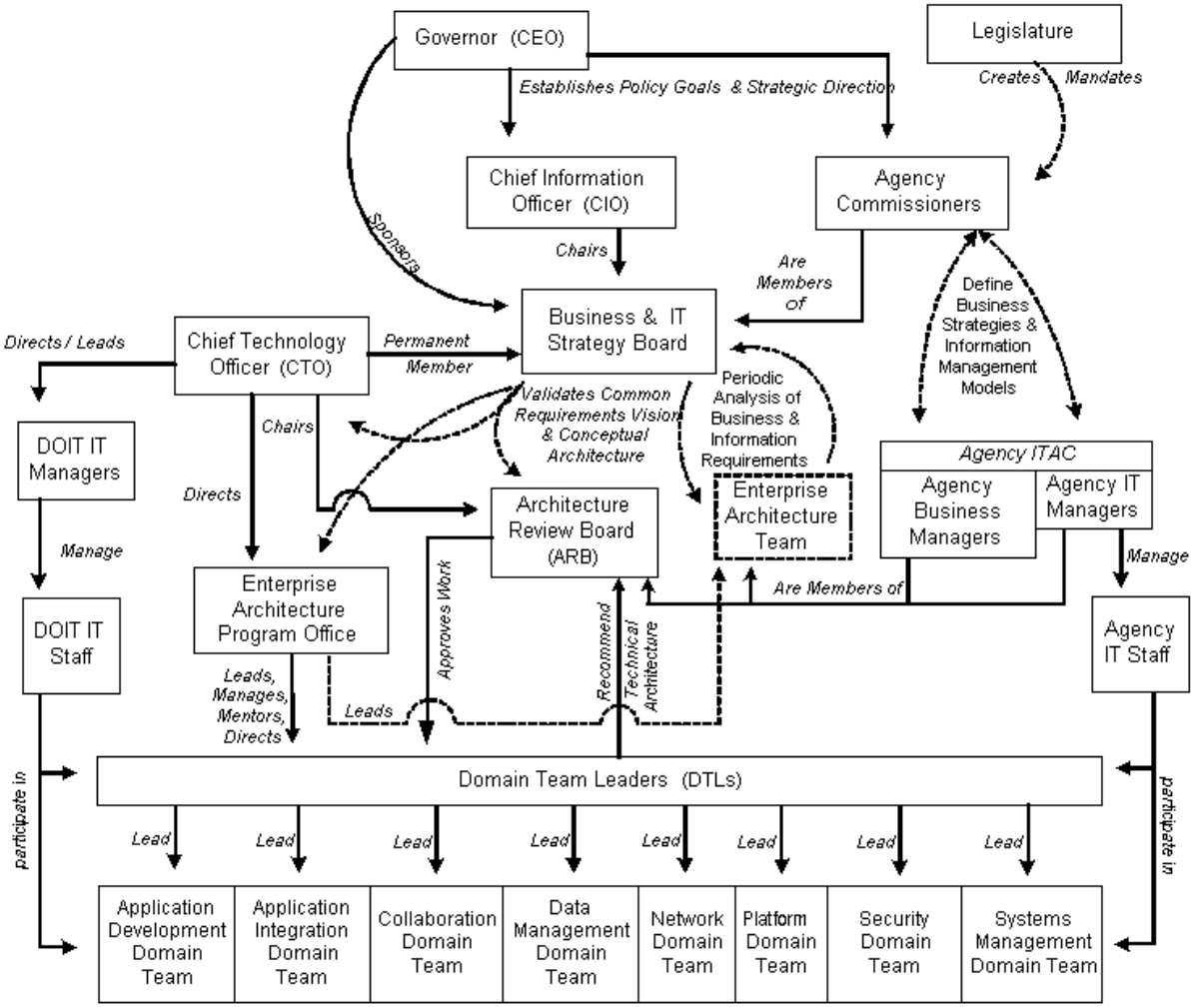
and the State. The Conceptual Architecture Principles represent the core business and technical principles on which all the technical domain architectures are based. That history and overview is captured in the Enterprise-wide Technical Architecture Introduction which can be found on the Internet at http://www.ct.gov/doit/lib/doit/downloads/intro.pdf .

The Architecture Team defined nine domains, or groups of related technology, that include most of the components utilized in information technology. Nine teams of technical experts from throughout the State of Connecticut were deployed to develop the initial technical architecture for each domain. The results are documented in the original nine Domain Technical Architecture Documents that were published in January of 2001. The current versions of the technical architectures and their associated appendices and guidelines are available online at http://www.ct.gov/doit/cwp/view.asp?a=1245&q=253968 . These documents define design principles, technical standards, product standards, and implementation guidelines that will be utilized by the agencies and DOIT, as well as vendors and consultants implementing state systems. It is the responsibility of the domain teams to maintain and update the domain technical architectures when changes in the environment occur. Major changes to the domain architectures are handled through a formal process that involves the Architecture Review Board.

Current Governance Model

State Government – Connecticut

The following diagram illustrates the Architecture Governance Model for the State of Connecticut.



Formal Governance Groups of the EWTA

To create and maintain the EWTA, an organizational structure was put in place. These EA specific groups interface with other organizational entities normally found in an enterprise IT services group. The following is a description of the different governance groups involved in the process and their roles.

CIO

The Chief Information Officer is the executive sponsor for the Enterprise Architecture Program. As DOIT's agency head, reporting directly to the governor, the CIO is a primary point of contact with the policy and program functions in State government, including the agency commissioners, who are both peers and customers.

Business and IT Strategy Board

The Business and IT Strategy Board exists to ensure the alignment of IT with the business requirements of the State and its agencies. This group verifies the Common Requirements Vision and approves the Conceptual Architecture Principles of the EWTA. The board works with the Architecture Team to keep the Requirements for Technical Architecture and the Conceptual Architecture Principles current with the business needs of the State. They provide important advice and support for new statewide IT initiatives and policies, as well as adjudicate final appeals for exceptions to architecture standards. This board is chaired by the Chief Information Officer.

Architecture Review Board

The Architecture Review Board (ARB) is responsible for the approval, promotion and enforcement of the technical standards. Its membership consists of senior State IT and business managers. The ARB approves domain team deliverables (i.e. technical standards, design principles, product standards, best practices, and standardized configurations) and adjudicates requests for exceptions to architecture standards. This board is chaired by the Chief Technology Officer.

Technical Domain Teams

The technical domain teams provide the knowledge and expertise required to develop the technical architectures and standards for the EWTA process. Each team consists of technical experts from throughout the State. These teams are responsible for the development and maintenance of the Domain Architecture Documents, including the domain specific deliverables. The teams are expected to keep abreast of new technology and make recommendations on new technology to address deficiencies in the current environment. The teams also participate in the Exception Process. Each team is lead by a senior technical person with broad knowledge in the subject areas covered by the team and deep knowledge in one or more of the technologies addressed within the domain technical architecture.

Enterprise Architecture Team

The architecture team translates the agencies' requirements into business driven IT direction statements. Its members include senior IT and agency business mangers. This important team develops and updates the Common Requirement Vision and Conceptual Architecture Principles that document the business requirements of the State that must be addressed by the technical architecture. This is not a permanent group. It is activated on a periodic basis or whenever a major change occurs that was not anticipated in the previous analysis of business requirements.

Enterprise Architecture Program Office

The Enterprise Architecture Program Office (EAPO) coordinates the execution of the EWTA processes. The office is responsible for coordinating all technical domain team activities, as well as communications and the publication of EWTA deliverables.

Director of Architecture

The Director of Architecture is responsible for the design and direction of the governance activities associated with the development and implementation of the enterprise technical architecture. The director ensures that the EA Program Office is aware of and attuned to evolving business requirements and information technology strategies. The director is also responsible for intra-agency and inter-agency communications related to the EA Program. The State of Connecticut Enterprise Architecture Program Office was previously the Division of Architecture & Planning which was headed by a Director level position. The Director retired in the spring of 2003 and the position was not refilled. The Chief Technology Officer has been serving as the Chief Architect for the EA Program. We believe the functions served by a full time Director are essential to the long term viability of an Enterprise Architecture Program.

Using the Guidebook

This manual is designed to provide guidance to domain team leaders, domain team and subcommittee members as well as subcommittee chairpersons in developing, updating, and refining the EWTA technical domain architectures and their associated appendices and implementation guidelines.

The chapters are organized as follow:

- Team Management Guidelines – for team leaders. Provides guidance on organizing and managing domain teams and their workload; also provides information on team member roles and responsibilities.
- Developing a New Domain Architecture – for new team members or team leaders developing a new technical domain. Provides basic information on what domain architecture is, and the process used to develop it in the first place.
- Updating a Domain Architecture –for team leaders, team and subcommittee members. Provides reference material about what triggers the need for a change to the domain architecture, the process for documenting recommendations for the update, and how updates are approved and published.
- Identifying and Closing Gaps in a Domain Architecture – for team leaders, team and subcommittee members. Provides guidance on how to perform gap identification, analysis and resolution for a domain architecture.
- Researching New Technologies, Products and Standards – for team leaders, team and subcommittee members. Provides guidance on how research of technology is conducted and documenting the outcome.
- Relating Domain Architecture to Infrastructure – for team leaders, team and subcommittee members, infrastructure service managers and project teams. Describes the relationship of the architecture work by domain teams and the enterprise infrastructure that is being planned and implemented by DOIT.
- Conducting Architecture Conformance Reviews – for team leaders. Describes the process used to assess conformance to architecture standards.

- The Appendices - provides the templates used to structure EWTA deliverables, EWTA process diagrams, roles and responsibilities of all EWTA governance bodies, an example of a domain specific configuration management process, and other relevant background information. In addition, these are many links back to the EWTA material and the published technical domain documents for reference.

Section 2. Team Management Guidelines

The following section is designed to provide guidelines for domain team leaders on managing domain team activities, organizing and prioritizing workloads, and documenting deliverables. In addition, it will provide clarification of roles and responsibilities for members of the domain team, subcommittee members and chairpersons involved with domain activities.

Roles and Responsibilities

Domain Team Leader

Each domain of the Enterprise-wide Technical Architecture (EWTA) has a leader who leads the activities of the domain team to keep the domain architecture current and relevant, and represents the team in cross-domain and enterprise architecture planning activities. The minimum time commitment for this role is .2 FTE.

The responsibilities of the team leader include leading or coordinating all team activities, communications and outputs. These include:

- Periodic updating of the content for the domain architecture and associated documents.
- Assigning and leading the domain team members, including scheduling regular meetings and ensuring a broad base of expertise on the team to cover the technical components making up the domain.
- Assuring that the technical components assigned to the domain are appropriate and providing any cross-domain coordination for components if needed.
- Developing and managing the execution of a work plan for all activities and deliverables that the team is responsible for, including:
  a. Decomposing Conceptual Architecture Principles into domain specific principles.
  b. Developing domain specific deliverables (i.e., design principles, technical standards, product standards, standard configurations, and guidelines).
  c. Coordinating on-going research activities of team members such as utilization of external research services and vendor presentations.
  d. Performing gap analyses to identify gaps between the installed base and the future state for each of the technologies within the domain team's purview.
  e. Recommending initiatives to resolve gaps.
  f. Evaluating projects or proposals for conformance to architecture.
  g. Ensuring that the domain architecture and documents are reviewed and refreshed as needed.
- Identifying resource needs required by the team for tasks listed above as part of work plan development.
- Overseeing subcommittees assigned to deliver specific tasks for the domain team.
- Coordinating and communicating with other domain teams and with infrastructure service managers, the Enterprise Architecture Program Office and the Architecture Review Board.
- Documenting the domain architecture, preparing status reports and other deliverables required for approval of domain architecture additions or modifications.

Domain Team Members

The domain technical teams provide the knowledge and expertise required to define the technical architectures. These teams are responsible for the development and maintenance of the content for the domain architecture documents, including all domain specific deliverables (i.e. design principles, technical standards, reference models, product standards, standard configurations, and best practices). The teams are expected to keep abreast of new technologies and make recommendations on their potential to address deficiencies in the current environment. The minimum time commitment for this role is .1 FTE, depending on how many components the individual is covering.

Each domain team of the EWTA consists of agency and DOIT technical personnel who have expertise in one or more technical components that make up the domain architecture. Membership is usually assigned on a year-to-year basis and members are expected to keep abreast of the technical trends and standards for their area of expertise. They provide support and consulting for the domain team based on what is best for the State of Connecticut as an enterprise.

Responsibilities of team members include:

- Attending regular domain team meetings.
- Ongoing enhancement of the domain architecture via tasks assigned by team leader.
- Ongoing research for assigned technical areas based on the member's expertise.
- Leading as chair or participating as a member of a technical architecture subcommittee.
- Providing technical consulting in assigned technical areas as directed by team leader.
- Communicating EWTA goals and the domain architecture to agencies and vendors.

Domain Subcommittees

Subcommittees are created by the domain team leader to work on a specific task or project related to the domain architecture. The domain team leader works with the subcommittee to define specific objectives, tasks, deliverables and evaluation criteria for these subcommittees, and assigns a subcommittee chairperson to oversee the group. The chairperson is typically the most experienced expert in the technology being investigated.

The subcommittee chair oversees the group and communicates the recommendations back to the domain team for discussion and approval. Subcommittees are often used to research, evaluate and make recommendations for new technical or product standards for the domain and to author associated implementation guidelines.

Responsibilities of the subcommittee chairperson include:

- Leading the activities of the subcommittee.
- Reporting status of activities back to the team leader.
- Ensuring completion and quality of deliverables assigned to the subcommittee.

Domain Team Meetings

Team meetings should be conducted at least quarterly with the entire domain team. Additional sessions can be scheduled at the discretion of the domain team leader, but subcommittees will conduct most domain teamwork between quarterly meetings. Subcommittees will meet at the discretion of the domain team leader or the subcommittee chairperson for that group. The

domain team leader should speak with all subcommittee chairs on a weekly basis to monitor progress and to surface any issues for resolution.

The quarterly meetings of the domain team should be documented with minutes or a meeting summary (see Form DT-6 Quarterly Status Report from a Domain Team in Appendix 2). Decisions made by the team that resulted in changes to the domain architecture should be reviewed and verified at the quarterly meetings.

How to target, qualify, obtain and retain team members

Each EWTA domain is made up of a group of related technologies or components. While it is ideal to have an expert on the team for each technology component, experts may not exist in the State for some components and the team size needs to be kept to a manageable number. Domain teams of six to ten members are recommended. The goal is to maintain a broad level of expertise across the team with some members responsible for one or more technologies. Additional technology expertise from outside the team can be used on subcommittees for specific research activities.

Recruiting the best-qualified personnel is one of the most difficult tasks of the domain team leader, since the best-qualified personnel are usually the busiest. Methods for targeting needed expertise include:

- Word-of-mouth among domain team members (the domain team members represent a community of technicians that often know who their peers are across the State and know it is in their best interests to have a qualified team).
- Utilizing the DP Skills Inventory, when implemented by DOIT, to get a profile of personnel experience in the state.
- Posting opportunities in various list services and newsletters that are available to these technical experts.
- Identifying agency or DOIT projects that will require training in-house personnel or acquiring outside expertise in a technology area that is not covered by anyone on the team. Specialized technical expertise that must be acquired for an agency or DOIT project could be utilized by the domain team to help the team evaluate the technology from a statewide perspective.
- Utilizing the other EWTA groups such as the EA Program Office, the ARB or the Business and IT Strategy Board to find in-house expertise.

Qualifying the potential new member will require an understanding of the experience and competence needed for that technology component. Ideally, members should have some hands on experience with major aspects of the targeted technology.

With the constant changes in technology, team leaders should look for a profile of expertise that demonstrates an understanding and aptitude for this area of technology. Team members should have an understanding of the technology and how it is applied, rather than just experience with one or two products or technology components. Team leaders can work with the EA Program Office to target appropriate training and access to research to round out the experience of team members.

Once a qualified person has been identified, the next step is to get them on-board. While knowledge of the EWTA process is reaching more agencies, you should not assume that the

person knows anything about EWTA or architecture. Getting their interest will depend on your ability to convince them that the time spent in this process has value to them and the State of Connecticut. It would be prudent to identify other people with source credibility that this person can talk to about the value of the process.

After an individual has agreed to participate in the domain team, the next step is to get clearance from their management to give them adequate time to participate. Team leaders should work with the EA Program Office to communicate the value of EWTA directly to the new member's management. The value must be articulated in terms of how it may help that agency, the projects being planned or implemented, the expertise of the person needed, and the ability to integrate systems with outside agencies and organizations. The time commitment may need to be limited at first until the qualified person or their management sees this value. This may mean limiting their involvement to a particular subcommittee or initiative at first. It may also mean getting an endorsement from the ARB, the Business &IT Strategy Board, or DOIT management to demonstrate the importance of their participation to the State of Connecticut.

To retain valuable technical expertise on the domain team or any subcommittee, it is important that members, and their management, are aware of the accomplishments of the team. Team members should always be encouraged and rewarded when possible for their work and never taken for granted.

Training requirements

All team leaders should attend the introductory training for EWTA. This provides context on how the process works and why, and on their role in the process. Periodic classes on EWTA for domain team members will be made available as the program evolves. In addition, all team members should be encouraged to receive training in their areas of expertise. While DOIT is not providing direct funding for individuals to do this, appropriate training is often a matter of knowing what classes are available and convincing members' management as to its value. Team leaders should obtain and share information on training opportunities in their domain. A team leader should expect to provide mentoring for a replacement team leader, through at least the first team meeting.

DOIT normally provides for half-day briefings by experts from external research services and web access to research materials. Some vendors provide product training at no cost. It is up to the domain team leader and team members to take advantage of these opportunities. There are also many specialized list services and web sites designed to keep technology communities updated and in touch. In addition, initiatives to define standards and best practices in new technologies will require vendor assessments and on-site visits, which provide opportunities to learn.

Documentation and status report requirements

The technical domain architecture documents themselves are the primary documentation responsibility of the team leader, using content provided by the team. These documents are the repository of information describing domain technology components, as well as the associated standards, design principles, reference models, and guidelines that will be used by agency personnel or vendors and consultants working for agencies to implement systems. It is important that these documents continue to be updated and enhanced so that the work of the domain team

has meaningful impact on all systems being built or enhanced. The process and associated documentation requirements are described in the Updating a Domain Architecture section of this guideline.

Monthly domain team meetings should be documented with minutes or a meeting summary and shared with the other domain teams to give everyone information on what activities and issues are being addressed. This provides information needed to identify and coordinate cross-domain activities (see Form DT-6 Monthly Status Report from a Domain Team in Appendix 2). Subcommittees must provide status reports on active initiatives to the domain team leader as well. The decision on the format of this report is left up to the domain team leader.

Managing and prioritizing workloads of domain teams

Domain team members are normally expected to be available for one day a month to support the work of the team. Additional time may be requested of a member for work on a subcommittee, with a subcommittee chairman possibly requiring up to one day a week. A team leader normally requires the equivalent of one day a week to manage a domain team, meet with other domain team leaders to discuss cross-domain issues, and to represent the team for consulting and compliance engagements. Additional time may be by team leaders to oversee the work of subcommittees, deal with gaps, track the status of domain work, and conduct their own research.

With limited available resources and the significant amount of work involved in the architecture process, it is important that workloads be identified and organized. This workload planning is one of the important responsibilities of the domain team leader.

Prioritizing Workloads

Before workload can be defined and delegated, it is important to categorize the work so that it can be prioritized on an ongoing basis. While work should be prioritized within each category, the categories have different priorities relative to each other. Domain team workload can be categorized and prioritized on the following basis:

Responding to changes in the State's business needs

The successful implementation of EWTA is dependent on the technical domain architectures being able to directly support the business drivers and their associated Conceptual Architecture Principles. Therefore, the domain architecture must be reviewed periodically to assess the impact of changes to the business drivers and environmental trends of the State. This review must be the highest priority because of the potential impact to the ongoing work of the team. This work normally is completed within two weeks of getting new Conceptual Architecture Principles or Requirements for Technical Architecture.

Gap Initiatives

Beyond the annual refresh of the domain architecture and ongoing work on the domain documents, completing gap initiatives is the core ongoing work of the teams (see section entitled Identifying and Closing Gaps in a Domain Architecture). Gaps are prioritized once or twice a year by the teams and in conjunction with the other teams. Project plans for the highest priority gap initiatives are completed by the domain team leader and assigned to subcommittees to complete them. Priorities for gap initiatives are usually based on team input, the dependencies of

other domains, DOIT priorities and availability of resources. While additional gaps may be found throughout the year, gap priorities do not change that often. Gap initiatives are the second highest priority for ongoing domain work.

Architecture Conformance Reviews

Domain teams have a role to play in the governance of the EWTA. One aspect of this is to review proposals to RFPs for architecture conformance. This activity can range from providing consultation on standards and implementation issues at a meeting with an agency, to a documented conformance review of a multi-million dollar vendor proposal to an RFP. The later can involve a significant amount of work (especially evaluating multiple proposals). This work is usually considered a high priority because it usually involves large projects and affects their timetables. Team leaders are dependent on good project planning by agencies to ensure that this work can be scheduled in a timely manner and with a minimum of interruption to the ongoing work of the team. Team leaders should work closely with the EA Program Office and resource owners or scheduling function to estimate resource requirements and schedule time for work. Conformance reviews can take two to three weeks to complete and may require several team members' participation. Reviews requiring significant resource time may require leaders to document the impact on other projects and report this to the ARB for assessment.

Evaluating agency and infrastructure projects, and exception requests

Another ongoing governance responsibility of domain teams is the review of new agency and infrastructure projects during architecture consultations and conformance evaluations. In addition, agencies may file exceptions to the architecture with the Architecture Review Board that may result in an ARB request to the domain team for a written evaluation.

These evaluations are also a high priority, team leaders should try to monitor ongoing agency and DOIT projects to better anticipate, and schedule resource needs. This requires a close working relationship with the resource owners or scheduling function to provide advanced planning and resource requirement information to the Architecture Division and the domain team leaders.

Updating the domain architecture

To be meaningful, the domain architecture must be updated periodically to relate to changes in the State's needs as well as the technology available. In addition, the domain architecture documents should be refined to make them more useful and to provide reference models and guidelines for implementing the architecture.

This ongoing updating and refinement process is not as high a priority as the previous categories, but the resources and work involved must be accounted for in work plans to ensure it takes place. Much of this updating is an outcome of the EWTA Update Process, while the refinement of documents requires a more diligent management approach by team leaders.

Researching technology components and training

Domain team members should be assigned specific technology components to keep abreast of and identify changes in technology trends that may effect the refresh cycle or cause a gap in the architecture. Adequate time and access to information and training should be allocated to each expert, although most IT professionals keep up with technology related to their expertise during work hours while completing other duties. See Section 6 Researching New Technologies,

Products and Standards section for more information on this activity.

Developing and documenting work plans for domain teams

With the need to balance the workload and priorities of different categories of work in a domain, team leaders need to organize all work with a comprehensive work plan. A template is provided in Appendix 2 (Form DT-4 Gap Analysis Report from a Domain Team) to help team leaders monitor resources needed, timeframes required and deliverables involved with each task involving the team.

Work involving gap initiatives will be documented in an Action Plan (Form DT-1 Action Plan for a Domain Architecture Update requiring Architecture Review Board Approval in Appendix 2) so that it can be delegated to subcommittees for completion. Other work of the team can be managed using only the work plan. The domain work plan should facilitate the organization and scheduling of work as well as to adjusting to the impact of new priorities such as compliance reviews and project evaluations.

Use of subcommittees for projects

Subcommittees should be used whenever work does not need the entire team. Managing a subcommittee involves more coordination, but the EWTA Update process has several forms to facilitate this. The subcommittee chair oversees the group and provides status reports to the domain team leader. When the subcommittee has completed its work, the chair communicates the recommendations back to the full domain team for discussion and approval. See the Updating a Domain Architecture section for more details on how to use subcommittees to manage workload.

Implementing Architecture

Question: Who is responsible for implementing the architecture? *Answer:* Everyone

Ideally, architecture guides **all** IT decision making (infrastructure, application development, operations, etc.). An awareness of architectural conformance must become second nature. The domain architectures are intended to provide guidance for many day-to-day IT activities. For example:

- IT procurement
- Buy-versus-build decisions
- Setting evaluation criteria in RFPs
- Hardware upgrading
- Software package/tool selection
- Design decisions in the context of a specific IT project/system

Section 3. Developing a New Domain Architecture

It's a creative process, not a cookbook!

This section is about creating a domain architecture for the first time. The process for updating an existing domain architecture is discussed in the next section of the guidebook. This section should be read by anyone who is unfamiliar with the EWTA process, in particular new members of existing domain teams or teams assigned to develop the architecture for a new domain. The most important thing to remember about developing a domain architecture is that it is a collaborative, iterative, creative process. A team effort is required because of the complexity of the individual technologies and their interdependencies. Domain architectures are never done because change is a constant in the realm of information technology and in the realm of government services. Architecture development is a creative endeavor that requires thoughtful analysis and inspired thinking to respond to the many challenges inherent in an architectural approach to deploying and managing technology to satisfy the business needs of the agencies.

What is a domain?

A domain comprises a group of related technologies, usually organized around common IT infrastructure services or information management functions. The Director of Architecture is responsible for determining how many technology domains are appropriate and assigning individual technologies to them. The list of technologies typically contains those currently in use and new technologies that are likely to be implemented in the near future. There are currently nine domains: Application Development, Collaboration & Directory Services, Data Management & Data Warehouse, Enterprise Systems Management, Middleware, Network, Platform, Security, and Web/E-Government. For the list of technologies covered by each of these domains see Appendix 3.

What is a domain architecture?

A domain architecture acknowledges and interprets the Conceptual Architecture and the Requirements for Technical Architecture in terms of the specific technologies and products associated with the domain. The architecture defines:

- General principles adopted from the Conceptual Architecture with rationales and implications further articulated for the domain technologies.
- Design principles specific to the domain technologies.
- Technical standards for the domain technologies.
- Reference models for implementing the domain technologies.
- Product standards for the domain technologies.
- Standardized configurations and reusable components for the domain technologies.
- Guidelines and methods for the implementation and management of the domain technologies.

Why do we want domain architectures?

The Enterprise-wide Technical Architecture (EWTA) is an interrelated set of domain architectures. They are intended to guide all IT activities to support the State's business

strategies and information requirements. These activities include the planning, design, selection, construction, deployment, support and management of information technologies. Over time, as the Enterprise Architecture Planning Program matures, the information requirements will be articulated as a formal information architecture. The EWTA also provides the basis for evaluating and prioritizing changes to the State's portfolio of information systems (referred to as the Applications Portfolio).

What is a domain architecture based on?

When a domain team is charged with developing the technical architecture for a group of related technologies, the framework for their research and deliberations is provided by the Conceptual Architecture. The rationale for doing this is twofold. First, the use of a common framework allows multiple teams to work in parallel with some assurance that their recommendations will align with each other and support the work of domains with which there is technological overlap. Secondly, the domain architecture is based on a set of principles and requirements that are derived from the agencies' business drivers and business strategies. Defining the domain architectures within this business context provides the initial alignment of information technology to the State's business needs.

To provide a context for domain decisions, it is useful to have a mental map of the relationships between the deliverables defined during the creation of the Conceptual Architecture. Those relationships are as follows.

Environmental Trends – The environmental and technological trends that are driving change in the agencies. They include important internal and external forces as well as government trends at the federal, state and local levels.

Agency Business Strategies – The intentional responses of the agencies to each of their respective business drivers.

Enterprise Business Drivers – A consolidated list of the essential business change drivers that are common to a majority of State agencies and require a statewide technological response.

Enterprise Business Information Requirements – Who needs information, what information do they need, where do they need it, when do they need it, where does it come from, and what are the currency and integrity issues for that information. These information management issues are considered for each of the State's enterprise business drivers.

Requirements for Technical Architecture - What is required of the technical architecture to support the business information requirements of the State as an enterprise.

The Conceptual Architecture Principles – the core business and technical principles upon which domain architecture principles are based.

For an explanation of the process via which each of these deliverables is created, the reader is referred to the description of the Enterprise Architecture Process documented on the DOIT web site at http://www.ct.gov/doit/cwp/view.asp?a=1245&q=253980.

Team Leader Activities

The Domain Team Leader must lead, guide, push, pull, cajole and encourage the team members to complete their individual assignments and to fulfill the responsibilities of the team. Architecture development is an iterative creative process. The team should be encouraged to approach its work with an open mind and leave sacred cows behind. Team leaders should strive to develop a rapport with each of the team members and to foster an atmosphere of mutual respect within the team. Delegation of work to team members is not only good survival strategy, but the team will be more effective when the members realize they are empowered to guide technology decisions for the State.

As coordinator of all domain team activities, it is imperative for the team leader to be well organized and to communicate openly and frequently with team members. Every member of the team must have complete and current documentation and understand what is expected of them at each step of the development of the domain architecture. Open and active communication with the Enterprise Architecture Program Office, with the other domain team leaders and with infrastructure service managers will be essential for the coordination and resolution of cross-domain issues. A number of technologies and technical standards impact multiple domains and will require creative thinking and collaboration across domain team boundaries.

The team leader is responsible for all documentation generated for publication as part of the domain architecture. Delegation of responsibility for meeting minutes and draft documents is appropriate, but the team leader is responsible for the quality and completeness of any documentation produced by the team and all its subcommittees. See Standard Format for Domain Team Documents below for information about the format and content requirements for domain team deliverables.

Domain Team Activities

Review and Acceptance of the Domain Technologies

The first task of a newly formed domain team is to review the technologies assigned to the domain by the Architecture Team. If the domain team believes that a technology is more appropriately addressed in another domain, that recommendation must be proposed to the Director of Architecture. When the list of technologies is finished, the domain team leader must assess whether the team has the knowledge and experience to address all the technologies. The EA Program Office can then assist with recruitment of missing subject matter experts.

Review of Functionality and Major Issues for the Domain Technologies

It is important to organize the working list of domain technologies into functional categories in order to establish a baseline understanding of the technologies, and to facilitate prioritization and delegation of work. The team then prepares a list of functions that should be addressed within each category. Missing technologies will be revealed during this brainstorming activity. The master list of domain technologies is then revised. A list of issues is defined for each of the technology categories within the domain. This information will help set priorities for the domain team's work, especially if the team will not be able to address all technologies within the time allowed for the initial development of the domain architecture.

Review and Adoption of Conceptual Architecture Principles

A thorough grounding in the Conceptual Architecture is essential to the successful development of the enterprise architecture. Therefore, the third major task of the domain team is to analyze and interpret the Conceptual Architecture Principles in terms of the domain's technologies. This analysis results in the adoption of Conceptual Architecture Principles as general principles for the domain, with rationales and implications that are specific to the technologies within the domain. Implications will become important during the completion of gap analysis activities. It is important that thoughtful consideration be given to implications of implementing domain technologies so that they conform to the Conceptual Architecture Principles.

Review and Interpretation of RTAs for Domain Technologies

The fourth major task of the domain team is to analyze and interpret the Requirements for Technical Architecture (RTAs) in terms of the domain's technologies. This will assist with the definition of domain architecture principles, and identification of gaps in infrastructure services and support organizations. RTAs will also guide the selection of technical standards within the domain.

Defining Design Principles Specific to the Domain Technologies

During the analysis of Conceptual Architecture Principles and the Requirements for Technical Architecture, it will become apparent that additional principles are needed to guide the implementation of domain technologies. These design principles must be documented in the same format as the general principles, complete with rationales and implications.

Setting Priorities for Domain Team Work

The team must establish priorities for its work based on a number of factors. These include:

- Availability of subject matter experts.
- Need for infrastructure services that conform to the Conceptual Architecture and satisfy the Requirements for Technical Architecture.
- Severity and urgency of issues, and the priorities and budget of the Department of Information Technology and the State's other agencies.
- Major agency projects that require architecture guidance.
- Availability of resources to define low-level architecture specifications for configurations and to write implementation guidelines based on practical experience.
- Time available to complete the first iteration of architecture development.

Domain Architecture Gap Analysis

The first time through the EWTA process, there is usually insufficient time or expertise on the domain team to cover everything. These are gaps within the domain architecture itself. If current products or standards are not capable of meeting the strategic goals of the EWTA, they are also gaps in the domain architecture. Each of the functional areas or technologies within the domain that require further research and analysis will be prioritized and incorporated into the domain team work plan by the team leader. See Section5 Identifying and Closing Gaps in a Domain Architecture for additional information.

Review and Acceptance of all Subject Matter Expert Work

Some of the domain team's work will be delegated to members with deep technical knowledge and practical experience with one or more of the technologies. This allows multiple architecture research and evaluation efforts to run concurrently. All deliverables from subcommittees are subject to review and acceptance by the full domain team. The team is responsible for ensuring that lower level decisions remain true to the Conceptual Architecture, conform to the domain's own principles and will not create conflict with other domain architectures.

Subject Matter Expert Activities

Descriptions and Status of Domain Technologies

For each of the domain technologies, a brief description is written to assure consistent definitions within and across the domains. These descriptions also help readers understand unfamiliar technologies and their relationships with other technologies. These descriptions are updated over time to reflect changes in the capabilities and maturity of the technologies. It is preferable that subject matter experts write each of the descriptions or at least have primary responsibility for researching the current state of each technology and its related technical standards. For ongoing work, these team members will assume responsibility for tracking those technologies and standards.

Conformance to Domain Architecture Principles

Each of the IT products and technical standards currently in use within State agencies should be rated for its conformance to technical standards, general conformance to the domain architecture principles and ability to satisfy the Requirements for Technical Architecture. Someone familiar with the technology or technical standard, preferably a deep subject matter expert, should perform these evaluations. Each product and technical standard is then categorized as Strategic, Transitional, Obsolete or Research/Emerging.

> Strategic - These are the standards and products selected by the state for development or acquisition, and for replacement of obsolete or transitional standards or products. (Strategic means a three to four year planning horizon.) When more than one similar strategic standard or product is specified for a technology category, there may be a preference for use in statewide or multi-agency development. These preferred standards and products are indicated where appropriate.
> Note: some strategic products may be in "pilot testing" evaluation to determine implementation issues and guidelines. Pilot testing must be successfully completed prior to full deployment by the agencies or the State.
> Transitional - These are standards or products in which an agency or the State has a substantial investment or deployment. These standards and products are currently supported by DOIT, the agencies, or the vendor (industry, manufacturer, etc.). However, agencies should undertake development using these standards or products only if there are no suitable alternatives that are categorized as strategic. Plans should be developed by the agencies or the State to move from transitional to strategic standards or products as soon as practical. In addition, the State should not use these standards or products for development.
> Note: many older versions of strategic standards or products fall into this category, even if not specifically listed in a domain architecture document.

Obsolete - It is highly likely that these standards or products, while still in use, will not be supported by the vendor (industry, manufacturer, etc.) in the future. Some products and standards have already reached the non-supported state. Plans should be developed by the agencies or the State to rapidly phase out and replace them with strategic standards or products. No development should be undertaken using these standards or products by either the agencies or the State.

Research / Emerging - This category represents proposed strategic standards and products that are in advanced stages of development and that should be evaluated by the State. Some of these standards or products may already be undergoing "hands-on" evaluation. Others will need to be tracked and evaluated over the next 6 to 18 months.

Recommending New Technical Standards and Technologies

During the course of technology and standards research, evolving standards and new technologies will be identified that support the domain architecture and the business goals implicit in the Conceptual Architecture. Standards that are expected to be worthy of inclusion in the domain architecture when they are adopted by the IT industry should be declared as emerging standards that will be tracked by the domain team. They can then be included in the domain team's work plan and be assigned a priority and adequate resource time. For information on the assessment of emerging technical standards during routine research and monitoring of technologies, see the chapter on Researching New Technologies, Products and Technical Standards. If a standard has evolved to the Request for Comment stage (RFC version published), or a product is available in a BETA version, it can be declared as a subject of research. The team leader can then draft a proposal for how to best proceed with evaluating the new technology or technical standard. (See Section 4 on Updating a Domain Architecture for specific information about this process and its deliverables).

Documenting Standard Configurations and Reusable Components

One of the Conceptual Architecture Principles requires that applications, systems and infrastructure employ reusable components across the enterprise. For infrastructure, reusable components are defined as standard configurations. For applications and systems, reusable components are defined as libraries of modular programming code and standardized infrastructure services respectively. Code libraries will be developed as a central resource for application development teams. Infrastructure components are typically those that DOIT is responsible for on a statewide basis, or that will be widely deployed by the agencies.

Documenting Guidelines and Methods for Implementation and Management

Guidelines are practical advice for implementation and management practices based on the experience and research of the State's most knowledgeable experts. Methods are more formal and more prescriptive. When approved methods are embodied in products, they will become strategic products.

Standard format for domain team documents

Templates for these documents are found in Appendix 2

Domain Architecture Document

Monthly Team Status Reports (DT-6)

Gap Analysis Report (DT-5)

Hands-on Research Work Plan (DT-3)

Cross-Domain Issues

A number of technologies and technical standards impact multiple domains and will require creative thinking and collaboration across domain team boundaries. It is essential that all members of all domains are familiar with the complete set of domain architectures. Some technology overlaps are more obvious than others are. For some technologies, the synergy between domain architectures is of overriding concern. Some domain technologies provide infrastructure services for other domains. In the practical application of architecture, systems are constructed with components from all the domains. Therefore, all the domain architectures must be in synch with each other. Open dialogue and cross-fertilization of ideas among the domains is very important. Cross-domain issues must be documented and discussed at the regular domain team leader meetings.

Section 4. Updating a Domain Architecture

> All changes to a domain architecture must remain true to the EWTA Conceptual Architecture and satisfy the Requirements for Technical Architecture (RTAs).

This section describes the types of changes that can occur while updating a domain architecture and the process and deliverables for making them. There is a formal approval process for specific types of changes that will have major impact. The domain team has the authority to make other types of changes on its own, as long as there is consensus among the team members and they conform to the prime directive for domain teams as stated above. The specifics of the types of changes that fall into these two classes are detailed below in this section.

Events leading to domain architecture changes

Strategic Planning

Annual agency planning activities can cause revisions to the EWTA source documents, which in turn will trigger a comprehensive review of all the domain architectures. New business change drivers and business information requirements will impact the Conceptual Architecture Principles and the Requirements for Technical Architecture (RTAs). Changes in industry best practices for information technology can also impact the Conceptual Architecture Principles. These too will require a comprehensive review of all the domain architectures to determine the impacts (if any).

Agency and Infrastructure Projects

Routine project activities such as requirements analysis and architecture consultations may reveal a need to rework or refine portions of the architecture. As the architecture specifications for infrastructure services are defined, a deeper understanding of the cross-domain dependencies may require domain changes to reconcile lower level architecture elements such as interface standards, standard configurations and implementation guidelines.

Domain Team Activities

A basic premise of the EWTA process is that the domain architectures can only remain relevant through constant refinement and the resolution of gaps that are identified by the domain team. Change is supported and driven by the domain team's research activities. Routine technology tracking and focused research related to specific conformance reviews and project consultations will reinforce the need for greater conformance is some areas and greater flexibility in others.

Frequency of domain architecture updates

The frequency of updates to the domain architecture depends on a number of factors. Some technologies are rather volatile and experience rapid or frequent changes, while other change little in six months. Infrastructure and agency projects, while usually keyed to budget cycles, may occur at any time.

Domain architecture updates should happen at least once per year and should occur and work in conjunction with the mid-June agency planning cycle. It is expected that a change requiring ARB approval (see below) will occur every 3 to 6 months on average.

Two primary classes of changes to architecture documents

There are two primary classes of changes to domain architectures and their associated documents, those that require the approval of the Architecture Review Board, and those that do not.

Changes that require ARB approval

- Adding or removing principles, technical standards, or product standards.
- Adopting methods that become mandatory or are embodied in products that are categorized as strategic.
- Significantly altering the meaning or intent of a principle, technical standard or product standard.
- Changing the status of a product, i.e., from research to strategic, from strategic to transitional, from transitional to obsolete.
- Making any change that will have major impact on technology products, agency financial or personnel resources, or on the ability of an agency to implement application systems.
- Requiring modification of a pending RFP (SOW etc.) or an RFP currently out for bid.
- Requiring changes to ongoing implementation projects.
- Greatly accelerating the agencies' transition planning for implementing a new architecture.

Changes that a domain team can make under its own authority

- Updating version numbers of product standards.
- Adding or refining narrative to provide a better explanation of component technologies or standards.
- Providing guidelines for the implementation and management of component technologies or technical standards.
- Documenting reusable components and configurations.
- Updating the technology review section of a domain architecture document.
- Adding, updating, or deleting a best practice, provided it does not have a major impact on an agency or on multiple agencies.
- Recommending changes in component technologies or their domain assignments.
- Adding new technologies, products or technical standards to the research category.
- Identifying new gaps in the architecture for the *To Be Determined* section.
- Removing technologies, products or technical standards from the research category if routine research and monitoring indicates that they are not viable or will not fit within the EWTA.

Process and deliverables for changes that require ARB approval

Changes to the domain architecture that require approval of the ARB will follow the "Approved EWTA Update Process – June 7, 2001 (see Update Process Workflows below) and will utilize the deliverables defined for that process.

Process and deliverables for changes that do not require ARB approval

See the section entitled *Researching New Technologies, Products and Standards* for a discussion of the process and expected deliverables related to research activities.

Changes that do not require approval by the Architecture Review Board must always be documented. This is accomplished by updating the *Table of Changes* located at the beginning of each domain architecture document. The change statement must include the date of the change. It must also include a succinct but complete description of the item that changed and its location in the architecture document, *e.g., "In Table 2 Middleware Product Selection Matrix added STC e*Gate™ to Messaging and Application Integration Products – Research"*.

Changes can be proposed by anyone on the domain team but must be reviewed and approved by the full domain team. The domain team must consider cross-domain implementation issues before making any change. Only then should the domain team leader edit the document and submit it to the Enterprise Architecture Program Office for review and publication. If the EAPO agrees that ARB approval is not needed, it will notify the other domain team leaders of the proposed change. The team leaders will provide a peer review and commentary.

The new version of the domain architecture document, with appropriate change notices, will be published on the DOIT web site. The EA Program Office will also provide a summary report to the ARB outlining the changes that the domain teams have made to the domain architectures. Advisory notices will be sent to the agencies by the EAPO.

Documenting reusable components and configurations

Domain team leaders must work with their technology experts to define the appropriate content and standard formats for documenting reusable components and standard configurations for each of the domain technologies. As this will vary significantly from domain to domain, there is no single prescribed format that can be used for all technologies. For some technologies the content and format may be governed by methods and tools selected for implementing or managing those technologies. Of equal importance to the elements used to define reusable components or configurations is the process for creating and updating them. As an example of how to approach both process and documentation for standard configurations see Appendix 6 Example of a Configuration Management Process for information about the Standard PC Configuration Specification developed by the Platform Domain Team.

The reader is also referred to the section entitled Section 6 Researching New Technologies, Products and Standards.

EWTA Update Process Workflows

On June 7, 2001, the Architecture Review Board (ARB) approved a formal process for updating domain architectures. The process accommodates three types of changes to the architecture. One, those changes not requiring hands-on research prior to board approval. Two, those changes requiring hands-on research prior to a final decision. Third, changes that would require a prototype or pilot project prior to a final decision (Proof of Architecture via Production Ready implementation). It is the responsibility of the domain team leader, in consultation with the domain team, to decide which type of change is required. Regardless of the proposed change, each workflow is preceded by a set of common activities.

Initial Workflow Activities

The process starts with a decision to affect a significant change in the domain. After consulting with the domain team, the team leader prepares a Form DT-1 Action Plan for Domain Team Research. A template for this can be found in Appendix 2. At this point the team knows how much effort is required and whether or not hands-on research will be required.

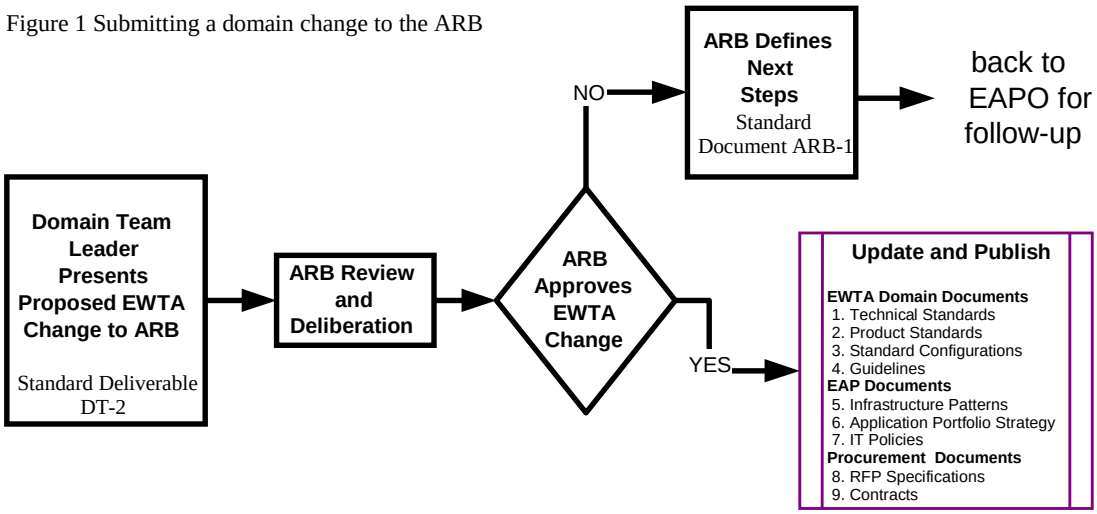
After a quality assurance review, the EA Program Office will coordinate with the resource owners or scheduling office for an assessment of resources that might be needed and for potential impact on DOIT or agency projects. EAPO handles the coordination with other domains that are impacted by the anticipated change to the domain architecture. EAPO will also maintain the involvement of other domain teams in the review process. Following a short commentary period for the other domain teams, EAPO consolidates the comments and communicates them to all involved domain team leaders. At this point, the domain team will update the action plan as needed, following which EAPO will forward the DT-1 to the Chief Technology Officer for a review of the research plan. EAPO will work with the domain team to resolve any problems with the scope of the research as identified by the CTO. The CTO determines that the research effort is significant enough to merit review and approval of the evaluation criteria by the Architecture Review Board. After the research plan has been approved, and the identified resources are committed, the domain team leader assembles the research subcommittee and appoints a chair. Subcommittees may be as small as one or two people, or as large as needed. Subcommittee members can be from inside or outside the domain team to provide the broadest participation by the agencies, to involve the optimal number of subject matter experts, and to address any cross-domain impacts.

The subcommittee is responsible for conducting any research and evaluations outlined in the action plan. See Section 6 - *Researching New Technologies, Products and Standards* for more information on research procedures and mandatory evaluation criteria. Following the conclusion of the research and evaluation, the subcommittee prepares a preliminary report and recommendation (Form DT-2 Recommendation for Domain Architecture Change found in Appendix 2) and submits it to the entire domain team for review and comment. After a final version has been accepted by the domain team, the team leader forwards the DT-2 to the EA Program Office for a quality assurance review and for a peer review by the other domain team leaders. The team leader adjusts the DT-2 and proceeds to the next steps in the process. The nature of these next steps depends on whether or not Hands-on Research or a Proof of Architecture (POA) is needed.

Flow One – No Hands-on Research

The simplest next step in the process is for the team to conduct the research effort, document the results and prepare a recommendation to change the technical architecture. The team leader presents the proposed architecture change to the ARB. This is for research efforts where no hands-on evaluation or proof of architecture is required. The flow is relatively straightforward (see Figure 1 Submitting a domain change to the ARB). The team leader makes a presentation to the ARB about the proposed change. The ARB then reviews the proposed change and votes either to approve it or send it back to the domain team for further work. Depending on the nature of the change this might take a week or more, and require additional information from the team leader.

Figure 1 Submitting a domain change to the ARB



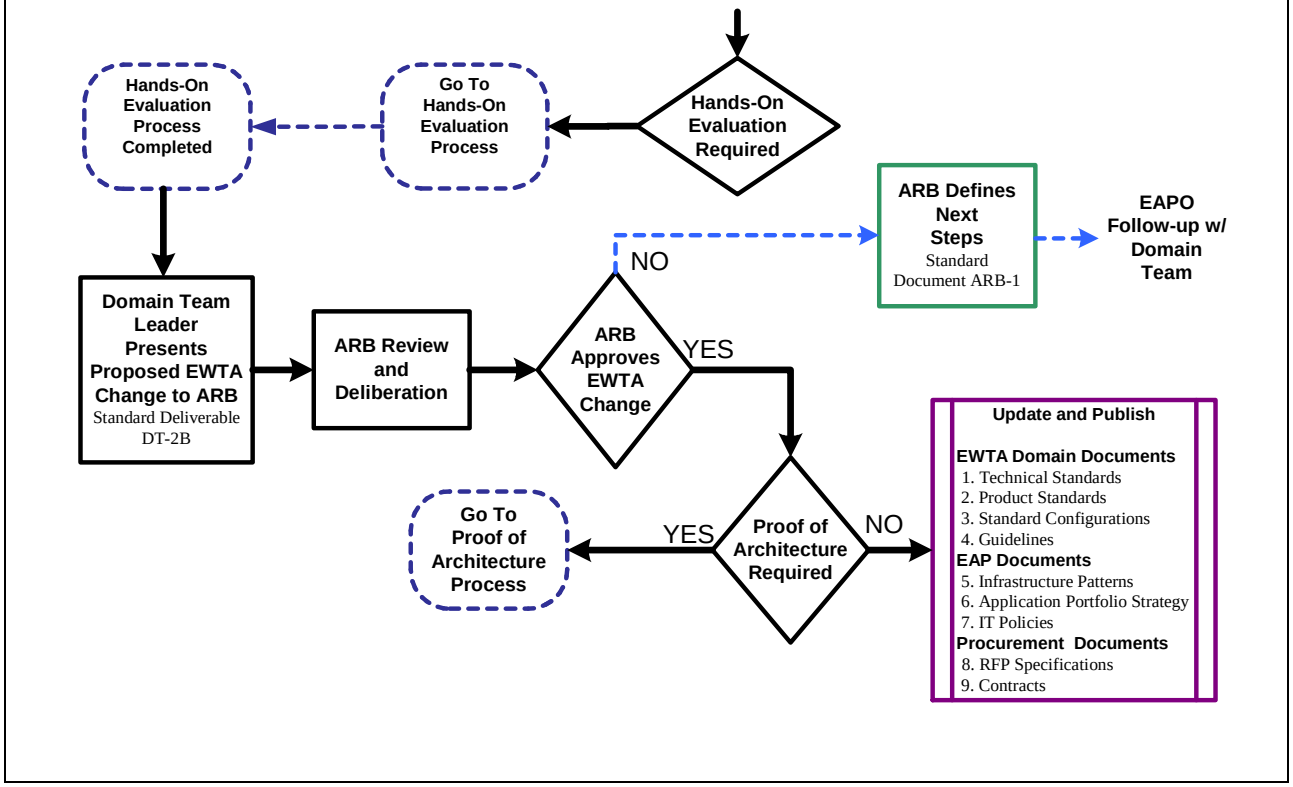
If the ARB approves the change to the domain architecture the EA Program Office will coordinate the updating and publication of the revised technical architecture documents. See Update and Publish box in Figure 1. Should the ARB decline to approve the change, they will document the decision and recommended next steps on a form ARB-1 Architecture Review Board Rejection of Request for Domain Architecture Change (in Appendix 2). The EAPO will work with the domain team on any follow-up activities or next steps.

Flow Two – Hands-on Research

There is a formal process and standard deliverables for research situations that require hands-on evaluation (see Figure 2 Approval process following hands-on evaluation, and Appendix 4 Diagram 2 - EWTA Hands-on Evaluation Process). The hands-on evaluation could involve interoperability testing with infrastructure components or a real world shoot-out between two products that appear to be equivalent in terms of functionality and usability. The subcommittee usually determines during the course of paper-based research effort that a hands-on evaluation is required. After review of the DT-2 deliverable by the full domain team and the EA Program Office, the subcommittee chair prepares the Form DT-3 Hands-on Project Plan Template Appendix 1) for the evaluation.

The EA Program Office completes a scripted quality assurance review and coordinates with the resource owners or scheduling office to review the proposal and prepare a report on the availability of the resources requested for the evaluation. The proposal is then reviewed by the Chief Technology Officer (CTO). The CTO can request that the proposed evaluation project be scaled down, that the priority for the project be reduced, or that the subcommittee does additional paper-based research. When the project proposal receives the blessing of the CTO, the resource owners assign staff and schedule their time on the Master IT Resource Schedule. The project manager for the evaluation (not necessarily the subcommittee chair) assembles and briefs the project team. The project manager procures or otherwise obtains necessary products, schedules time in the lab, oversees the lab set up and manages the hands-on evaluation. The project manager prepares regular status reports for the research subcommittee and the EA Program Office. The ARB receives monthly updates on the status of all evaluations. When the evaluation is complete, the project team prepares the form DT-2B Post Hands-on Evaluation Report and Recommendation (found in Appendix 2) in collaboration with the subcommittee, for review and

Figure 2 Approval process following hands-on evaluation



acceptance by the full domain team. After a scripted quality assurance review by the EA Program Office, the report is released to the domain team leader for final resolution. If no further action is required the report is filed and a final report is given to the ARB. If the hands-on evaluation results in a request to change the domain architecture, the domain team leader follows the process described in figure 2 above for submitting a domain change to the Architecture Review Board. In this case, a formal presentation is made to the ARB after the board has had time to review the DT-2B and supporting documentation.

If the change request is not approved, the ARB defines next steps in standard deliverable ARB-1 and EA Program Office coordinates with the appropriate groups to accomplish them.

If the change request is approved, the EAPO will coordinate the update and re-publication of appropriate architecture documents as well as the development and release of an advisory memorandum.

Flow Three – Proof of Architecture Concept

If a hands-on evaluation is successful but the complexity or risks indicate the need for a formal pilot or prototype implementation, the subcommittee prepares a proposal to conduct a Proof of Architecture (POA). The process is illustrated in Figure 3 Approval following Proof of Concept below, and Appendix 4 Diagram 3 – Proof of Architecture Process. The proposal is documented in Form DT-5 Proof of Architecture Project Plan Template (found in Appendix 2). As with the hands-on evaluation, the EA Program Office completes a quality assurance review and

coordinates with the resource owners or scheduling office for a report on the availability of resources.

Unlike the request for hands-on evaluation, which only requires the blessing of the CTO, a request for a Proof of Architecture requires formal approval by the Architecture Review Board. The ARB can request that the scope of the project be revised, that additional research be done, that another agency project be chosen as the basis for the assessment, or that the priority for the project be reduced.

If the ARB approves the proposal, the EA Program Office works with the Agency IT manager to negotiate a memorandum of understanding with the agency to use its project for the POA. DOIT and the agency then prepare for and launch the project. The management of the project should follow the State's standard project management protocol. Proof of Architecture requirements and deliverables are incorporated into the agency's project plan and procurement documents. The resource owners or scheduling office assign staff and schedule their time on the Master IT Resource Schedule. The project manager assembles and briefs the project team.

During each of the phases in the agency's project, there will be specific EWTA evaluation criteria that are considered. The agency-specific criteria may vary somewhat from project to project but there is a core set of mandatory assessment topic areas, requirements and viewpoints which are required for all technology and product research efforts. These mandatory evaluation criteria are defined in Section 6 - Researching New Technologies, Products and Standards. In general, the shift in focus through the project phases will be as follows:

- During the design phase of the project, design principles, technical standards and best practices are the focus.
- During the build or construction phase of the project, standard configurations, methods and documentation are the focus.
- During the test phase, interoperability with standard infrastructure services is conducted.
- During phased implementations, an assessment of scalability and usability will be made.
- During full implementation of the product, rigorous analysis of reliability and scalability will be accomplished.

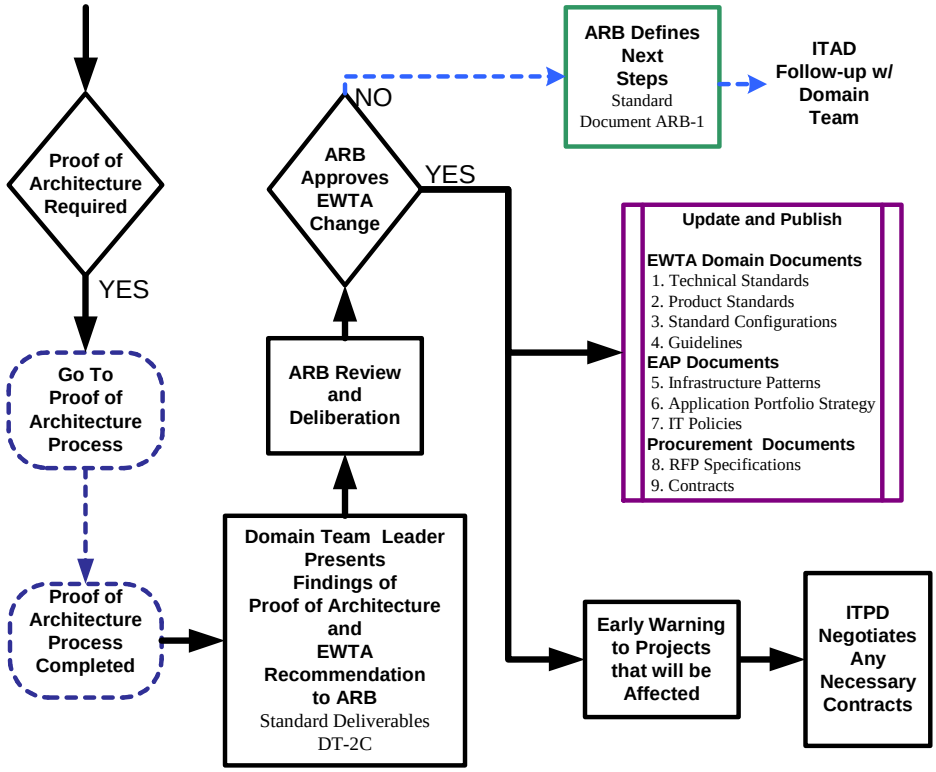
Regular status reports on project progress and EWTA evaluation results will be provided to the subcommittee and EA Program Office for ARB updates and review by the domain team. Regular status reports also go to the project stakeholders for project quality assurance review.

At the conclusion of the project, the project manager and the subcommittee chair prepare a formal report on the results of the POA (see Form DT-5B Post Proof of Architecture Report and Recommendation found in Appendix 2). As usual, the report must be reviewed and accepted by the full domain team and pass quality assurance review by the EA Program Office before being released.

If no further deployment is recommended, the report is filed and a final report is given to the ARB. If the Proof of Architecture results in a request to change the domain architecture, the domain team leader follows the process described below in Figure 3 *Approval following Proof of Architecture*. In this case, the DT-2C is presented to the board.

If the change request is not approved, the ARB defines next steps in standard deliverable ARB-1 and EA Program Office coordinates with the appropriate groups to accomplish them.

Figure 3 Approval following Proof of Architecture



If the change request is approved, the Project Management Office issues an early warning to agencies for projects that will be affected by the change. IT Procurement negotiates any necessary contracts. At this point the EA Program Office will coordinate the update and publication of the appropriate architecture documents as well as the development and release of an advisory memorandum.

Section 5. Identifying and Closing Gaps in a Domain Architecture

As part of their ongoing research, or in reviewing and revising products or technical standards, domain teams will undoubtedly identify "gaps" in domain technologies. Gaps are component technologies that do not exist in the current IT environment, are improperly structured or non-standard, or have yet to be addressed in the technical architecture.

Once identified, these gaps should be captured in the Form DT-4 Gap Analysis Report from a Domain Team (found in Appendix 2 of this guidebook).

This document an be utilized as a reference and planning tool by enterprise planning teams and the resource managers. It is important that domain team leaders have their gap identification document completed prior to mid-June in order for the document to be beneficial to the agency planning process.

The Key Steps in Gap Analysis

1. Complete the identification of differences between the "as-is" ("current state") and target domain architecture.
2. Analyze gaps between the "as-is" and the target domain architecture.
3. Develop recommendations (actions) to close the gap.
4. Identify and prioritize interdependencies of recommendations.

Step One – Identifying Domain Gaps

Differences between the current and target architecture

Most of the gap identification occurs during the creation of the domain architecture. The domain team completes the identification of differences between "as-is" (or "current state") and target domain architecture within the context of principles, technical standards, product standards and best practices. Some gaps identify technologies needed to satisfy Requirements for Technical Architecture (RTAs) in the target domain architecture. They are focused on technologies and products, not on how they are used or implemented. The additional work of gap identification focuses on the latter requirements. Some sources of gaps are:

- Requirements for technical architecture (RTAs) that are not met by current technical infrastructure
- Policies that do not exist but may be needed
- Standards, either existing or new
- Products, either existing or new
- Configurations and current infrastructure patterns
- Lack of training in new skills

Other sources of gaps are "overlaps" - needless complexity of products/solutions in the same technology category, and insufficient product standards for implementation (see Gaps created by the Exception Process or Agency Project Needs below).

Figure 4 Example Gaps for Data Management illustrates typical gaps for the Data Management and Warehouse domain.

Using Fundamental Questions

Teams often find it useful to focus on the following fundamental questions when discovering gaps.

- What will this (Principle, Architectural Requirement, etc.) mean to us?
- What are its impacts/issues?
- What dimensions reveal the impacts (i.e., processes, policies, metrics, culture, structure, technologies?)

Gaps created by the Exception Process or Agency Project Needs

Given the dynamic nature of technology and changing agency needs, it is likely that there will be required solutions using products or standards not covered in the domain architecture. In such cases, the team should designate these products or standards as gaps and assign them to be researched.

Refining Gaps

After new gaps are identified, the team should collect, aggregate, and sort the gaps, followed by the consolidation of related gaps. Gaps should be reworded for clarity and reviewed by the entire domain team to confirm the gap.

Figure 4 Example Gaps for Data Management

- No policies for decisional data analysis
- No data warehouse
- No metadata repository
- Multiple databases with duplicate data copies — No authoritative source identified
- No standard data movement technology
- No standard data cleansing technology — same data cleansed (using different tools) multiple times for multiple target databases
- Inconsistent usage of query and OLAP tools
- Too many products deployed

Step two – Analyzing Domain Gaps

Once the gaps have been identified, they need to be analyzed by the team. The analysis of domain gaps requires creative and collaborative minds. There is no set procedure for the analytic process.

For each gap identified, the team should develop alternative solutions to "fill" the gap. For example:

- Is a new solution (application, data, technology) required?
- Is major research including Hands-on or Proof of Architecture required?
- Are new skills required?
- Is a new approach required?
- Is a new implementation of old technology required?
- Are new behaviors required?
- Are new IT policies required?
- Are new or expanded support resources required?

The domain team should "flesh out" the solution details: description, components, rationale (principles, RTAs, gaps being addressed), business benefits, dependencies (if any), and the specific actions steps required to close the gaps. If time permits, the team should provide sufficient detail in the initiative description for use in future comparisons and the capital budgeting process.

For the larger or more complex gaps, it is helpful to consider incremental steps for closing it.

Step Three – Develop Recommendations

Recommendations on closing the gaps can take many forms. For example:

- Eliminate duplicate and inconsistent databases, functionally duplicate applications, or obsolete and unused technology components.
- Enhance and support database sharing.
- Promote shared applications and component reuse.
- Replace nonstandard products/configurations with standard offerings.
- Other changes (e.g., re-training to develop new skills, restructuring working groups or organizations, it policy making).

Step Four – Prioritize Recommendations

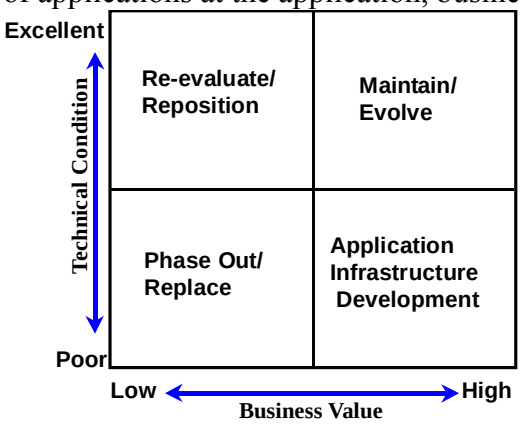
Not all gaps require immediate action, for instance, some gaps

- Can not be filled right away,
- Should not be filled (for business reasons),
- May never be filled due to priorities, or
- May be optionally filled by business units or an enterprise effort.

The gaps that do need action need to have priorities established for them. These priorities can be internal to the domain team, or can be external, if a project is recommended to fill the gap. This latter prioritization should be done jointly with enterprise planning functions. This helps to ensure that the priorities are as consistent as possible with those of the business and other active or planned initiatives.

Interdependencies must be identified between applications, infrastructure, information recommendations, and other gap-closing efforts. For applications or infrastructure the planning should address the technology 'fit' and business value of applications at the application, business process and enterprise levels. One model that META Group recommends is to look at a matrix comparing the business values and the technology condition of applications (see Figure 5).

Figure 5 Migrating the Application Portfolio to meet enterprise business needs



Section 6. Researching New Technologies, Products and Standards

The two main ongoing activities of domain teams are doing research and analyzing gaps. This section of the manual deals with the research activity.

Reasons for Doing Research

The fundamental reasons for conducting research are a reflection of the original factors that lead to the creation of the domain architecture. These are:

Reviews of Technology in the Marketplace and Technology Trends

One of the primary on-going activities of the domain team is the regular review of technology trends and changes. Domain architectures are meant to be adaptive, not static.

Gap Analysis Activities

Another primary activity of a domain team is filling known or newly created gaps in the architectures (see Section 6 Identifying and Closing Gaps in a Domain Architecture).

Conceptual Architecture Changes

The EWTA Conceptual Architecture is not static although the frequency of changes is less often than seen with domain architectures. The same basic influences on the development of new domain architectures can also lead to changes in existing domain architectures:

- Business Change Drivers.
- Requirements for Technical Architecture.
- Conceptual Principles.
- Application Portfolio.

As indicated in the section on Team Management, analysis of, and dealing with, the impact of changes in the Conceptual Architecture is the highest priority task of a domain team

New and Planned Projects

- DOIT and multi-agency infrastructure activities.
- Multi-agency and single agency IT projects.

Assigned Research

Assigned research is limited duration, topic specific research that has been assigned to the domain team by either the CTO or the Architecture Review Board. Assignments from the Architecture Review Board would normally derive from the EWTA exception process (Appendix 8).

Domain Team Research

What needs to be researched?

The predominant research topics are trends and changes in the domain technologies, product standards and technical standards, and specific research undertaken by subcommittees for proposed changes to the domain architecture. Additionally, the gap analysis / closure process often generates a need for specific research. Other research topics are generally assigned by the domain team leader.

How often should technology be researched?

The timing for tracking trends and technology changes is up to individual team members based on their own personal styles and work schedules. However, a sweep through the major sources of information should be undertaken at least monthly. A shorter refresh cycle might be needed based on the marketplace dynamics of the technologies that make up the domain, or if the domain is conducting research for an on-going project or conformance review. The team should determine what the refresh cycle should be for the domain and the team leader should ensure that this is adhered to. Research for the ARB, gap analysis and domain architecture updating is triggered by those events.

Who does the research?

Research into trends and changes in technology should be undertaken by all domain team members according to their areas of expertise and team assignments. Research on specific topics or membership on subcommittees will be assigned by the domain team leader.

What sources should be used for research?

A variety of sources is available to domain team members. Team members, in all likelihood, have specific publication **web sites** that they visit on a regular basis. Most manufactures and most publishers of software have product web sites, as do standards bodies. In addition, the State usually has research and advisory organizations under contract.

The Research Process

The research process for domain member research or for internal team activities has no formal structure, but it does have mandatory evaluation criteria and a standard documentation set (see below). The process for research conducted for domain architecture changes that require the approval of the ARB is more highly structured. A complete explanation can be found in EWTA Update Process Workflows (see Section 4 and Appendix 4).

Initial Steps in Structured Research

The formal change process starts with a decision to affect a significant change in the domain architecture. After consulting with the domain team, the team leader prepares a Form DT-1 Action Plan for Domain Team Research. A template for this can be found in Appendix 2. By this point in time, the domain team should have determined the degree of effort required and whether or not hands-on research will be required.

After a QA review, the EA Program Office will coordinate with the resource owners or scheduling office for any resources that might be needed and for potential impact on DOIT or agency projects. EAPO handles the coordination with other domains that are impacted by the anticipated change to the domain architecture. EAPO will also maintain the involvement of other domain teams in the review process. Following a short commentary period for the other domain teams, EAPO consolidates the comments and communicates them to all involved domain team leaders. At this point, the domain team will update the action plan as needed, following which EAPO will forward the DT-1 to the CTO for a review of the research plan. EAPO will work with the domain team to resolve any problems with the scope of the research as identified by the CTO. After the CTO has approved the plan and the requested resources have been committed, the domain team leader assembles a research subcommittee and appoints a chair. Subcommittees may be a small as one or two people, or as large as needed. Subcommittee members can be from inside or outside the domain team

to provide the subject matter expert necessary, to address cross-domain impacts, and to involve as many agencies as possible in the decision..

The subcommittee is responsible for conducting any research and evaluations outlined in the action plan. Following the conclusion of the research and evaluation, the subcommittee prepares a preliminary report and recommendation (the Form DT-2 Recommendation for Domain Architecture Change) and submits it to the entire domain team for review and comment. After a final version has been accepted by the domain team, the team leader forwards the DT-2 to the EA Program Office for a QA review and for a peer review by the other domain team leaders. The team leader adjusts the DT-2 and proceeds to the next steps in the process. The nature of these next steps depends on whether or not hands-on research or proof of architecture is needed. The reader is directed to the EWTA Update Process Workflows (Section 4 and Appendix 4) for more information.

Mandatory Evaluation Criteria

The Architecture Review Board has established the following technology assessment topic areas, requirements and viewpoints which are required for all technology and product research efforts.

Problem Definition

1. Business stakeholders and goals associated with this technology selection and implementation, i.e. what are we trying to accomplish for each of the people or groups of people that will be impacted by this decision; and what do we want this technology or product to do for them.
2. Scope of the target deployment: agency-specific (program, project, agency-wide), agency cluster, state-wide, nation-wide.
3. Technology boundaries: what is covered and what is not. How do external technologies on the boundaries affect this decision? What are the alternatives to this technology? Why this technology rather than one of the alternatives?
4. Use case definition (scenarios).
5. Deployment environment description and timeframe.
6. Constraints: identify how the target product must fit into the existing environment. For example, the product might have to interface with or use some existing hardware, software or business practice, or it might have to fit within a defined budget or be ready by a defined date.

Requirements That Must Be Addressed In All Assessments

1. Architecture requirements: what requirements for technical architecture are relevant to this class of technology?
2. EWTA Principles and Standards (design standards, technical standards and implementation practices) that are relevant to this assessment.
3. Required Product Capabilities: features and functions, key differentiating factors, product strengths and limitations, correct functioning, effective features, fit criteria (quantify the requirement by specifying an objective measure of the requirement's meaning by which to determine whether the product satisfies each requirement).
4. Performance and capacity requirements. Service level requirements.

5. Security requirements for confidentiality, integrity and availability. Security enforcing controls for satisfying requirements, e.g. access control, auditing, intrusion detection, etc. Non-technical security requirements that must be supported by the technology, or at least not subverted by the technology. Security vulnerabilities.
6. Legal/ Regulatory requirements: legislative (federal and state), executive orders, regulations, court orders (e.g. consent decree).
7. Business continuity requirements for service restoration after disaster, sabotage, equipment failure, or human error.
8. Weeding requirements: selection criteria that will be used to determine which products will be evaluated during each stage of the assessment, such as market position (e.g. magic quadrant), market share, and mandatory requirements.
9. Testing requirements: acceptability of hands-on evaluations performed by external parties, what hands-on testing will be done by State employees, what testing must be done within the context of a production deployment (i.e. Proof of Architecture).
10. Data Requirements: Identify any data conversion or data integration requirements. Identify data retention requirements, from both State public records administration and agency perspectives.
11. Training requirements: based on the scope of deployment and use case scenarios identify the number and type of support staff and users that will need to be trained. If this is a replacement product, identify the number and type of support staff and users and their current level of training and expertise.
12. Maintenance requirements: FTE skills and experience required for self-support, maintenance contract requirements (24x7, 8x5, per call, etc) for outsourced support.

Analysis Viewpoints – beyond basic assessment of functionality

1. Interoperability & Integration: support of open integration standards, layering (engineering design), 3rd party integration, and data integration.
2. Cost: licensing policies, pricing models, cost of skilled support, training requirements. Cost versus effectiveness analysis, price/performance balance point.
3. Stability: dependability, reliability (as tested in real world deployments), meantime to failure, routine downtime for updates, frequency of patching required.
4. Usability: developer perspective, user perspective, look and feel requirements (consistency with current electronic work environment and applications), cultural and political issues, stylistic concerns, knowledge and training assumptions. Compliance with relevant Accessibility requirements for support of persons with disabilities [WCAG, Section 508, etc.]
5. Manageability: availability (as required to satisfy standard service level agreements, supportability (support skills and knowledge required to support use of product), cost of managing the product.
6. Maintainability: maintained by technical or non-technical, local deployment versus central deployment, in-sourced versus outsourced maintenance of product. For Commercial Off The Shelf products where code maintenance is not required assess maintenance requirements for such things as parameter tables, access controls, etc.
7. Implementability: deployment models, technical maturity, complexity, fit with current infrastructure services, leveraging current skills versus development of new skills, training requirements.
8. Flexibility: scalability, evolvability, portability.

9. Dependencies: reuse of installed technologies, need for new technologies.
10. Strategic viability of company: market overview, market consolidations, key differentiators among market leaders and followers, corporate vision and strategy, corporate commitment and ability to execute vision, presence in market, financial stability of company, percentage of earning allocated to research and development.
11. Strategic viability of technology or product. Maturity of technology or product. Potential for rapid diffusion. Relation to successor technologies.
12. Securability: ability to satisfy all legal, regulatory, policy and architectural requirements for security in all environments relevant to the deployment of the product(s) under review. Environments include network, database, SAN, applications, data, identify management, testing, auditing, interfaces. Vulnerability remediation practices of company.2

Outcomes from Research

Category of Change

- Creating new principles, standards or product standards.
- Moving a standard or product standard between categories, (e.g., From *research* to *strategic,* from *strategic* to *transitional* or from *transitional* to *obsolete).*
- Editing or modifying principles.
- Updating the version of an existing strategic standard or product standard.
- Adding a new technology category to the domain architecture.

Documentation Requirements

All comparative analysis matrices, narratives and transcriptions of all other information gathered and analyzed during the research effort, plus the following standard documents.

DT-1 Action Plan for Domain Team Research

DT-2 Recommendation for Domain Architecture Change

DT-2B Post Hands-on Evaluation report and Recommendation

DT-3 Hands-on Project Plan Template

DT-5 Proof of Architecture Project Plan Template

DT-5B Proof of Architecture Report and Recommendation

DT-6 Monthly Status Report from a Domain Team or Subcommittee

Section 7. Relating Domain Architecture to Infrastructure

A major characteristic of an adaptive infrastructure is increasing reuse of technology assets. However, an adaptive infrastructure does not begin with implementing software, networks, and hardware; it begins with an adaptive, Enterprise-wide Technology Architecture (EWTA) to provide engineering guidance and Enterprise Business & Information Architectures to define common patterns of business organization and information management practices. .

Role of Domain Architectures and Infrastructure

A primary role of domain architectures is to organize technologies and their usage rules to assist architects in identifying common uses of technologies, and to eliminate as much redundancy as possible. This is essential to providing reusable infrastructure technology across the enterprise. The distinction between domain architectures and infrastructure patterns is in the way they are used. One is an architecture aid, used to guide the identification, selection, and implementation of technologies in standard configurations; the other is an engineering aid used to guide the identification and implementation of standard infrastructure services that have corresponding business and information management patterns.

Relationship of Domain Architectures to Infrastructure

The relationship between domain architectures and infrastructure is bi-directional. To define the domain architectures, architects must know what types of services the business requires so the requisite technology standards are defined. Likewise, to design and implement the reusable infrastructure access services, infrastructure developers must know which technology standards and principles have been defined within the domain architectures (see Figure 6 below). Also, there is a great amount of overlap in the content of each. For instance, platform domain architecture is likely to define the mainframe, midrange, and workgroup server, as well as the desktop hardware/operating system vendors and products.

Issues Involving Infrastructure Development

The principles and standards of domain architectures are defined by taking into account the need to optimize technology across the enterprise, including across different infrastructure patterns and domain architectures. An explicit implication of this practice is that individual components and lower level services may have to be sub-optimized in order to achieve the overall optimization goals.

The primary role of an infrastructure pattern is to speed the identification, configuration, and implementation of technologies by defining a proven set of technology services enabling a particular style of information system services. These services define reusable interfaces for applications to access the reusable infrastructure technologies defined in domain architectures. Examples include security access services, middleware connectivity services, enterprise directory services, and common data access services. It is interesting to note the majority of services required are not new to most project teams. The difference is that in an adaptive environment, these services are not built by project teams for the use of one or two applications, but by an infrastructure development group for use across as many applications as possible.

Section 8. Conducting Architecture Conformance Reviews

> Ideally, architecture guides all IT decision making (infrastructure deployment, application development, operations management, etc.)

As awareness of the need for architectural conformance becomes second nature, the domain architectures will provide guidance for many day-to-day IT activities. For example:

- IT procurements and contract requirements
- Buy-versus-build decisions
- Setting evaluation criteria in RFPs and SOWs
- Upgrading hardware and infrastructure
- Software package or tool selection
- Design decisions in the context of a specific IT project or application system

Therefore, from time to time, domain teams are expected to participate in architecture conformance reviews of Requests for Proposals (RFP), vendor responses to RFPs, agency IT architectures and agency IT projects. This can be accomplished as a team effort, or as a subcommittee effort. The reviews assess and evaluate conformance of project or system proposals to EWTA conceptual principles, and domain principles, standards and guidelines.

How to conduct a conformance review

Existing domain architecture documents serve as a basis for the reviews. The reviews evaluate conformance to EWTA conceptual principles, domain architecture principles, technical and product standards, and implementation practices.

Process for architecture conformance reviews by domain teams

Domain team conformance reviews result in the domain team leader submitting to the EA Program Office a report with any necessary questions, items for clarification and/or requests with specific source document references. It is the responsibility of the EA Program Office to create a composite view and complete the final report that is submitted to the requestor of the conformance review and the CIO.

Documentation Requirements

Documentation formats have not yet been defined for architecture conformance reviews because of the variations in the size and complexity of the system proposals that have been reviewed to date. A Systems Architecture section for RFPs has been defined. See Appendix 7. Until specific architecture conformance requirements are routinely included in RFPs, there will be a need for clarifications from vendors regarding specific products, design decisions and other implementation recommendations. This is assembled as a combined list of questions from the domain team leaders with reference to specific RFP sections and the documentation submitted by a vendor as part of its proposal. The EA Program Office provides specific guidance to the domain team leaders as to the approach and content of review deliverables. In general our philosophy is to identify what is good about a proposal as well as what aspects of the proposal do not conform to the architectural elements that define the ideal system. To date we have found this approach more useful to RFP evaluation committees and project teams.

Appendix 1. Glossary of Abbreviations

Explanation of Abbreviations

ARB	Architecture Review Board
BITSB	Business and Information Technology Strategy Board (also abbreviated as B&ITSB
CIO	Chief Information Officer
CTO	Chief Technology Officer
DOIT	Department of Information Technology
DT	Domain Team
DTL	Domain Team Leader
DTSC	Domain Team Sub Committee
EAP	Enterprise Architecture Planning
EWTA	Enterprise-wide Technical Architecture
EAPO	Enterprise Architecture Program Office
POA	Proof of Architecture.
RFP	Request for Proposal
SOW	Statement of Work

Appendix 2. Deliverables (Templates) for Domain Team Activities

A self-extracting ZIP file of all templates is available for download from the DOIT web site. The resulting extracted files will be found in a local folder entitled: C:\State of CT EWTA Domain Templates

DT-1 Action Plan for Domain Team Research

(Required for all research by a Domain Team)

Basic Information

Submittal Date:

Domain Team:

Team Leader:

Contact Information (phone, email):

Overview

Goals and Objectives

What are the specific goals and objective of this research?

Summary

Please provide a summary of the proposed research basic approach, what is being evaluated, etc. (**note:** details should be provided below).

Priority

What is the priority of this research? When do you anticipate the research will start and when it will be completed? (**Note:** detailed information on estimated time is to be provided below in Work Plan below)

Need or justification (may be more than one)

Please check off the reason for requesting the research and then provide a brief description. If there is more than one reason for requesting the research, describe them in decreasing order of importance.

Please copy the checkmark ✓ and past it over the ❑ to indicate a "check off"

- ❑ Domain team reviews of technology in the marketplace and technology trends
- ❑ Domain team gap analysis activities
- ❑ Changes to the conceptual architecture
- ❑ Agency project – Architecture consultation
- ❑ DOIT and multi-agency infrastructure activities
- ❑ Agency ETWA Exception process
- ❑ Infrastructure implementation or proposed DOIT service offering

- ❑ Assigned research other than research for the exception process
- ❑ Other (please specify)

Describe the business and technical reasons for the research here.

Architectural Impact

Domain Architecture Impact

What is the potential impact on domain architecture and EWTA? Please check off the reason for requesting the research. If there is more than one reason for requesting the research, check all that apply. Provide a brief description of the impact below.

Please copy the checkmark ✓ and past it over the ❑ to indicate a "check off"

- ❑ Adding or removing principles, technical standards, or product standards
- ❑ Adopting methods that become mandatory or are embodied in products that are categorized as strategic
- ❑ Significantly altering the meaning or intent of a principle, technical standard or product standard
- ❑ Changing the status of a product, i.e., from research to strategic, from strategic to transitional, from transitional to obsolete
- ❑ Making any change that will have major impact on technology products, agency financial or personnel resources, or on the ability of an agency to implement application systems
- ❑ Requiring modification of a pending RFP (SOW etc.) or an RFP currently out for bid
- ❑ Requiring changes to ongoing implementation projects
- ❑ Greatly accelerating the agencies' transition planning for implementing a new architecture
- ❑ Other: specify here

Please provide a brief description of the anticipated impact:

Provide a brief description of the changes to the domain architecture that are the subject of the proposed research (check off specific architecture impacts below). Please describe the justification for this research in the justification section.

What is the impact on other Domain Architectures (if any)?

Type of Research and Information Sources

Please check off the type of research and then provide a brief description. If there is more than type of research, describe them in decreasing order of importance.

Please copy the checkmark ✓ and past it over the ❑ to indicate a "check off"

- ❑ Web or paper research
- ❑ Use of IT Research and Advisory Service Contracts or other consultant services.

Note: if this item is checked please include any anticipated costs in the work plan below; please include staffing and other resources in the work plan below.

- ❑ Publications from national or international standards bodies
- ❑ Publications from industry consortia
- ❑ Manufacturer (or publisher) presentation, seminar, etc.
- ❑ Agency experiences (identify agencies and projects below)
- ❑ Hands-on evaluation (**Note:** if hands-on research is proposed, a DT-2 will be required once the research has been approved.)
- ❑ Other specify here

Web or Research

Research and Advisory Service

Standards Bodies

Manufacture or publisher

Agency experiences

Etc.

Scope of Work

The intent of this section is to provide the CTO (and the ARB) with enough information to reach a decision in support of resource commitment need for this research.

List the proposed assignments to subcommittee

chair for subcommittee

domain team members

team members from other domains

agency staff

Briefly describe what other resources will be needed, other than staffing, such as consultants, vendor or manufacturer presentations, etc.

Financial Cost

What is the estimated financial cost of this conducting this research? (acquisition of hardware, software, research, facilities, consultants, etc.)

Time Estimates

Provide an estimated time to complete research (work hours, meeting hours, start/end dates, etc.).

Description of Work Plan

Provide a basic description of the work plan for conducting the research needed to support this change request; indicating major activities and milestones. (A simple GANTT chart would be useful but is not required.)

Evaluation Approach

Evaluation Criteria to Be Used

Describe the evaluation criteria to be used:

Products Or Standards to Be Evaluated

Describe the products or standards that will be considered. Include alternatives, even if not subjected to a complete evaluation.

Additional Comments

Use this space for any additional comments

DT-2 Recommendation for Domain Architecture Change

Basic Information

Date of Approval of DT-1

Submittal Date of DT-2:

Domain Team:

Team Leader:

DTL Contact Information (phone, email):

Sub-Committee Name and Members (if applicable)

Sub-Committee Chair Contact Information (phone, email)

Scope of the change

Note: This information should be copied from the approved DT-1, if available.

Description

Provide a brief description of the proposed change or changes. A complete description is to be provided in Recommendation(s) below.

Priority and Time Frame

What is the priority of this change request? When do you anticipate making the change?

Architectural and Financial Impact

Full details, including a TCO analysis when possible, are to be provided in Impact Assessment below.)

EWTA Impact

What is the impact on other domains (if any)? What is the impact on the EWTA (if any)?

Financial Impact

What is the estimated overall financial impact of this change request?

Need or justification (may be more than one)

Note: This information should be copied from the approved DT-1, if available.

Please check off the reason for requesting the change and then provide a brief description. If there is more than one reason for requesting the change, describe them in decreasing order of importance.

Paste this ✓ over any of the items below to indicate a "check off".

- ❑ Domain team technology tracking activities
- ❑ Domain team gap analysis activities

❑ Agency project – Architecture consultation
❑ Agency ETWA Exception process
❑ Strategic planning and business planning (business drivers, RTAs, *etc*.)
❑ Infrastructure implementation or proposed DOIT service offering
❑ Changes to State or agency application portfolio(s)
❑ Other please indicate

Summary of Research Performed

Note: This information should be based on the content of the approved DT-1, if available.

Type of Research and Approach

If hands-on research conducted, please complete section 2 below,

Scope of the research

Please describe the scope of the research. Indicate team members in this description.

What alternative standards or products were considered?

Outcomes based on evaluation criteria

Evaluation Criteria

Describe the evaluation criteria that were used.
Note: This information should be copied from the approved DT-1, if available, and augmented with any additional criteria that were added during the research or evaluation process.

Results

Describe the results of the evaluation. If more than one standard or product was included in the evaluation, provide comparative results.

Recommendation(s)

Please choose the appropriate recommendation and provide details or justifications as required.

YES – change the domain architecture and associated documents

Provide the exact text of the proposed change, *e.g.*, proposed or modified principle, version number or standard numbers, *etc*. Changes involving a significant amount of text may be attached as documents, as long as the new material is easily identified when it is mixed with existing approved EWTA content.

Domain architecture principles

Standards and/or product standards tables

Domain architecture best practices / guidelines

Impact Assessment

Describe the impacts on the following areas should the recommended changes be implemented (use all that are appropriate).
Note: This information should be copied from the approved DT-1, if available, and modified as needed.

Infrastructure (patterns, components, services)

Impacts on other domain architectures

Existing or proposed projects, RFPs, SOWs, transition planning, *etc*.

Financial (include TCO when possible)

Request for Comment

Identify groups or individuals outside of the EWTA Domain Teams who reviewed the recommendation and provided comments. Identify changes that were made to the recommendation based on those comments.

Next Steps

Use this space to describe any next steps or following action that are needed.

Additional Comments

Use this space for any additional comments.

Section 2 - Supplemental Materials for Hands-on Evaluation

Description of the Research

Please describe the hands-on research that was conducted.
Note: staffing and other resources should be included in the work plan below.

Basic work plan

Provide a basic description of the work plan used for conducting the research that supports this change request; indicate major activities and milestones. Include time used to complete the research (work hours, start/end dates).

List the assignments to subcommittee to conduct the hands-on research

chair for subcommittee

domain team members

team members from other domains

agency staff

Describe what other resources were used, other than staffing? Indicate any costs.

DT-2B Post Hands-on Evaluation Report and Recommendation

Basic Information

Submittal Date:

Domain Team:

Team Leader:

Contact Information (phone, email):

Research Project

Indicate which research project this report is for.

Outcomes based on evaluation criteria

Evaluation Criteria

Describe the evaluation criteria to be used.
Note: This information should be copied from the approved DT-1 or DT-2

Results

Describe the results of the evaluation. If more than one standard or product was included in the evaluation, provide comparative results.

Recommendation(s)

Please choose the appropriate recommendation and provide details or justifications as required.

YES – change the domain architecture and associated documents

Provide the exact text of the proposed change.

Domain architecture principles

Standards and/or product standards tables

Domain architecture best practices / guidelines

YES – but need to conduct a proof of architecture prior to final decision

If this is the recommendation of the research team, then a Proof of Architecture Work Plan (DT-5) must be completed and submitted along with this recommendation form.

NO – take no action at this time, consider in the future, *etc*.

Please select a reason and then provide a brief explanation for that choice.

High risk, immature – continue tracking

Needs more "paper" evaluation

Inconclusive results of comparative evaluation

Inappropriate or negative evaluation

Other (specify)

Impact Assessment

Describe the impacts on the following areas should the recommended changes be implemented (use all that are appropriate).

Note: This information should be copied from the approved DT-1 or DT-2 and modified as needed.

Infrastructure (patterns, components, services)

Impacts on other domain architectures

Existing or proposed projects, RFPs, SOWs, transition planning, *etc*.

Financial (might include TCO)

Next Steps

Use this space to describe any next steps or following action that are needed, other than a Proof of Architecture.

Additional Comments

Use this space for any additional comments.

DT-3 Hands-on Project Plan Template

Basic Information

Date of Approval of DT-1

Submittal Date:

Domain Team:

Team Leader:

Contact Information (phone, email):

Justification

Scope of Change to Domain Architecture

Indicate what change to the domain architecture is supported by this research.
Note: Can be copied from DT-1 or DT-2.

Purpose of the Research

Briefly, describe why this hands-on research is needed.

Scope of the Research

Description of the Research

Please describe the hands-on research to be conducted.
Note: staffing and other resources should be included in the work plan below.

Time Estimates

Provide an estimated time to complete research (work hours, start/end dates)

Work Plan

Project Plan

Provide a basic description of the work plan for conducting the research needed to support this change request; indicate major activities and milestones. A detailed Gantt chart with resource assignments, milestones and deliverable dates must be attached (this can be in the form of a MS Project file along with a print-out).

Committee Assignments

List the proposed assignments to subcommittee to conduct the hands-on research (indicate if same or new)

chair for subcommittee

domain team members

team members from other domains

agency staff

Training

Describe any training that will be required by the evaluation team members; include method, duration and location of training. The cost for training should be included in the resources section below.

Resources

Describe what other resources will be needed, other than staffing? Itemize the individual costs, including training costs here. Examples of resources include facilities, consulting services, and equipment or software acquisition.

Evaluation criteria to be used

Describe the evaluation criteria to be used.

DT-4 Gap Analysis Report from a Domain Team

Note: This is in Excel spreadsheet format (see sample below)

Instructions

Column A	Planning Category Or Technology Category	attempt to group similar gap items that could be incorporated in the same (future) plan
Column B	Gap Description	brief description of the gap item (or a label)
Column C	Priority	relative priority within the domain for resolving the gap item; ranked from **A** highest to **C** lowest
Column D	Cross Reference	list of other gap items that are related or linked to this gap item, based on the gaps identified in the domain architecture document
Column E	Short List?	gap items to be acted upon first
Column F	Order	used to order the short list and remaining gaps as part of the planning process
Column G	Domain Principles Supported	list of domain principles supported by resolving the gap
Column H	Comment / Action Item	indicate how the gap will be resolved, and any other comments that are relevant; this cell can include historical actions
Column I	Skills	skills required as an aide to resource planning and assignment of team members to activities or research

Sample Template

This example is based on a Gap Analysis Report from the Application Development Domain.

Planning Category	GAP	Prio.	xref	Short List?	Order	Domain Principles Supported	Comment/Action Item (from May meeting)	Skills Required
Merge as single GAP.	Web-based enterprise reporting tools	A	5	X		Anytime/Anywhere Access	Select tool based on EWTA principles and standards. Style Report and Crystal Reports in use.	Reporting and web development experience.
	Reporting Tool Standard for legacy systems	A	6				Agency Suggestion. Roll into Web-based reporting - recommend Web for legacy reporting.	
Move to eGov.	GUI front-end tools for legacy systems	X	8				Agency Suggestion. Recommend moving to "Web enable legacy systems" in eGOV domain.	
Document Update	Evaluation of 2nd tier baseline technologies (e.g. Oracle tools)	A		X		Reduce Integration Complexity	Gap in original assessment (Include disposition of all "research" items)	Development experience/research.
Document Update	Consider OO Cobol as a strategic language	C	9			Reduce Integration Complexity	Agency Suggestion.	
skills required as an aide to resource planning	Research VA Generator, VA Business Rules	c				Reduce Integration Complexity	Re-evaluate as part of document review.	Advanced developer, research.

DT-5 Proof of Architecture Project Plan Template

Basic Information

Date of Approval of DT-1

Submittal Date:

Domain Team:

Team Leader:

Contact Information (phone, email):

Additional Justification

Briefly, describe why this proof of architecture via production ready implementation is needed. This description should go beyond that of the DT-1 or DT-2b and include information on the following:

5. Immediate or near term business need at agency or multi-agency level (might be part of the EWTA Exception Process).
6. Proposed as a service offering or architecture component.
7. Clearly identified business drivers or RTAs with immediate strategic impact.

Scope of the Research

Description of the Research

Please describe the research to be conducted. Include the product or products to be evaluated. **Note**: staffing and other resources should be included in the work plan below.

Time Estimates

Provide an estimated time to complete research (work hours, start/end dates)

Participating Agencies

Provide name(s) and contact(s) at the agencies that will be involved in this proof of architectural project.

Work Plan

Project Plan

Provide a basic description of the work plan for conducting the research needed to support this change request; indicate major activities and milestones. A detailed Gantt chart with resource assignments, milestones and deliverable dates must be attached (this can be in the form of a MS Project file along with a print-out).

Committee Assignments

List the proposed assignments to subcommittee to conduct the hands-on research (indicate if same or new)

chair for subcommittee

domain team members

team members from other domains

agency project manager

agency staff

Training

Describe any training that will be required by the evaluation team members or agency staff; include method, duration and location of training. The cost for training should be included in the resources section below.

Resources

Describe what other resources will be needed, other than staffing? Itemize the individual costs, including training costs here. Examples of resources include facilities, consulting services, and equipment or software acquisition.

Funding

Describe what sources and amounts of funding will be available, including agency funds.

Evaluation criteria to be used

Describe the evaluation criteria to be used.

DT-5B Post Proof of Architecture Report and Recommendation

Basic Information

Submittal Date:

Domain Team:

Team Leader:

Contact Information (phone, email):

Proof of Architecture Project

Indicate which proof of architecture project this report is for.

Summary of project activities

Briefly summarize the major activities of the project and approach used.

Outcomes based on evaluation criteria

Evaluation Criteria

Describe the evaluation criteria to be used.
Note: This information should be copied from the approved DT-5

Results

Describe the results of the evaluation. If more than one standard or product was included in the evaluation, provide comparative results.

Recommendation(s)

Please choose the appropriate recommendation and provide details or justifications as required.

YES – change the domain architecture and associated documents

Provide the exact text of the proposed change.

Domain architecture principles

Standards and/or product standards tables

Domain architecture best practices / guidelines

The following are optional recommendations that would be in addition to the above.

Add as a service or component offering (describe)

Proceed to full deployment or production mode at the agency or agencies participating in project.

NO – take no action at this time, consider in the future, *etc*.

Please select a reason and then provide a brief explanation for that choice.

High risk, immature – continue tracking

Inconclusive results of comparative evaluation

Inappropriate or negative evaluation

Other (specify)

Impact Assessment

Describe the impacts on the following areas should the recommended changes be implemented (use all that are appropriate).

Note: This information should be copied from the approved DT-1 or DT-2 and modified as needed.

Infrastructure (patterns, components, services)

Impacts on other domain architectures

Existing or proposed projects, RFPs, SOWs, transition planning, *etc*.

Financial (might include TCO)

Next Steps

Use this space to describe any next steps or following action that are needed.

Additional Comments

Use this space for any additional comments.

DT-6 Monthly Status Report from a Domain Team or Subcommittee

Meeting Information

Domain Team or Subcommittee:

Team Leader or Subcommittee Chair:

Meeting Date:

Members in attendance:

Members absent:

Details

Reports for On-Going Individual Work

Briefly, describe results and recommendations from on-going reviews and research by team members with individual assignments. Attach any written reports prepared by them.

Subcommittee Status Reports

Briefly, describe status of any subcommittee activities and attach subcommittee reports.

Action Items

Use this space to report on items requiring resolution, indicating next steps, information or resources needed, etc.

Domain Team Decisions During Meeting

Use this space to report any decisions made by the team.

Domain Team Feedback

Use this space for any comments or suggestions the team wishes to submit to the EAP managers.

DT-7 Report on Monthly Domain Team Leaders Meeting

Meeting Information

Meeting Date:

Members in attendance:

Members absent:

Details

Agenda Item One

Agenda Item One

Action Items

Use this space to report on items requiring resolution, indicating next steps, information or resources needed, etc.

Domain Team Leader Decisions During Meeting

Use this space to report any decisions made by the team.

Domain Team Leader Feedback

Use this space for any comments or suggestions the team leaders wishes to submit to the CTO.

ARB-1 Architecture Review Board Rejection of request for Domain Architecture Change

Basic Information

Date of Rejection of DT-1 or DT-2

Domain Team:

Team Leader:

Scope of the Rejection

Description

Provide a description of the change proposed, include the exact text of proposed or modified principle, version number or standard numbers, etc.
Note: copied from DT-1 or DT-2

Nature of the Rejection

Provide a description of the rejection. If a partial or conditional rejection, please be clear as to which part of the change request is rejected, or what the conditions are.

Recommended Next Steps

Please indicate what the domain team should do for follow-up activities (if any).

Form EX-1 Request from Agency for Exception to EWTA
Part B – Domain Team Recommendation

This section should be completed by all of the domain teams that are impacted by this exception request.

EWTA Domain Team: _____

Team Leader: _____

Contact Information: _____

Project Description

Exception Request Received Date: _____

Project Title: _____

Participating Agency or Agencies: _____

Current Project Life Cycle Stage: _____

Nature of Exception Request

- ❑ Conceptual Architecture Principles
- ❑ Domain Architecture Principles,
- ❑ Technical Standards
- ❑ Product Standards

Exception Requested:

Recommendation

Is the domain team supporting this exception request?

[ ] Requires Additional Research To Make Recommendation

If additional research is required, then a matching DT-1 must be submitted along with this recommendation.

[ ] YES [ ] NO

If yes, will changes to the domain architecture be proposed? [ ] YES [ ] NO

If technical architecture changes will be proposed, then a matching DT-2 must be submitted separately by the domain team.

What is the recommendation of the domain team with respect to the exception request?
(simple declarative statements, including any recommended implementation constraints)

Briefly describe the justification or rationale for the above recommendation.
(*e.g.*, Requested product is consistent with domain principles or technical standards as noted below, or, Requested implementation violates domain principles or best practices, as noted below)

Conceptual Principles

Technical Standards

Product Standards

Best Practices

Supporting Research For This Recommendation

Supporting Research

Please check off the type of research the domain team did in support of this agency exception request and then provide a brief description. If there is more than type of research, describe them in decreasing order of importance.
(copy this ✓ and paste over the box)

- ❑ Web or paper research
- ❑ Use of consultant services
- ❑ Other please specify

Please provide a description of the research that was conducted:

Please check off the information sources used and then provide a brief description below each source including specific names as appropriate.
(copy this ✓ and paste over the box)

- ❑ IT Research and Advisory Services

- ❑ Publications from national or international standards bodies

- ❑ Publications from industry consortia

- ❑ Information provided by manufacturer or software publisher

- ❑ Other please specify

Impact of Approving This Exception Request

If the Architecture Review Board approves this exception request, what will the impact be on the following:

This Domain Architecture

Provide a brief description of the changes to the domain architecture that will result from the approval of this exception request. **Note**: If the technical architecture will not change, indicate no impact.

Domain Team Workload

- ❑ Adding non-standard products to the IT environment that the domain architecture team must account for, track or accommodate in the technical architecture and implementation documents
- ❑ Adding a non-conforming design or configuration to the IT environment that the domain team must account for, track or accommodate in the technical architecture and implementation documents
- ❑ Other please specify

Cost of Ownership

What is the estimated financial impact of this exception request?

(Include TCO analysis when possible. i.e. Hard Costs – hardware, software, systems management, support, development, communications fees; Soft Costs – end-user peer support, self support and casual learning, planned and unplanned downtime, etc.)

Additional Comments

Add any additional comments that are deemed necessary.

Appendix 3. Descriptions of the Technical Domains

The nine technical domains created by the Architecture Team were classified as either basic technology or application domains.

Basic Technology Domains

These architectures cover the commonly used technologies that almost every information system or utility depends on. Typically these include network, computer hardware, operating systems and other system software, middleware, database management system, distributed environment management tools. We have added data warehouse (typically an applied technology domain) by combining it with the data management domain.

Domain	Description	Technology Categories
Network	Network architecture provides for all aspects of the communications infrastructure for a distributed computing environment. This includes logical elements, physical hardware components, carrier services and protocols. The scope of the architecture includes voice, data, and video and directory services.	Wiring, hubs, routers, LAN switches, ATM switches, Frame Relay switches, network operating systems, carrier services, LAN / WAN protocols, directory services.
Distributed Environment Management	This architecture defines how the hardware and software components of the environment will be controlled. It focuses on issues of configuration management, fault detection/isolation, testing, performance measurement, problem reporting, software upgrades/control, and remote systems management.	Networks and systems management, LAN management, software distribution, storage management, asset management, help desk, security, performance management, capacity planning, change control.
Middleware	The middleware architecture defines the components that create an integration environment between clients and the legacy and server environments. Middleware sites between the application and network communication mechanisms, and provides for application integration independent of network and platform technologies.	Messaging oriented middleware, object request brokers, transaction processing monitors, database gateways.

Domain	Description	Technology Categories
Platform	The Platform architecture defines the technical computing components of the infrastructure including client/server hardware platforms, operating systems, database engines and environments, and interfaces.	Workstations, client software, groupware servers, midrange boxes and mainframes, operating systems, and OLTP and OLAP database management systems.
Data Management and Data Warehouse	This architecture defines the mechanics for managing, securing, and maintaining the integrity of an enterprise's significant logical entities, and specifies standards for accessing business data. Also describes the internally consistent logical structure of authoritative databases and provides the standards for decision support and OLAP data.	Data repositories, data modeling tools, data replication tools, data administration tools, data extraction tools, OLAP tools, multidimensional databases, etc.
Security	The security architecture facilitates appropriate access to information while ensuring integrity and availability. It supports innovative business process as well as compliance with all government regulations and standards related to information security. It is concerned with is identification, authentication and access rights. Other aspects of security architecture include virus protection, intrusion prevention and privacy.	Digital certificates, intrusion detection systems, Public Key Infrastructures, encryption, administrative tools, firewalls, directory services, access lists and methods, anti-virus tools, etc.

Applied Technology Domains

These architectures are more specific to the way in which technology is being applied to support the business.

Domains	Description	Technology Categories
Application Development	Application architecture is the focal point of an organization's systems inventory. It defines how applications are designed and constructed, how they communicate and cooperate, and where they reside. A subset of this architecture is the object architecture, which defines the internally consistent set of relationships between business relevant entities; it defines how real-world things interact, and defines the expected behaviors of each object.	Application development tools, 3GLs and 4GLs, languages, web development and authoring tools, repositories, ERP applications, project management, CASE tools, testing tools, object development tools, object repositories.
WEB / E-Government	Web / E-Government architecture defines the technologies, standards and guidelines that relate to web based universal access for employees, customers and partners to business information and applications. It covers web based business to business, business to customer, and employee to agency, and inter- and intra-agency transactions. This architecture addresses user interfaces, electronic commerce, digital government, database connectivity and business logic, e-forms processing, etc.	Electronic commerce (procurement, payment, EDI), Web browser, intranet servers (mail, web, news, proxy), PKI, web portals, forms processing, middleware, content management, database connectivity, development and authoring tools, search engines, etc.

Domains	Description	Technology Categories
Collaborative / Workflow	The collaborative and workflow architecture defines the environment for facilitating and automating business processing and content management. It addresses the rules, behaviors of conversation focused business behavior, and the rules and practices of activity focused business behavior.	Collaborative tools, workflow, middleware, groupware tools, E-Mail, document management, imaging, content management, videoconferencing, middleware, etc.

Appendix 4. EWTA Update Process Workflow Diagrams

This appendix contains diagrams that illustrate the EWTA update process workflows.

Diagram 1 – EWTA Update Process – Paper-based Research

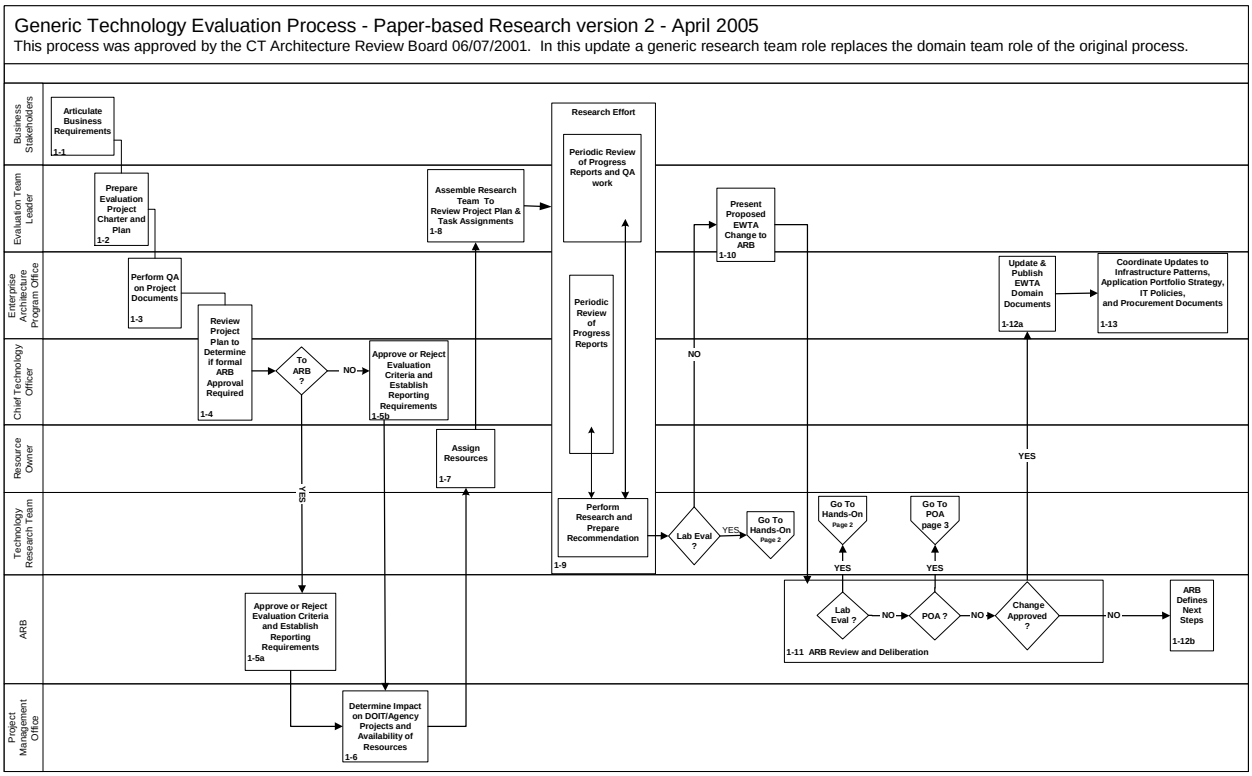


Diagram 2 – EWTA Hands-on Evaluation Process

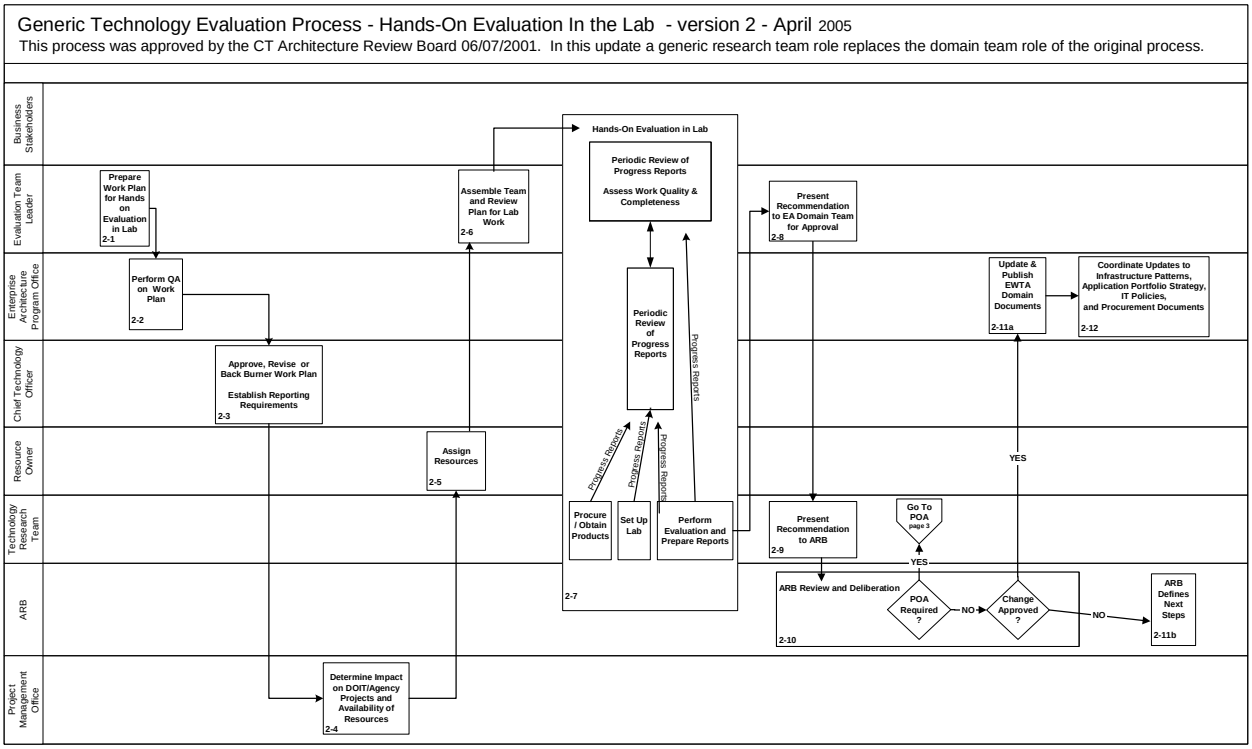


Diagram 3 – Proof of Architecture Process

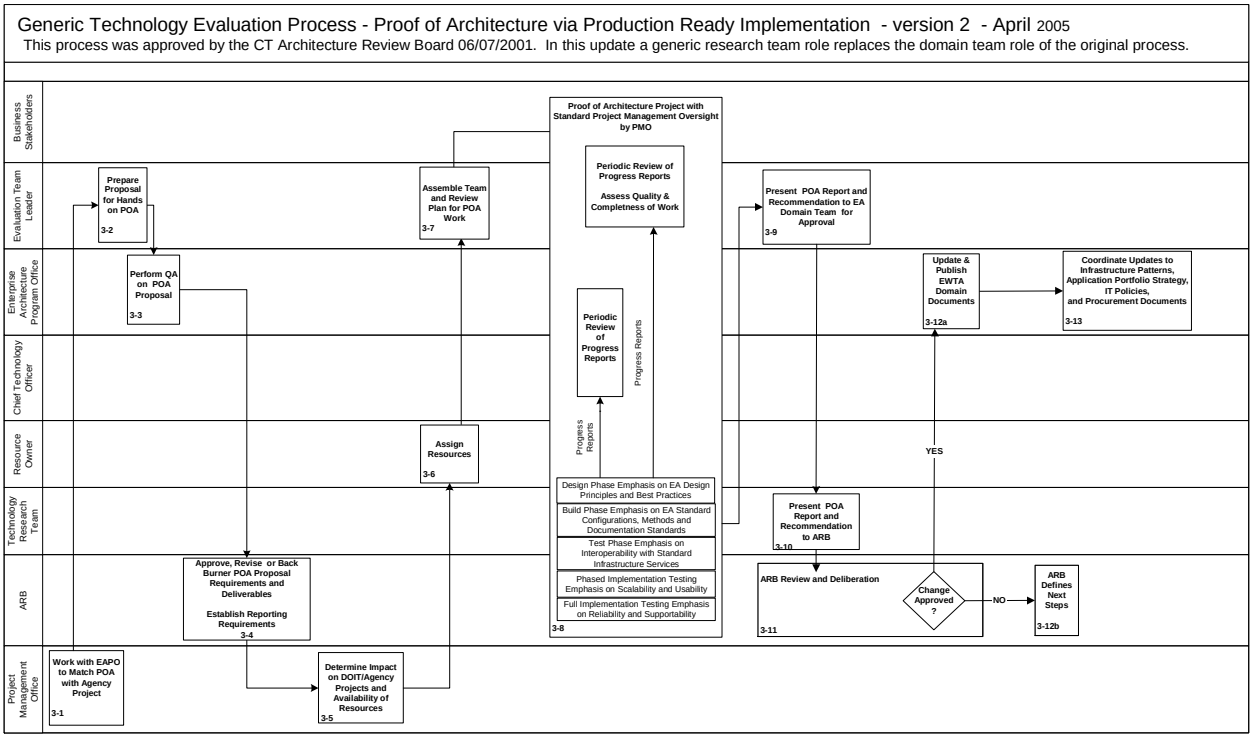
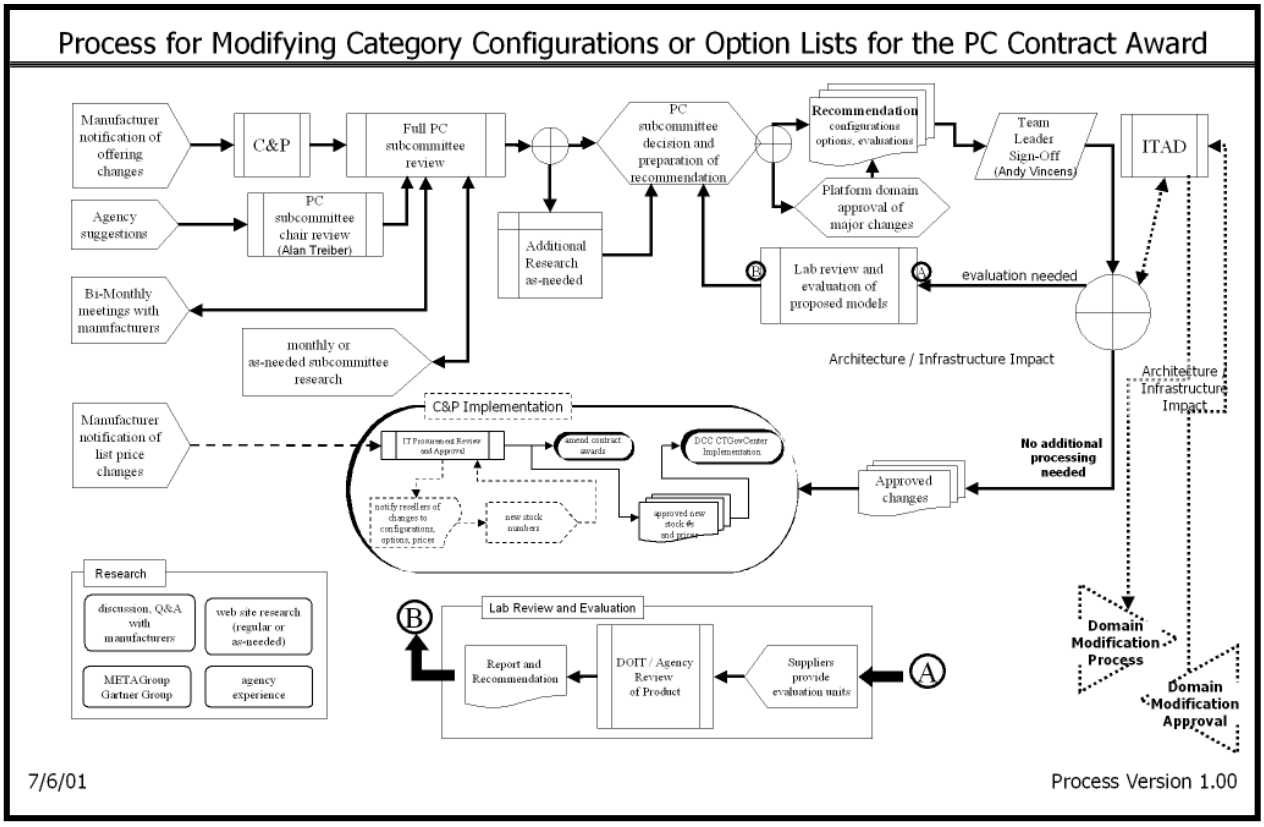


Diagram 4 PC Configuration Management Process



Appendix 5. Roles and Responsibilities

Business and IT Strategy Board

The Business and IT Strategy Board exists to ensure the alignment of IT with the business requirements of the State and its agencies. This group verifies the Common Requirements Vision and approves the Conceptual Architecture Principles of the EWTA. The board works with the Architecture Team to keep the Requirements for Technical Architecture and the Conceptual Architecture Principles current with the business needs of the State. They provide important advice and support for new statewide IT initiatives and policies, as well as adjudicate final appeals for exceptions to architecture standards.

Responsibilities include:

- Work closely with the Architecture team to provide input on business drivers and their subsequent decomposition into Requirements for Technical Architecture (RTAs).
- Approve the Common Requirements Vision and the Conceptual Architecture.
- Charter the Architecture Review Board (ARB) and authorize them to approve certain lower level EWTA deliverables, specifically the domain architecture documents, and to deny/approve/escalate exceptions to the EWTA standards. Note: the Strategy Board is the final "court of appeal" for exception requests.
- Charter the Enterprise Program Management Office (EPMO) to manage resources associated with (but not limited to) architecture development or infrastructure projects on behalf of the Strategy Board or ARB.
- Recommend to the CIO IT policies for adoption.

Architecture Review Board

The Architecture Review Board (ARB) is responsible for the promotion, approval and enforcement of the technical standards. Its membership is made up of senior IT and agency personnel. The ARB approves domain team deliverables (i.e., technical standards, design principles, product standards, best practices, and standardized configurations) and adjudicates appeals for exceptions to architecture standards. The Architecture Review Board (ARB) role is to promote, approve and enforce the technical standards. Its membership is made up of senior IT and agency personnel, and is chaired by the DOIT Chief Technology Officer.

Responsibilities include:

- Maintaining the EWTA process discipline and sponsoring new and revised standards.
- Approving domain team deliverables that impact agencies (i.e. technical standards. design principles, product standards, best practices and standardized configurations).
- Adjudicating appeals for exceptions to architecture standards.
- Reviewing domain and architecture team initiatives and recommend priorities.
- Reviewing possible infrastructure impacts of planned projects.
- Utilizing EWTA teams as a resource in understanding domain deliverables.

Enterprise Architecture Team

The architecture team translates the agencies' requirements into a business driven IT direction. This team is made up of the members of the Architecture Division, senior technical management

from DOIT, and senior business management from agencies who are familiar with the use of IT to solve business problems. This important team develops and updates the Common Requirement Vision and Conceptual Architecture Principles that document the business needs of the State for the technical architecture. This team is usually assembled when a new iteration of the common requirements and conceptual architecture is needed. Between iterations, the DOIT Architecture Division covers the responsibilities of this team.

Responsibilities include:

- Development of the common requirement vision and conceptual architecture required for EWTA.
- Assure that that technical domain teams are organized and sized correctly and the technology components are assigned to the appropriate domain team.
- Charter and oversee domain team activities.
- Consolidate and identify additional initiatives from domain teams to fill domain gaps.

Technical Domain Teams

The technical domain teams provide the knowledge and expertise required to develop the technical architectures and standards for the enterprise architecture process. Each team consists of technical experts from throughout the State. These teams are responsible for the development and maintenance of the Domain Architecture Documents, including the domain specific deliverables (i.e. design principles, technical standards, product standards, standard configurations, and best practices). The teams are expected to keep abreast of new technology and make recommendations on new technology to close gaps in the current environment.

DOIT Architecture Division

The DOIT Architecture Division coordinates the EWTA process and its associated activities. The division is responsible for coordinating all technical domain team activities as well as communications and web site content. They also provide the function of the EWTA Architecture Team in between iterations of the Business Vision and Conceptual Architecture.

Responsibilities include:

- Ongoing enhancement, communication and governance of EWTA and EAS.
- Coordination of activities and deliverables between domain teams.
- Coordination and QA of deliverables and presentations to ARB.
- Provide staff support to ARB and the Business and IT Strategy Board.
- Coordinating publication of domain architecture documents.
- Coordinating use of research services.

Enterprise Program Management Office (EPMO)

The PMO exists at the enterprise level to coordinate and track: IT projects, schedules, and the architecture compliance process. DOIT personnel staff this office

Responsibilities include:

- Act as the facilitator for an architecture assurance function at the project level)
- Create / update the projects portfolio.
- Manage the projects portfolio

- Provide the strategy board and DOIT management with project scheduling recommendations.
- Coordinate the enterprise resource management and scheduling information.
- Track and coordinate interdependencies among projects.
- Monitor, report and communicate significant changes to projects.
- Provide project management for DOIT initiated enterprise-wide projects
- Track the progress and completion of projects.
- Coordinate the architecture compliance process to ensure that the integrity of the architecture is maintained as systems and infrastructure are acquired, developed and enhanced.

Appendix 6. Example of a Configuration Management Process

The following process is used by the Platform Domain team and the PC Subcommittee to manage the configurations for the personal computers available to State agencies.

Procedures for Maintaining the PC Contract Award and CTGovCenter web site
Version 1.00
Author: Alan H. Treiber
Additional materials submitted by: Mark Bannon, Gary Therrien, Richard May, Andy Vincens, Holly Miller-Sullivan.

Involved Parties and Major Roles (Responsibilities)

DOIT Contracts and Purchasing Division (CPD)

Administration of the contract award, including meetings with manufacturers and Suppliers as needed.
Audit product offerings and pricing.
Interface with Digital Commerce Corporation (DCC)
Provide oversight of CTGovCenter web site.

Manager of DOIT Mgmt. Oversight Group (MOG) IT Architecture Division (shortened to EA PROGRAM OFFICE below)

Responsible for governance of the modification process.
Coordination with other domain teams as necessary
Coordinate the presentation of any major Domain Architecture changes requiring the approval of the Architecture Review Board (ARB).

DOIT Platform Domain Team and PC Subcommittee

Creation and modification of categories and configuration specifications.
Approval of "major" or substantial changes to product offerings.

At present
Andy Vincens (DOIT) is the team leader of the Platform Domain;
PC subcommittee members are Gary Clauss (DOIT) Steven Lynch (DSS), Rick May (DMR) and Alan Treiber (DOIT); Alan Treiber serves as PC subcommittee chairperson.

Manufacturers of the Personal Computers

Provide up to date model component specifications and web site addresses (or URLs) for product information on a publicly accessible web site.
Provide product line direction and planned changes in offering.
Provide updated list prices to CPD along with URLs to publicly accessible list prices.

Suppliers (Resellers) of the Personal Computers

Provide discounted pricing and stock numbers (to CPD) for use on CTGovCenter.
Provide required reporting requirements (for example see:
http://www.doit.state.ct.us/purchase/awards/CA0017021/vendinst.htm).

Digital Commerce for Contracts (DCC)

Process orders for PCs from the CTGovCenter web site.
Provide maintenance of the CTGovCenter web site, including maintenance of links to manufacturers' web sites.
Provide required reporting.

State of Connecticut Agencies

Responsible for reporting problems with deliveries, billing/receipting, warranty support issues, *etc.* to Contracts and Purchasing (CPD).

Major Activities

Administration (by CPD)

- Modification of the contract awards by amendment process.
- Processing of changes to list prices and discounted prices.
- Quality Assurance auditing of product offerings and prices for compliance with contract award provisions.
- Updating information and prices on CTGovCenter.
- Resolving issues involving problems with deliveries, billing/receipting, warranty support issues, etc. and any other matters with suppliers and manufacturers.

Configuration Management (by the subcommittee or Platform Domain)

- Changes to category configurations, i.e., specifications; this includes category options.
- Responding to agency requests for changes.
- Hands-on product reviews for compliance with configuration specifications.
- Additions or deletions of categories.

Meetings

- Regular meetings of the PC subcommittee with manufacturers to discuss technical and/or product updates or changes; – these would be either monthly or bimonthly depending on market place volatility and vendor preference.
- Monthly meetings of the PC subcommittee to consider modifications to configurations or specifications, and to consider agency requests; these meetings may be conducted electronically or by phone, conditions permitting.
- Regular meetings of CPD with Suppliers (and DCC) on contract administrative matters – the frequency of these meeting would be determined by CPD.
- CPD meetings with manufactures on contract administrative matters – as needed.

Information and Process Flows

There are three primary information / process flows:

1. Modifications to the PC categories and their specifications, i.e., configurations, and the options offered.
2. Processing of requests by agencies for modification (changes or additions) to the PC configurations and options.
3. Contract Administration, *e.g.*, processing of reseller information (prices, stock numbers, product descriptions, etc.) for updating CTGovCenter and for quality assurance audits,

resolving disputes between agencies and resellers, enforcement of contract award provisions, *etc*.

1. Modifications of Categories and Specifications (Adds, Deletes, Changes)

Changes to the specification of and/or approval of manufacturer models for those categories and changes to options are the responsibility of the PC subcommittee of the Platform Domain team. As part of the process, manufacturers may request changes, but the Platform Domain team or PC subcommittee will originate all modifications. Major changes to category specifications will be the joint responsibility of the PC subcommittee and the full Platform Domain team.
The Suppliers have no role to play in the final determination of categories, specifications or product offerings. Under no circumstances will CPD approve changes to specifications, models or options by manufacturers and suppliers.

The PC subcommittee will conduct regular reviews of technology and product offerings. This can be accomplished by:

- researching Internet web sites and manufacturer web sites,
- gathering & reviewing information from the State's IT consultants (METAGroup or Gartner Group),
- receiving regular communications from, and conducting discussions with, the manufacturers, and
- gathering & reviewing agency experience or research.

In addition, the manufacturers will notify DOIT Contracts and Purchasing (CPD) of substantial changes to components or models that were not available for disclosure at the regular meetings between the PC subcommittee and the manufacturers. CPD will then forward that information to the PC subcommittee.

Based on its review, the PC subcommittee will make recommendations on the modification to the specifications for any category. The subcommittee will make recommendations on the models that will meet those specifications. The PC subcommittee will also make recommendations on the options for each category.

If needed, the PC subcommittee can request that a hands-on review of products be conducted by designated team(s). In some cases, it may be possible to use agency level product research. Optionally, the manufacturers may be charged with evaluating their offerings based on DOIT supplied evaluation criteria. Gary Clauss (DOIT LAN Support and PC Subcommittee member) will coordinate the evaluation, and will define and maintain the testing criteria and process steps as approved by the Platform Domain leader.
The chairperson of the subcommittee will compose the final recommendation and present it to the entire subcommittee and, once approved by the subcommittee, to the Platform Domain team leader for action.

The entire Platform Domain team will review and approve any major changes to categories, or the addition or deletion of a category. The Platform Domain team leader (Andy Vincens) will sign off on all final recommendations, prior to forwarding the recommendations to CPD for implementation. The team leader will notify EA PROGRAM OFFICE of the recommended changes and outcome of the implementation.

NOTE: Some additions or changes to the configurations or categories may have substantial impact on the Platform Domain Technical Architecture. (An example would be the proposed addition of a thin-client category.) In such cases, the Platform Team will also follow the defined Platform Architecture Modification Process. EA PROGRAM OFFICE will coordinate any involvement of other domain teams and all interactions with the Architecture Review Board.

2. Agency Requests

Agencies will present suggestions for changes to configurations, or changes or modifications to the option lists to the chairperson of the PC subcommittee. Normally this will be done by e-mail to the subcommittee chairperson (alan.treiber@po.state.ct.us). Should any of these be sent to IT CPD, they would then route those requests to the chairperson, and will also notify the requestor. The chairperson will review the agency requests and then forward the suggestions to the PC subcommittee for review and determination of action. The review process for options and some configuration changes would probably be limited to Internet based research. The review process for all new configurations or major changes would follow the process outline in point 1 above.

Should the PC subcommittee have a positive recommendation, the Platform Domain team leader (Andy Vincens) will sign off on the recommendations and forward them to CPD for implementation. CPD will notify the original requestor of the final decision on their request.

3. Contract Administration

All approved recommendations and changes to configurations and options will follow the contract supplement processes of CPD. CPD will notify the suppliers of the changes to configurations and options. CPD and obtain appropriate information on reseller model numbers, descriptions, list prices, discounted prices etc. After review by CPD, this information will then be sent to DCC for updating the CTGovCenter web site. CPD will also update the appropriate Contract Award posted on the DOIT Internet web site [http://www.doit.state.ct.us/purchase/awards/CA0017021/award.htm].

The manufacturers are responsible for notifying CPD of changes to list prices on base configurations and options. CPD will verify all list prices and discounts (using the manufacturer's public web site, prior to posting changes on the CTGovCenter web site. Only CPD will initiate changes to the CTGovCenter web site.

The manufacturers will notify CPD of any major changes to product offerings that occur between the regular meetings between the manufacturers and the PC subcommittee. CPD will forward that information to the PC subcommittee for consideration.

CPD will conduct regular audits of product availability and pricing by examination of the publicly accessible configuration pages on the manufacturer's publicly accessible web site.

Appendix 7. RFP Section for System Architecture

This System Architecture section is designed to be used in RFP's to create a free-standing technical architecture section in respondent proposals to facilitate and expedite architecture conformance reviews during an RFP evaluation process. Without a separate section it is difficult and time consuming to create an integrated view of the architecture from thousands of facts and tens of diagrams spread throughout proposals that can be hundreds of pages in multiple documents.

SYSTEM ARCHITECTURE

State of Connecticut Enterprise-Wide Technical Architecture

DOIT has established an Enterprise Architecture Program (EAP) as part of its mission to develop and support a statewide IT environment for State agencies using standardized IT components and services. The EAP has established formal processes for the development and implementation of an Enterprise-Wide Technical Architecture (EWTA) for the State of Connecticut. The EWTA is currently comprised of the following nine technical architecture domains:

Application Development

Collaboration and Directory Services

Data Management and Data Warehouse

Enterprise Systems Management

Middleware

Network

Platform

Security

Web/E-government

DOIT has developed a document for each domain to serve as a reference guide to the technical architecture for the technologies covered by the domain. Vendors will need to reference these documents to identify the policies, principles, product and technical standards, best practices and guidelines that are relevant to this RFP. Current domain documents are on-line at http://www.ct.gov/doit/cwp/view.asp?a=1245&q=253968 . As the domain architectures can change from month to month, each document has a History of Changes table that can be consulted to quickly identify what changed in each revision.

The policies, principles, standards, best practices and guidelines referred to in these documents are considered **State IT architecture requirements** for any new system or major enhancement to the current IT environment. Vendors are strongly encouraged to propose solutions that both satisfy the functionality stipulated in this RFP and conform to the EWTA. Vendors should be aware that the proposal evaluation process includes a conformance review, which may result in rejection of proposed architectural elements.

EWTA Conformance Review

Vendor proposals will be evaluated for conformance to the EWTA. The conformance evaluation will be based on a review of the response to this System Architecture section. All necessary information must be provided in this section and should not be included by reference to other sections. Proposals will be evaluated against relevant aspects of all nine EWTA domains. Non-conforming architectural elements of otherwise favorable Vendor proposals may be subject to approval by the State's Architecture Review Board (ARB), through an exception process described online at http://www.ct.gov/doit/cwp/view.asp?a=1245&q=253972. The ARB is the governing body charged with reviewing and resolving architecture conformance issues. The ARB's architecture exception process examines the impact and cost of allowing the implementation of non-conforming products, standards and design practices. Among the issues considered during the exception process are the satisfaction of agency information and process management requirements, consistency with conceptual architecture principles, and Total Cost of Ownership (cost of implementation as well as ongoing support, maintenance and enhancements). All software included in the proposal is subject to EWTA conformance review, including Commercial Off The Shelf (COTS) products, whether they are the primary means of providing business functionality or merely a component of the proposed solution. Vendors are reminded that the EWTA includes design principles and practices that govern how some products are implemented. How strategic products are deployed is as important to the State as which product is used.

Overall System Architecture

The Vendor's proposal must provide information needed for the State to determine the extent to which the proposed solution conforms to the Enterprise-Wide Technical Architecture (EWTA).

Overview of Architecture

Vendor must provide an overview of how its proposal conforms to the State of Connecticut Enterprise-Wide Technical Architecture. Vendor must explicitly address conformance from the perspective of the principles, product and technical standards, as well as best practices and guidelines relevant to the major components of the proposed system.

The overview must specifically address the issues of:

- Logical N-Tier design, consisting of modular components and sub-components with partitioning of components by defined interfaces and messaging based communications (inter-application and intra-application);
- Use of XML for application to application messaging.
  - The Vendor must explain how the proposed design utilizes XML for inter-application messaging.
  - If your design also uses XML for intra (component to component) messaging, please explain that as well.
  - The Vendor must identify the source of the XML Schema or Document Type Definitions (DTDs) utilized in the proposed design;

Open system implementation using established standards and non-proprietary components. All proprietary extensions to open standards specifications must be identified;

A multiple zone security model (e.g., DMZ, server zone, database zone) separated by firewalls and access restriction mechanisms; and

Use of the State's LDAP-enabled enterprise directory as the primary authentication service for system users in conjunction with a role-based authorization method within application components.

Vendor Rationale for Architectural Choices

The State does recognize that IT standards and products evolve over time, often rapidly. To ensure that functional requirements are met, the State may consider proposals that include architectural elements that do not conform to the EWTA, but vendors must thoroughly describe the rationale for their recommendations. Rationales are to be comprehensive but concise. Do not cut and paste manufacturer's marketing literature. Vendors may attach manufacturer technical specifications as supporting documentation, but the rationale itself must be sufficient to justify the recommendation. Rationales should provide documentation of how the Vendor's recommended technologies are consistent with the State's Conceptual Architectural Principles (http://www.ct.gov/doit/cwp/view.asp?a=1245&q=253964) and with the relevant domain architecture principles.

Where the Vendor proposes architectural elements for which standards do not exist, or for which the EWTA provides for more than one product, technology or approach, the Vendor must provide a rationale for the recommended choice.

Where the proposal does not conform to the EWTA, the Vendor must itemize the exception(s), and provide a rationale for each item. Rationales for non-conforming items must also address suitability for functional requirements, and applicability to the objectives of this RFP. The Vendor must identify, by section number and heading, where, in the proposal, the proposed technologies or design approaches have impact or are referenced.

Rationales for non-conforming items must compare the recommended element against the element provided for in the EWTA, including the functional, technical and cost considerations that make it a better choice for the State than one that conforms to the EWTA. (Note: specific costs must not be included in the rationale, only a description of cost considerations.) Rationales for non-conforming items must also describe the skills, training and experience necessary to implement and support the non-conforming elements, and provide an FTE estimate for these activities. This information will be used by the State to evaluate the risk and implied costs of non-conforming elements.

If the Vendor's proposed design does not use message-based interfaces between components or systems, or an N-Tier design, the Vendor must explain the rationale for such a design. The Vendor must explain what the impact would be if the Vendor is required to use message-based interfaces between components or systems.

If the Vendor's proposed design does use message-based interfaces but does not utilize the products specified in the relevant domain architecture documents, the Vendor must explain the rationale for choosing alternative products. The Vendor must explain what the

impact would be if the Vendor is required to use the products specified in the domain architectures.

Technology View – Structural Diagram and Component Specification

Structural Diagram

The Vendor's proposal must provide a diagram showing all the physical components of the system and how they are interconnected. The diagram must include the components required for the application and data environments – Development, QA/Test, Staging and Production. The diagram must include the proposed backup solution. Organize the components by the tiers of the n-tier architecture (see the Conceptual N-Tier Architecture diagram in the Attachment entitled *EWTA Patterns: N-Tier, Security Zones, Principles, Partitioning*). A detailed description of the hardware and software that comprise each component must be provided in the Detailed Technology Component Specification section (below).

Use the following formatting conventions in the Structural Diagram:

1. All physical components in the proposed system must be represented by an icon in the structural diagram whether they will be provided by the vendor, the State, or a third party. See Note 1 below for instructions on making those distinctions through labeling and component specifications. Use standard IT icons and be consistent in their use within and across diagrams. Each component icon in the structural diagram must be labeled to indicate the function of the component in the system. The label format is "System Component Function (n)". The number (n) in the label for the physical component is the number of these physical components required for the system, e.g. Production Database Server (3), Production Application Server (2), Development Application Server (1). The detailed description of the hardware and software that comprises the component must be provided in the Detailed Technology Component Specification section.

2. Icons representing system components must be boxed with a dashed line to indicate different physical locations (e.g. vendor data center, State data center, agency regional office, etc.), with each box labeled at the bottom.
   - For situations where there are multiple instances of the physical location, include the number of instances in the label for the box, e.g. Branch Offices (5). The diagram should indicate the components to be installed in each physical location, e.g., Application Server (1). The cost sheet should indicate the total quantity of components for each location. In this example the quantity in the cost sheet would be five application servers (one in each of five branch offices).
   - If necessary because of the complexity of the system, additional diagrams may be provided for some physical locations. The primary diagram should include a box for the physical location with the appropriate label and a reference to the second diagram. The primary diagram and the secondary diagram must include the connection lines and labeling information so that we can correctly match up the interfaces between components.
   - Additional diagrams may also be used to provide structural details about interfaces with other systems.
3. The major functional tiers of the system (client tier, presentation/interface tier, applications tier, database tier) should be indicated by using different colors for the background and

labeling each one at the top. This should remind the vendor that the State has architecture design principles and practices related to physical and logical partitioning of system components, which should be reviewed and carefully considered when developing proposals. Place the icon for each physical component on the background color that corresponds to its appropriate tier in the system. The Conceptual N-Tier Architecture diagram is an example of this format. Vendors are to use separate icons to represent the client platforms for public users, external State and Partner users (outside the firewall), mobile users, and internal State users (network attached inside the firewall) in order to differentiate the application design, implementation and security details for those different clients and environments.

4. It is not necessary to include firewalls in the structural diagram, however the proposed system must be able to communicate between the tiers through a firewall. The Security Focused N-Tier Architecture diagram in the Attachment entitled *EWTA Patterns: N-Tier, Security Zones, Principles, Partitioning* shows the partitioning of the environment into security zones through the use of multiple firewalls. Vendors should double check the structural layout of the proposed system by overlaying it on the security zones. Vendors may include this additional security view in this section if they wish.
5. Use lines to indicate how the physical components are interconnected, and label each with the transport protocols, messaging protocols, data packaging formats, and encryption methods.
6. Circles, ellipses or clouds can be used to indicate networks (LAN, WAN, MAN, mobile communication networks, Internet) but each should be clearly labeled.

Notes:

1. See the Current State and Agency Infrastructure section in the RFP for the existing infrastructure components that must be accommodated in the vendor's proposed system. Where a vendor is proposing to use existing infrastructure components, the component icon in the diagram should indicate (Existing) below the icon label. The corresponding Detailed Physical Component Specification should also include the word "existing" where appropriate to indicate which elements within the component will be reused, upgraded or added. This will allow for situations where hardware will be upgraded, existing software and licenses reused, or new licensing units added.
2. The (n) in the System Component Function label for each icon in the structural diagram is the number of these physical components proposed for the system, e.g. Database Server (3), Production Application Server (2), Development Application Server (1). If the detailed specification for the component is not the same for each instance, then a separate icon must be used in the diagram for each differing component, with a different label used for each, and a separate detailed description provided. If redundant components and communication channels are used to provide parallel processing, they should also be shown as separate.

Detailed Technology Component Specification

The Vendor's proposal must provide a detailed technology component specification that includes the requested information (items 1-15 below) in the specified format.

For each Technology Component represented in the Structural Diagram the following detailed information must be provided. If an information item is not relevant for the technology component, respond with "Not Applicable" rather than leaving the item blank.

1. System Component Function (n) [Matches label used on structural diagram].
2. Reason for multiple components, e.g. load balancing, fail-over, etc.
3. Hardware Manufacturer, Product Name, and Product Model. Detailed manufacturer's technical literature is to be attached as an appendix that is referenced in this item. Do not include manufacturer's marketing verbiage in this section.
4. Hardware Operating System and Version.
5. Hardware CPU Type (n).
6. Hardware Motherboard.
7. Hardware Memory Types and Size of each.
8. Hardware Cache Types and Size of each, including L2.
9. Hardware Storage Types and Size of each.
10. Backup Method. Identify the system component that provides the backup medium for this component. Specify the frequency, duration, and bandwidth requirement for each type of backup provided by the proposed system. Be sure to address system software backup, application software backup, and data backup as appropriate.

Provide the following information for each software product installed on the component. Embedded Software Products that have a significant functional role in the system, e.g. an embedded web server, must be specified separately.

11. Software Function
12. Software Manufacturer, Product Name and Product Version. Detailed manufacturer's technical literature is to be attached as an appendix that is referenced in this item. Do not include manufacturer's marketing verbiage in this section.
13. Software License Type (n)

Provide the following information about the connections between this component and other system components.

14. Network Connection Type, Communication Protocols, Network Interface Card Manufacturer, Model and Bit Rate. If more than one network interface card is included in this component, provide the quantity. If different network interface cards are included in this component, provide the manufacturer, model, bit rate and quantity for each one.
15. Identify all other components that this component communicates with. For each one provide the interface type, communication protocols, including protocols encapsulated in other protocols, whether it is a synchronous or asynchronous link, any specific port requirements, bandwidth requirements and encryption methods to be used.

Partitioned Systems

The Vendor must provide the following additional information for system components that are partitioned to perform multiple functions:

1. An additional separate diagram showing how the component is partitioned.

2. For each partition provide the following information: Partition Name, Function, Resources Allocated to Function, access methods (indicate which components or partitions this partition is connected to, and the method used).
3. For functions that are required by the State's security model to communicate through a firewall, but will instead be communicating on a partition-to-partition basis, describe the mechanism for providing equivalent firewall functionality.
4. The partitioned component's icon label in the primary and secondary diagram must reflect the multiple functions performed by the component.

Notes:

1. The (n) in the System Component Function label is the number of these physical components proposed for the system, e.g. Database Server (3), Production Application Server (2), Development Application Server (1). If the detailed specification for the component is not the same for each instance, then a separate icon must be used in the diagram for each differing component, with a different label used for each, and a separate detailed description provided.
2. The (n) in the item Hardware CPU Type is the number of CPU's included in the proposed system component.
3. The (n) in the item Software License Type is the number of these licenses included in the proposed component, e.g. Server License (1) [one for each instance of the component]. If three instances of the same component are included in the proposal, this would be reflected in the cost sheet as a quantity of three.
4. For any of the information items in the Detailed Technology Component Specification where existing products, software or licenses will be used, include the word "Existing" at the beginning of the response. For existing physical devices, identify the organization that is providing the item, and where it is located, e.g. "3. Hardware Manufacturer, Product Name, and Product Model: Existing OSC Dell server, model 8450 located at DOIT Data Center." If upgrades to existing components are required include that information in the response for the appropriate item, e.g. "4. Hardware Operating System and Version: Existing Windows 2000 Server SP2, Upgrade to Windows 2000 Advanced Server SP3".

Appendix 8. The EWTA Exception Process

An exception to the principles and comprehensive standards defined in the EWTA can be requested by a State agency at several stages during the life-cycle of a project.

- Non-conformance to the EWTA may be identified during an initial architecture review as part of project approval by DOIT. The agency can file a request for a one-time exception to the architecture for the project. The exception will be addressed at a regularly scheduled Architecture Review Board (ARB) meeting.

- After a project has been approved and the project is in an implementation phase, an agency may find a need to deviate from the EWTA for business reasons. This type of exception request would also cover procurement situations where an agency is in the process of evaluating proposals to an RFP, SOW, etc. An agency can request an expedited review if the situation warrants it and the ARB will convene a special meeting to adjudicate the request. Otherwise it will be taken up at a regularly scheduled ARB meeting.

An agency must submit a formal request to the ARB for an exception to the architecture. The request must document the justifications for the exception and the impact of granting versus not granting the request. The domain team leaders of the affected domain architectures assess the request, and their recommendations are documented in a standardized format for the ARB. The agency and the domain team leaders are required to present oral arguments along with the written documentation to the ARB.

If an exception is not granted to the agency, an appeal can be filed to the Chief Information Officer. This appeal must be in writing and state clearly the business reasons for granting the exception.

The DOIT Enterprise Architecture Unit manages the exception process.

Agency requests for exceptions and appeals must use the approved template, Exception Request Form EX-01 Part A. (see below)

The Domain Teams provide an analysis and recommendation regarding the exception request. This is documented on Part B of the form.

The EA Program Office creates a summary of the analysis and recommendations on Part C of the Exception Request form.

Form EX-1 Agency Request for Exception to EWTA

Submittal Date:

Part A – To be completed by agency requesting the exception

Project Description

Project Title: _____

Participating Agency or Agencies: _____

Project Manager: _____

Contact Information (phone, email): _____

Outside consultant or vendor: _____

Contact Information (phone, email): _____

Start and End Dates: _____

Anticipate date of "roll-out" into production mode at agency: _____

Note: If phased roll-out, provide dates for each phase.

Current Project Life Cycle Stage
(copy and paste this symbol ✓)

- ❑ IT Planning
- ❑ Project Planning
- ❑ IT Architecture Design
- ❑ RFP/SOW Requirements Definition
- ❑ RFP/SOW Evaluation
- ❑ Contract Negotiation
- ❑ System Implementation

Is this an internal agency application or system? ❑Yes ❑ No
If no, please list which State agencies are users of this application or system.

Project Architecture

Do you have an agency IT architecture defined? ❑Yes ❑ No
If yes please attach or e-mail a copy.

Is this application or system compliant with the agency's IT architecture? ❑Yes ❑ No

Provide a description of the architecture proposed for the application/system including any interfaces to other systems within the agency, to other agencies, and to external parties. Please attach or e-mail a diagram.

Nature of Exception Request

Check all exemptions that apply (copy and paste this symbol ✓) and then describe the nature of the request in the appropriate boxes below.

- ❑ Conceptual Architecture Principles
- ❑ Domain Architecture Principles
- ❑ Technical Standards
- ❑ Product Standards
- ❑ Implementation Guidelines or Best Practices

Exemption from Conceptual Architectural Principles

Exemption from Domain Architectural Principles

Exemption from Domain Technical Standards

Exemption from Domain Product Standards

Exemption from Implementation Guidelines or Best Practices

Briefly, describe the products that are being proposed, or have been chosen, to implement the application/system. Indicate if the products are currently in use, obtained from another State or Federal agency, commercial off-the-shelf, vendor package or custom built.

Justification for Exception Request

Is this a temporary solution to fix a critical problem, until a replacement system or application can be developed or implemented? ❑Yes ❑ No
If yes, please indicate the duration involved.

Briefly, describe all other business reason(s) for requesting the exception, including functional impacts of not using proposed standard(s) or product(s).

Briefly, describe technical reason(s) for requesting the exception, including functional impacts of not using proposed standard(s) or product(s).

Impact Assessment

Briefly describe the impact on the agency's IT architecture, infrastructure and existing or planned systems should this exception request be approved.

In the event, this exception request is approved, describe the time frames for transitioning away from the non-conformant principles, standards, products or practices granted in the exception and implementing EWTA-conformant principles, standards, products or practices.

Briefly, describe the financial impacts of using the proposed exception(s) to EWTA principles, standard(s), product(s) or practice(s). This description should include Total Cost of Ownership (including upgrades, maintenance, support, training, etc.) over the estimated lifetime of the application or system.

Briefly, describe the alternative(s) for design or implementation should the Architecture Review Board decline the request for an exception.

Form EX-1 Request from Agency for Exception to EWTA
Part B – Domain Team Recommendation

This section should be completed by all of the domain teams that are impacted by this exception request.

EWTA Domain Team: _____

Team Leader: _____

Contact Information: _____

Project Description

Exception Request Received Date: _____

Project Title: _____

Participating Agency or Agencies: _____

Current Project Life Cycle Stage: _____

Nature of Exception Request

- ❑ Conceptual Architecture Principles
- ❑ Domain Architecture Principles,
- ❑ Technical Standards
- ❑ Product Standards

Exception Requested:

Recommendation

Is the domain team supporting this exception request?

[ ] Requires Additional Research To Make Recommendation

If additional research is required, then a matching DT-1 must be submitted along with this recommendation.

[ ] YES [ ] NO

If yes, will changes to the domain architecture be proposed? [ ] YES [ ] NO

If technical architecture changes will be proposed, then a matching DT-2 must be submitted separately by the domain team.

What is the recommendation of the domain team with respect to the exception request?
(simple declarative statements, including any recommended implementation constraints)

Briefly describe the justification or rationale for the above recommendation.
(*e.g.*, Requested product is consistent with domain principles or technical standards as noted below, or, Requested implementation violates domain principles or best practices, as noted below)

Conceptual Principles

Technical Standards

Product Standards

Best Practices

Supporting Research For This Recommendation

Supporting Research

Please check off the type of research the domain team did in support of this agency exception request and then provide a brief description. If there is more than type of research, describe them in decreasing order of importance.
(copy this ✓ and paste over the box)

- ❑ Web or paper research
- ❑ Use of consultant services
- ❑ Other please specify

Please provide a description of the research that was conducted:

Please check off the information sources used and then provide a brief description below each source including specific names as appropriate.
(copy this ✓ and paste over the box)

- ❑ IT Research and Advisory Services
- ❑ Publications from national or international standards bodies
- ❑ Publications from industry consortia
- ❑ Information provided by manufacturer or software publisher

- ❑ Other please specify

Impact of Approving This Exception Request

If the Architecture Review Board approves this exception request, what will the impact be on the following:

This Domain Architecture

Provide a brief description of the changes to the domain architecture that will result from the approval of this exception request. **Note**: If the technical architecture will not change, indicate no impact.

Domain Team Workload

- ❑ Adding non-standard products to the IT environment that the domain architecture team must account for, track or accommodate in the technical architecture and implementation documents
- ❑ Adding a non-conforming design or configuration to the IT environment that the domain team must account for, track or accommodate in the technical architecture and implementation documents
- ❑ Other please specify

Cost of Ownership

What is the estimated financial impact of this exception request?

(Include TCO analysis when possible. i.e. Hard Costs – hardware, software, systems management, support, development, communications fees; Soft Costs – end-user peer support, self support and casual learning, planned and unplanned downtime, etc.)

Additional Comments

Add any additional comments that are deemed necessary.

Form EX-1 Request from Agency for Exception to EWTA
Part C – To be completed by the Architecture Team

Submittal Date:

Project Description

Project Title: _____

Participating Agency or Agencies: _____

Project Manager: _____

Nature of Exception Request (copied from Agency Exception Request)

Check all exemptions that apply (copy and paste this symbol ✓) and then describe the nature of the request in the appropriate boxes below.

- ❑ Conceptual Architecture Principles
- ❑ Domain Architecture Principles,
- ❑ Technical Standards
- ❑ Product Standards

Exemption from Conceptual Architectural Principles

Exemption from Domain Architectural Principles

Exemption from Domain Technical Standards

Exemption from Domain Product Standards

Briefly, describe the products that are being proposed, or have been chosen, to implement the application/system.

(Indicate if the products are currently in use, obtained from another agency, State or federal agency, off-the-shelf, vendor package or custom built.)

Summary Recommendation

What is the overall recommendation of the architecture and domain teams?

If the recommendation is negative, what acceptable or existing alternatives can be proposed to solve the business and technical problems of the agency are being proposed?
(Details should be included in the domain team section.)

What is the anticipated impact on the relevant domain architecture(s) should this exception be granted?

What is the anticipated impact on the State IT architecture should this exception be granted?

What is the anticipated impact on the State IT infrastructure should this exception be granted?

Include impact on Total Cost of Ownership if possible.

What is the anticipated impact on the State IT support services and staffing should this exception be granted?

Include impact on Total Cost of Ownership if possible.

Is the technical standard or product being proposed re-usable or suitable for inclusion in the affected domain architecture(s)?

Domain Teams Contributing Recommendations

MISSOURI ADAPTIVE ENTERPRISE ARCHITECTURE

Implementing a Blueprint for Standards and Methods

State of Missouri
Office of Information Technology (OIT)

MAEA Domain Facilitator's Guide

April 2004, Version 2.0

TABLE OF CONTENTS

INTRODUCTION

The ***MAEA Domain Workgroup Facilitators Guide*** is intended to assist MAEA Domain Committees, committee chairs, committee members, and external facilitators in preparing for and facilitating MAEA Domain Committee working sessions. This guide is primarily designed as a training tool to help facilitators create a setting of highly participative discussion, provide a setting of collaboration, work through social and political issues, connect to the policy making processes of the MAEA, and build a sense of community among the Domain Committee members.

This document is part of the continuing development of Missouri's Adaptive Enterprise Architecture Program, developed in concert with the Missouri Office of Information Technology (OIT), the Missouri Information Technology Advisory Board (ITAB), the Architecture Review Committee (ARC), and the Security Domain. National Systems & Research Co. (NSR) has been retained to assist in the coordination, document design, process development, and overall production of this document.

Productive MAEA Domain Committee meetings play a critical role in developing the Missouri Adaptive Enterprise Architecture Blueprint.

In general this guide has been produced to make the role of the facilitator easier by providing tools and topics that will be valuable to both new and experienced facilitators. Topics covered in this guide include:

- Specific guidance for facilitation of MAEA Domain Committees
- An overview of facilitation and general facilitation skills, which will be useful for Domain Committee working sessions
- Guidelines for Domain Committee productivity and dealing with conflict
- Additional resources for group facilitation included in the appendices

Though subject to the same over-arching Architecture Lifecycle Processes, it is not likely that any two MAEA Domain Committees will function in exactly the same manner. It is the role of the facilitator to ensure that what happens within each working session is consistent with the overall goals of the Missouri Adaptive Enterprise Architecture program: producing Architecture Blueprint assets through democratic deliberation, broad and diverse participation, and shared problem solving.

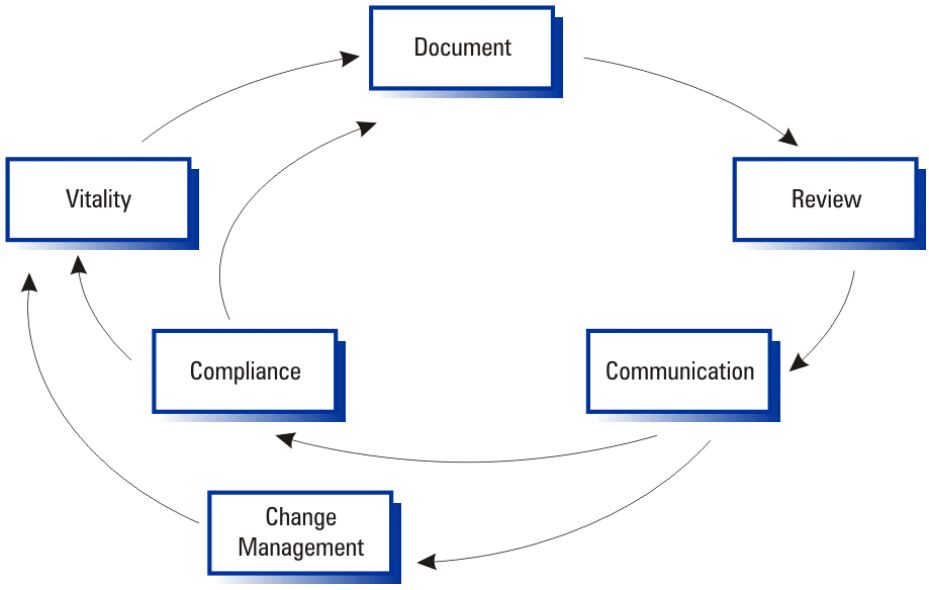
Productive MAEA Domain Committee working sessions play a critical role in developing the Missouri Adaptive Enterprise Architecture Blueprint. Given the potential diversity of the Domain Committee members' professional and personal
experiences, facilitating MAEA Domain Committee working sessions can be both challenging and rewarding.

As a reminder, this guide is not meant to be a substitute for the MAEA Manual, but as a supplement to it. Facilitators should have read and become familiar with the MAEA
Manual and with the Architecture Lifecycle Processes and should have participated in MAEA Education Sessions prior to facilitation of any Domain Working Sessions.

WHAT IS FACILITATION AND WHY IS IT IMPORTANT?

Facilitation is the act of assisting a group with the process of communication, enabling the group to complete its mission. Facilitation is the art and science of managing working sessions and group processes. Facilitation of the MAEA Domain Committee working sessions involves guiding the group as their activities touch each of the MAEA Architecture Lifecycle Processes as shown in Figure 1 below.

Figure 1. Missouri Adaptive Enterprise Architecture Lifecycle Processes



The facilitator's job is to guide the Domain Committee to use the MAEA Architecture Lifecycle Processes correctly, while at the same time, keeping the group focused on delivering those Architecture Blueprint items most useful to the State's IT decision makers. The following quote, adapted from a resource book for facilitators - *How to Make Meetings Work*, paraphrases the characteristics of the ideal facilitator.

> Facilitation is the act of assisting a group with the process of communication, enabling the group to complete its mission.

"The best facilitator has unobtrusive chameleon-like qualities; gently draws group members into the process; deftly encourages them to interact with one another for optimum synergy; lets the dialog flow naturally with a minimum of intervention; listens openly and deeply; uses silence well; plays back group member statements in a distilling way that brings out more refined thoughts or explanations; and remains completely non-authoritarian and non-judgmental."[1]

Facilitators create an environment in which Domain Committee members share ideas, opinions, experiences, and expertise to achieve a common goal. A skilled facilitator smoothes the way for the Domain Committee to brainstorm Enterprise Architecture options, identify the viable IT issues, and develop and implement specific Architecture Blueprint assets.

[1] Paraphrased from *How to Make Meetings Work*, Doyle and Straus, 1987

Good facilitators possess a variety of qualities and skills. Some of the qualities spring from such innate personality traits as being able to recognize one's own biases while remaining neutral, enjoying interaction with diverse groups, and inspiring trust. Although some people possess a natural talent for facilitation, most develop the skills through experience and with guidance from experienced facilitators.

The following "Checklist for Facilitation Skills," will appear throughout this guide as a reminder of the core skills that a facilitator should use to evaluate their effectiveness in dealing with Domain Working Session situations.

Checklist for Facilitation Skills

ARE YOU USING YOUR FACILITATION SKILLS?
Making Everyone Feel Comfortable And Valued
Encouraging Participation
Preventing And Managing Conflict
Listening And Observing
Guiding The Group
Ensuring Quality Decisions

With these core skills and this checklist in mind, a facilitator acts as a presence in the Domain Committee working sessions for the following reasons:

- To "balance" (facilitators are impartial)
- To ensure all voices are heard
- To mediate if necessary
- To pick up on subtle emotions and undercurrents
- To help the Domain Committee come to consensus
- To keep the Domain Committee on schedule

A skilled facilitator smoothes the way for the Domain Committee to brainstorm Enterprise Architecture options, identify the viable IT issues, and develop and implement specific Domain Architecture assets.

Facilitation is also about building a social relationship. Not all professionals work effortlessly in groups. As a facilitator you will need to tailor your style to build a strong rapport with the Domain Committee members. How well you facilitate matters little if you do not earn the trust and respect of the Domain Committee members. The combination of the core skills and a good rapport are the foundation of a strong facilitation process.

WHO SHOULD READ THIS GUIDE?

Potential Domain Committee facilitators, Committee Chairs, Committee Members, external facilitators and anyone else interested in MAEA Domain Committee working sessions will benefit from reviewing this guide. Those who have little or no formal training in facilitation will find a pragmatic summary of basic concepts and skills. Those with facilitation training or experience will find a targeted review of the unique facilitation activities associated with MAEA Domain Committee working sessions.

The facilitator's role is multi-faceted. Having a group made up primarily of facilitators does not necessarily mean the facilitation will be easy; in fact, the situation could be quite the contrary. If you don't have a facilitator in the group, it does not mean the group cannot accomplish anything. Facilitation is not a mystical or magical role. It's not one that most of us do naturally, but that many of us do intuitively.

We can all learn to do it. There is no personality that makes it impossible to be a facilitator. And there isn't a wrong way to do it. Facilitation, like teaching or parenting, is different fore each one of us. Each one of us develops strengths and abilities based on our own approach to the world and our own attitudes. There is no cookie cutter model.

How to Use This Guide?

> Facilitation is not a mystical or magical role…we can all learn to do it.

This guide presents facilitation skills and tools in the order in which they are most commonly used within a Domain Committee working session. Nevertheless, this guide is not meant to be opened and followed during a working session. Study of this guide before facilitating a working session can be extremely helpful for preparation, while a review of the information after a working session can help to determine ways to do a better job next time.

If facilitation is new to you, you should read, or at least scan, all sections and then go back and concentrate on those you find the most useful. Remember that this guide only touches a small portion of the vast knowledge available regarding facilitation, communication and group dynamics. If you have experience or training as a facilitator, you may want to go directly to the sections that address the needs particular to facilitating MAEA Domain Committee working sessions.

The first three sections of this guide suggest specific approaches to use when conducting MAEA Domain Committee working sessions, namely:

- Facilitating The Domain Committee Kick-Off Session
- Facilitating Domain Working Sessions
- Work Session Wrap-Up Activities

The next section of this guide, **Core Facilitation Skills and Tools**, provides an overview of the skills and tools that a facilitator will use throughout most working sessions.

The **Facilitation Creativity and Productivity** section presents ideas for coping with challenging situations, such as members carrying on private conversations.

The **Appendices** provide various facilitation support tools, including agenda and minutes templates, as well as sample agendas and minutes from the Security Domain pilot.

Facilitating the Domain Committee Kick-Off Session

The purpose of the Domain Committee Kick-off session is to set a climate of welcome and efficiency for work. A good climate is more likely when people use introductions to get to know each other's experiences and interests, and when the group members take responsibility to agree on agenda and guidelines as a structure for their work.

The Domain kick-off session is your best opportunity, as a facilitator, to energize the group and establish a common purpose toward completing the work. A great kick-off is the result of good planning. Before you go to the kick-off working session, you should prepare carefully for your role by reviewing those core facilitation skills and tools that are documented in the last two sections of this guide, **Core Facilitation Skills and Tools** and **Facilitation Creativity and Productivity**.

The facilitation process needs to feel inclusive from the beginning, so it's important not only to encourage but also to validate all input.

Checklist for Facilitation Skills

ARE YOU USING YOUR FACILITATION SKILLS?
Making Everyone Feel Comfortable And Valued
Encouraging Participation
Preventing And Managing Conflict
Listening And Observing
Guiding The Group
Ensuring Quality Decisions

WELCOME, INTRODUCTIONS, EXPECTATIONS

Before diving into the main agenda, take a few moments to welcome participants. If you and key group members make everyone feel welcome, all will participate. Full participation is vital, for each person brings a different perspective that can contribute to the Domain Committee's success. Be personable and have fun; everyone will enjoy participating more if you take this approach.

Welcome Domain Committee Members and Participants

Take immediate charge of the working session and welcome everyone officially. Acknowledge that they are contributing their valuable time to attend this working session and thank them for coming. By doing so, you validate and legitimize their comments and contributions.

Introductions help participants feel welcome and remind them who their team members are. Introductions also give you an opportunity to clarify your role as facilitator for the working session and to explain the role of any outsider. Require everyone to say a few words, even if only, *"My name is ... but I*

want to pass on this." Once people have heard their voices in a group, they feel more inclined to speak up again later.

Consider an icebreaker. You may ask people to share their favorite ice cream flavor, their first pet's name, or anything else light and personal but non-threatening as they introduce themselves.

Give precise instructions - list the information you would like members to give as they introduce themselves, e.g., name, role, and relevant identifying information (e.g., agency they represent). Consider asking them to each limit the introduction to 10 to 20 seconds. This is an opportunity to build a sense of community and collaboration and to break the pattern of name, rank, and serial number.

If your group has the time, consider inviting participants to expand their introductions by briefly talking about their expectations for the working session. This can help Domain Committee members clear their minds and focus on the working session.

Affirm the Roles of the Domain Committee Members

As the facilitator of the Domain Committee kick-off it is important to remind each of the committee members what is expected of them to make the most of the Domain Committee experience, and to suggest ways in which they can help the group. Part of the kick-off should include restating the Roles and Responsibilities of each Domain Committee Member as outlined in the MAEA Manual.

As the facilitator of the Domain Committee kick-off it is important to remind each of the committee members what is expected of them to make the most of the Domain Committee experience.

Each Domain identified will be developed and documented by a Domain Committee made up of subject matter experts who are familiar with the State's IT environment. Domain Committee members are select by the ARC and represent a cross-section of State of Missouri agencies and/or branches of government.

By procedure the ARC should have appointed the Domain Committee Chairperson. There may be instances, however, where the ARC has left this determination to the Committee itself. If this is the case, one of the agenda items during the kick-off should be to elect the Domain Committee Chairperson. Prior to this election, the following should be said regarding the role of the Domain Committee Chairperson:

- **The Domain Committee Chairperson must be able to** lead, guide, push, pull, cajole and encourage the team members to complete their individual assignments and to fulfill the responsibilities of the team.
- **As coordinator of all domain team activities**, it is imperative for the Domain Committee Chairperson to be well organized and to communicate openly and frequently with team members.
- **The Domain Committee Chairperson is responsible for all documentation** generated for review and publication as part of the domain architecture. The Domain Committee Chairperson attends any ARC meetings in which Domain assets are being reviewed to present this documentation and help the ARC with any questions or clarifications.

All Domain Committee members are expected to provide knowledge, experience, and expertise towards development of the Domain's Architecture Blueprint. As Subject Matter Experts, all members are responsible for the development and maintenance of the content of domain architecture documents, including the domain specific deliverables (i.e. technical standards, product standards, standard

configurations, and compliances). Members are expected to keep abreast of the technical trends and standards for their area of expertise.

Affirm Domain Implementation Approach

When a Domain Committee is charged with developing the technical architecture for a group of related technologies, the framework for their research and deliberations is provided by processes and templates found in the MAEA Manual. These templates and processes are intended to provide structure and rigor to the Domain development effort. Facilitating the definition of Domain architectures within the MAEA Framework context provides a straightforward "top-down" approach to planning, selection, construction, review, deployment, and management of Architecture Blueprint assets.

As Facilitator, it is important to understand that one-size does not fit all. Developing domain architectures is a collaborative, iterative, creative process.

As Facilitator, it is important to understand that one-size does not fit all. Developing domain architectures is a collaborative, iterative, creative process. Architecture development is a creative endeavor that requires thoughtful analysis and inspired thinking to respond to the many challenges inherent in an architectural approach to deploying and managing technology to satisfy the business needs of the State and its agencies.

The primary outcome of the Domain Kick-off should be an affirmation of how to organize work with a comprehensive implementation approach. The first task of a newly formed domain team is to review the technologies assigned to the domain by the ARC. If the domain team believes that a technology is more appropriately addressed in another domain, that recommendation must be proposed to the Architecture Office. When the list of technologies is finished, the Domain Committee must assess the Domain Implementation Approach.

The Domain Implementation Approach will help set priorities for the Domain Committee's work. The approach and priorities can be influenced by a number of factors. These include:

- **Severity and urgency of issues** – There may be a specific state-wide need or intent behind the launch of a given Domain dictating that particular Technology Areas are addressed ahead of Domain and Discipline definitions.
- **Level of Architecture Blueprint detail** – Not all Domains will need to, or want to, document to all levels of the Architecture Blueprint. For example, the Domain Committee may decide not to document Product Components to avoid any vendor biases. They may choose, instead, to document explicit selection criteria as Compliance Components at the Technology Area level.
- **Availability of Existing Standards** – In order to gain comfort with the Architecture Documentation Process, the Domain Committee may want to start with some proverbial "low-hanging-fruit." This could entail adapting ITAB approved assets into the appropriate Architecture Blueprint assets.
- **Availability of Information from other Government or Standards Bodies** – Enterprise Architecture is not about re-inventing the wheel. Several Federal, State and Local governments are progressively documenting architecture standards. The Domain Committee should capitalize on these published efforts to help kick-start their own documentation efforts. Using publications from organizations such as the National Institute of Standards and Technology (NIST), IEEE or W3C can also dictate the implementation approach.

The Domain Implementation Approach should also establish a baseline set of requirements regarding how subsequent levels of the Domain Architecture Blueprint will be documented. This approach, along with any other Discipline specific documentation details, should be recorded in the "Discipline Documentation Requirements" section of the Discipline Template.

SET TONE AND PACE

A great deal of the tone of future Domain Committee working sessions will be determined by the set-up and opening of the kick-off working session. It's always important to establish a spirit of collaboration, trust, and respect early in the kick-off working session, and it's absolutely critical when you expect conflict. While conflict can promote the airing of different perspectives and increase the options being considered, conflict that is hurtful or angry can impede the Domain development process. One of the best ways to deal with negative conflict is to prevent it from happening.

It's always important to establish a spirit of collaboration, trust, and respect early in the kick-off meeting.

Reaffirm the charge of the Domain Committee, its purpose, and expected goals and deliverables. Briefly discuss the role of each person as a Domain Committee member. You, as the facilitator, should do most of the talking in this first working session. The kickoff is intended to bring everyone up to speed, not to discuss every item in detail. Every participant needs to see you taking charge of the working session agenda.

Focus on driving home the following points during the kick-off:

- **Listen carefully to others.** Try to understand the concerns, values and experiences that underline each Domain Committee member's views.
- **Maintain an open mind.** You don't score points by rigidly sticking to and constantly repeating your earlier statements. Feel free to explore ideas that you have rejected or not considered in the past.
- **Strive to understand the position of those who disagree with you.** Your own knowledge is not complete until you understand other committee members' points of view and why they feel the way they do.
- **Help keep the discussion on track.** Make sure your remarks are relevant.
- **Speak your mind freely, but don't monopolize the discussion.** Make sure you are giving others a chance to speak.
- **Address you remarks to the group members rather than the facilitator.** Feel free to address your remarks to a particular committee member; especially one who has not been heard from or who you think may have special insight.
- **Communicate your needs to the facilitator.** The facilitator is responsible for guiding the discussion, summarizing key ideas, and soliciting clarification of unclear points, but he/she may need advice on when this is necessary. Chances are you are not alone when you don't understand what someone has said.
- **Value your own experience and opinions.** Don't feel pressured to speak, bur realize that failing to speak means robbing the group of your wisdom.
- **Engage in friendly disagreement.** Differences can invigorate the group, especially when it is relatively even on the surface. Don't hesitate to challenge ideas, and don't take it personally if someone challenges your ideas.

Remind the Domain Committee of Their Charge

Now that you've set the tone, discuss the MAEA, Architecture Review Committee and Architecture Office expectation of the Domain Committee that set the stage for how they will develop their Domain architecture assets.

Refer to the MAEA Manual that they should have reviewed in training and highlight the activities of the Domain Committee process by process. Explain and reinforce to everyone that membership on the committee is a commitment. Explain that the routine Domain Committee working sessions become the foundation for status reports and are used as the primary communication vehicle for managing the Domain effort. As you step through the mission, point out key dependencies or factors you noted in preparing for the working session that affect the completion of documenting the Domain.

Keep your discussion to the point. Reinforce key success factors and explain why they are important.

Establish a Timeline

Determine an appropriate time and day and schedule (day of week, frequency, etc.) for Domain Committee working sessions. Reinforce the need for everyone to attend and to have each working sessions required tasks completed.

Take time to remind the group that teamwork is essential.

Take time to remind the group that teamwork is essential. Reinforce the need for participants to look out for one another. The objective is to complete the Domain successfully, and it is up to everyone to do their part and to help one another.

Empower Domain Committee Members

Empower team members to own their responsibilities and to ask for help. Repeat that you expect everyone to attend Domain Committee working sessions prepared and with all tasks completed, unless you know ahead of time that there are obstacles. Part of your facilitation job is to help the team identify bottlenecks and eliminate obstacles.

If you have agenda items that could cause conflict (e.g., voting of a Domain Committee Chairperson or Scribe), emphasize to Domain Committee members that their success is dependent on working together and agreeing on similar issues.

Plan Team Building and Social Time

Throughout your work with the Domain Committee, you will need to use team-building techniques. Through teambuilding, committee members get to know each other better and develop a group rapport. They also better understand each other's motivations and intentions, and that helps when conflicts arise.

Plan social time, such as coffee breaks, so that participants may talk to each other informally. At a minimum such breaks should occur every 90 minutes and should last no more than 15 minutes.

OPERATIONS, LOGISTICS AND ADMINISTRATION

All Domain Committee working sessions should operate under a set of procedures that ensure fairness and equality. One of the most widely read and used resources for establishing meeting operating procedures is ***Robert's Rules of Order*** or some variation thereof. Robert's Rules focus on voting, but much of the work done in the Domain Committee working sessions is done more so through consensus.

Whether you use Robert's Rules or other operating procedures be sure to include administrative and logistics rules that include:

- Establishing an organized presence
- Creating of a set of ground rules
- Reaching agreement and taking action

Establishing an Organized Presence

As a facilitator it is critical that you demonstrate to the Domain Committee that you are on top of things. The Domain Committees are most effective in completing their mission if the facilitator maintains an organized presence. Establishing an organized presence requires little more than the fundamentals of planning and running effective working sessions, which includes:

As a facilitator it is critical that you demonstrate to the Domain Committee that you are on top of things.

- Setting up a Domain kick-off agenda
- Working session location logistics
- Starting the working session on time
- Keeping the group focused on the topics listed in the agenda

Set Up a Domain Kick-Off Agenda

The working sessions kick-off, or opening session, is a great opportunity to show the Committee members that many different agencies and organizations are involved in the MAEA program, that the State's IT leaders have "bought in" to the idea of Enterprise Architecture, and that taking part in the Domain Committee will give the members a real opportunity to effect change on the IT issues they care about. As in any effective working session, participants are better off when they have a clear understanding of how it will progress.

For the kickoff, the facilitator should plan an event that includes some combination of high-profile speakers (i.e., members of the ARC, the Chief Architect, or the State CIO), and testimonials from people who participated in the pilot Domain working sessions or from members of other Domain Committees.

The Domain Committee opening session will be different from the usual recurring working session agendas as it is designed to call attention to the mission of the specific Domain Committee and encourage participation. An MAEA Domain working session agenda template can be found in **Appendix A**. Using this format, the typical kick-off session agenda should include the following major parts:

- Introductions (30 minutes)
- Guest speakers, testimonials (30 minutes)
- Roles of the facilitator and participants (20-30 minutes)
- Overview of the mission and objectives of the Domain Committee (30 minutes)
- Ground rules (30 minutes)
- Discussion Questions/Study of Domain priorities (30 – 45 minutes)
- Summary (15 minutes)
- Debriefing the session/Action items (15 minutes)

Working Session Location Logistics

Make sure that you have a working session location that can easily be found by the members of the Domain Committee and/or guests; try to use the same location for all of your working sessions. The ideal working session location will be free from potential hurdles such as parking issues, distractions (e.g., open, public facing windows), and noise (such as construction).

Be sure the working session location is large enough to accommodate all Domain Committee members and potential representatives from the ARC, Architecture Office, or guests.

As a facilitator, you should arrive at the working session early in order to prepare the room for the working session. This includes making sure projection facilities are available, white boards or flip charts are available (including markers), and any other working session necessities are in place. You should familiarize yourself with such logistics issues as restroom locations, break locations, and emergency procedures.

Start the Working Session on Time

Waiting too long for the latecomers to start the working session will show that you don't care about those who arrived on time. You are inconsiderately wasting the time of the loyal members, waiting for a few stragglers. This applies to breaks as well – the continuance of a working session should begin immediately after the designated break period is over.

Waiting to long for the latecomers will show that you don't care about those who arrived on time.

Keep the Group Focused On the Topics Listed In the Agenda

Don't let discussions stray away from the goals of the working session. Rather, encourage group "bonding" through organized icebreakers before the session, during an appropriate break, or plan social time after the session. The purpose of the working sessions is Domain Committee business, not socializing. Don't let side conversations prevent or disrupt the business of the group.

Creating a Set of Ground Rules

A simple ground rules exercise for the group, which only takes a few minutes, is to brainstorm a list of behaviors and attitudes that enhance the effectiveness of working sessions. A good framing question to set up the brainstorm is to ask the participants to list the actions that they have observed that in their judgment were helpful to groups they have worked in.

As facilitator, you will need to clarify to the group that actions are observable behaviors and if ideas come up that may not be actions you can ask the question, "How do you know this is happening?" Write down the actions so all the committee members can see them and then have the group choose the ones they want to adopt.

Here are a few sample ground rules for enhancing the effectiveness of working session participants. There are lots of others; a simple search of the Internet using the keywords *Ground Rules* is likely to find many more ideas.

- **Be a good listener** – Ask for clarification about why people think or feel as they do. Never interrupt.
- **Be open to outcome** – Don't come to working sessions with the ***plan*** come with ***ideas***. Let the group expand on the ideas and be open to the change.
- **Be concise** – Think out what you are going to say before you say it and then be brief. Don't ramble and don't repeat what others have said. If you think the same as someone else, then simply say, "I agree."
- **Be patient** – Ask if committee members need more time. Some may need more time to understand or may need more information.
- **Take a dose of humility** – Just because you think you have the answer does not mean it's the best answer for everyone, or that what meets your needs meets the needs of others.
- **Learn when to let go** – Don't get hung up on small details (e.g., wordsmithing), let the decision go forward and then examine it later. Be willing to let the group go ahead so they can learn, even if it means they might make a mistake or two.
- **Give the reasons behind your thinking** – Whenever you state an opinion, you can add valuable information by giving the committee the reasons for your opinion. Be open to questions and comments about your opinions.
- **Do your homework** – Don't wait until the working session to get or give information. Call other committee members, hold small gatherings, etc. Read everything you are given closely and think about it before the session.

Reaching Agreement and Taking Action

It should come as no surprise that without agreement and action, nothing happens. Every one of the Domain Committee members should have a say in what is produced, especially concerning assignments they themselves worked on. It is possible for the group to get bogged down in endless discussions over trivial points, especially when the committee members don't think they're so trivial. It is the role of the facilitator to determine when such a discussion is really warranted, and to cut it off when it's not.

It should come as no surprise that without agreement and action, nothing happens.

The important thing is that people generally feel happy with the actions and stances taken when taken as a group. If there is disagreement, if 60% of the group likes an idea but you don't want to alienate the remaining 40%, remember that you can always encourage people to take action or speak out. You should be constantly encouraging people to participate, give their input, and feel a part of the group.

People generally feel happy with the actions and stances taken when taken as a group.

How do you define when the Domain Committee agrees on something? The idea of consensus is that you talk and refine until pretty much everyone agrees. The downside of this is that a few dissenters can paralyze the group, even when the vast majority endorses something.

For MAEA Domain Committee decisions requiring a vote, such as completed Architecture Blueprint assets being submitted to the Architecture Office, a simple majority vote is all that is necessary. In this model, in order for a vote to be conducted at least 51% of the Domain Committee must be present (1 more than half of the designated members present). Should this level of attendance occur, full consensus of those present is necessary in order to reach agreement and take further action.

Facilitating Domain Working Sessions

When facilitating Domain working sessions, you are responsible for making sure the working session runs smoothly, the agenda is followed, and discussions proceed constructively. As facilitator, you should begin to develop a sense for when the Domain Committee is approaching consensus and be able to determine when Architecture Blueprint assets are concrete enough to be voted on.

The facilitator has the responsibility to make sure the group dynamics are good. The facilitator must balance the conversation so that some people are not dominating the conversation, making it difficult for others to provide input. The facilitator must also make sure that everyone gets a chance to speak and that everyone listens to each other. Remember, are you using your facilitation skills?

Checklist for Facilitation Skills

ARE YOU USING YOUR FACILITATION SKILLS?
Making Everyone Feel Comfortable And Valued
Encouraging Participation
Preventing And Managing Conflict
Listening And Observing
Guiding The Group
Ensuring Quality Decisions

DEVELOPING THE AGENDA

The agenda is the template for Domain working sessions. It should be developed thoughtfully so that the Domain Committee spends the bulk of the session time addressing deliverables, issues and matters that require decisions and less on time for "housekeeping" or routine subjects.

By treating agenda development seriously, you will be rewarded with more orderly and productive meetings.

The best approach for agenda development involves collaboration from the Facilitator, the Domain Chairperson, the Architecture Office, the scribe, and the Domain Committee members. The agenda should delineate plainly what topics will be addressed, how much time they will get, etc. By treating agenda development seriously, you will be rewarded with more orderly and productive working sessions.

Setting Agenda Priorities

As is evidenced by the order of launch of the individual Domain Committees, the priorities for developing the MAEA program and its assets is based on the information needs of a wide variety of stakeholders including the ARC, the Architecture Office, Legislative issues, Homeland Security, etc. Such priorities

trickle down to the actual order of issues the Domain Committee is to address through the appropriate development of Architecture Blueprint assets.

It is important to recognize that if the Domain Committee is to stand a chance of success, the desires of the individual committee members must also be taken into account. For an active group, it is probably best to mix issues with obligation, interest and opportunity where the group can learn a lot about networking with other people, researching issues, and have a chance of success.

There are essentially three categories of activity that influence Domain direction and session-to-session agenda development:

- **Agendas items based on obligation -** There is an obligation to address needs and issues identified by the ARC or ITAB. Tackling issues based on obligation is an essential part of the service component of the Domain Committee and its mission.
- **Agenda items based on interest** – Domain development is a long-term focus and pursuing issues in particular areas of interest to the Domain Committee members enables a greater sense of motivation.
- **Agenda items based on opportunity** - Sometimes agenda items will be based on the opportunity they provide to support a particular project, address a particular political issue, current technology trends or collaborative efforts between Domains.

Developing agendas that recognize multiple motivations helps to further the service provided by the Domain Committee. Setting agendas that include more balance can increase the value generated by Domain efforts and promote greater growth for individual committee members and the MAEA as a whole.

Developing agendas that recognize multiple motivations helps to further the service provided by the Domain Committee.

The Working Session Agenda

At a minimum, the Domain working session agenda should include a review of correspondence from past minutes, reports from the Architecture Review Committee or Architecture Office or Domain Committee Chair, old business and new business. As a facilitator, you will need to check-in with the Architecture Office and committee chairpersons before placing time for their report on the agenda. A working session that has many "no reports" or poorly prepared reports will weaken the effectiveness of the working session.

A sample agenda template has been included in **Appendix A**; this agenda can be modified depending on the specific needs of the Domain Committee or the topics being covered in the working session. At a minimum, however, the typical working session agenda should typically cover the following topics:

1. Call to order by the Committee Chair (or Facilitator)
2. Review of the minutes from the last working session
3. Domain Chairperson's report
4. Reports from the ARC and/or Architecture Office
5. Old Business
6. New Business
7. Action Items
8. Close of the working session

The agenda should be distributed at least 48 hours in advance of the working session. Each Domain Committee member will be responsible to bring a copy of the Agenda to the working session. As a facilitator, it is good practice to bring additional copies in the event that guests attending the working session will need one.

The agenda will help the Domain Committee members follow the flow of the working session, will serve as a reminder of the topics covered during the session, and most importantly, will help keep the session focused on relevant issues.

GUIDING THE DOMAIN COMMITTEE THROUGH THE AGENDA

Often Domain Committee agendas are packed with discussion on multiple levels of the Architecture Blueprint (Technology Areas, Compliance Components, Products, etc.). To ensure the committee meets it objectives, you must focus attention and energy on the objectives for that working session. It helps to start each working session with a review of the objectives for each agenda item.

To ensure the committee meets it objectives, you must focus attention and energy on the objectives for that meeting.

Make Sure the Domain Committee and the Agenda Are In Synch

A Domain Committee makes quality decisions only after all committee members have had an opportunity to contribute relevant expertise, experience, and the majority have come to support the best possible solutions. Rushing can lead to ill-considered decisions and the loss of members' support. If you are running out of time faster than you are running out of agenda items, stop and choose one of the following options:

- Determine if you have enough time to complete the agenda and closing tasks
- Extend the working session
- Help the group set priorities and decide which remaining agenda items to address in the time remaining.

The following lists some tools to assist in guiding the Domain Committee through the agenda and keeping them focused on the activities at hand.

- **Delegate a timekeeper.** Set a time limit for discussion on each topic and ask someone to help you stay on schedule. "Since we still have four other agenda items to discuss today, let's give ourselves about 15 minutes to conclude discussion on this item. Judy, can you let us know when 15 minutes is up?"
- **Refer back to the working session objectives and agenda.** When the group strays, remind members of their decision to accomplish specific objectives in an agreed upon period. "Though this topic is not one of our objectives for today, there seems to be a great deal of interest in this discussion. Should we re-assess today's agenda or post-pone this discussion until the next working session?"
- **Allot extra time if needed.** Don't cut short a valuable discussion or let a conflict fester because the allocated time is up. Ask the group to approve the departure from the schedule. "We originally planned to discuss the 'Fit Matrices' until 2:00. It seems that they may take a few minutes longer. Is everyone okay with delaying Product Component discussions until we finish talking about the matrices?"

- **Postpone non-agenda topics.** Use a 'parking lot' as a tool for staying on topic, not as a way to ignore comments on other topics. "Pete that is definitely an issue we will need to discuss. Would it be okay to place it in the parking lot now so that we can focus on the fit matrices?"
- **Speed the group up.** At times, members may prolong a discussion because of their interest rather than new ideas. To push the group to wrap it up and come to a decision, summarize the main points. Then you may say, "Did I accurately summarize the issues regarding this Technology Area? To keep on schedule, should we make a decision?"
- **Slow the group down.** At times, members may be tired or uncomfortable and rush through a decision to to meet an ARC deadline. Say something like, "I know that we are almost to the end of the working session, but it seemed we rushed through that last product discussion. This is a fairly important decision. Let's make sure we've identified all the potential aspects."

BRAINSTORMING AND CONCEPT DEVELOPMENT

The goal of brainstorming and concept development is to build a plan for success by integrating the needs of the Missouri statewide enterprise for IT information with the experience of each Domain Committee member. As Domain Committees tackle the issues they will begin by researching them and applying their experience to develop a set of quality concepts that through collaboration with the committee will guide the production of Architecture Blueprint assets.

The goal of brainstorming and concept development is to build a plan for success by integrating the needs of the Missouri statewide enterprise for IT information with the experience of each Domain Committee member.

Brainstorming

Brainstorming is the standard, democratic technique, for figuring out what the current and alternative approaches and technologies are for a given piece of the Architecture Blueprint. As new Technology Areas, Products and/or Compliance Components are introduced during a working session, the first thing the committee will do is brainstorm. This simply means tossing ideas into the air and recording these ideas, without much discussion or scrutiny.

Brainstorming allows the Domain Committee to suggest ideas in an atmosphere of openness, without the fear of being put down. Sometimes it is good to have some order in the process to avoid a collision of voices and so that each member can speak and be heard. The best method for this is to simply go around the room allowing each person to name a couple of new ideas – ideas should be brief with enough explanation to get the point across. Meanwhile, the scribe should record the ideas for the subsequent detailed discussion and verification of ideas.

Concept Verification

Concept verification begins the detailed discussions and evaluation of the quality of those generated ideas for a given Architecture Blueprint topic. This should be an active discussion in which the Domain Committee determines what the best ideas are and begin to shape the outline of what will be included in the planned Architecture Blueprint documentation.

Concept Documentation

The Domain Committee will use the templates provided in the MAEA Manual to document the Architecture Blueprint assets. When drafting these assets, having the entire Domain Committee work the specific wording during a working session can be a nightmare.

Once all of the key ideas and general direction for a blueprint item have been set, it's good to assign an individual committee member or two to come up with the initial draft that the group can discuss. This development, or "homework", should be done between working sessions and distributed to the whole group at least 48 hours prior the next working session to begin the process of revision and consensus.

Domain Committee Research and Technology Scans

The main activity of the Domain Committees, prior to documenting Architecture Blueprint assets, is conducting research. The predominant research activities are in the form of Technology Scans as outlined in Part II of the MAEA Manual. Technology Scan research topics center around individual Technology Areas and involve investigating product standards and technical standards specific to a particular topic.

The main activity of the Domain Committees, prior to documenting Architecture Blueprint assets, is conducting research.

Research and Technology Scans should be undertaken by all Domain Committee members. Research on specific topics may also be assigned or delegated by the Domain Committee Chair. Technology Scans are triggered by three major events:

1. **Launch of a new Technology Area.** The initial step to begin initial documentation of a Technology Area is conduct a scan of the enterprise to determine any existing or proposed Products and Compliance Components used throughout the state that relate to this technology. Technology Scans can also includes external scans of other government entities and the technology industry for information related to this Technology Area.
2. **During Compliance Reviews.** As more and more agencies interact with the Architecture Blueprint, there may be occasions when help may be sought from the Domain Committee to address an identified gap in the architecture. Reviews of existing architecture product components and new technology scans can be conducted to aid in finding a technology solution.
3. **During the Vitality Process.** Technology Scans should be included as part of the Vitality Process by taking a sweep through the major sources of information to verify the original factors that lead to the creation of the domain architecture assets.

A variety of sources are available to the Domain Committee members to assist with research. Team members, in all likelihood, have specific publication web sites that they visit on a regular basis. Most manufactures and most publishers of software have product web sites, as do standards bodies. In addition, there are usually sub-committees of ITAB, user groups or other statewide committees that can assist.

FACILITATING THE DOCUMENTATION PROCESS

Probably the most effort-filled architecture lifecycle activity that each Domain Committee faces is the Documentation Process. Documentation of MAEA Architecture Blueprint assets will be the majority focus of the Domain Committee for the first few years of working sessions. As a facilitator of these sessions it is critical that you understand the MAEA documentation process. This will help you to effectively guide the Domain Committee in working collaboratively to plan, research, write, edit, revise, review, evaluate and produce Architecture Blueprint documentation.

How to Get Documentation Started

During the Domain Committee Kick-off working session both ground rules and a Domain Implementation Approach should have been agreed upon by the Domain Committee. With these rules and approach in hand, the first task of a newly formed Domain Committee is to review the technologies assigned to the domain by the ARC, as well as any preliminary definitions and boundary topics for the Domain.

The Domain Committee should then begin to organize and categorize a working list of discipline technologies to establish a baseline understanding of the technologies, and to facilitate prioritization and delegation of work. Missing topics and technologies should be revealed during this brainstorming activity.

Open and active communication with the Architecture Office and ARC will be essential for approval of architecture assets and development priorities, coordination and resolution of cross-domain issues, and managing the expectations of all MAEA stakeholders.

Generally speaking, this activity should produce a "master-list" of Discipline technologies as well as some categorical hierarchy that can then be applied to form the Domain→Discipline→Technology Area structure that will be addressed by the Domain Committee. This information will also help set priorities for the Domain Committee's work.

Unless the Domain Committee is being driven by an urgent enterprise-wide issue, the first set of Domain deliverables should include the following assets:

- **Domain Definition** – Completed Domain template that clearly demonstrates the Domain Committee understands the Domain boundary and relationship with other Domains.
- **Discipline Definitions** – Completed Discipline templates that clearly illustrate the categorization of Domain related technologies so that requisite Technology Area standards and products may be defined.
- **List of Technology Areas and Priorities**. As part of the Communication Process, the Domain Committee should submit its list of Technology Area priorities in order that MAEA stakeholders (Architecture Office and ARC) are aware of upcoming documentation and to serve as a feedback mechanism to ensure that the needs of the stakeholders are being addressed in a timely fashion.

From here, the Documentation Process continues as the Domain Committee must work to define the appropriate content to populate the Compliance and Product Component templates for each of the Discipline Technology Areas. As this will vary significantly from Domain to Domain, there is no single prescribed method that can be used for all technologies. For some technologies the content may be governed by methods and tools selected for implementing or managing those technologies.

Confirm Priorities with the Architecture Office and ARC

Open and active communication with the Architecture Office and ARC will be essential for approval of architecture assets, development priorities, coordination and resolution of cross-domain issues, and managing the expectations of all MAEA stakeholders. A number of technologies and technical standards impact multiple domains and will require cross-functional domain activities that will be prioritized and established by the ARC through the Architecture Office.

One of the first Domain Committee deliverables, mentioned above, is a list of Technology Areas and priorities. The Domain Committee should seek the guidance and approval of the ARC for each of the identified priorities. There may be statewide issues of which the Domain is unaware that could cause a shift in priorities.

Annual agency planning activities can also cause shifts in priorities, which in turn will trigger a comprehensive review of all the domain architectures. New business drivers and business information requirements will impact the MAEA Principles, Best Practices and Trends. Changes in industry best practices for information technology can also impact the MAEA architecture documentation priorities. The ARC and Architecture Office must be aware of existing Domain activities and priorities to determine the impacts.

Producing Architecture Blueprint Documents

Having the entire Domain Committee simultaneously working on the documentation of a specific Architecture Blueprint asset can be time defeating. It's better that just a few Domain Committee members work up an initial draft that the group can discuss as a starting point for the documentation process.

> As a facilitator it is your responsibility to ensure that Domain Committee working session time is focused on the content of the Architecture Blueprint documentation…

As a facilitator, it is your responsibility to ensure that Domain Committee working session time is focused on the **content** of the Architecture Blueprint documentation – making sure that critical ideas are captured and that major sections are not missing or poorly constructed. All too often working sessions can become sessions in "wordsmithing", where members critique the language, sentence structure or particular words used in communicating the content.

To ensure working sessions are focused on the content of each document, document ownership must be clearly assigned. The Domain Committee should collectively identify a document owner (single point of contact) for a particular draft document or set of documents (such as a group of related Compliance Components). It is the responsibility of this "Documenter" to:

- **Collect all related working drafts** – As "homework" is assigned and due dates given, the designated Documenter should collect these drafts on the date due (a date in advance of the next working session). As multiple Domain Committee members could be working on the same document, it is critical that a central point-of-contact is established for collection.
- **Consolidate working draft content** – In the event that multiple committee members were working on the same Architecture Blueprint asset, the Documenter must consolidate these individual drafts into a single deliverable that can be presented to the committee at large.
- **Distribute working drafts for comment** – Once collected and consolidated, the Documenter should work with the Facilitator and/or Scribe to distribute the working draft to the entire Domain Committee at least two full days prior to the working session in which these items will be reviewed.

To further facilitate the documentation process, each Domain Committee member is responsible for reviewing the working drafts prior to the next working session. Group members should submit electronic or hand-written comments to the Documenter for revision of the document. These comments should include any wording or semantics that could help clarify the content.

During the designated working sessions, the Committee at large once again reviews the draft documentation for content. This process could go back and forth between the committee and the designated Documenter until all members of the committee generally agree upon the content of the document. While any documentation is going through this iterative cycle, its status should remain as "In Development."

SCRIBING AND NOTE TAKING

Delegation of responsibility for working session minutes and draft documents to a Domain Committee "Scribe" is not only appropriate, but it is encouraged. The Scribes role may be appointed, elected, or handled on a rotating basis based on time, topic or workload; however the Facilitator **should never** carry the dual role of scribe and facilitator. No matter who the scribe may be, it is strongly encouraged that everyone on the Domain Committee take some notes. Otherwise, members must depend on their memory as to what was said and agreed upon.

> The Facilitator should never carry the dual role of scribe and facilitator…the Scribe's primary role is to create a record of the deliberations of the Domain working sessions.

Recording Parking Lot Issues, Action Items and Decisions

The Scribe's primary role is to create a record of the deliberations of the Domain working sessions. This serves many purposes: it helps to committee members stay on track and move the discussion along; it provides a means of capturing the wisdom and common themes that are identified during discussions; and most importantly, these notes serve as the basis for the development of the working session minutes. A template for Working Session Minutes has been provided in Appendix B.

Recording the working sessions issues, action items and decisions can be accomplished in many ways. Recording issues can be done on a tablet, a PC, a whiteboard or flip chart. Whatever the means, there are a few key points to keep in mind.

- **Notes need not be a detailed account of everything.** These notes do not have to be word-for-word but should include all key ideas, issues, and action items.
- **Notes should truly reflect the discussion.** Try to use the words the speaker used, rather than paraphrasing. Always check back with the speaker/group to see if the notes capture the essence of their thoughts.
- **Write down something for each person who speaks.** Make sure the notes are inclusive of all who participated in the discussion.
- **Do not let recording detract from the discussion.** People should be talking to each other, not the flip chart!

Preparing Assets for Review

Once the Domain Committee is satisfied with the content of a particular Architecture Blueprint asset, it should be called to a vote by the committee for inclusion in the next "package" to the Architecture Office for ARC review. Typically, a simple majority vote is sufficient for approval to include the artifact in the next Architecture Periodic Review Packet that is submitted to the ARC.

As a facilitator, you should be aware of those items that have been voted on in order that the Domain Committee Chair can decide when sufficient assets have been completed for submission to the Architecture Office. Though there are no set specifics for what should be included in the Architecture Periodic Review Packet and when it should be delivered, the following is a list of simple guidelines:

- At a minimum, the packet should include a completed set of assets related to a Technology Area including the Technology Area definition.
- Any assets reviewed as part of the Vitality Process should be included in the next scheduled Architecture Periodic Review Packet.
- The Domain Committee should strive towards a monthly delivery of assets for review.

Once the Architecture Periodic Review Packet contents have been agreed upon, all documented assets included should have their status updated to "Under Review" and then delivered to the Chief Architect (*OITArchitect@mail.oit.state.mo.us)*.

BEHIND THE SCENES ACTIVITIES

The facilitator's role does not begin and end with the start and conclusion of each Domain Committee working session. In fact, many responsibilities exist outside of the working sessions. In addition to the preparation activities discussed earlier (e.g., agenda development), there are other areas of support that fall to the facilitator.

> The most important factor in the success of using a parking lot concept is the commitment of the facilitator to ensure issues are not lost.

Review Parking Lot Issues

There will always be some issues that arise during a working session that cannot be resolved before the end of the session. This is usually because consensus could not be reached or because more research was needed outside of the working session. These issues are moved to a parking lot – a place to 'park' issues for later follow-up.

The most important factor in the success of using a parking lot concept is the commitment of the facilitator to ensure these issues are not lost. The facilitator should routinely examine the parking lot issues to determine if any offline follow up is needed, determine who will address these issues offline and adjust future agendas to include necessary parking lot issues.

Action Items – Assignments and Resolutions

Much like parking lot issues, inevitably during a working session, some tasks or follow-up assignments will result. It is the responsibility of the facilitator to ensure that someone is assigned to complete each

task. In addition to the task assignment, the facilitator should note the importance of the action item or context in which it came up. A simple action item planning sheet could look like the following example:

Sample Action Item Planning Work Sheet

ACTION ITEM	*ACTION ITEM IMPORTANCE/CONTEXT*	*DATE ITEM RAISED*	*RESPONSIBILITY*	*DUE DATE*
Confirm location for next Domain Working Session	Need to determine invitation specifics	June 21	John Doe	June 21
Collect agency data on ant-virus software in use on desktops	Use for input and sampling for Virus Detection Product Components	July 19	Jane Doe	July 19

Provide Behind the Scenes Support via Email

Email is a good response mechanism for addressing both parking lot issues and action items – to prod Domain Committee members into completing their assignments and homework without embarrassing them during a working session. If Domain Committee members start saying interesting content-related comments via email, carefully capture their comments so that their ideas can be shared with the rest of the group. Be careful to remain unobtrusive and share these comments anonymously if desired.

Email is a good way to gather feedback about whether the working sessions are meeting the Domain Committee's expectations…

An email should be sent to the entire Domain Committee at least 48 hours prior to the next working session to direct participants to the location of working session, minutes, assignments, and agenda items (these could also be attachments to the email itself). These are handy reminders for people who might otherwise "forget" the what, where, when and why of an upcoming session.

Email is also a good way to gather feedback about whether the working sessions are meeting the Domain Committee's expectations, so that adjustments can be made if necessary.

Work Session Wrap-Up Activities

At the conclusion of each Domain Committee working session, you can help the group tie everything together and outline the next steps, assignments and deadlines. Your primary tasks as a facilitator are to *Identify the Next Steps* and *Adjourn on a Positive Note.*

Now is not a time to forget your facilitation skills. If Domain Committee members leave the working session feeling they've had their say and the group has accomplished its goals, you have laid the foundation for success at your next working session.

Checklist for Facilitation Skills

ARE YOU USING YOUR FACILITATION SKILLS?
Making Everyone Feel Comfortable And Valued
Encouraging Participation
Preventing And Managing Conflict
Listening And Observing
Guiding The Group
Ensuring Quality Decisions

IDENTIFY NEXT STEPS

Looking at the next steps instills a sense of momentum. There's some skill involved in getting assignments and deadlines across to people, especially in groups, like the MAEA Domain Committees, that have a lot of things are going on. Sometimes you might find in the whirlwind of discussion that has occurred in the working session, nobody realizes what needs to be accomplished for the next working session or maybe even where and when the next working session is to occur.

At the conclusion of each Domain Committee meeting, you can help the group tie everything together and outline the next steps, assignments and deadlines.

Review Action Items and Plans

With the assistance of the working session scribe, keep a running list of action items on a flip chart, white board or in a spreadsheet and add to it whenever the group identifies a "next step" or "to do". At the end of the working session, review the items in the list and develop action items that specify what needs to be done, who will take each action, and when each action is to be completed.

Visit Your Parking Lot

During the wrap-up is your last chance to review any topics you put in the parking lot. If time doesn't allow the Domain Committee to discuss all of these items, propose adding some topics to the next working session's agenda or assigning items to committee members to report upon in the next working session.

Update the Domain Committee Calendar

Remind each Domain Committee member to jot down any action items or issues assigned to them and their due dates. Announce any upcoming Domain Committee working sessions and logistics changes including:

- Where and when the next working session will take place
- What the tentative goals and agenda items will be
- Who will be facilitating, scribing and documenting the working session
- Who may need to be invited outside of Domain Committee members
- Updates to any contact information for the group.

ADJOURN ON A POSITIVE NOTE

Before adjourning the Domain Committee working session, take a few minutes to accentuate the positive.

Before adjourning the Domain Committee meeting, take a few minutes to accent the positive.

- First and foremost, thank all of the committee members for their perseverance and hard work.
- Recall agreements – remind the group of decisions that received strong support.
- Practice being proactive – discuss what worked well and what could be done differently to foster success.
- Lastly, make it official – Close the working session with a signal. This could be as formal as banging a gavel or as simple as turning off the projector – anything to indicate closure.

Core Facilitation Skills and Tools

The Missouri Adaptive Enterprise Architecture is an interrelated set of Domain Architectures that together form the State of Missouri's Enterprise Architecture Blueprint. Each MAEA Domain Committee must develop a comprehensive set of Architecture Blueprint assets that support the State's business strategies and information requirements. These activities include the documentation, review, communication, compliance and vitality of statewide information technologies.

When a Domain Committee is charged with developing the technical architecture for a group of related technologies, succeeding in these tasks requires numerous facilitation skills. This section identifies the core facilitation skills and tools a facilitator will use most throughout Domain Committee working sessions.

One way to approach these core facilitation skills is to think of them in terms of people, processes and product.

One way to approach building your core facilitation skills is to think of them in terms of people, processes and product.

- **People:** How do the Domain Committee members feel about their involvement? How do they relate to one another? In a well-facilitated working session, members must trust and respect and trust each other. All should feel their expertise and opinions are valued.
- **Process:** How are decisions made? How are working sessions run? In a well-facilitated working session, members understand how the group decides or how the facilitator runs the working sessions. The decision-making methods encourage members to participate, yet respect the limited time members have together. Part II of the MAEA Manual details the Domain Documentation Process that addresses many of the decision points that impact the Domain Committee.
- **Product:** What are the key deliverables or results from the working session? In a well-facilitated working session, members produce quality products in a timely manner. The products and deliverables for which MAEA Domain Committees are responsible include those assets that form the MAEA Architecture Blueprint which are produced using the templates found in Part II of the MAEA Manual.

The table on the following page, *"The 3 Ps of Facilitation",* places the core facilitation skills within this framework. Certain skills, of course, may be used in more than one area. The sections that follow will further define the core facilitation skills and tools.

Making Everyone Feel Comfortable and Valued

Most people will not participate fully in a working session unless they feel comfortable with other members and believe their opinions will be heard. The facilitator, with the Domain Committee's support, must create an environment in which members value the potential contributions of those with various perspectives.

The 3 Ps of Facilitation Skills

3 PS	SKILLS	TOOLS
People	Make Everyone Feel Comfortable and Valued	• Use Body Language • Thank Participants
	Encourage Participation	• Encourage Silent Members • Use Open-Ended Questions • Consult The Committee • Use Visual Aides
	Prevent and Manage Conflict	• Set Ground Rules • Search For Agreement • Use Conflict To Improve Decisions • Agree To Disagree
Process	Listen and Observe	• Listen Actively • Scan The Room
	Guide the Group	• Refer Back To Objective And Agenda • Stray From The Agenda If Necessary • Use A Parking Lot
Product	Ensure Quality Decisions	• Remind The Group Of Deadlines • Poll Group Before Major Decisions • Review The Decision
	Ensure Outcome-Based Working Sessions	• Review Objectives And Agenda Items • Record Decisions • Develop Action Plans

Use Body Language

Body language is probably the most powerful part of communication. A person's words may be saying one thing, but tone of voice, posture, and eye contact, may be saying another. You send messages with your movements as well as your voice, so be aware of what your body language is saying.

Know what your "listening face" looks like. Get feedback from committee members. There are no hard and fast rules regarding what you should and should not do in every situation, but you have to be aware of any contradiction between the verbal and non-verbal language you convey. By using body language to show warmth and acceptance, you encourage others to relax and respond in kind. Be genuine!

Body language is probably the most powerful part of communication… you send messages with your movements as well as your voice, so be aware of what your body language is saying – be genuine!

Thank participants

This sounds minor, but by merely thanking the Domain Committee members and any attendees during each working session, you legitimize their comments, contributions and continued commitment to the MAEA.

ENCOURAGING PARTICIPATION

Some Domain Committee members will be outspoken and energetic. Others will be quiet and reserved. As a facilitator, you should balance these extremes so that everyone has an equal opportunity to participate.

Encourage Silent Members

Some people are taught not to interrupt. These people often need to be "invited" to speak and given that opportunity free from others speaking. If members are silent or disengaged, catch their eye or ask them (even at the individual level) to share their expertise.

You want to be the one doing the least amount of talking – you want the Domain Committee members to do the talking.

Use Open-Ended Questions

Ask questions that committee members cannot answer with a *yes* or *no*. You want to be the one doing the least amount of talking – you want the Domain Committee members to do the talking.

Questions beginning with *when*, *what*, or *how* usually encourage members to provide detailed answers, which can spark additional ideas from other members. The following table illustrates the differences between closed questions and open questions.

The Difference between Closed and Open Questions

CLOSED QUESTIONS	*OPEN QUESTIONS*
Encourage One Word Answers	Encourage Discussion
Questions Start With:	Questions Start With:
Do (E.G., "Don't You Like This Model?"	Who…
Is…	What…
Can…	Where…
Would…	When…
Could…	Why….
Should…	How…
Will…	

Closed questions discourage discussion and are often based on assumptions (e.g., "Did you have a previous problem with this vendor?" assumes something about their reason for selecting a particular product). Asking questions that don't imply or assume an answer allows the group to open up. You may have to learn some "mental gymnastics" to rephrase your questions.

There are times, however, when closed questions can be useful. They can be used to begin a conversation with someone who is reluctant to talk, given enough information on which to base further questions. They can also be used to change the topic, or to re-focus a conversation on the topic at hand when it has strayed.

Consult the Committee

When a Domain Committee member addresses a question to you, prompt participation from other members by consulting the group at large. This is also an effective technique for shifting the focus of discussion from one member to the whole group. Remember, you're the one looking for information, so don't lecture. When someone in the group provides an answer, keep on topic to get more answers in the topic area.

Use Visual Aids

Most people process information better if they can see it, so use a white board, flip chart, an overhead projector, handouts, etc. Writing the working session objectives on a flip chart that everyone can see can help keep the working session focused. If a Domain Committee member has done some extensive work or research on a particular topic of discussion, it will benefit the group as a whole if he/she provides hard copies of any documentation during the discussion.

CONFLICT PREVENTION AND MANAGEMENT

One of the best ways to deal with conflict is to prevent it, but some conflict is inevitable and can on occasion even be helpful to the Domain working session process. Use conflict to develop options the group would not have considered otherwise.

Set Ground Rules

Ground rules help a group by defining the actions that help the group work together, and ideally form a commitment by the group participants to working together as effectively as possible. Ground rules are guidelines to encourage the use of effective processes and behaviors.

Ground rules help a group by defining the actions which help the group work together, and ideally form a commitment by the group participants to working together as effectively as possible.

Domain Committee members' agreement on ground rules makes your job easier when conflict arises. Basic ground rules may include items such as: that the group will hear all views and no one will make personal attacks.

Search for Agreement

Drawing attention to points that Domain Committee members agree upon helps create an atmosphere of positive collaboration and forward momentum. If at any point during the working session the group reaches agreement on one or more topics, move to full closure by asking the group if they are ready to make a decision and indicate preferences among the top suggestions.

Use Conflict to Improve Decisions

Conflict can be used to clarify individual points of view and to underscore how strongly people feel. Disputes don't have to mean disrupted working sessions. Many people can think of only two ways to manage conflict – fighting or avoiding the problem.

Take a step back. Get the facts straight, brainstorm all ideas that might help resolve the argument, and discuss the pros, cons, and consequences. That way, you will use conflict to improve the situation and to learn from past mistakes.

Agree To Disagree

No decision is ever going to be without its down side; eventually decisions need to be made. Make certain that you always end discussions with an agreed upon outcome. In a conflict situation you must guide the committee away from blaming or being judgmental and help the members to agree to disagree. Urge members to treat each other with respect even when they disagree.

LISTEN AND OBSERVE

Throughout a working session keep your eyes and ears open and stay attuned to the group. Pay attention not only to the group as a whole but also to individuals. Some people are splendid listeners. They can recite verbatim, they can hear and memorize, but they don't have any sort of heart for what the person ***meant*** as opposed to what they ***said***.

> Letting a Domain Committee member know you hear them can be an incredibly powerful act.

Listen Actively

Apply the basic skills of one-on-one conversation. If you've ever taken a course in interpersonal relations, active listening sounds a lot like, *"So what I'm hearing you say is…"* This is a very valuable skill because letting a committee member know you hear them is an incredibly powerful act.

The following list provides 10 simple steps to improve active listening skills:

1. Stop Talking
2. Focus on the speaker
3. Keep an open mind
4. Summarize out loud when appropriate
5. Observe both content and body language
6. Do not offer advice (especially silently)
7. Do not argue mentally
8. Avoid judgments
9. Ask open questions
10. Do not be defensive

Scan the Room

While maintaining eye contact with the speaker, note how other members are responding to that person's message. The importance of body language was mentioned earlier, we instinctively rely on the information we gain from body language. While scanning the room, pick up on the body language of the other participants.

Some of the most common body language indicators involve eye contact, facial gestures, torso and arm behavior, and leg activity. You have it in you to recognize some of the most common body language signs:

- Positive Behaviors
  - *Direct eye contact* – Interested, likes speaker or subject

- *Open posture, leaning forward* – Very interested in what you are saying
- *Fingers interlocked behind the head, elbows open* – very open to ideas
- *Smiling* – is comfortable, positive attitude
- Negative Behaviors
- *Limited or no eye contact* – Lying, uninterested, uncomfortable, distracted
- *Closed off posture, rigid, crossed arms* – Lacking interest, anxious, uptight
- *Bouncing legs, tapping feet or fingers* – agitated, anxious or bored

GUIDING THE GROUP

At any point during a Domain Committee working session you may need to guide the group to move along or stick to the topic. In each group, you must be clear about the task that is to be accomplished. Each working session is part of the high-level task of completing the Domain Architecture Blueprint. It is important to have a good understanding of the session goals prior to the working session.

> Your task as a facilitator is to be aware of the meeting objectives and issues…you have to be on the same track as the Domain Committee members.

Refer Back To Working Session Agenda and Objectives

When the group strays, remind members of their decision to accomplish specific objectives in an agreed upon period. Your task as a facilitator is to be aware of the working session objectives and issues. As a facilitator you need to ask if you are not clear. You have to be on the same track as the Domain Committee members.

Stray From the Agenda When Necessary

Recognize that an agenda is a tool to reach an end, not an end unto itself. If your working session is having a particularly useful discussion, consider straying from your agenda, but ask the group's permission before doing so.

Use a Parking Lot

If members bring up important topics or questions unrelated to the current discussion, put these in the "parking lot," which may be on a flip chart or a spreadsheet on an overhead. Don't end the working session without discussing or otherwise generating action items related to or disposing of these topics.

ENSURE QUALITY DECISIONS

Quality decisions are based on agreed-upon criteria backed by sound information that decision makers consider thoroughly. They use an agreed-upon process that all understand and, at a minimum, they agree to accept the outcomes.

Remind the Domain Committee of Decision Deadlines

Provide a calendar that details the key dates when Domain Committee members must make decisions (e.g., the date the Domain and Discipline definitions are due).

Poll the Domain Committee before Major Decisions

Avoid surprises. The committee should know before making a big decision that different perspectives exist. Poll the group before the official decision – making certain to clarify the various points of view and to work toward compromise.

OUTCOME-BASED WORKING SESSIONS

Every Domain encompasses many related topics and technologies, and committee members sometimes try to discuss all of these at once. As the facilitator, you bear primary — but not sole — responsibility for focusing discussions on accomplishing the objectives of the working session and of the planning process.

Review Objectives for Each Agenda Item

Keep Domain Committee members focused on the task at hand by providing objectives for each presentation, discussion, or other activity on your agenda. Remind members of the objectives as you take up each item.

As the facilitator, you bear primary — but not sole — responsibility for focusing discussions on accomplishing the objectives of the meeting and of the planning process.

Record Decisions

Your group must record activities and decisions. While taking minutes is not the facilitator's responsibility, you can assist by writing key decisions on flipcharts, a chalkboard, computer presentation, etc. that all committee members can see.

Develop an Action Plan

For each decision, write down when action steps need to occur and who is responsible for these. This can be done by reviewing any recorded decisions or common themes from throughout the Domain Committee working session. The action plan should include actions to be taken by individuals and/or the Domain Committee at large. As facilitator you should work with the Chairperson to help members prioritize and plan for action.

Facilitation Creativity and Productivity Techniques

Probably the hardest thing about facilitating any working session is keeping the group motivated and creative. Any Domain Committee can become more creative and more productive if you have the skills to facilitate that evolution. The topics in this section can help, as long as you realize you must build your own style. Try out several things you find here, and then let your experiences help develop your own style of facilitation.

General Guidelines

Facilitators provide continuity. They act as the glue for binding together the assets of a group into an organic process that is meaningful for the participants. In some sense, a good facilitator is the narrator of the working session, a human face and voice that gives form to the MAEA Domain development processes.

Friendliness, openness and good communication skills are by far the most essential facilitation attributes.

Friendliness, openness and good communication skills are by far the most essential attributes. Facilitators need to be sensitive to the input and reactions of each participant while keeping an eye on the bigger picture, namely the group dynamic and the overall direction of the group.

Assess the Committee's Concentration and Engagement

When assessing the Committees concentration and engagement, monitor the group as a whole and the individual committee members.

- **Read the group's energy level** – Assess the tone in members' voices as they speak. Are they energized? What is the group's body language telling you?
- **Check involvement** – How involved is the group? What are people asking? How are people responding to you as a facilitator or to each other?
- **Give them a break** – If you sense the committee is losing energy or the ability to concentrate, take a quick break. Use energizers or games that last no more than five minutes. *"How many three- to six-letter words can you make out of the work 'architecture' in the next two minutes?"*

Clarify Confusing Discussions

As a discussion twists and turns, it's easy to lose a couple of the committee members. You can do several things to make sure that all stay with you and participate fully.

- **Listen for unfamiliar terms** – In the jargon filled IT world over time terms and acronyms can often hold different meanings to the various Domain Committee members. When someone uses acronyms or terms that others may not know or you as a facilitator may not know, clarify these by asking the speaker to explain them or provide further context.

- **Restate the issue before a decision** – Summarize key points or ask the speakers to clarify (*"I'm not sure we all understand that. Do you mind clarifying that point?"*), or ask the scribe to write the points down.
- **Make sure everyone has had a chance to comment** – Before the Domain Committee decides on an action, make sure that all committee members present have had the opportunity to comment.

Provide Feedback to the Committee When Necessary or Appropriate

Providing feedback to Domain Committee members can be difficult during working sessions. In most facilitation situations there isn't a moment where a facilitator gets to say, "Would you like a bit of feedback on the last comment you made?" In fact, using that opening would not solicit a positive response.

So how do you provide feedback to the committee? As a facilitator you should always be maintaining an objective perspective on the group's discussion and provide feedback to the group only when necessary. In a controlled way, you have to be able to say what you really think.

> As a facilitator you should always be maintaining an object perspective on the group's discussion and only provide feedback to the group when necessary to encourage positive group behavior…

- **Check your personal biases** – Be aware and manage your own personal biases. Stay as objective as possible. Evenly distribute any feedback. Do not favor or disfavor any individual in the group.
- **Be specific in describing what you observe** – This helps committee members focus on a specific behavior or comment. *"I have noticed that every time we have said the word 'vitality', several people have winced."*
- **Describe or probe the impact of what you observe –** Let Domain Committee members express their feelings. *"Can one of you explain your reaction to the word 'vitality'?"*
- **Ask for and summarize suggestions –** Request suggestions from the group and then summarize these. *"Perhaps we should use the word 'continuity' instead of 'vitality'."*
- **Point out similarities between committee members' statements –** Use this technique when you sense that people are close to agreement but may not understand or recognize common ground.

Enforce Ground Rules

Ground rules help maintain a comfortable, productive environment for all participants. But ground rules are effective only if they are enforced. The entire Domain Committee is responsible for monitoring and pointing out when group members violate any of the rules and lessen the chances of accomplishing the committee's objectives. As a facilitator you can support this process.

- **Know the ground rules** – To monitor ground rules everyone needs to be familiar with them. Renegotiate, or at least revisit, ground rules periodically.
- **Correct violations the first time, and as soon as, they occur –** Be gentle. Simply address the behavior and move on.
- **Be fair and consistent when enforcing the rules –** Take great care to be evenhanded in pointing out violations. Follow the rules consistently throughout all working sessions.

MAINTAINING FOCUS AND ORDER

Often agendas are packed with discussions, documentation, and decisions. To ensure the Domain Committee meets its objectives, you must focus attention and energy on the objectives for that working session and for the overall mission of the Domain Committee.

Staying With the Group

Staying with the group means that you're able to filter the variety of messages you're receiving and know where you are in relation to the task and to every one else. You may think that you're listening, then someone asks you a question, and you realize you haven't got a clue where you are. One thing you can do to stay with the group is to do a mental paraphrase of the last thing said while you're listening to the present statement, and to create a string of statements, with a mental "bead" to represent each speaker.

Remember that disruptive behavior is typically the sign of an unmet need. Domain Committee members are considered experts in their field, and experts need recognition.

Side Conversations

MAEA Domain Committees are designed to be a small group of experts in a particular set of technologies. Working sessions tend to be in conference rooms where it can be very distracting to the entire committee if two or more members are engaged in a side conversation. Consider why this might be happening:

- The conversation may relate to the subject.
- The conversation may be personal.
- The members are bored because the working session or a topic is dragging on.

Remember that disruptive behavior is typically the sign of an unmet need. Domain Committee members are considered experts in their field, and experts need recognition. When you can give them what they need, the behavior will disappear. Since this is not always possible, there are ways you can deal with it.

- **Catch their eye –** Making eye contact with the talkers may be enough to get them to stop.
- **Bring them into the discussion –** Call on one of them by name, restate the last remark made by the group, and ask for an opinion on the topic.
- **Walk towards the conversation** – If you move around the room during working sessions, saunter over and stand casually behind them and keep talking. They will get the message.
- **Approach them during a break** – Inform them that their side conversation was distracting and ask them to refrain or share with the group.

Dealing with Silence

Absolute silence during a working session rarely means content or consensus. Major disasters or poor decisions can occur because of this assumption. Say, for an example, you ask for comments on a new Compliance Component that is being considered and no one responds. Consider why this might be happening:

- They may not understand the topic or what is going on.
- They may be tired or indifferent.
- They may still be concerned or angry about the previous topic.

Recognize that Domain Committee members have other day-to-day responsibilities and these priorities can make it difficult to focus. There are ways to break the silence.

- **Acknowledge the situation** – Check with the group by saying, "I notice that everyone is being quiet. Can someone tell me what you're thinking?"
- **Allow some silence –** Give the group some time to process what is happening. They may need to organize their thoughts or locate some research they have done on the topic.
- **Take a break –** Perhaps the group is drained or tired and could use a rest. Or perhaps someone should conduct an energizer exercise to get people motivated.

PERSONALITY AND MOTIVATION TECHNIQUES

One challenge of a facilitator is in understanding the personalities of the Domain Committee members and how to keep them motivated. Some behaviors contribute to the success of the groups work, most have no direct effect, and others detract from the group's effectiveness. Getting each person at the working sessions motivated begins with you taking it upon yourself to be a good role model.

Awareness of Your Own Attending Behavior

One of the things you, as a facilitator, have to be aware of is your own attending behavior. If you show your emotion in obvious ways, this may affect Domain Committee members. You should know what you look like when puzzled, unhappy, etc. Make sure your words and your non-verbal signals are saying the same thing.

Be aware of your biases and acknowledge them. If you really do want to say something, call on yourself, but make sure you don't use your role to dominate the discussion. For example, you may say *"Excuse me, let me step out of my role as a facilitator for a moment…"* then state your point and let the discussion continue.

Understanding Group Behavior and Dynamics

Acting as a facilitator requires some understanding of group behavior related to issues of leadership, power, and feelings.

- **Leadership issues** relate to the designated Domain Committee positions (e.g., Committee Chairperson, Scribe, etc.). Leadership issues arise from changes in leadership over time, and the leaders must have the consensus of the group.
- **Power issues** can accrue from a particular Domain Committee member's position, knowledge, personal strength, or factional alignment.

> One challenge of a facilitator is in understanding the personalities of the Domain Committee members…every working session will be full of behaviors by the members mixed with your own behaviors as a facilitator.

- **Feelings issues** relate to the fact that everyone comes to a group with feelings including old feelings, present time feelings and group feelings.

The personalities of group members can have an important bearing on group performance. Different personalities are suited to different tasks and aspects of group dynamics. Understanding the dynamics and performance of groups is clearly a complex matter. As a facilitator it is important to:

> Understanding the dynamics and performance of groups is clearly complex matter…acting as a facilitator requires some understanding of group behavior related to leadership, power, and feelings.

- Have an understanding of the personal goals and motivations of the members of the Domain Committee by talking with the Architecture Office.
- Have a correct evaluation of what you can expect form each one in terms of commitment to the Domain Committee.
- Make clear what is expected of each member as soon as the tasks that need to be completed are clear and assigned to individual committee members.

Motivating Domain Committee members

Motivation is what gets the Domain Committee members interested in Enterprise Architecture. It is important to remember that the Domain Committee members have been hand-selected by ITAB, the ARC or Architecture Office – in most cases they are not volunteers. Each Domain Committee member's verbal and non-verbal cues can show you whether or not they are motivated to contribute. The table below lists the most common cues as to whether or not a committee member is motivated.

Motivational Cues

	Motivated to Learn	
	Yes	*No*
Nods head	✓	
Smiles	✓	
Asks relevant questions	✓	
Leans forward	✓	
Shares experiences	✓	
Tries things on their own	✓	
Adds relevant information to topic	✓	
Makes eye contact	✓	
Drums fingers		✓
Shrugs		✓
Closes eyes		✓
Looks away		✓
Crosses arms and legs		✓
Easily distracted		✓
Consistently late to working sessions		✓

> Motivation is what gets the Domain Committee members interested in Enterprise Architecture.

There are virtually an exhaustive number of things you can do as a facilitator to motivate the members of the Domain Committee. The list below provides just a few of the most basic ways in which you can begin to motivate the Domain Committee:

- Be a good listener.
- Praise members on their contribution during working sessions.
- Show what value Enterprise Architecture brings to them and their agency
- Avoid domination or forcefulness.
- Show interest and appreciation for each and every member.
- Let committee members in on the planning of working sessions from the start.
- Be consistent.
- Ask members for their counsel and assistance.
- Give members goals, a sense of direction, something to strive for.

CONFLICT RESOLUTION

Occasionally you will face challenging behaviors and situations as you facilitate MAEA Domain Committee working sessions. Because Domain Committee members come from many different agencies, different backgrounds, and their individual experiences are what have helped them become the experts they are – their views, opinions and methods will sometimes conflict. They can misunderstand each other, and react in ways that could hinder what was otherwise promising progress.

When conflicts occur, how you deal with them as a facilitator is what is important. It will help you to realize that regardless of differences, each member of the Domain Committee likely shares the same basic need for acceptance and being understood – a need that, when unmet, is at the bottom of virtually every conflict.

Conflict Advantages and Disadvantages

Too often, conflict is seen as negative, something to be avoided. Conflict is an essential part of working together as a group. In fact, too little conflict can be just as harmful to the Domain Committee's progress as too much. Conflict can be both constructive and destructive:

- **Conflict is Constructive** when it results in clarification; serves as a release to pent-up emotions and stress; when parties understand each others needs, and use the conflict to build cooperation and trust. Through constructive conflict the best Architecture Blueprint assets are developed that support he overarching needs to the State as a whole.
- **Conflict is Destructive** when it diverts energy; polarizes the group and deepens differences; parties take 'either – or' positions, believing their way is right and develop negative feelings towards each other.

Conflict is neither good nor bad. It is part of human nature and to be expected when humans interact. Conflict can provide the Domain Committee with opportunities to learn new skills, develop problem-solving abilities and infuse energy. As a facilitator, you don't want to squash all conflict. Focus your efforts on directing the energy of a conflict toward a positive result. Help the Domain Committee stay open to different perspectives.

Managing Conflict: Six Steps

The evolution of a conflict usually starts with a difference of opinion. Open expression and discussion of differing opinions at that time can often diffuse the conflict. If the conflict is left unattended, the conflict builds, factions may be formed, positions may become entrenched, and it becomes very difficult for those involved to resolve the conflict without the use of the facilitator. It is critical that you deal with conflict openly and fairly before emotions get committee members too entrenched in their positions.

It is critical that you deal with conflict openly and fairly before emotions get committee members too entrenched in their positions.

Managing conflict can be dealt with in six simple steps. In general, when conflict arises you should:[2]

1. Make sure all sides have an opportunity to be heard.
2. Help to clearly define the issues, perhaps by having each side of the debate restate the position of the other side to its satisfaction.
3. Keep discussion focused on the substance rather than the individuals.
4. Encourage the various sides to meet separately and come back to the full group for further discussion.
5. Help individuals to save face and be able to change their position.
6. Bring in outside assistance – individuals not directly involved in the situation – to help provide an outside perspective.

As a facilitator, some key messages about conflict resolution to remember are:

- Conflict is inevitable.
- Conflict does not have to result in winners and losers
- In conflict, both parties tend to believe that their opinion is fact
- Conflict is neither good nor bad

[2] Adapted from *Training Guide: A Resource for Orienting and Training Planning Council and Consortium Members.* U.S. Department of Health and Senior Services, 1997

Conclusion

There is an old adage *"give a man a fish and he has a meal, teach a man to fish and he has a meal for life"*. One major goal of the Missouri Adaptive Enterprise Architecture is to equip its IT professionals with the capability for making life-long IT decisions for the benefit of the citizens of the State of Missouri. The skills for this are acquired through the efforts of the Domain Committees in developing the Architecture Blueprint assets that will help guide statewide IT efforts.

It is important that the facilitators of the Domain Committee working sessions understand the MAEA processes, as well as the professional skills of facilitation outlined in this manual. Facilitating Domain Committee working sessions is not 'lecturing' wherein the facilitator is active and the committee members are passive. In fact, Domain Committee facilitation is quite the opposite – working sessions require the committee members to be active and the facilitator to be relatively passive.

The Facilitator is the guide and monitor of the working sessions, concerned with the group dynamics and the mechanisms of discussion and ensures that the Domain Committee is making quality decisions and producing quality assets to be added to the Architecture Blueprint.

The Facilitator is the guide and monitor of the working sessions, someone who is concerned with the group dynamics and the mechanisms of discussion, and inquiry to ensure that the Domain Committee is making quality decisions and producing quality assets to be added to the Architecture Blueprint. The facilitator maintains a state of 'passive control' where the dominant activity involves listening and monitoring the committee members' discussions in parallel with the working session agenda.

The Domain Committee working session facilitator guides the group by supporting the chair, the scribe and the committee members, encouraging positive dialog, suggesting strategies, structures and ideas that enable group comprehension of the Architecture Lifecycle Processes. Above all else, the facilitator fosters an atmosphere in which the individuals feel confident about collaboration.

Appendices

The following appendices contain additional information that may be useful to those involved in facilitation MAEA Domain Committee working sessions. The appendices include templates for developing working session agendas and working session minutes, as well as actual agenda and minutes taken from the Security Domain pilot working sessions that can be beneficial in launching future MAEA Domain Committees.

Appendices are included for the following

- Appendix A: Working Session Agenda Template
- Appendix B: Working Session Minutes Template
- Appendix C: Security Domain Sample Agendas
- Appendix D: Security Domain Sample Minutes
- Appendix E: Lessons Learned – Domain Pilot

APPENDIX A – WORKING SESSION AGENDA TEMPLATE

The following Working Session Agenda Template can also be found in the Microsoft Word document entitled "MAEA Domain Working Session Agenda Template.doc".

<NAME> DOMAIN AGENDA

Date / Time <INSERT DATE> <INSERT TIME>
Location: <INSERT LOCATION>

BRING TO SESSION

- ❑ Agenda
- ❑ MAEA Manual
- ❑ Documentation Specific to discussion item (Research, Templates, Materials, etc.)

BRING TO SESSION

Old Business (estimated time – e.g., 15 min.)

- ❑ Review and approve minutes from previous working session
- ❑ Action Item Updates

New Business (estimated time – e.g., 30 min.)

- ❑ Communications from the ARC
- ❑ Communications from the Architecture Office
- ❑ Communications from the Domain Committee Chair
- ❑ Communications from Domain Committee Members

*Architecture Blueprint Items (*estimated time – e.g., 2 hrs.*)*

- ❑ Domain
- ❑ Discipline(s)
- ❑ Technology Area(s)
- ❑ Compliance Component(s)
- ❑ Product Component(s)

Action Items/Assignments (estimated time – e.g. 15 min.)

Logistics and Close (estimated time – e.g., 5 min.)

- ❑ Next Working Session Date, Time, Place

APPENDIX B – WORKING SESSION MINUTES TEMPLATE

The following Working Session Minutes Template can also be found in the Microsoft Word document entitled "MAEA Domain Working Session Minutes Template.doc".

<NAME> DOMAIN MINUTES

Date / Time <INSERT DATE>

ATTENDEES

- ❑ Attendee 1
- ❑ Attendee 2
- ❑ Attendee 3
- ❑ Attendee 4
- ❑ Attendee 5
- ❑ Attendee 6
- ❑ Attendee 7
- ❑ Attendee 8
- ❑ Attendee 9
- ❑ Attendee n

OLD BUSINESS

REVIEWED <INSERT DATE> MINUTES

Minutes reviewed and accepted with the following changes:

Content Changes

Additions, Deletions, Corrections

Grammatical Changes

Change 1…n

ACTION ITEM UPDATES

Items Completed since last working session

Item, Person Responsible, Resolution Description, Date Completed

Outstanding Items (Items not completed since last working session)

Item, Person Responsible, Item Description, Date Due

NEW BUSINESS

COMMUNICATIONS AND UPDATES

Communications from the ARC

List Communications

Communications from the Architecture Office

List Communications

Communications from the Domain Committee Chairperson

List Communications

Communications from Domain Committee Members

List Communications

ARCHITECTURE BLUEPRINT ITEMS

DOMAIN, DISCIPLINE, TECHNOLOGY AREA, PRODUCT OR COMPLIANCE COMPONENT #1

General Discussion

Brainstorming and content creation

Documentation

List any content discussion (creation, deletion, or changes)

Review and Approval

List any discussion regarding final acceptance by Domain Committee
Record approval (vote) and details related to submission of item to Architecture Office

DOMAIN, DISCIPLINE, TECHNOLOGY AREA, PRODUCT OR COMPLIANCE COMPONENT *N*

General Discussion

Brainstorming and content creation

Documentation

List any content discussion (creation, deletion, or changes)

Review and Approval

List any discussion regarding final acceptance by Domain Committee

Record approval (vote) and details related to submission of item to Architecture Office

ACTION ITEMS

- ❑ Item 1 – Description, Importance, Person Responsible, Due Date
- ❑ Item *n* – Description, Importance, Person Responsible, Due Date

LOGISTICS AND CLOSE

- ❑ Next Working Session Date, Time and Location
- ❑ Close Working Session

APPENDIX C – SECURITY DOMAIN SAMPLE AGENDAS

The agendas for the first twelve Security Domain working sessions can be found in the compressed file "Appendix C – Sample Agendas.zip"

APPENDIX D – SECURITY DOMAIN SAMPLE MINUTES

The minutes for the first eleven Security Domain working sessions can be found in the compressed file "Appendix D – Sample Minutes.zip"

APPENDIX E – LESSONS LEARNED – DOMAIN PILOT

During the course of the Security Domain Pilot project, several important lessons were learned that should guide the initiation of future MAEA Domains working sessions. Six of the lessons learned from the pilot are discussed below.

Lesson 1: Remain Flexible

The Missouri Adaptive Enterprise Architecture program is an ongoing, ever-changing process. An intergovernmental team, such as the Domain Committee, needs to be flexible and open to change. Be prepared to shift directions or discontinue the project if factors change. Expect that the players will change and may change extensively as the political winds of a jurisdiction changes. By the end of the pilot, at least two Domain Committee members changed and priorities shifted numerous times.

Lesson 2: Make Effective Use of Other Committees

As with many broad technology topics, the Security Domain Committee was one of many State of Missouri Committees tackling issues related to security. In many cases, such as with the ITAB Network Security Sub-Committee, these committees have many more members that can provide additional knowledge and expertise to topics being covered by the Security Domain. The Security Domain saw this as an opportunity to leverage this larger committee to do some "leg-work' in the form of research and Technology Scans that could be used for architecture documentation.

Lesson 3: Meeting Every Other Week Is Not Enough

When the Security Domain was launched, working sessions were scheduled as four-hour blocks, every other week. When launching a Domain, this is simply too few working sessions to get the ball rolling and produce any sizable amount of work. Once the Security Domain started meeting 3 out of every 4 weeks, the difference in both the quantity and quality of the Architecture Blueprint documents was markedly noticeable.

Lesson 4: Do More "Virtually"

Too much time was being spent in Domain Committee working sessions focused on "wordsmithing" or making grammatical changes that had little to do with the actual content of the deliverables. E-mail can be a powerful tool for handling reviews, feedback and approval cycles if used correctly. As more and more staff have fewer and fewer hours to devote to activities outside of critical job functions, using online collaboration or other virtual mediums will become a critical part of the success of Domain Committee Architecture assets.

Lesson 5: Schedule "Homework" On Two-Meeting Advance Notice

Assigning homework at the end of a working session to be due prior to the next working session (delivered to the "Documenter" 48 hours prior to the session) left very little time for Domain Committee members to complete this work in addition to their day-to-day responsibilities. Homework was often done the morning of a working session and made for some inefficient working sessions as time was spent during the session consolidating input. It was decided that "homework" assigned during a working session would not be due until the meeting following the next one (two-meeting advanced notice). This proved much more effective.

Lesson 6: Routinely Seek direction from ITAB and the ARC

Having felt as though they were often "working in a vacuum", the Security Domain Committee took it upon themselves to re-evaluate their priorities after 6 months of Architecture Blueprint documentation. They pulled up their original priority list, checked-off the completed items, and re-evaluated all of the remaining Technology Areas. Then they produced a priorities report and delivered this as part of their monthly package to the ARC specifically requesting their approval and guidance. It is highly encouraged that future Domain Committees provide a similar report both at the outset of the Domain and every six months until the Domain is in vitality process.

September 5, 2003

State of South Carolina Enterprise Technology Architecture

Domain Subcommittee Guidebook

Developed By

Division of the State CIO

September 2003

Table of Contents

Section 1: Introduction to the Domain Subcommittee Guidebook

The South Carolina Enterprise Architecture (SCEA) is constantly changing and evolving. This is because the information needs of state agencies are continually changing, and the SCEA provides a means to address these needs through a structured review, evaluation and adoption of new and emerging technologies. It also provides a method to contain and eventually retire technologies that are no longer cost effective. It is for these reasons that the Division of the State CIO (CIO) has developed this Guidebook. It is to be used as a reference to guide participants through the processes involved in establishing, maintaining and updating the SCEA. This document contains information for domain subcommittees, discipline committees and workgroups that will help them understand the various technical and governance processes that have been adopted by the Architecture Oversight Committee to make the SCEA a self-sustaining program.

Background and Goals

The CIO embarked on a project in May 2002 to establish an enterprise technical architecture to be used as a framework for making strategic information technology decisions on a cost effective, statewide basis. These IT decisions must meet the diverse business needs of agencies in the executive, legislative and judicial branches of state government. It was determined from the beginning of the project that to be successful, the State of South Carolina's enterprise technical architecture would have to:

- Be based on the strategic business direction of the State as an enterprise.
- Involve agency business managers as well as IT staff throughout the process.
- Be developed and maintained through a shared vision and the use of collaborative processes involving all state agencies.
- Provide strategic direction for making technology decisions without requiring wholesale changes to the current IT environment.
- Allow agencies to share many IT infrastructure components without sacrificing responsiveness to the changing business needs of individual agencies.
- Reduce the time it takes IT to satisfy ever shorter agency business change cycles by making the IT environment adaptable to change.
- Reduce the cost of IT over the lifecycle of each system.
- Have a governance process that supports the ongoing evolution of the architecture as well as its enforcement.
- Evolve in unison with changes in business strategies.

Figure 1: Six Technology Architecture Domains

1. Presentation Services
2. Communication Services
3. Security
4. Computing Services
5. Enterprise Applications
6. System Management Services

In July 2002, an Enterprise Architecture Committee, made up of managers from the CIO and nineteen state agencies, was established to develop a Technology Baseline for the State (an inventory of the technology being used in state agencies) and to identify the enterprise business requirements of the State for use within the SCEA process. The business requirements were documented in the Enterprise Architecture

Framework published by this Committee in May 2003. The Enterprise Architecture Framework is divided into two parts: the Business Architecture Structure and the Technology Architecture Structure.

The Business Architecture Structure includes the State's major business drivers, business information requirements, implications for technology and principles for making technology decisions, and provides the link between the technical architecture and the business needs of agencies and the State. The Business Architecture Structure provided the core business principles on which all the technical domain architecture recommendations are based. The current business drivers, technology implications, technology vision and technology principles are documented on the SCEA Web site at http://www.cio.sc.gov.

The Technology Architecture Structure includes three major components: the IT taxonomy, domain profiles and discipline profiles. The IT taxonomy categorizes related technologies, called disciplines, into domains which logically comprise the Technical Infrastructure. There is a profile for each domain, which describes each portion of the Technical Infrastructure, including the plan of action and rules to guide decision-making concerning a discipline. This profile establishes limits as to the architectural decisions that can be made for each discipline. The Technology Architecture Structure also includes discipline profiles, which document the boundaries, life cycle and standards for each discipline.

The Enterprise Architecture is divided into six domains (see Figure 1 above), or groups of related technologies, that include the major technology components utilized by most state agencies. Six domain subcommittees, composed of technical experts from across State government, have been established to recommend standards concerning the technical architecture for each domain. The results will be documented in domain and discipline profiles. These profiles define the domain strategies, domain principles, technical standards, product standards (if appropriate), and implementation/migration guidelines to be utilized by state agencies. It is the responsibility of the domain subcommittees to maintain and update the domain and discipline profiles when changes in the environment occur. Requests by state agencies for exemptions from the domain architectures and appeal of decisions by the Architecture Oversight Committee are handled through formal processes that include review and recommendations from the domain subcommittees and approval by the Architecture Oversight Committee.

Contents of this Guidebook

This manual is designed to provide guidance to the chairpersons and members of domain subcommittees, as well as workgroups and discipline committees, as to their roles in developing, updating, and refining the enterprise technology architecture and the related profiles.

The chapters are organized as follow:

- Subcommittee Management Guidelines – for subcommittee chairpersons. Provides guidance on organizing and managing domain subcommittees and their workload; also provides information on subcommittee member roles and responsibilities.

- Developing a New Domain Architecture – for new domain subcommittee members and/or chairpersons charged with developing a new technical domain. Provides basic information on what a domain profile is, and the process to be used to develop the new version of the architecture.

- Updating a Domain Architecture – for subcommittee chairpersons and members, workgroups and discipline committees. Provides reference material about what triggers the need for a change to the domain architecture, the process for documenting recommendations for the update, and how updates are approved and published.

- Identifying and Closing Gaps in a Domain Architecture – for subcommittee chairpersons and members. Provides guidance on how to perform gap identification, analysis and resolution for a domain architecture.

- Researching New Technologies, Products and Standards – for subcommittee chairpersons and members. Provides guidance on how research of technology is conducted, documented and used to make decisions concerning changes to, and to assess compliance with, the domain architecture.

- Coordination with IT Planning and IT Procurement – for subcommittee chairpersons and members. Describes activities that may be requested of domain subcommittee members in coordination with IT Planning and IT Procurement.

- Appendices - provides the templates used to structure SCEA deliverables, SCEA process diagrams, roles and responsibilities of all SCEA governance bodies, and other relevant background information.

Section 2: Domain Subcommittee Management Guidelines

This Section is designed to provide guidelines for the domain subcommittee chairperson on managing domain subcommittee activities, organizing and prioritizing workloads, and documenting deliverables. In addition, it clarifies the roles and responsibilities of domain subcommittee members, workgroups and discipline committees.

Roles and Responsibilities

Domain Subcommittee - Chairperson

Each domain subcommittee has a chairperson who will oversee and coordinate the activities of the subcommittee to keep the domain architecture current and relevant, and to represent the subcommittee in cross-domain and enterprise architecture planning activities.

The responsibilities of the subcommittee chairperson include managing all subcommittee activities, communications and outputs to include:

- Periodic updating of the domain architecture and associated profiles.
- Coordinating the meetings and managing the operations of the domain subcommittee, including the need to have regular meetings and ensuring that there is a broad base of expertise on the subcommittee to cover the technical disciplines making up the domain.
- Ensuring that the disciplines assigned to the domain are appropriate and providing any cross-domain coordination needed.
- Provide an environment where all domain subcommittee members are encouraged to participate and where research/learning can occur.
- Developing and managing the execution of a work plan for all activities and deliverables for which the subcommittee is responsible, to include:
  a. Developing an understanding of the goals set forth in the Enterprise Architecture Framework.
  b. Developing domain specific deliverables (i.e., domain and discipline profiles).
  c. Coordinating on-going research activities of subcommittee members to include utilization of external research services (e.g. Gartner) and vendor presentations.
  d. Performing gap analyses to identify gaps between the Technology Baseline and the "future state" for each of the technologies within the domain subcommittee's purview.
  e. Identifying and developing initiatives to resolve gaps.
  f. Evaluating requests, projects and proposals to determine conformance with the domain architecture.
  g. Ensuring that the domain architecture and documents are refreshed as needed.
- Identifying the resources required for the tasks listed above as part of work plan development.
- Assigning tasks to subcommittee members and establishing workgroups and discipline committees as needed to satisfy the responsibilities of the domain subcommittee.
- Coordinating and communicating with other domain subcommittees, the CIO Architecture Support Group (CIO-ASG) and the Architecture Oversight Committee (AOC).

- Documenting domain subcommittee activities, domain and discipline profiles, and preparing status reports and other deliverables required for approval of domain architecture additions or modifications.

Domain Subcommittee - Members

The members of the domain subcommittees provide the knowledge and expertise required to develop the domain architectures. These subcommittees are responsible for the development and maintenance of the content of the domain architecture and related documents, including domain specific deliverables such as disciplines profiles, technical standards, product standards, migration strategies, dependencies and best practices. Subcommittee members are expected to keep abreast of new technology and make recommendations on new technology to close gaps in the current environment.

Each domain subcommittee will consist of state agency technical personnel who have expertise in one or more of the disciplines that make up the domain architecture. Membership is usually assigned on a year-to-year basis, and members are expected to keep abreast of the technical trends and standards for their area of expertise. Members are to provide support and consultation for the domain subcommittee based upon what is best for the State of South Carolina as an enterprise.

Responsibilities of domain subcommittee members include:

- Attending regular domain subcommittee meetings.
- Ongoing enhancement of the domain architecture through the successful completion of tasks requested by the subcommittee chairperson.
- Ongoing research in assigned technical areas based on the member's expertise.
- Serving as chairperson or member of a workgroup.
- Providing technical consulting in assigned technical areas as requested by the subcommittee chairperson.
- Communicating the SCEA and the domain architecture to state agencies and vendors.

Temporary Workgroups

The domain subcommittee chairperson may establish workgroups to conduct research on specific issues and to evaluate technologies related to the domain architecture. The domain subcommittee chairperson will appoint a chairperson to oversee the activities of the workgroup. The workgroup chairperson must be a member of the domain subcommittee. Other members of the workgroup should include interested domain subcommittee members, and subject matter experts from other government agencies, etc. that have knowledge of the specific issue or technology. Upon formation of a workgroup, the domain subcommittee will provide the workgroup with a charter, mission statement and list of expected deliverables.

Responsibilities of the workgroup chairperson include:

- Directing the activities of the workgroup.
- Reporting status of activities back to the subcommittee chairperson.
- Ensuring completion of deliverables assigned to the workgroup.

Discipline Committees

Discipline committees may be established by the Architecture Oversight Committee or the domain subcommittee chairperson to oversee specific technologies or projects related to the domain architecture. The discipline chairperson works with the subcommittee to develop specific objectives, tasks and deliverables. The chairperson is typically an expert in the technology being investigated.

The discipline chairperson communicates recommendations back to the domain subcommittee for discussion and approval. The discipline committee's tasks include research, evaluation and formulation of recommendations for new technical or product standards for the discipline and their implementation. (See SCEA Update Process)

Responsibilities of the discipline chairperson include:

- Directing the activities of a discipline committee.
- Reporting status of activities back to the subcommittee chairperson.
- Ensuring completion of deliverables assigned to the discipline committee.

Domain Subcommittee Meetings

Domain subcommittee meetings should be conducted on a regular basis. The frequency of such meetings should be dictated by workload, but it is recommended that they be conducted at least quarterly. Sessions will be scheduled at the discretion of the domain subcommittee chairperson. Discipline committees will meet at the discretion of the chairperson for these groups.

The meetings of the domain subcommittee should be documented with minutes or a detailed meeting summary (see Form SCEA-6, Status Report from a Domain Subcommittee, in Appendix 2). Recommendations for additions, deletions and modifications to the domain architecture are to be submitted to the Architecture Oversight Committee with supporting documentation for approval. Any dissenting opinions must also be submitted to the Architecture Oversight Committee.

How to Target, Qualify, Obtain and Retain Subcommittee Members

Each domain is made up of a group of related technologies called disciplines. While it is ideal to have an expert on the domain subcommittee for each discipline, experts may not be available from state agencies for some components and the size of the subcommittee needs to be kept to a manageable number. Gartner Group recommends domain subcommittees of approximately eight to ten members, with eight as the ideal size. The goal is to maintain a broad level of expertise on the subcommittee with some members responsible for one or more technologies. Additional technology expertise from outside the subcommittee can be used to conduct specific research activities, when necessary.

Recruiting the best-qualified personnel is one of the most difficult tasks of the domain subcommittee chairperson, since the best-qualified personnel are usually the busiest. Methods for targeting needed expertise include:

- Word-of-mouth among domain subcommittee members (the domain subcommittee members represent a community of technical experts that often know who their peers are across the State and know it is in their best interests to have a qualified team).
- Utilizing the Skills Gap Analysis, when completed by the CIO, to secure a profile of technical experience across state government.
- Posting opportunities in various listservs and newsletters that are available to these technical experts.
- Working with the IT Planning Office to identify agency projects that may require personnel trained in the desired technologies or the acquisition of outside expertise in a technology area that is not covered by any expertise on the subcommittee. Specialized technical expertise that must be acquired for an agency project could be utilized by the domain subcommittee to help evaluate this technology from a statewide, as well as, the project perspective.
- Utilizing the other SCEA groups such as the CIO or the AOC to find in-house expertise.

Qualifying the potential new member will require an understanding of the experience and competence needed for that technology component. Ideally, members should have some hands on experience with major aspects of the targeted technology.

With the constant changes in technology, chairpersons should look for a broad profile of expertise that demonstrates an understanding and aptitude for this area of technology. Subcommittee members should have an understanding of the technology and how it is applied, rather than just expertise with one or two products or technology components. The chairperson can work with the CIO to identify training opportunities and to access research needed to augment the experience of a subcommittee member.

Once a qualified person has been identified, the next step is to "get them on-board". While knowledge of the SCEA process will increase over time, the chairperson should not assume that the person knows anything about SCEA or architecture. Capturing their interest will depend on the chairperson's ability to convince them that the time spent in this process has value to them and the State of South Carolina. It would be prudent to identify other people that this person can talk to about the value of the architecture program. The CIO will also assist the domain chairperson in orienting this person to the benefits of an enterprise technology architecture.

Once an individual agrees to participate on a domain subcommittee, the next step is to obtain approval from their management to provide them adequate time to participate. A chairperson should work with the CIO to communicate the value of SCEA directly to the new member's management. The value must be articulated in terms of how it may help that agency, the projects being planned or implemented, the expertise of the person needed, and the ability to integrate systems with outside agencies and organizations. The time commitment may need to be limited, at first, until the person or his/her management sees this value. This may mean limiting the person's involvement on workgroups or initiatives at first. It may also mean securing an

endorsement from the AOC to demonstrate the importance of this person's participation to the State of South Carolina.

To retain valuable technical expertise on the domain subcommittee, it is important that members and their management are aware of the accomplishments of the subcommittee. Subcommittee members should be encouraged and acknowledged for their work, whenever possible.

Training Requirements

All domain subcommittee chairpersons should attend a half-day training session on the SCEA program. This provides context on how the architecture processes works, the purpose of each process, and on their role in these processes. Periodic sessions on the SCEA program for workgroup and discipline chairpersons will be made available as well. In addition, all subcommittee, workgroup and discipline committee members are encouraged to receive training in their areas of expertise. While the CIO does not provide direct funding for individuals to do this, appropriate training is often a matter of knowing what classes are available and members convincing their management as to its value. Chairpersons should obtain and share information on training opportunities about technologies within their domain. A chairperson should also provide mentoring for a new/replacement subcommittee member, through, at least, their first few subcommittee meetings.

The CIO will coordinate briefings by experts from external research services (e.g. Gartner, META, etc.) and provide research materials on specific topic upon request by domain or discipline committees. The CIO will also monitor and disseminate information from standards organizations and the federal government, as appropriate. Some vendors will provide product training at no cost. It is up to the domain chairperson and subcommittee members to take advantage of these opportunities. There are also many specialized listservs and Web sites designed to keep technology communities updated and in touch. In addition, initiatives to define standards and best practices in new technologies will require vendor assessments and on-site visits, which will provide additional opportunities to learn about the technologies.

Documentation and Status Reporting Requirements

The domain and discipline profiles are the primary deliverables of a domain subcommittee, and are the responsibility of the domain chairperson. These profiles document the decisions of the domain subcommittee and the research/input from workgroups and discipline committees. This document is a repository of information describing domain disciplines, as well as the associated standards, migration strategies, dependencies, and guidelines that will be used by state agencies to implement technologies and systems. It is important that these profiles continue to be updated and enhanced so that the work of the domain subcommittee has meaningful impact on all systems being built or enhanced. The process and associated documentation requirements are described in the Updating a Domain Architecture Section of this Guidebook.

Domain subcommittee meetings should be documented with minutes or a meeting summary and shared with the other domain subcommittee and the Architecture Oversight Committee to give everyone information on what activities and issues are being addressed. This provides information needed to identify and coordinate cross-domain activities (see Form SCEA-6, Status

Report from a Domain Subcommittee, in Appendix 2). Workgroups and discipline committees must provide status reports on active initiatives to the domain chairpersons as well. The decision on the frequency of these meetings and the format of the status reports is left up to the domain chairperson.

Managing and Prioritizing Workloads of Domain Subcommittees

Domain subcommittee members are normally expected to be available for one day a month to support the work of the subcommittee. Additional time may be requested of a member for work on a workgroup, with such work possibly requiring up to one or two days a month. A domain subcommittee chairperson normally requires the equivalent of an extra half day a month to manage a domain subcommittee, meet with other domain chairpersons to discuss cross-domain issues, and to represent the subcommittee at planning and compliance meetings. Additional time may be required by chairpersons to oversee the work of workgroups, deal with gaps, track the status of domain work, and conduct their own research.

With a limited amount of available resources and the significant amount of work involved in the architecture process, it is important that workloads be identified and organized. Workload planning is one of the important responsibilities of the domain subcommittee chairperson.

Prioritizing Workloads

Before workload can be defined and delegated, it is important to categorize the work so that it can be prioritized on an ongoing basis. While work should be prioritized within each category, the categories have different priorities relative to each other. Domain subcommittee workload can be categorized and prioritized on the following basis:

- Responding to Changes in the State's Business Needs - The successful implementation of SCEA is dependent on the technical domain architectures being able to directly support the business drivers and the associated IT architecture principles. Therefore, the domain architecture must be reviewed periodically to assess the impact of changes to the business drivers and environmental trends of the State. This review must be the highest priority because of the potential impact to the ongoing work of the team.

- Identifying Gaps in the Domain Architecture - Beside the annual refresh of the domain architecture and ongoing work on the domain and discipline profiles, completing gap initiatives is the core ongoing work of the subcommittee (see Section 5, Identifying and Closing Gaps in a Domain Architecture). Gaps are prioritized once or twice a year by the subcommittee and in conjunction with the other domain subcommittees. Project plans for the highest priority gap initiatives are completed by the domain chairperson and assigned to discipline committees or workgroups. Priorities for gap initiatives are usually based on subcommittee input, the dependencies of other domains, CIO priorities and availability of resources. While additional gaps may be found throughout the year, gap priorities do not change often. Gap initiatives are the second highest priority for ongoing domain work.

- Conducting Architecture Conformance Reviews - Domain subcommittees have a role to play in the governance of the SCEA. One aspect of this is to review requests from agencies for

architecture conformance. This activity includes comparison of technology and projects with existing standards. This work is usually considered a high priority because it usually involves large projects and affects their timetables. Domain chairpersons are dependent on good project planning by agencies to ensure that this work can be scheduled in a timely manner and with a minimum of interruption to the ongoing work of the subcommittee. Chairpersons should work closely with the CIO and the AOC to estimate resource requirements and schedule time for work. Conformance reviews can take two to three sessions to complete and may require the participation of multiple subcommittee members. Reviews requiring significant resource time may require chairpersons to document the impact on other projects and report this to the AOC for assessment.

- Evaluating Exemption Requests - Another ongoing responsibility of domain subcommittees is the review and evaluation of requests for an exemption from an architecture standard. Requests from agencies for exceptions to the architecture will be submitted to the domain subcommittee for a written evaluation and recommendation to the Architecture Oversight Committee.

- Updating the Domain Architecture - To be meaningful, the domain architecture must be updated periodically to relate to changes in the State's needs as well as the technology available. In addition, the domain and discipline profiles should be refined to make them more useful and to provide guidelines on implementing the architecture.

  This ongoing updating and refinement process is not as high a priority as the previous categories, but the resources and work involved must be accounted for in work plans to ensure it takes place. Much of this updating is an outcome of the SCEA Update Process, while the refinement of documents requires a more diligent management approach by the domain subcommittee chairperson.

- Researching Technology Components and Training - Domain subcommittee members should be assigned specific technology components to keep abreast of and identify changes in technology trends that may effect the refresh cycle or cause a gap in the architecture. Adequate time and access to information and training should be allocated to each expert, although most IT professionals keep up with technology related to their expertise during work hours while completing other duties. See Section 6, Researching New Technologies, Products and Standards, for more information on this activity.

Developing and Documenting Work Plans for Domain Subcommittees

With the need to balance the workload and priorities of different categories of work in a domain, the subcommittee chairperson needs to organize all work with a comprehensive work plan. A template is provided in Appendix 2 (Form SCEA-7, Work Plan for a Domain Subcommittee) to help monitor resources needed, timeframes required and deliverables involved with each task.

Work involving gap initiatives will be documented on a Gap Analysis Report from a Domain Subcommittee, Form SCEA-9, which requires Architecture Oversight Committee Approval (see

Appendix 2) so that it can be conducted by the subcommittee or delegated to discipline committees or workgroups for completion.

All work of the subcommittee should be managed based on the priorities in the work plan. The domain subcommittee work plan should facilitate the organization and scheduling of work as well as to adjusting to the impact of new priorities such as compliance reviews and project evaluations.

Use of Workgroups to Conduct Research and Provide Recommendations

Workgroups may be established by a domain subcommittee chairperson to conduct research and provide recommendations on specific technology issues/topics. A workgroup should be used whenever the work to be performed is temporary in nature (e.g. evaluate a new/emerging technology) and does not require the efforts of the entire domain subcommittee. A workgroup chairperson is assigned to oversee the group and provides status reports to the domain chairperson. When the workgroup has completed its work, the chairperson of the workgroup communicates/presents the recommendations back to the full domain subcommittee for discussion and approval. See Section 4, Changes to a Domain Architecture, for more details on how to use workgroups to manage workload.

Implementing the Enterprise Architecture

Ideally, the enterprise architecture will guide all IT decision making (infrastructure, application development, operations, etc.). An awareness of architectural conformance must become second nature. The domain architectures are intended to provide guidance for many day-to-day IT activities and decisions. For example:

- IT procurements,
- State term contracts,
- Buy-versus-build decisions,
- Development of evaluation criteria in RFPs,
- Hardware upgrades,
- Software package/tool selection, and
- Design decisions in the context of a specific IT project/system.

Section 3: Developing a New Domain Architecture

This section is about creating a domain architecture for the first time. The process for changing an existing domain architecture is discussed in the Section 4 of this Guidebook. This Section should be read by anyone who is not familiar with the SCEA process, in particular, new members of domain subcommittees or individuals assigned to develop the architecture for a new domain. The most important thing to remember about developing a domain architecture is that it is a collaborative, iterative, creative process. A team effort is required because of the complexity of the individual technologies and their interdependencies. Domain architectures are never complete because change is a constant in the realm of information technology and in the realm of government services. Architecture development is a creative endeavor that requires thoughtful analysis and inspired thinking to respond to the many challenges inherent in an architectural approach to deploying and managing technology to satisfy the business needs of state agencies.

What is a Domain?

A domain is comprised of a group of related technologies called disciplines, usually organized around common IT infrastructure services or information management functions. The Architecture Oversight Committee is responsible for determining how many technology domains are appropriate and assigning individual disciplines to them. The list of disciplines typically included technologies currently in use and new technologies that are likely to be implemented in the near future. There are currently six domains: Presentation Services, Communication Services, Security, Computing Services, Enterprise Applications and System Management Services.

What is the Purpose of a Domain Architecture?

The purpose of a domain architecture is to identify, through a structured process, the technologies, industry standards and/or products in a specific technology group that best support the business and technical requirements of South Carolina State government. The technologies, industry standards and/or products identified through this process should comply with and further the principles set forth in the Business Architecture and Technical Architecture. A domain architecture provides:

- An overarching strategy for the selection of technologies and products in a domain that meet the business and information technology needs of state agencies.
- Principles that "flow down" from and support the Business Architecture and Technical Architecture Structures with rationales and implications further articulated for the specific disciplines.
- The design principles specific to the domain technologies.
- Technical standards for the domain technologies.
- Product standards for the domain technologies.
- Strategies to migrate from the present technical environment to the selected technologies and products.
- Guidelines, methods and dependencies for the implementation and management of the domain technologies.

Why Do We Need Domain Architectures?

The South Carolina Enterprise Architecture (SCEA) is divided into an interrelated set of six domain architectures. They are intended to guide all IT activities to support the State's business strategies and information requirements. These activities include the planning, design, selection, construction, deployment, support and management of information technologies. The SCEA will also provide the basis for evaluating and prioritizing changes to the State's portfolio of information systems.

What is a Domain Architecture Based On?

When a domain subcommittee is charged with developing the technical architecture for a group of related technologies, the framework for their research and deliberations is provided by the Enterprise Architecture Framework. The rationale for doing this is twofold. First, the use of a common framework allows multiple subcommittees to work in parallel with some assurance that their recommendations will align with each other and support the work of domains with which there is technological overlap. Secondly, the domain architecture is based on a set of principles and requirements that are derived from the agencies' business drivers and business strategies. Defining the domain architectures within this business context provides the initial alignment of information technology to the State's business needs.

To provide a context for domain decisions, it is useful to have a mental map of the relationships between the deliverables defined during the creation of the Enterprise Architecture Structure. Those relationships are as follows.

<u>Business Architecture</u>

- Enterprise Business Drivers – Major areas of focus for an organization based on its mission, services and constituents.

- Enterprise IT Implications – Key business issues relevant to IT that should be addressed in order to satisfy the business drivers.

- Enterprise IT Vision – Foundation statement regarding the role of IT in serving the business needs and direction of the organization.

- Enterprise IT Principles – Fundamental guides for technology decision-making. These principles are based on key values, standards and beliefs that provide the foundation upon which the architectural design is built.

<u>Technology Architecture</u>

- IT Taxonomy - Categorizes related technologies (disciplines) into domains which logically compose the technical infrastructure.

- Domain Profile – Describes each portion of the technical infrastructure, including the plan of action and rules to guide decision-making concerning a discipline. Sets limits as to the architectural decisions that can be made for each discipline.

- Discipline Profile – Documents the boundaries, life cycle and standards for each discipline.

For an explanation of the process via which each of these deliverables is created, refer to the description of the Enterprise Architecture Process documented on the CIO web site at http://www.cio.sc.gov.

Domain Chairperson Activities

The domain chairperson must lead, guide, push, pull, cajole and encourage subcommittee members to complete their individual assignments and to fulfill the responsibilities of the subcommittee. Architecture development is an iterative, creative process. The subcommittee should be encouraged to approach its work with an open mind and leave "sacred cows" behind. The chairperson should strive to develop a rapport with each of the subcommittee members and to foster an atmosphere of mutual respect within the subcommittee. Delegation of work to subcommittee members is not only good survival strategy, but the subcommittee will be more effective when the members realize they are empowered to guide technology decisions for South Carolina State government.

As coordinator of all domain subcommittee activities, it is imperative for the chairperson to be well organized and to communicate openly and frequently with subcommittee members. Every member of the subcommittee must have complete and current documentation and understand what is expected of them at each step of the development of the domain architecture. Open and active communication with the CIO, with other domain chairpersons and with the AOC will be essential for the coordination and resolution of cross-domain issues. A number of technologies and technical standards impact multiple domains and will require creative thinking and collaboration across domain boundaries.

The chairperson is responsible for all documentation generated for publication as part of the domain architecture. Delegation of responsibility for meeting minutes and draft documents is appropriate, but the chairperson is responsible for the quality and completeness of any documentation produced by the subcommittee and all its workgroups. See Standard Format for Domain Subcommittee Documents below for information about the format and content requirements for domain subcommittee deliverables.

Domain Subcommittee Activities

Review and Acceptance of the Domain Technologies

The first task of a newly formed domain subcommittee is to review the disciplines assigned to the domain by the Architecture Oversight Committee. If the domain subcommittee believes that a technology is more appropriately addressed by another domain subcommittee, that recommendation must be proposed to and approved by the Architecture Oversight Committee. When a list of disciplines is finalized, the domain subcommittee chairperson must assess whether

the subcommittee has the expertise and experience to address these technologies. The recruitment and retention of appropriate membership is critical to the success of a domain subcommittee. The CIO-ASG can assist with recruitment of missing subject matter experts.

Review of Functionality and Major Issues for the Domain Technologies

It is important to organize the disciplines by relevant factors (i.e., types and number of users, types of applications, total expected investment in a technology, total volume, total expected benefits from standardization, etc.) in order to identify all functionality and interrelationship between disciplines, and to also facilitate prioritization and delegation of work. The subcommittee should prepare a list of issues that impact all or multiple disciplines within the domain. Missing technologies may be revealed during this brainstorming activity. The master list of domain technologies should be revised accordingly. A list of issues should also be compiled for each discipline within the domain. This information will help the subcommittee establish priorities, especially if it is not able to address all technologies within the time allowed for the initial development of the domain architecture.

Review and Adoption of Conceptual Architecture Principles

A thorough grounding in the Enterprise Architecture Structure is essential to the successful development of a domain architecture. Therefore, the third major task of the domain subcommittee is to analyze and interpret the principles set forth in the Enterprise Architecture Framework in terms of the domain's technologies. This analysis results in the adoption of these principles as the general principles for the domain, with rationales and implications that are specific to the technologies within the domain. Implications will become important during the completion of gap analysis activities. It is important that thoughtful consideration be given to implications of implementing domain technologies so that they conform to the principles in the Enterprise Architecture Framework.

Development of a Domain Strategy

The fourth major task of the domain subcommittee is to develop a strategy for the domain that aligns with the IT vision and principles of the enterprise architecture in terms of the domain's technologies. This strategy for the domain will provide the overarching concepts to drive/direct the decision-making processes of the subcommittee. This strategy also establishes the boundaries of the domain, and will guide the selection/scope of technical standards for the domain. The domain strategy is documented on the form SCEA-4, Domain Profile (see Appendix 2).

Defining Domain Principles Specific to the Domain Technologies

After the development of a domain strategy, it will become apparent that principles specific to the domain are needed to guide the development of standards. These domain principles should be documented in the same format as the general principles, complete with rationales and implications. The domain principles/boundaries are documented on the form SCEA-4, Domain Profile (see Appendix 2).

Setting Priorities for Domain Subcommittee

The subcommittee must establish priorities for its work based on a number of factors. These include:

- Availability of subject matter experts.
- Number of requests received and pending from agencies, the AOC, etc.
- Severity and urgency of issues.
- Major agency projects that require architecture review.
- Availability of resources to define low-level architecture specifications for configurations and to write implementation guidelines based on practical experience.
- Time available to complete the first iteration of architecture or mandatory reviews of existing standards.

Domain Architecture Gap Analysis

The first time through the SCEA process, there is usually insufficient time or expertise on the domain subcommittee to cover everything. These are gaps within the domain architecture. If current products or standards are not capable of meeting the strategic goals of the SCEA, these are additional gaps in the domain architecture. Each of the functional areas or technologies within the domain that require further research and analysis will be prioritized and incorporated into the domain subcommittee work plan by the domain chairperson. See Section 5, Identifying and Closing Gaps in a Domain Architecture, for additional information.

Review and Acceptance of Work by Discipline Committees and Workgroups

Some of the domain subcommittee's work will be delegated to members with deep technical knowledge and practical experience with one or more of the technologies. This allows multiple architecture research and evaluation efforts to run concurrently. All deliverables from discipline committees and workgroups are subject to review and acceptance by the full domain subcommittee. The subcommittee is responsible for ensuring that lower level decisions remain true to the Enterprise Architecture Framework, conform to the domain's own principles and will not create conflict with other domain architectures.

Discipline Profiles

The domain subcommittee must analyze each discipline within a domain to determine if a new standard is needed or if an existing standard should be updated, and if the enterprise will be best served by this being an industry, technical or product standard. This is accomplished by reviewing a number of factors including the industry status of the technology, the state's existing technology baseline, and the state's future business and technology needs. The domain subcommittee must also determine what industry standards already exist (e.g., formal or de facto), the potential cost of implementing the new standard, and if state personnel are available/trained for this purpose. This requires a significant amount of research and discussion by domain subcommittee members. The recommendations of the domain subcommittee are then documented on a Discipline Profile Form, Form SCEA-5. This Form documents the life cycle and recommended deployment decisions for the discipline using the definitions set forth below:

- Baseline: The current technology or process discipline in use by the agency or enterprise.

- Tactical: Technologies that the State may use in the near term, tactical time frame, approximately the next two years. Currently available products needed to meet existing business needs are identified here.

- Strategic: Technologies the State envisions using in the future that provide strategic advantage. Usually, anticipated marketplace products are identified here.

- Retirement: Technologies and/or process disciplines targeted for deinvestment during the architecture planning horizon (e.g., the next five years).

- Containment: Technologies and/or process disciplines targeted for limited (maintenance or current commitment) investment during the architecture planning horizon.

- Mainstream: Technology and/or process disciplines targeted as the primary deployment/investment option for new systems or legacy system migration over the architecture planning horizon.

- Emerging: Technology and/or process disciplines to be evaluated for future integration into the target architecture (e.g., mainstream) based on technology availability and business need (key for "evergreening" or keeping the architecture current).

Other information such as dependencies, notes, migration considerations, and a review date are also included as part of the development of a Discipline Profile. Once completed, Discipline Profiles are submitted to the CIO-ASG for review by other domain subcommittees and approval by the Architecture Oversight Committee. They then become part of the Technical Architecture Domain Report.

Recommending New Technical Standards and Technologies

During the course of technology and standards research, evolving standards and new technologies will be identified that support the domain architecture and the business goals implicit in the Enterprise Architecture Framework. Standards that are expected to be worthy of inclusion in the domain architecture when they are adopted by the IT industry should be declared as emerging standards that will be tracked by the domain subcommittee. They can then be included in the domain subcommittee's work plan and assigned a priority. For information on the assessment of emerging technical standards during routine research and monitoring of technologies, see Section 6 on Researching New Technologies, Products and Technical Standards.

Documenting Guidelines and Methods for Implementation and Management

Guidelines are practical advice for implementation and management practices based on the experience and research of the State's most knowledgeable experts. Methods are more formal and more prescriptive. When approved methods are embodied in products, they will become strategic products.

Standard Format for Domain Subcommittee Documents

Templates for the following documents are found in Appendix 2.

- Status Reports From a Domain Subcommittee (SCEA-6)

- Work Plan for Domain Subcommittee (SCEA-7)
- Gap Analysis Report From a Domain Subcommittee (SCEA-9)
- Domain Profile (SCEA-4)
- Discipline Profile (SCEA-5)

Cross-Domain Issues

A number of technologies and technical standards impact multiple domains and will require creative thinking and collaboration across domain subcommittee boundaries. It is essential that all members of all domains be familiar with the complete set of domain architectures. Some technology overlaps are more obvious than others. For some technologies, the synergy between domain architectures is a significant concern. Some domain technologies provide infrastructure services for other domains. In the practical application of architecture, systems are constructed with components from all the domains. Therefore, all of the domain architectures must be in congruence with each other. Open dialogue and cross-fertilization of ideas among the domains are very important. Cross-domain issues must be documented and discussed at domain subcommittee and Architecture Oversight Committee meetings.

Section 4: Changes to a Domain Architecture

This Section describes the types of changes that can occur within a domain architecture, the role of the domain subcommittee in reviewing these changes, and the processes and procedures for recommending changes to the Architecture Oversight Committee (AOC). First, there are formal approval processes for specific types of changes that will have a major impact on South Carolina's Enterprise Architecture. These changes include: (1) the Technical Compliance Assessment Process (see Figure 1 in Appendix 2) and (2) Change to Existing Technical Architecture Process (see Figure 2 in Appendix 2). Secondly, the domain subcommittee has the authority to make other types of changes on its own, as long as there is consensus among subcommittee members and the changes are consistent with the conceptual principles of the enterprise architecture as reference above, and the changes are reported to and accepted by the AOC. The specifics of the types of changes that fall into these two classes are detailed below.

Events Leading to Domain Architecture Changes

Federal /State Mandates

Federal/State mandates can prompt agencies to request revisions to the SCEA standards, which in turn should trigger a review of the appropriate domain architecture elements.

Requests From Agencies

Annual agency planning activities can result in requests to revise the SCEA source documents, which in turn will trigger a comprehensive review of the appropriate domain architectures. New business drivers and business information requirements, as well as changes in industry best practices for information technology, can also impact the enterprise architecture. These too will require a comprehensive review of all domain architectures to determine the impacts (if any).

Enterprise-wide Technology Projects

Routine and enterprise-wide technology project activities such as requirements analysis and architecture consultations may reveal a need to rework or refine portions of the architecture. As the architecture specifications for infrastructure services are defined, a deeper understanding of the cross-domain dependencies may require domain changes to reconcile lower level architecture elements such as interface standards, standard configurations and implementation guidelines.

Industry Best Practices, New Products/Applications, and Domain Subcommittee Activities

A basic premise of the SCEA process is that the domain architectures can only remain relevant through constant refinements based upon industry best practices, the assessment of new products and applications, and the resolution of gaps that are identified by the domain subcommittee. Change is supported and driven by the domain subcommittee and on-going research activities. Routine technology tracking and focused research related to specific conformance reviews and project consultations will reinforce the need for greater conformance in some areas and greater flexibility in others.

Frequency of Domain Architecture Updates

The frequency of updates to the domain architecture depends on a number of factors. Some technologies are rather volatile and experience rapid or frequent changes, while others change little in twelve months. Infrastructure and agency projects, while usually keyed to budget cycles, may occur at any time. As such, domain architecture review/updates should happen at least once per year, and should occur and work in conjunction with the CIO IT Planning cycle. The appropriate frequency of update should be established when a domain standard is approved by the AOC, and should be monitored by the CIO-ASG to ensure a review is initiated in a timely manner.

Two Primary Classes of Changes to Architecture Documents

There are two primary classes of changes to domain architectures and their associated documents: those that require the approval of the Architecture Oversight Committee and those that do not.

Changes that Require AOC Approval

The types of changes that require AOC approval are as follows:

- Adding or removing principles, technical standards, or product standards.
- Adopting methods that become mandatory or are embodied in products that are categorized as strategic.
- Significantly altering the meaning or intent of a principle, technical standard or product standard.
- Changing the status of a product, i.e., from research to strategic, from strategic to transitional, from transitional to obsolete.
- Making any change that will have major impact on technology products, agency financial or personnel resources, or on the ability of an agency to implement application systems.
- Requiring modification of a pending RFP, SOW, etc. or an RFP currently out for bid.
- Requiring changes to ongoing implementation projects.
- Greatly accelerating the agencies' transition planning for implementing a new architecture.

Changes that a Domain Subcommittee Can Make Under its Own Authority

Changes that can be made by a domain subcommittee, but must be reported to the AOC as information, include:

- Updating version numbers of product standards.
- Adding or refining narrative to provide a better explanation of component technologies or standards.
- Updating guidelines for the implementation and/or migrating to component technologies or technical standards.
- Updating the technology review section of a domain architecture document.

- Adding, updating or deleting a best practice that supports an existing product or standard, provided it does not have a major impact on an agency or on multiple agencies.
- Making changes to assignments within a domain.
- Adding new technologies, products or technical standards to the research category.
- Identifying gaps in the architecture.
- Removing technologies, products or technical standards from the research category if routine research and monitoring indicates that they are not viable or will not fit within the SCEA.

Process and Deliverables for Changes that Require AOC Approval

Changes to the domain architecture that require approval of the AOC will follow the Request for Change to Existing Technical Architecture Process (see Figure 2 in Appendix 2) or Technical Compliance Assessment Process (see Figure 1 in Appendix 2) and will utilize the Request for Assessment of Technical Architecture Form, SCEA-1 (see Appendix 2).

Process and Deliverables for Changes that Do Not Require AOC Approval

Changes that do not require approval by the Architecture Oversight Committee must always be documented and presented to the CIO-ASG for AOC review and for information. The domain subcommittee can request that the CIO-ASG update the Table of Changes located at the beginning of each domain architecture document. The change statement must include: (1) the date of the change, (2) a succinct, but complete description of the item that changed, (3) its location in the architecture document, and (4) the type or basis of the change (research, prototyping, revisions, etc.). An example of such a change may include, "*Middleware Product Selection Matrix added STC e*Gate™ to Messaging and Application Integration Products – Based on Gartner Research"*.

Changes can be proposed by anyone on the domain subcommittee, but must be reviewed and approved by a majority of the full domain subcommittee and submitted to the CIO-ASG as information for AOC review. The domain subcommittee must consider cross-domain implementation issues before making any change. Only then should the domain chairperson edit the document and submit it to the CIO-ASG. If the CIO-ASG concurs that AOC approval is not needed, the recommendation will be placed on the agenda of the next AOC meeting for information and review purposes only. Once accepted, the CIO-ASG will notify the other domain subcommittee chairpersons of the proposed change. The domain chairpersons will respond to any questions arising from peer review and commentary.

The new version of the domain architecture document, with appropriate change notices, will be published on the CIO web site. The CIO-ASG will also provide a summary report to the AOC outlining the changes that all domain subcommittees have made to the domain architectures. Once accepted by the AOC, advisory notices will be sent to the agencies by the CIO-ASG.

SCEA Update Process Workflows

In July 2003, the Architecture Oversight Committee (AOC) approved formal processes for updating domain architectures that include (1) Change to Existing Technology Architecture, (2) Technical Compliance Assessment, (3) Request for Waiver/Exception, and (4) Appeal of Architecture Decision. At this time, the processes do not address whether hands-on research or a

prototype or a pilot project will be required prior to reaching a final decision. It is the responsibility of the domain subcommittee chairperson, in consultation with the domain subcommittee, to decide if such research or testing is required. Regardless, each workflow is preceded by a set of common activities.

Initial Workflow Activities

The process starts with a request to the CIO-ASG to affect a change in the domain architecture or to assess technical compliance (Request for Assessment of Technical Architecture Form, SCEA-1) with the domain architecture. After consulting with the requesting entity, the CIO-ASG performs a preliminary review of the request, determines whether the request is a change to the architecture or is in compliance, and whether additional research will be required. The CIO-ASG posts the request and their preliminary determinations to the Web Site. When compliance is not obvious, the CIO-ASG will conduct necessary research and then forward the request, including the research and any other available information related to the request, to the appropriate domain subcommittee for evaluation.

The domain subcommittee handles the coordination with other domains that are impacted by the anticipated change to the domain architecture. The domain subcommittee will seek to involve the other domain subcommittees in the review process to the extent necessary. Following a commentary period for the other domain subcommittees, the domain subcommittee consolidates the reviews and communicates those results to all involved domain chairpersons. The CIO-ASG will work with the domain subcommittee to resolve any problems with the research, the information provided to the subcommittee, and coordination responsibilities.

If needed, the domain chairperson will assemble a workgroup and appoint a chairperson to proceed with the evaluation. Workgroups may be as small as two or three people, or as large as needed. Workgroup members are generally domain subcommittee members, unless a non-member is needed because of their subject matter expertise, or because the topic has cross-domain impacts. The domain subcommittee may also request that the CIO-ASG provide additional research/information for its evaluation. Following the conclusion of the research and evaluation, the domain subcommittee (with the assistance of the workgroup or discipline committee that evaluate the technology) will prepare a preliminary report and recommendation (Form SCEA-8, Recommended Action by a Domain Subcommittee, found in Appendix 2) and submit it to the CIO-ASG. This Form summarizes all the research and evaluation activities related to a recommendation. The CIO–ASG will finalize an information packet, post an agency notice, and prepare the recommendation for inclusion on the agenda of the next Architecture Oversight Committee meeting.

The domain chairperson will make a presentation to the AOC outlining the domain subcommittee recommendation. The domain chairperson will also present any dissenting views from the domain subcommittee or workgroup. In situations where the domain subcommittee is making a recommendation that is in conflict with a request from an agency, the agency will be given the opportunity to make a brief presentation (approximately 10 minutes) to the AOC.

The AOC will then review all information and come to a consensus. Depending on the nature of the requested change, this might take more than one meeting and require additional information

from the domain subcommittee and/or the CIO-ASG. Should the AOC approve the change to the domain architecture, the CIO-ASG will coordinate the updating and publication of the revised architecture. Should the AOC decline to approve the change, the CIO-ASG will document and publish the decision. The CIO-ASG will work with the domain subcommittee on any follow-up activities, requests for clarification, etc. requested by the AOC.

Section 5: Identifying and Closing Gaps in a Domain Architecture

As part of their ongoing research, or in reviewing and revising products and technical standards, domain subcommittees will identify "gaps" in domain technologies. Gaps are areas that are nonexistent or inadequate in the current IT environment. For example, gaps may occur as a result of the emergence of a new technology, the merger of existing technologies, or the need to deploy a technology that is non-standard in nature.

Once identified, these gaps should be captured on the Form SCEA-9, Gap Analysis Report from a Domain Subcommittee (found in Appendix 2 of this Guidebook).

This document will be utilized as a reference and planning tool by the CIO IT Planning Office, the CIO-ASG and the AOC. It is important that domain subcommittee chairpersons complete the process on a regularly basis (at least annually) to identify and document gaps in the architecture in order to be beneficial to the IT planning process.

Key Steps in Gap Analysis

1. Complete the identification of differences between the Technology Baseline (or "current state") and the target domain architecture.
2. Analyze gaps between the "as-is" and the target domain architecture.
3. Develop recommendations (actions) to close the gaps.
4. Prioritize recommendations taking into consideration interdependencies of technologies.

Step One – Identifying Domain Gaps

Differences Between Technology Baseline and Target Architecture

A large portion of the gap identification process occurs during the creation of the domain architecture. The domain subcommittee completes the identification of differences between the Technology Baseline (or "current state") and the target domain architecture within the context of strategies, principles, technical standards and product standards. Gaps are identified and become the basis for domain subcommittee activities and recommendations. See Figure 2 below, Example of Gaps for Data Management. The domain subcommittee identifies the technologies needed to satisfy the target domain architecture. Thus, the domain subcommittee must focus on technologies, industry standards and/or products, not how they are used or implemented. The additional work of gap identification focuses on the latter requirements.

Some sources of gaps are:

- Requirements for technical architecture that are not met by current technical infrastructure.
- Policies that do not exist but may be needed.
- Standards do not exist or are out-of-date.
- Products not included in architecture or are out-of-date.
- Ineffective/inconsistent configurations and infrastructure patterns.
- Lack of training in necessary skills.

Other sources of gaps are "overlaps" - needless complexity of products/solutions in the same technology category, and insufficient product standards for implementation.

Using Fundamental Questions

The domain subcommittee may find it useful to focus on the following fundamental questions when discovering gaps:

- What will this (principle, architectural requirement, etc.) mean to us?
- What are its impacts/issues?
- How was the gap revealed and does it impact other parts (i.e., processes, policies, metrics, culture or structure) of the architecture?
- Will the gap create exceptions to the architecture?

Figure 2: Example of Gaps for Data Management

- No policies for decisional data analysis
- No data warehouse
- No repository
- Multiple databases with duplicate data copies — No authoritative source identified
- No standard data movement technology
- No standard data cleansing technology — same data cleansed (using different tools) multiple times for multiple target databases
- Inconsistent usage of query and OLAP tools
- Too many products deployed

Gaps Created by the Exception Process or Agency Project Needs

Given the dynamic nature of technology and changing agency needs, it is likely that solutions using products or standards not covered in a domain architecture will be required. In such cases, the subcommittee should designate these products or standards as gaps and assign them to be researched and reviewed.

Refining Gaps

Once new gaps are identified, the subcommittee should put them into logical groupings and consolidate related gaps. Gaps should be reworded for clarity and reviewed by the entire domain subcommittee to confirm the gap.

Step Two – Analyzing Domain Gaps

Once the gaps have been identified and logically grouped, they need to be analyzed by the subcommittee. The analysis of domain gaps requires creative and collaborative thinking. There is no set procedure for this analytic process.

For each gap identified, the subcommittee should develop alternative solutions to "fill" the gap. For example:

- Is a new solution (application, data, technology) required?
- Is major research including hands-on or Proof of Architecture Assessment required?
- Are new skills required?
- Is a new approach required?
- Is a new implementation of old technology required?

- Are new behaviors required?
- Are new IT policies required?
- Are new or expanded support resources required?

The domain subcommittee should "flesh out" the solution details: description, components, rationale (principles, requirements and gaps being addressed), business benefits, dependencies (if any), and the specific actions steps required to close the gaps. If time permits, the subcommittee should provide sufficient detail in the initiative description for use in future comparisons and capital budgeting process.

For the larger or more complex gaps, it is helpful to consider incremental steps for closing these gaps, and if additional research or information is needed, request assistance from the CIO-ASG.

Step Three – Developing Recommendations

Recommendations on closing the gaps can take many forms. For example:

- Eliminate duplicate and inconsistent databases; functionally duplicate applications; obsolete and unused technology components.
- Enhance and support database sharing.
- Promote shared applications and component reuse.
- Replace nonstandard products/configurations with standard offerings.
- Other changes (e.g., re-training to develop new skills, restructuring working groups or organizations, it policy making).

Step Four – Prioritizing Recommendations

Not all gaps require immediate action, for instance, some gaps:

- Cannot be filled right away,
- Should not be filled (for business reasons),
- May never be filled due to priorities, or
- May be optionally filled by business units or an enterprise effort.

Gaps that require action must have priorities established for them. These priorities can be internal to the domain subcommittee or external, if a project is recommended to fill the gap. This latter prioritization should be done jointly with CIO-ASG. This helps to ensure that the priorities are as consistent as possible with those of enterprise business needs, other active or planned initiatives, and those of other domain subcommittees.

Section 6: Researching New Technologies, Products and Standards

The ongoing activities of domain subcommittees will require access to professional research services. The CIO has contracted with Gartner Group to perform these services. Other research services (e.g. META) are also available on an as needed basis. The CIO-ASG will conduct preliminary research prior to forwarding requests to domain subcommittees. If a subcommittee requires additional information, the chairperson may request that the CIO-ASG obtain additional information or may request the information directly from the research services. This Section of the Guidebook deals with these research activities.

Reasons for Conducting Research

The fundamental reasons for conducting research are a reflection of the original factors that lead to the creation of a domain architecture. These are as follows:

Reviews of Technology in the Marketplace and Technology Trends

One of the primary on-going activities of the members of a domain subcommittee is the regular review of technology trends and changes. Because domain architectures are not static, but adaptive, members must remain current with major changes in technology.

Gap Analysis Activities

Another primary activity of a domain subcommittee is filling known or newly created gaps in the architectures (see Section 5, Identifying and Closing Gaps in a Domain Architecture). In most instances, this will require access to new or additional research.

Technical Compliance Assessment

Another primary activity of a domain subcommittee is to determine if a proposed technology product, application or solution is in compliance with an existing IT enterprise architecture standard.

SCEA Changes

The Enterprise Architecture Framework is not static, but adaptive, though the frequency of changes occurs less often than with domain architectures. The same basic influences on the development of a domain architecture (see Section 3, Developing a New Domain Architecture) can also lead to changes in existing domain architectures:

- Change in enterprise business drivers.
- Change in requirements for enterprise technical architecture.
- Change in enterprise IT principles.
- Additions to or changes in enterprise applications portfolio.

Analysis of the impact of changes on the Enterprise Architecture Framework is the highest priority task of a domain subcommittee and will generally require new or additional research.

New and Planned Projects

Projects often result from federal/state mandates, from needs internal to an agency and from enterprise initiatives. Types of projects that may require additional research include:

- CIO and multi-agency infrastructure projects.
- Multi-agency and single agency IT projects.

Assigned Research

Assigned research is limited duration, topic specific research that is being undertaken by the CIO, a domain subcommittee, workgroup or discipline committee. Assigned research is normally derived from one of the four SCEA processes and is necessary to make or clarify a recommendation for review by the AOC.

Domain Subcommittee Research

What Needs to be Researched

The predominant research topics are trends which produce changes in the domain technologies, product standards or technical standards. Such trends generally require that specific research be undertaken by subcommittees for proposed changes to the domain architecture. Additionally, the gap analysis/closure process often generates a need for specific research. Other research topics are generally assigned by the domain subcommittee chairperson.

How Often Should Technology be Researched

A review date for all standards approved by the AOC will be established when such approval takes place. The domain subcommittee will determine what the review/refresh cycle should be for each standard, and the CIO-ASG will ensure that this schedule is adhered to. The term of the refresh cycle shall be based on the marketplace dynamics for the specific technology involved. However, the review/refresh cycle may be modified if required by a new project or by a request for conformance review by an agency. The need for research may be triggered by any number of such events.

The timing of the tracking of trends and changes in technology is up to the domain subcommittee members and will be based on their own personal styles.

Who Does the Research

Research into trends and changes in technology must be available to all domain subcommittees, workgroups and discipline committees on a timely basis. Such research will initially be conducted by the CIO-ASG through its contract with Gartner Research Services. Additional research may be requested/performed by the domain chairperson as appropriate.

What Sources Should be Used for Research

A variety of sources is available to domain subcommittee members. Subcommittee members, in all likelihood, have specific publication Web sites that they visit on a regular basis. Most manufacturers and most publishers of software have product Web sites, as do standards bodies.

In addition, the State has contracted with Gartner Group for professional research services and can obtain research from META Group on specific topics on an as needed.

Gartner Group

Gartner Group provides research material to the CIO on a regular basis. Subcommittee members interested in seeing this material should contact their domain subcommittee chairpersons. The CIO will consolidate these materials in a library, as well. Specific questions for Gartner Group should be directed to CIO-ASG.

META Group

Meta Group provides a variety of research options ranging from 1-3 pages (called Deltas and Meta Faxes), on up to 20 or more pages (Meta Briefings and Meta Practices). META also offers conference proceedings and teleconference proceedings. The CIO-ASG can acquire materials on specific topics on an as needed basis.

The Research Process

The research process for domain subcommittee research activities has no formal structure. The only requirements are for documentation of the research (see below). The process for research conducted for domain architecture changes that require the approval of the AOC is more highly structured.

Initial Steps in Structured Research

The formal change process starts with a decision to affect a significant change in the domain architecture (see above). After consulting with the CIO-ASG, a domain chairperson prepares a Form SCEA-7, Work Plan for a Domain Subcommittee. A template for this can be found in Appendix 2. By this point in time, the domain subcommittee should have determined the degree of effort required and whether or not hands-on research will be required.

The CIO-ASG will coordinate any resources needed with the CIO's Project Management Services Group to determine the potential impact on CIO or agency projects. The domain subcommittee handles the coordination with other domains that are impacted by the anticipated change to the domain architecture. Domain subcommittee will also maintain the involvement of other domain subcommittees in the review process. Following a short commentary period for the other subcommittees, the domain subcommittee coordinates the reviews and communicates the results to all involved domain chairpersons. At this point, the CIO-ASG will work with the domain subcommittee to resolves any problems with the scope of the research. The domain chairperson assembles a workgroup and appoints a chair. Workgroups may be as small as two or three people, or as large as needed. Workgroup members are generally from the domain subcommittee, unless a non-member is needed because they have special expertise, or because the topic has significant cross-domain impacts.

If a workgroup is established, it should be responsible for conducting the research and evaluation outlined in the action plan. Following the conclusion of the research and evaluation, the workgroup prepares a preliminary report and recommendation (the Form SCEA-8, Recommended Action by a Domain Subcommittee) and submits/presents it to the

entire domain subcommittee for review and comment. Once a final version has been approved by the domain subcommittee, the chairperson forwards the SCEA-8 to CIO-ASG for review and for a peer review by the other domain chairpersons. The chairpersons make recommendations for adjusting the SCEA-8 and proceed to the next step in the process. The nature of the next step will depend on whether additional research is needed.

Outcomes from Research

Category of Change

- Creating new principles, disciplines, and technical or product standards.
- Moving a technical or product standard between categories, (e.g., from mainstream to containment or from containment to retirement).
- Editing or modifying principles.
- Updating the version of an existing technical or product standard.
- Adding a new discipline to the domain architecture.

Documentation Requirements

Various reports must be completed by the domain subcommittee chairperson each month, depending on the activities occurring during that month, including:

SCEA-6 Status Report for Domain Subcommittee
SCEA-7 Work Plan for Domain Subcommittee, and
SCEA-8 Recommended Action by a Domain Subcommittee.

Section 7: Coordination with IT Planning and IT Procurement

Decisions made by the Architecture Oversight Committee (AOC) will be distributed to both the IT Planning and IT Procurement Groups. The IT Planning Group will use this information to evaluate agencies' IT plans and planning requests. This information will become the basis for the state's information technology plan. The IT Procurement Group will use this information to develop state term contracts for products that conform to the standards established by the AOC, and also to assist agencies in conducting procurement related activities such as:

- Developing IT procurement and contract requirements,
- Making buy-versus-develop decisions,
- Determining evaluation criteria in RFPs,
- Upgrading hardware and infrastructure,
- Selecting software package and/or tools, and
- Making design decisions in the context of a specific IT project or application system.

From time to time, domain subcommittee members may even be asked to review Requests for Proposals (RFPs), vendor responses to RFPs, agency IT architectures and/or agency IT projects. This can be accomplished as an individual or as a team effort. The reviews will assess and evaluate conformance of projects or proposals to SCEA business drivers, IT principles, and domain principles, standards and guidelines.

IT Planning Processes

The IT Planning Group will follow its standard practices in evaluating IT plans and planning requests. If this Group determines that a plan and request is in compliance with SCEA standards, it will approve this plan or request, and no action is required by the domain subcommittee or the AOC. If not in compliance with SCEA standards, the IT Planning Group will first attempt to resolve any differences with the agency. If this effort is unsuccessful, the IT Planning Group will submit the plan or request to the appropriate domain subcommittee for review and action. Existing domain architecture documents shall serve as a basis for such evaluations. Such reviews should evaluate conformance of the plan or request to SCEA principles, domain architecture principles, technical and product standards, and best practices.

IT Procurement Coordination

There may be a need for a domain subcommittee to assist the IT Procurement staff in developing or reviewing technical specifications, providing clarifications to vendors regarding specific RFP requirements and evaluating responses to RFPs. If a review is requested by the IT Procurement Group, a list of questions will be provided to the domain chairperson with reference to specific documents, sections, etc., along with a description of the assistance needed. The IT Procurement Group will provide specific guidance to the domain subcommittee chairperson as to the approach and content of the desired deliverables.

Appendix 1: Glossary of Abbreviations

Explanation of Abbreviations:

AOC	Architecture Oversight Committee
CIO	Division of State Chief Information Officer
CIO-ASG	Division of State Chief Information Officer – Architecture Support Group
CTO	Chief Technology Officer
IT Planning	IT Planning Group
PMSG	Project Management Services Group
SCEA	South Carolina Enterprise Architecture
RFP	Request for Proposal
SOW	Statement of Work

Appendix 2: Templates/Processes for Domain Subcommittee Activities

Form SCEA-1

Tracking Number:

REQUEST FOR ASSESSMENT OF TECHNICAL ARCHITECTURE

This form is to be used for the following purposes: (1) to recommend a technology product, application or solution for inclusion in the technical architecture; (2) to recommend an update to a product, application or solution that is currently included in the technical architecture; or (3) to determine if a product, application or solution is in compliance with the existing technical architecture. Once, complete, the requester may submit this form either manually or electronically to the Division of the State Chief Information Officer. Where possible, additional information should be submitted to enhance assessment. This additional information may also be submitted with this form either manually or electronically. If submitting information manually, mail to: Division of State CIO, 1201 Main Street, Suit 820, Columbia, SC 29201.

BASIC INFORMATION (required for all requests):

Name of Requestor:	Submittal Date:
Agency:	Telephone Number:
Address:	Email Address:
Position:	Fax Number:
Architecture Domain:	Discipline:
Agency Director/Committee Chair Authorization: (if applicable)	

TYPE REQUEST (required for all requests):

Change to Existing Technical Architecture: ❑ Addition to Technology Architecture ❑ Update to the Existing Technology Architecture
❑ Assessment of Compliance with Existing Technology Architecture

IF ADDITION TO TECHNOLOGY ARCHITECTURE ONLY - PROPOSED TITLE/NAME:
(The title or name should uniquely identify the technology to be assessed. It might include product name, copyright owner, version/release identification, etc.)

PRIORITY (required for all requests):

❑ High Priority (s*ignificant impact on agency operation*)
❑ Medium Priority (*normal processing*)
❑ Low Priority *(can be delayed if necessary)*

DESCRIPTION OF TECHNOLOGY TO BE ASSESSED FOR COMPLIANCE ONLY:
(Provide a description of the technology to be assessed for compliance with an existing technical architecture standard)

Describe the proposed addition/change to the technology architecture:
Describe any known areas in which this technology may conflict with existing technical architecture standards:
Describe the current base of installation and history associated with its implementation:
Identify additional requirements for the implementation of this technology:
Identify where the technical expertise necessary to manage this proposed technology will be acquired:
Provide other information as appropriate:

PURPOSE, PRIORITY AND CONSTRAINTS/MANDATES (required for all requests):
(Describe briefly the need or problem being addressed with this technology from the agency perspective)

Describe areas or processes to which the technology would be applied:

Describe any changes in business processes that would result from the adoption of the technology as a standard:
Describe the degree to which the adoption of this proposed standard might impact suppliers, peers, customers, or clients:
Proposed addition/change significantly altering the meaning or intent of which principle, technical standard or product standard?
How will proposed addition/change impact the status of a product, i.e. from mainstream to containment, from emerging to mainstream, from containment to obsolete or introducing a new product as emerging?
Provide other information as appropriate:

IMPACT ON OTHER DOMAINS (required for all requests): *(if known, what is the requestor's estimate of the impact of an assessment of technical compliance on the any of the following domains and their disciplines)*

Presentation Services:
Communication Services:
Middleware and Messaging:
Computing Services:
Enterprise Applications:
Systems Management Services:

FINANCIAL IMPACT (required for all requests):

What do you expect this implementation to cost, over what time period:
What are you currently spending to perform this function:
If savings and efficiencies are anticipated, identify the efficiencies, the estimated amount of savings, and if known, the source(s), over what period of time and whether or these cost savings are recurring.
If known, what is your peer group/benchmark spending, using what technology: *(identify source(s) of data)*

***MIGRATION CONSIDERATIONS (if any*)**: (outline your migration strategy, including timetable and resource requirements.)

ADDITIONAL BACKGROUND: *(List evaluation criteria, alternatives considered, and any other pertinent information and analysis used in preparing this proposal)*

Figure 1. Technical Compliance Assessment Process

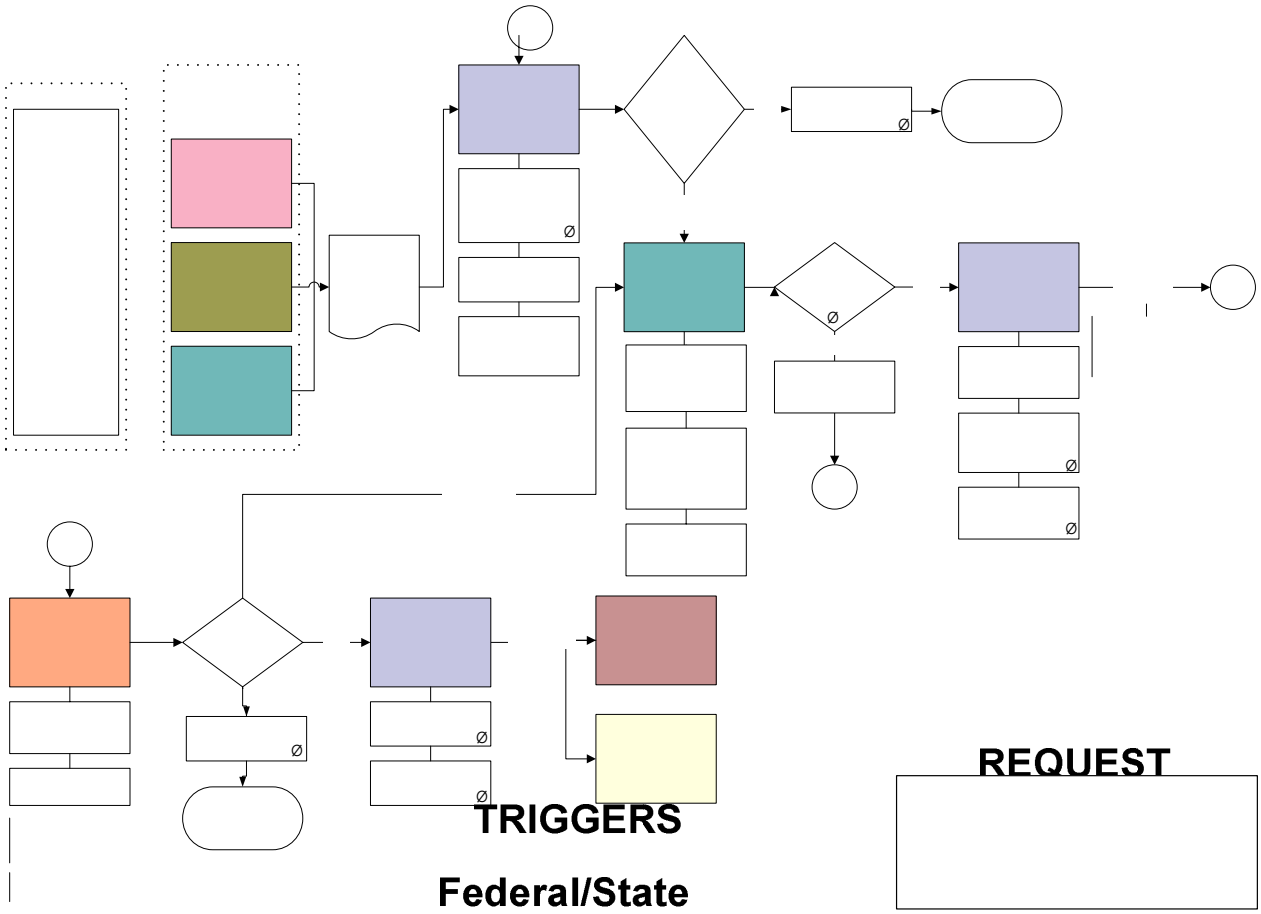
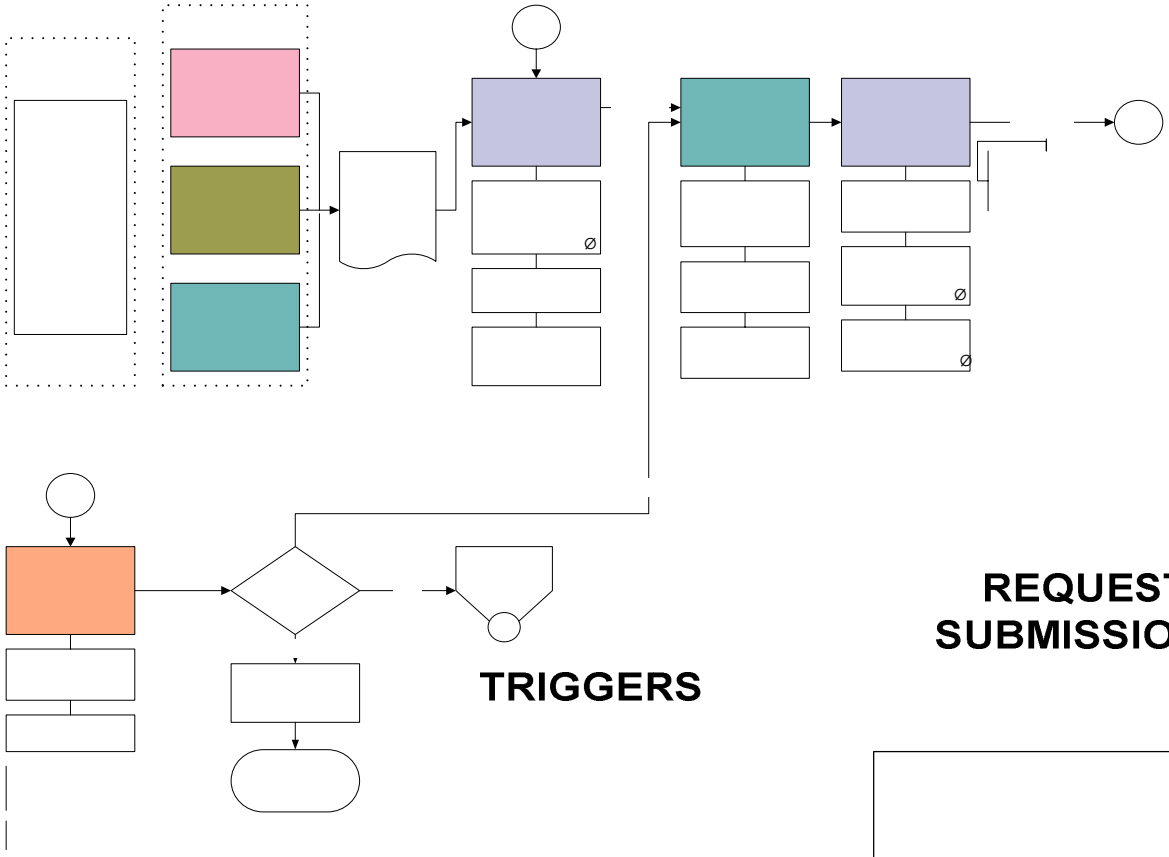


Figure 2: Request for Change to Existing Technical Architecture Process



Form SCEA-2

Tracking Number:

REQUEST FOR WAIVER/EXCEPTION TO TECHNICAL ARCHITECTURE

This form is to be used for the purpose of requesting a waiver or exception to a technology product, application or solution that is currently included in the technical architecture. Once, complete, the requester may submit this form either manually or electronically to the Division of the State Chief Information Officer. Where possible, additional information should be submitted to enhance assessment. This additional information may be submitted with this form either manually or electronically. If submitting information manually, mail to: Division of State CIO, 1201 Main Street, Suit 820, Columbia, SC 29201.

BASIC INFORMATION (required for all requests):

Name of Requestor:	Submittal Date:
Agency:	Telephone Number:
Address:	Email Address:
Position:	Fax Number:
Architecture Domain:	Discipline:
Agency Director/Committee Chair Authorization: (if applicable)	

IDENTIFICATION OF TECHNICAL STANDARD TO BE WAIVED/EXCEPTED:

SCOPE OF THE PROPOSED WAIVER/EXCEPTION: *(Provide a description of the waver/exception, include the impact on introducing a non-standard technology on existing applications, infrastructure, and resources)*

REASON FOR WAIVER/EXCEPTION:

❑ Federal/State Mandate
❑ New technology products/application
❑ Special agency requirements
❑ Grant requirements
❑ Technology Project
❑ Other (please specify)

PRIORTY:

❑ High Priority (s*ignificant impact on agency operation*)
❑ Medium Priority (*normal processing*)
❑ Low Priority *(can be delayed if necessary)*

IMPACT ON OTHER DOMAINS: *(if known, what is the requestors estimate of the impact of an assessment of technical compliance on the following domains and their disciplines)*

Presentation Services:
Communication Services:
Middleware and Messaging:
Computing Services:
Enterprise Applications:
Systems Management Services:

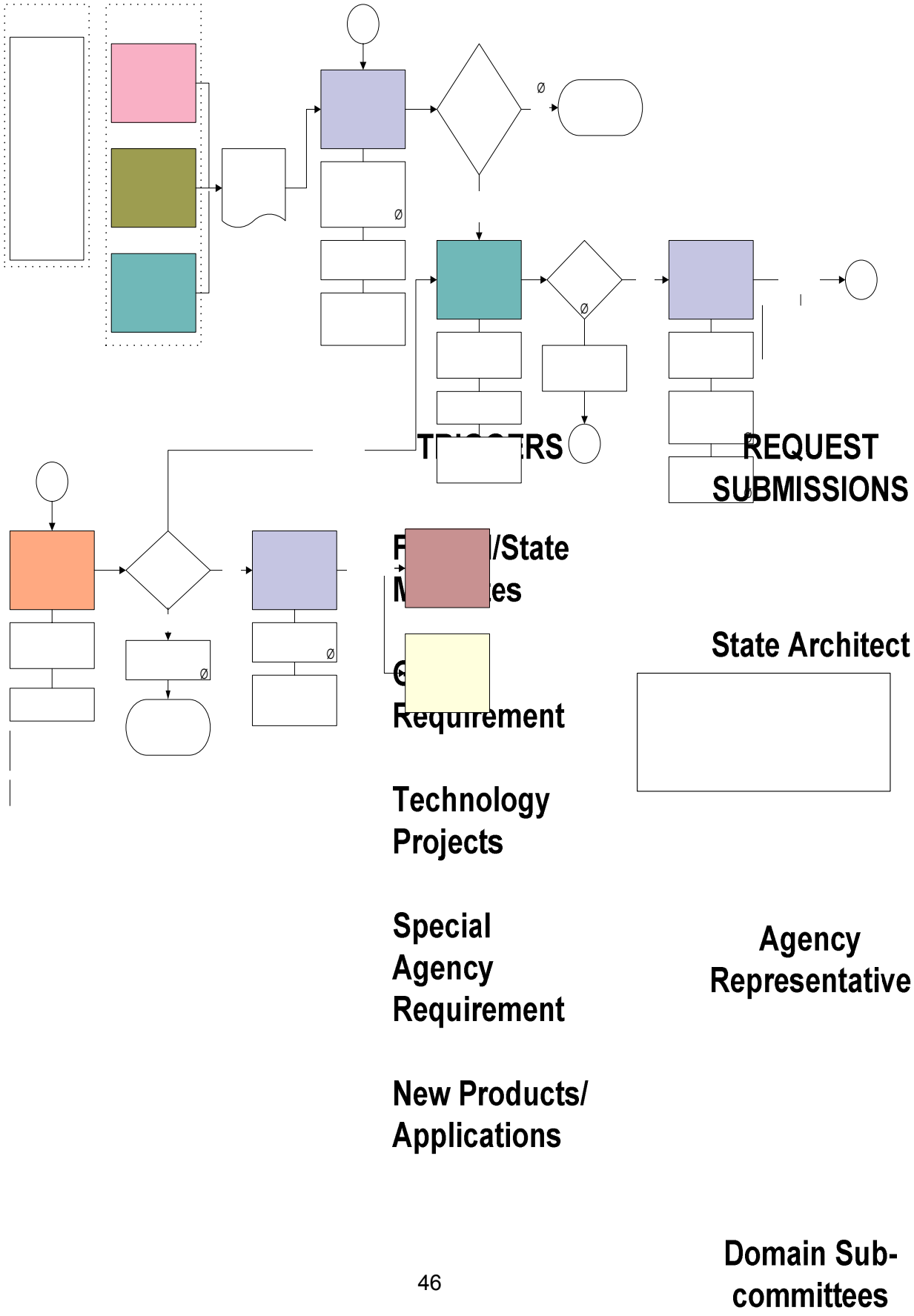
BUSINESS JUSTIFICATION FOR WAIVER/EXCEPTION:

FINANCIAL IMPACT:

What is the estimated financial impact of this waiver/exemption:
What are you currently spending to perform this function:
If know, identify the source(s) and amount(s) of savings associated with this waiver/exemption:

ADDITIONAL BACKGROUND: *(List pertinent information and analysis used in preparing this proposal)*

Figure 3: Request for Waiver/Exception Process



Form SCEA-3

Appeal Number: **Original Tracking Number:**

REQUEST FOR APPEAL OF TECHNICAL ARCHITECTURE DECISION

This form is to be used to request a review or hearing on a previous decision by the Architecture Oversight Committee. Once, complete, the requester may submit this form either manually or electronically to the Division of the State Chief Information Officer. Where possible, additional information should be submitted to enhance assessment. This additional information may be submitted with this form either manually or electronically. If submitting information manually, mail to: Division of State CIO, 1201 Main Street, Suit 820, Columbia, SC 29201.

BASIC INFORMATION (required for all requests):

Name of Requestor:	Submittal Date:
Agency:	Telephone Number:
Address:	Email Address:
Position:	Fax Number:
Architecture Domain:	Discipline:
Agency Director/Committee Chair Authorization: (if applicable)	

SCOPE OF APPEAL: *(Provide a description of the appeal, address specific issues and/or concerns that would impact a previous decision made by the Architecture Oversight Committee)*

PRIORTY:

❑ High Priority (s*ignificant impact on agency operation*)
❑ Medium Priority (*normal processing*)
❑ Low Priority *(can be delayed if necessary)*

REASONS FOR THE APPEAL:

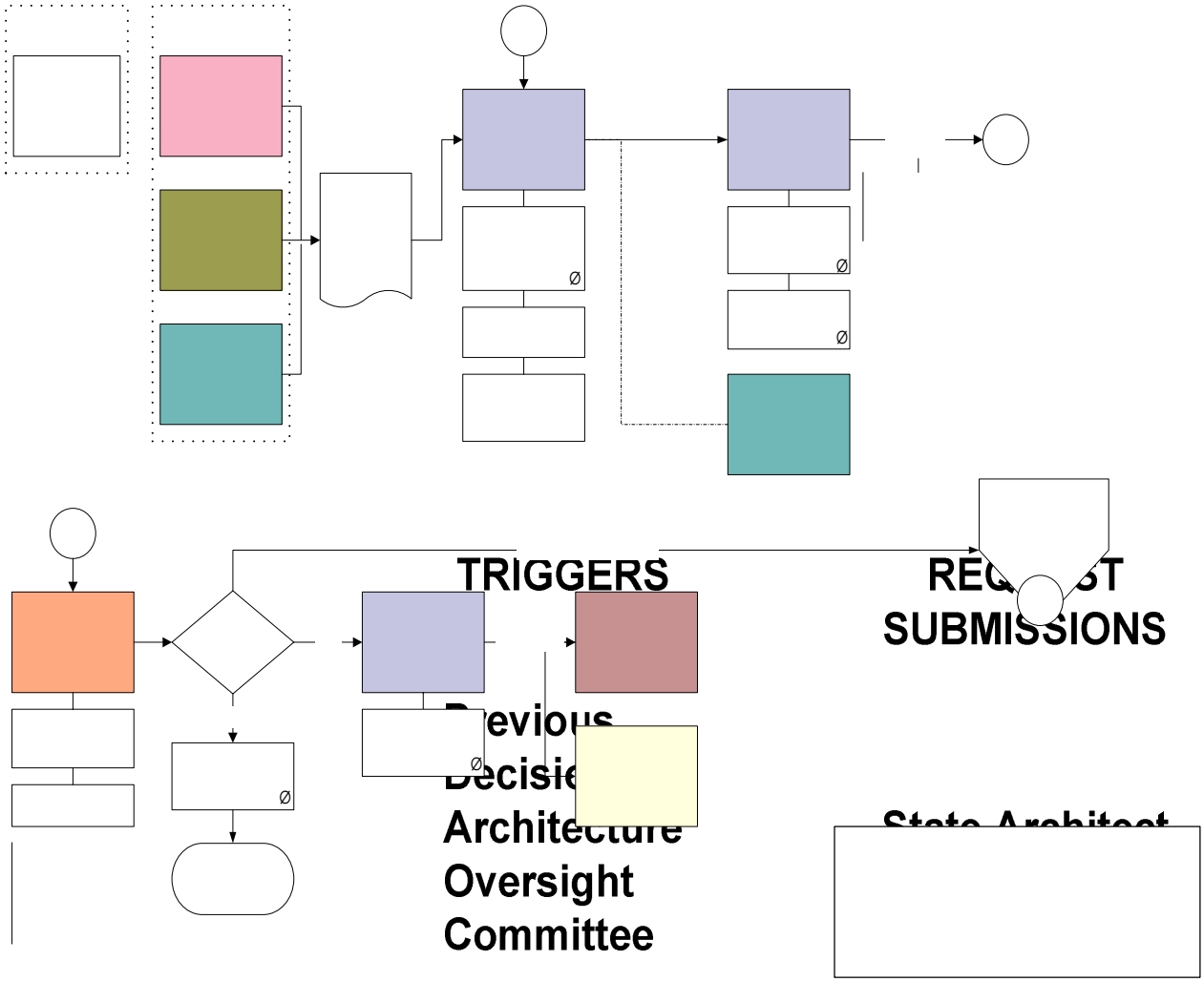
Addresses issues/concerns outlined in the original decision.

Describe any additional relevant information regarding the appeal.

BUSINESS JUSTIFICATION FOR APPEAL:

ADDITIONAL BACKGROUND: *(List pertinent information and analysis used in preparing this appeal)*

Figure 4: Appeal of Technical Architecture Decision Process



Form SCEA-4

DOMAIN PROFILE

DISCIPLINES

DOMAIN STRATEGY

DOMAIN PRINCIPLES/BOUNDARIES

Form SCEA-5

DISCIPLINE PROFILE

Discipline Boundaries:

Discipline Roadmap For:

Current	2 Years	5 Years	
Baseline Environment	**Tactical Deployment**	**Strategic Direction**	
		Shared	**Agency**

Retirement Targets	**Mainstream Platforms** (must be supported)
Containment Targets (fully supported but no new development)	**Emerging Platforms**

Implications and Dependencies

Roadmap Notes

DISCIPLINE PROFILE

Discipline Standards:

Migration Considerations:

Exception Considerations:

Miscellaneous Notes:

Date Last Updated:

Form SCEA-6

STATUS REPORT FROM A DOMAIN SUBCOMMITTEE

Meeting Information

Meeting Date and Time:

Domain Subcommittee:

Subcommittee Chairperson:

Members Attending the Meeting:

Meeting Details

Meeting Agenda

Adapt as needed, but these should be probable items.

- member reports on on-going research
- workgroup status reports (if any)
- discipline committee reports (if any)
- action items
- new business

Results of On-Going Research

Briefly, describe results and recommendations from on-going research.

Subcommittee Status Reports

Briefly, describe status of any subcommittee activities.

Recommendations to be Submitted to AOC

Use this space to describe recommendations by the subcommittee for proposed changes to the domain architecture

Action Items

Use this space to report on items needed resolution, next steps needed, etc.

Comments

Use this space for any comments, suggestions, etc.

Form SCEA-7

WORK PLAN FOR DOMAIN SUBCOMMITTEE

Priority	Description	Req. No.	Date Received	Received From	Assigned To	Projected Completion Date

Priority	Description
1	Critical/emergency request submitted by an agency or the AOC. These requests take precedence over other issues until they are resolved (e.g., a time critical Federal or regulatory mandate or a legislative directive with a short implementation timeframe).
2	Expedited request, the delay of which would hinder normal operations of an agency or the enterprise.
3	Request involving an issue (e.g. change of software version from containment to retirement) that does not hinder an agency's ability to operate.
4	Request representing an issue that will take a significant time commitment to complete (e.g. evaluate new line of products) and for which there is no pressing deadline.
5	All other requests.

Form SCEA-8

RECOMMENDED ACTION BY A DOMAIN SUBCOMMITTEE

Basic Information

Submittal Date:

Domain Subcommittee:

Subcommittee Chairperson:

Contact Information (phone or email):

Scope of the Change

Description

Provide a description of the requested/proposed change.

Priority and Time Frame

Indicate the priority of this change – if it needs to be expedited, explain why and indicate date needed.

Architectural Impact

Briefly describe impact on domain architecture and SCEA. Also, indicate if there will be any impact on other domains.

Financial Impact

Provide estimated financial impact of the proposed change, if available. Include TCO analysis when possible.

Need or Justification (may be more than one)

Check the reason for requested change. If there is more than one reason for the requested change, check all appropriate boxes. (Copy this ✔ and paste over the box)

- ❑ Domain subcommittee technology research activities
- ❑ Domain subcommittee gap analysis activities
- ❑ Agency project
- ❑ Agency waiver/exception process
- ❑ Change in enterprise strategies and/or business direction
- ❑ Infrastructure implementation or proposed CIO service offering
- ❑ Appeal of AOC decision

❑ Other (please specify _____)

Summary of Research Performed

Type of Research

Summarize the research that supports the subcommittee's recommendation. Attach copies of research, if appropriate.

Scope of the research

Describe the scope of the research. Indicate workgroups or discipline committees involved in this research.

Describe any alternative standards or products considered by the subcommittee.

Recommendation(s)

YES – change the domain architecture as follows (attach domain or discipline profiles as appropriate):

Domain architecture strategies/principles

Discipline profiles (technology standards, product standards, life cycle designation, etc.)

NO – action not recommended at this time

High risk, technology not mature – continue tracking

Needs further evaluation

Inconclusive results/insufficient information at this time

Negative evaluation or results

Other (specify)

Dissenting Opinions

Summarize dissenting opinions from members of domain subcommittee, workgroup or discipline committee, if any.

Agency Position/Comments

Briefly indicate agency's desired outcome if different from recommendation of domain subcommittee.

Form SCEA-9

GAP ANALYSIS REPORT FROM A DOMAIN SUBCOMMITTEE

Note: This is in Excel spreadsheet format

Basic Information

Meeting Date and Time:

Domain Subcommittee:

Subcommittee Chairperson:

Members attending the meeting

Instructions

Column A	Planning Category	attempt to group similar gap items that could be incorporated in the same (future) plan
Column B	Gap Description	brief description of the gap item (or a label)
Column C	Priority	relative priority within the domain for resolving the gap item; ranked from **A** highest to **C** lowest
Column D	Cross Reference	list of other gap items that are related or linked to this gap item, based on the gaps identified in the domain architecture document
Column E	Short List	gap items to be acted upon first (low hanging fruit, most impact, etc.)
Column F	Order	used to order the short list and remaining gaps as part of the planning process
Column G	Domain Principles Supported	list of domain principles supported by resolving the gap
Column H	Comment/Action Item	indicate how the gap will be resolved, and any other comments that are relevant; this cell can include historical actions
Column I	Skills	skills required as an aide to resource planning and assignment of subcommittee members to activities or research

Planning Category	GAP	Priority	Cross Reference	Short List	Order	Domain Principles Supported	Comment/Action Item	Skills Required

Appendix 3: Summary of Roles and Responsibilities

Architecture Oversight Committee

The Architecture Oversight Committee (AOC) is responsible for the review and approval of technical standards, and for the promotion of the SCEA statewide. Its membership is made up of senior IT leaders and senior agency management personnel. The AOC approves domain subcommittee recommendations/deliverables (i.e., technical standards, design principles, product standards, best practices, and standardized configurations) and adjudicates exceptions to architecture standards and appeals of architecture decisions. The AOC is chaired by the State's Chief Technology Officer.

Responsibilities include:

- Maintaining the SCEA process discipline and sponsoring new and revised standards.
- Approving domain subcommittee deliverables that impact agencies (i.e. technical standards. design principles, product standards, best practices and standardized configurations).
- Adjudicating appeals for exceptions to architecture standards.
- Reviewing domain and Architecture Oversight Committee initiatives and recommend priorities.
- Reviewing possible infrastructure impacts of planned projects.
- Utilizing SCEA teams as a resource in understanding domain deliverables.

Domain Subcommittees

The domain subcommittees provide the knowledge and expertise required to develop the technical architectures and standards for the enterprise architecture process. Each subcommittee consists of technical experts from across the State. These subcommittees are responsible for the development and maintenance of Domain Architecture Documents, including the domain specific deliverables (i.e. domain principles, technical standards, product standards, and best practices), and administrative documents such as meeting minutes, action plans, gap analyses, etc. The subcommittees are expected to keep abreast of new technology and make recommendations on new technology to close gaps in the current environment.

CIO Architecture Support Group (CIO-ASG)

The CIO Architecture Support Group coordinates the SCEA process and all associated activities. This Group is responsible for coordinating/supporting all domain subcommittee, as well as communications and web site content/maintenance.

Responsibilities of the CIO Architecture Support Group include:

- Ongoing enhancement, communication and governance of SCEA.
- Coordination of activities and deliverables between domain subcommittees.
- Coordination and quality assurance of deliverables and presentations to AOC.
- Provide staff support to AOC and the domain subcommittees.
- Coordinating publication of domain architecture documents.

- Conduct research and coordinating the use of research services by the AOC and the domain subcommittees.

Project Management Services Group (PMSG)

The PMSG exists at the enterprise level to coordinate and monitor major IT projects. CIO personnel staff this Office

Responsibilities include:

- Establish and promote the use of a standard project management methodology including forms, templates, reports, etc.
- Monitor the state's portfolio of major IT projects reviewing standard reports and providing the CIO and agency management with recommendations on project activities.
- Develop project management training and certification programs for state employees.
- Provide project management services upon request by an agency and for enterprise projects.

APPENDIX A: GLOSSARY/LEXICON

The glossary provides the definitions for critical terminology as used in this Tool-Kit.

Term	Definition
Adaptive	Able to support a wide variety of applications and evolve as technology changes.
Agency	A governmental unit – in the narrowest sense, a governmental unit of the executive branch.
Approach	Approaches are devised to deliver work products that are consistent. An approach can be project specific or apply to the enterprise as a whole. For example, use of Unified Modeling Language (UML) case models *versus* entity relationship diagrams. These may be viewed as two different approaches for information modeling. *(see http://www.uml.org/)*
Architecture Blueprint	The dynamic detail of the business, information or technology captured utilizing standardized, structured processes and templates. This is the actual content. Typically this is implemented and communicated using visual modeling tools.
Architecture Framework	The combination of structured processes, templates and governance that facilitate the documentation of the architecture in a systematic manner.
Architecture Governance	The processes necessary to direct or guide initiatives, to ensure that performance aligns with the enterprise, to enable the enterprise business by exploiting opportunities, and to ensure resources are used responsibly and architecture-related risks are managed appropriately.
Architectural Patterns	The expression of a fundamental structural organization or schema for a system or solution. It provides a set of predefined subsystems, specifies their responsibilities, and includes rules and guidelines for organizing the relationships between them.
Artifact	The whole of the individual pieces of data captured on a template. Each populated architecture document is considered an artifact. Each Architecture Blueprint contains multiple artifacts. Artifacts constitute any object, or work product that is developed as a component of the enterprise architecture. Artifacts include trends, principles, mission, goals, objectives, strategies, capabilities, processes, process steps, entities, attributes, relationships, subject areas, application components, applications, data bases, etc.
Baseline	The current or "as is" state of the business, information or technology environment, captured in a set of graphic and textual models.
Benchmark	A set of conditions against which a product or system is measured. A benchmarking instrument was developed and implemented to determine the readiness of municipal, county and state governments to adopt the national architecture model.

Term	Definition
Best Practices	Trends and approaches that are successful at providing services and information over time.
Blueprint	The dynamic content of a given architecture that is captured utilizing standardized, structured processes and templates..
Business Architect	An individual responsible for developing business architecture frameworks, components, and blueprints based on stated business strategies and goals. Specific responsibilities and contributions to Enterprise Architecture include: ▪ Understanding current business architecture. ▪ Producing new business objects and process models. ▪ Developing and communicating the new business architecture: ▪ Identifying and developing a business case and strategy for future applications. ▪ Determining the major components of the reengineered business enterprise. ▪ Determining the mechanisms by which these components will collaborate in order to fulfill its operational and quality requirements.
Business Architecture	An architecture within EA that provides the high-level representation of the business strategies, intentions, functions, processes, information and assets critical to providing services to citizens, businesses, governments and the like. Business architecture should include an environmental context, market or need assessment, strategic business intent, traceability to capabilities and the management initiatives that will deliver or further leverage those enabling capabilities. Business architecture is defined by some as constituting the top two rows of the Zachman Framework. *(see www.zifa.com)*
Business Architecture Component	Elements of the Business Architecture Blueprint that specifically identify what information, service, location/logistics, organizational roles/responsibilities, and strategies will be used for implementation of the Business Domain.
Business Architecture Framework	The combination of templates and structured processes that facilitate the documentation of the enterprise's business artifacts (e.g., strategies, processes, events) in a systematic and disciplined manner.

Term	Definition
Business Domain	• A functional or topical subset of the business operations that is integral to the success of the enterprise. Examples of Domains might include: – Functional Domains • Education • Health and Social Services • Justice and Public Protection • Resource and Economic Development • Transportation and Engineering – Topical Domains • Customer • Location • Payments
Business Domain Model	A graphical representation for describing business operations of the enterprise, independent of the agencies, bureaus, departments and/or offices that perform the operations or provide the services.
Business Drivers	Organizational and environmental influences on business and technology that are captured within the architecture to show their acceptance and adoptability into the environment. Internal goals and strategies and external trends that influence the business. Three common categories of Business Drivers include Principles, Best Practices and Trends.
Business Perspective	A breakdown of the Business Domain based on a specific viewpoint, such as Who, What, Where, When, Why, How, or a logical combination of one or more of these viewpoints.
Business Portfolio	Refers to the implemented baseline business environment (i.e. implemented business processes, strategies and data of the business organization).
Cardinality	Cardinality helps describe the nature of a relationship between two entities. A relationship's cardinality is the number of objects on one side of a relationship that may be related with objects on the other side.
Component	Within this Tool-Kit, component refers to a level of architectural detail. Within each of the allied architectures, the component level detail is captured utilizing a respective template. Examples of component levels addressed in this version of Tool-Kit include: Business Architecture - Business Architecture Component Information Architecture – Process Component and Information Meta Component Technology Architecture – Product Component and Compliance Component

Term	Definition
Concept for Operations	A description, at a relatively high level, of the participants in information sharing, the information flows involved and the functional requirements at each step of sharing.
Conceptual Information Model	A diagram and it related narrative that defines the functional requirements and the business users' view of the information at a conceptual level.
Conceptual Patterns	A pattern whose form is described by means of terms and concepts from a business, technology or application domain.
Current Technologies	Technologies that are the current standard for use within the enterprise, tested and generally accepted as standard by industry. These items comply with or support the principles listed for the discipline.
Data	The atomic bits of fact that constitute the raw material of knowing about our business. The home address of a single person is data. It is atomic (not divisible) because to divide it renders it useless.[1]
Data Element	A unit of data for which the definition, identification, representation, and permissible values are specified by the means of a set of attributes[2]
Data element Concept	An object, any part of the conceivable or perceivable work, that can be represented in the form of a data element, described independently of any particular representation (the combination of a value domain, data type, and if necessary, a unit of measure or a character set.)[3]
Design Patterns	Structure that provides a scheme for refining the subsystems or components of a system, or the relationships between them. It describes commonly recurring structure of communicating components that solves a general design problem within a particular context.
Digital-Government	In the NASCIO publication *Citizen-Centric Digital Government,* Digital Government is defined as "the electronic delivery of government services via the Internet". A broader definition can include all electronic transactions, regardless of whether they occur on the Internet or another device.
Discipline	Logical functional areas to address when building the architecture blueprint. The descriptions of the disciplines used in this document are found in Appendix B.
Domain	High-level logical groupings of functional or topical operations that form the main building blocks within the architectural framework.

[1] Mosshamer, E. L., A Word on Semantics: Data, Information, Knowledge, Insight, Illinois Mathematics and Science Academy
[2] ISO/IEC 11179-1:1999(E)
[3] ISO/IEC 11179-1:1999(E)

Term	Definition
e-Business	Electronic-business; conducting business online. The term is often used synonymously with e-commerce, but e-business encompasses more than just buying and selling of products on the Web.
Emerging Technologies	The most current technologies. These items will usually require testing prior to acceptance by industry as the current standard. It is generally understood that emerging technologies be considered carefully before implementing in an enterprise-wide architecture.
Enterprise	Represents an organization in total, including all subordinate entities, encompassing corporations, small businesses, non-profit institutions, government bodies, as well as other kinds of organizations.
Enterprise Architecture	Enterprise architecture defines an enterprise-wide, integrated set of components that incorporates strategic business thinking, information assets, and the technical infrastructure of an enterprise to promote information sharing across agency and organizational boundaries. The Enterprise Architecture is supported by Architecture Governance and the allied architectures of, Business, Information, Technology and Solution Architectures.
Enterprise Architecture Development Tool-Kit	A guide for municipal, county, state and federal government to develop and define adaptive enterprise architecture. Includes process models and templates with several examples.
Enterprise Architecture Portfolio	A consolidated view of the relationships, packages or patterns built from the disparate Business, Information, and Technology components. Often, the packages are referred to as application and infrastructure patterns. In addition, application profiles and technology services are also grouped and presented as a cross view of the specific, individual architecture components
Entity	Individual people, places, concepts, things and events about which the enterprise needs to store and maintain information.
Framework	The combination of the templates and structured processes that facilitate the documentation of the architecture in a systematic and disciplined manner. In this Tool-Kit, the term Architecture Framework is used to refer to the combination of the structural elements of the architecture, such as the structure of the Blueprint, the templates and the structured processes for documenting, reviewing communicating, implementing and maintaining the architecture. However, there are other definitions of framework. In many methodologies, the framework only depicts relationships between methodological work products. This is the case with the Zachman Framework *(see www.zifa.com)*. In this case, the Zachman *Framework* does not include a methodology for navigating through the framework. Rather, the Zachman Framework only shows relationships among work products and various perspectives – who, what, where, when, how, why – at various levels of abstraction.

Term	Definition
Function	A major work element that accomplishes the mission or business of an organization, such as accounting, marketing, etc. A sub-function is defined as a component of a function such as accounts receivable, accounts payable, etc. within the accounting function.
Gap	The differences between the "baseline" environment and the "target" environment.
HIPAA	Acronym for the Health Insurance Portability and Accountability Act of 1996, which addresses such items as privacy and electronic sharing of information.
Information	The organization of data into usable formats. Information encompasses both structured (data marts, databases, database tables and data exchanges) and unstructured information (web content, jpeg or video files, and documents).
Information Architect	An individual responsible for developing information architecture frameworks, components, and blueprints based on stated information strategies and goals. Specific responsibilities and contributions to Enterprise Architecture include: ▪ Determining information components needed for the enterprise, business applications, and processes. ▪ Determining the overall structure of the information components. ▪ Identifying requirements necessary to support and integration the business at the information level.
Information Architecture	The compilation of the business requirements of the enterprise, the information, process entities and integration that drive the business and rules for selecting, building and maintaining that information. This includes data and process architecture.
Information Relationship	The description of how one Entity/Class is related to another.
Information Subject Area	Topical or functional subset of the business processes that is integral to the operations of the enterprise such as Customer, Product/Service, etc.
Infrastructure	The basic, fundamental architecture of the system that supports the flow and processing of information, determines how it functions and how flexible it is to meet future requirements.
Integration	The ability to access and exchange critical information electronically at key decision points throughout the enterprise.
Interoperability	*Interoperability:* The ability of a system or a product to work with other systems or products without special effort on the part of the customer, either by adhering to published interface standards or by making use of a "broker" of services that can convert one product's interface into another product's interface "on the fly"[4]

[4] http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci212372,00.html

Term	Definition
IEEE	Institute of Electrical and Electronics Engineers, involved with setting standards for computers and communications.
ISO	The International Organization for Standardization, Geneva, is an organization that sets international standards. The U.S. member body is ANSI.
Legacy systems	An automated system built with older technology that may be unstructured, lacking in modularity, documentation and even source code.
Logical Information Model	Shows the main functional [information] components and their relationships within a system, independent of the technical detail of how the functionality is implemented.[5]
Mandate	An authoritative command or instruction.
Metadata	Literally, "data about data." Metadata includes data associated with either an information system or an information object, for purposes of description, administration, legal requirements, technical functionality, use and usage, and preservation.[6] Therefore, metadata gives us detail about both what the data means and how it's stated. Metadata is one of the greatest critical success factors to sharing information because it provides business users, developers and data administrators with consistent descriptions of the enterprise's information assets.
Methodology	A technique with a set stages of distinct, structured rules of application and a set of heuristics for judging when the various stages are complete. A methodology incorporates a management process in addition to the technical process in the determination of a workable solution. It is not NASCIO's intent to prescribe a methodology, but rather to provide examples of the processes and steps that are important to address as organizations develop their own EA Programs
Middleware	Systems integration software for distributed processing and database and user interfaces.
Migration	The evolution from the baseline to the target state.
Model	The graphical representation or simulation of a process, relationship or information, along with the narrative that supports the diagram.
NASCIO	The National Association of State Chief Information Officers represents state chief information officers and information resource executives and managers from the 50 states, six U. S. territories and the District of Columbia. State members are senior officials from any of the three branches of state government who have executive-level and statewide responsibility for information resource management.

[5] http://msdn.microsoft.com/architecture/enterprise/default.aspx?pull=/library/en-us/dnea/html/eaarchover.asp#eaarchover_topic3
[6] http://www.getty.edu/research/conducting_research/standards/intrometadata/4_glossary/index.html

Term	Definition
Policies	The rules and regulations set by the organization. Policy determines the type of internal and external information resources employees can access, the kinds of programs they may install on their own computers, as well as their authority for reserving network resources.
Principle	A statement of preferred direction or practice. Principles constitute the rules, constraints and behaviors that a bureau, agency or organization will abide by in its daily activities over a long period. Business practices and approaches that the organization chooses to institutionalize to better all provided services and information.
Proprietary	Owned by a private individual or corporation.
Protocol	Rules governing transmitting and receiving of data.
Repository	An information system used to store and access architectural information, relationships among the information elements, and work products.[7]
Scalability	The ability to use the same applications and systems on all classes of computers from personal computers to supercomputers.
Solution Architect	An individual responsible for developing solution architecture frameworks and solution set designs. The solution architect's primary role is to translate what is required to run the business (from the Business and Information Architecture gaps and migration strategies) into actual design specifications and models that can be supported and fulfilled by components within the Technology Architecture.
Solution Architecture	An architecture within EA that guides the solution architect in the design of a particulate solution set. For each solution set, Solution Architecture assists in: ▪ The identification of business requirements, ▪ The determination of the design specifications necessary to deliver the business requirements, ▪ The development of the solution set design. Integrating designs based on details with the Business, Information and Technology blueprints.
Solutions Architecture Model	The graphical representation of concepts to portray a desired future state, as well as an undesirable current state. Used for communicating, analyzing, testing, simulating, or exploring options.
Solution Pattern	The bundling of tested solutions or configurations commonly used together, which can be addressed as a whole.
Solution Set	The combination of the scope, requirements, design specifications, and logical models that define the solution.

[7] Federal Chief Information Officer (CIO) Council, Federal Architecture Working Group, A Practical Guide to Federal Enterprise Architecture, Version 1.0, February 2001.

Term	Definition
Standard	Sets of criteria, voluntary guidelines and best practices. Some may be mandatory.
Strategic Elements	Strategic direction, drivers or goals establishing a vision statement, objectives, business plans, business drivers and goals.
Sunset Technologies	Technologies that have been phased out and cannot be used within the organization past a specified date.
System	A set of different elements so connected or related as to perform a unique function not performable by the elements alone (Rechtin 1991).
Target	The desired future or "to be" state of the business, information or technology environment, typically captured in a set of graphic and/or textual models.
Technology	Tools or tool systems by which we transform parts of our environment and extend our human capabilities (Tornatzky and Fleischer 1990).
Technology Architect	An individual responsible for developing technical architecture frameworks, components, and blueprints based on stated technology strategies and goals. Specific responsibilities and contributions to Enterprise Architecture include: ▪ Understanding the current technology architecture. ▪ Producing new technology patterns and services. ▪ Developing and communicating the new technology architecture. ▪ Identifying and developing a business cases and strategies for evolving technologies and the retirement of obsolete technologies ▪ Determining the mechanisms by which these components will collaborate in order to fulfill organizational operational and quality requirements.
Technology Architecture	A disciplined approach to describing the current and future structure and inter-relationships of the enterprise's technologies in order to maximize value in those technologies. It examines the technologies that are required to run the enterprise and develops a unified vision of the enterprise's infrastructure and technology platforms.
Technology Architecture Blueprint Levels	The term used to refer to the various levels of the Technology Architecture Blueprints. In this Tool-Kit, the levels include Domain, Discipline, Technology Area, Product Component and Compliance Component.
Template	The empty form that serves as a guide for capturing detail about the business, information or technology of an enterprise to be documented for the architecture. The resulting dynamic content, referred to within this Tool-Kit as the Architecture Blueprint, ultimately resides in an EA repository.
Trends	Emerging influences within the business world that are impacting how services and information will be provided. Trends include governmental trends as well as architecture specific tends, i.e. technology trends, information management trends, etc.
Twilight Technologies	Technologies being phased out by the enterprise.

NASCIO Online
Visit NASCIO on the web for the latest information on the Architecture Program or to download the current version of the Enterprise Architecture Development Tool-Kit.

www.nascio.org

APPENDIX B: ROLES & RESPONSIBILITIES CHART

This matrix provides an "at-a-glance" reference of the responsibilities of each architecture governance role, the activity performed, the EA Lifecycle process step addressed and the architecture artifacts acted upon.

Architecture Processes	Roles (P – Primary, S – Support)													Process Contributions					Architecture Artifacts				
EA Process Models denoted by italics	Advisor	Approver	Audience	Champion	Communicator	Documenter	Manager	Overseer	Proj/Serv Team	Solution Architect	SME	Team Manager	Reviewer	Document	Review	Communicate	Refresh	Compliance	Blueprints	Frameworks	Reports/Requests	Solution Sets	Strategic Elements
General Architecture Responsibilities																							
Promote, advertise, market, participate in architecture efforts	S	S	S	P	S	S	S	S					S			●				●			
Assure enterprise goals and objectives for architecture are met			S	P			S	S										●					●
Cheerleading and public relationship for success	S	S	S	P	S	S	S	S					S			●					●		
Coordination off the overall architecture effort	S	S	S	S	S	S	P	S					S			●		●		●			
Seeks guidance and support for the architecture effort				S			P									●				●			
Obtains clarity and support for the architecture effort	S						P									●							●
Chairs and directs the architecture review efforts	S					S	P						S		●					●			
Receive and evaluate recommendations regarding architecture efforts	S					S	P						S		●					●			
Approve/reject architecture requests	S					S	P						S		●				●		●		
Appoint architecture documenters				S		S	P																
Direct architecture documenters on process and scope of work						S	P																
Provide information to the communicator about the architecture components			S		S		P									●				●			
Architecture Governance Process																							
Determine Architecture Governance																							
Determine Enterprise Elements	S			S			P											●					●
Determine Enterprise Elements Information Flow	S			S			P											●					●
Determine Governance Roles	S			S			P											●					●
Determine EA Framework Elements	S			S			P											●		●			
Determine EA Framework Elements Information Flow	S			S			P											●		●			
Determine Architecture Governance Roles	S			S			P											●		●			
Create Architecture Governance Structure							P											●		●			
Document/Update Architecture Lifecycle Processes							P											●		●			
Confirm Architecture Governance Structure							P											●		●			

Create Architecture Governance Structure																							
Determine Resources Available							P											●		●			
Set-up Architecture Governance Committees							P											●		●			
Set-up Architecture Governance Titles							P											●		●			
Map Architecture Governance Roles							P											●		●			
Document Governance Organizational Chart							P											●		●			
Review Governance Organizational Chart	S			S			S						P					●		●			
Approve Governance Organizational Chart	S			S			S						P					●		●			
Document/Update Architecture Lifecycle Processes																							
Document/Update Documentation Process							P											●		●			
Document/Update Review Process							P											●		●			
Document/Update Communication Process							P											●		●			
Document/Update Compliance Process							P											●		●			
Document/Update Framework Viability Process							P											●		●			
Document/Update Blueprint Vitality Process							P											●		●			
Review Lifecycle Processes	S			S			S						P					●		●			
Approve Lifecycle Processes	S			S			S						P					●		●			
Confirm Architecture Governance Structure																							
Document/Update Architecture Lifecycle Processes							P											●		●			
Update Governance Elements							P											●		●			
Update Governance Roles							P											●		●			
Map Governance Roles							P											●		●			
Update Governance Organizational Chart							P											●		●			
Review Governance Organizational Chart / Review Lifecycle Processes	S			S			S						P					●		●			
Approve Governance Organizational Chart / approve Lifecycle Processes	S			S			S						P					●		●			
Denote Architecture Governance Organization Reviewed							P											●		●			
Architecture Documentation Process - General																							
Initiate Enterprise Documentation Process																							
Develop Enterprise Business Drivers	S						P						S	●									●
Develop Architecture Frameworks	S						P						S	●						●			
Define Initial Scope	S						P						S	●						●			
Develop Architecture Introduction Training	S						P						S	●							●		
Appoint Architecture Documenters/Authors	S						P						S	●							●		
Receive EA Introduction Education						P								●							●		
Receive Architecture Specific Education						P								●							●		
Conduct Work Sessions						P								●					●				
Create/Update Blueprint Items						P								●					●				
Architecture Review Process																							
Propose Architecture Change																							
Adaptive EA Framework Viability Process	S						P				S		S				●			●			
Architecture Blueprint Vitality Process							P										●		●				
Architecture Documentation Process						P								●						●			
Architecture Compliance Processes												P						●		●			
Present Proposed Architecture Review Request						S	P					S			●					●			
Consider Proposed Architecture Review Requests	S												P		●					●			
Clarify/State Architecture Opinion						S	P				S	S			●					●			
Debate/Discuss Proposed Architecture Review Request													P		●					●			

Determine Architecture Review Decisions																							
Prepare Change Proposal							P								●					●			
Present Change Proposal							P								●					●			
Consider Change Proposal	P														●					●			
Debate/Discuss Change Proposal	P														●					●			
Make Recommendation on Change Proposal	P														●					●			
Accept/Reject Review Request													P		●					●			
Document Architecture Review Decision							P								●					●			
Document Architecture Review Decisions																							
Summarize Architecture Review Decisions							P								●					●			
Determine Affected Domains/Subject Areas							P								●					●			
Apply Approved Architecture Framework Changes							P								●					●			
Architecture Framework Vitality Process							P										●			●			
Communication Architecture Review Decisions							P													●			
Architecture Communication Process							P									●				●			
Understand Architecture Review Decisions						P									●					●			
Create/Update Blueprint Items - Architecture Specific						P								●					●				
Architecture Communication Process																							
Communicate Architecture Information																							
Request Review Items							P						P			●					●		
Request Information			P			P	P					P				●					●		
Receive Information Request					P											●					●		
Create Information Document					P											●					●		
Send Information Document					P											●					●		
Architecture Framework Vitality Process							P										●			●	●		
Architecture Documentation Process						P								●						●	●		
Architecture Review Process													P		●					●	●		
Receive Information Document			P		P	P	P					P	P			●					●		
Architecture Compliance Process																							
Request Architecture Help																							
New/Update Functionality Requested									P									●	●				
Identify Affected Architecture Blueprint Items												P						●	●				
Create Architecture Help Request												P						●	●				
Receive Architecture Help Request							P											●	●				
Review Affected Architecture Blueprint Items							P											●	●				
Review Architecture Help Request						P												●	●				
Review Existing Architecture Component						P												●	●				
Architecture Documentation Process						P								●					●				
Provide Recommendation						P												●	●				
Determine Options																							
Review Recommendations							P											●			●		
Review Recommendations (Advice Requested)											P							●			●		
Provide Oversight Recommendation											P							●			●		
Summarize Recommendation							P											●			●		
Determine Options									P			P						●			●		
Create Architecture Variance Business Case												P						●			●		
Architecture Review Process							P								●				●	●			

Create Architecture Variance Business Case																									
Research Business Strategy Plans													P					●							●
Research IT Strategy Plans													P					●							●
Determine Funding Source													P					●							●
Document Architecture Blueprint Impact Statement							S	S					P					●				●			
Document Physical Implementation Requirements							S	S	S				P					●				●			
Determine Total Cost of Ownership							S	S	S				P					●				●			
Summarize Architecture Variance Business Case													P					●				●			
Architecture Framework Viability Process																									
Determine Architecture Framework Changes																									
Identify Changed Business Strategies	P																●								●
Identify Change IT Strategies	P																●								●
Recommend Framework Enhancements						P							P				●					●			
Review Architecture Governance Framework							P										●					●			
Review Architecture Frameworks							P										●					●			
Create Architecture Review Document							P										●					●			
Architecture Review Process													P			●						●			
Confirm Architecture Governance Structure							P											●				●			
Architecture Communication Process					P												●					●			
Architecture Documentation Process						P									●							●			
Architecture Blueprint Vitality Process																									
Determine Architecture Blueprint Changes																									
Identify Changed Business Strategies													P					●							●
Identify Changed IT Strategies													P					●							●
Review Business Drivers							P											●							●
Determine Impacted Domain/Subject Areas							P											●			●				
Kick-off Periodic Architecture Review							P											●				●			
Identify New Projects or Modifications													P					●				●			
Architecture Documentation Process						P									●							●			
Create Architecture Review Document							P											●					●		
Architecture Review Process													P			●						●			
Business Architecture Documentation Process																									
Initiate Business Architecture Documentation Process																									
Review Enterprise Business Drivers	S						P						S			●									●
Develop Business Architecture Framework	S						P						S		●						●				
Review/Update Domain Scope	S						P						S		●						●				
Develop Architecture Education Session	S						P						S		●							●			
Appoint Architecture Documenters/Authors	S						P						S				●					●			
Create/Update Business Architecture Blueprint Items						P									●						●				
Receive EA Introduction Education						P											●					●			
Receive Architecture Specific Education						P											●					●			
Conduct Business Architecture Work Sessions						P									●						●				
Develop Business Architecture Framework																									
Develop Business Architecture Processes/Templates	S						P						S		●							●			
Identify/Define Enterprise Business Domains	S						P						S		●							●			
Select Initial Business Domains for Documentation	S						P						S		●						●				
Identify/Define Business Perspectives	S						P						S		●						●				

Create/Update Business Architecture Blueprint Items																							
Set-up Interview Meetings						P								●					●				
Conduct Interview Meetings						P					S			●					●				
Conduct Follow-up						P					S			●					●				
Produce Meeting Notes						P								●					●				
Document/Update Business Architecture Components						P								●					●				
Create/Update Component Diagrams						P								●					●				
Create Association Matrices						P								●					●				
Perform Quality Assurance						S	P							●					●				
Prepare Confirmation Presentation						P								●					●				
Confirm Diagrams/Documents/Matrices						P	S				S			●					●				
Finalize Documentation						P								●					●				
Conduct Business Architecture Work Sessions																							
Review/Update Business Domain Scope						S	P						S	●					●				
Review Business Architecture Perspectives						S	P						S	●					●				
Identify Subject Matter Experts						S	P						S	●					●				
Determine Interview Strategies						S	P						S	●					●				
Create/Update Business Architecture Blueprint Item						P								●					●				
Compile Baseline/Target Packet						P								●					●				
Review Baseline/Target Packet							P						S	●					●				
Contribute to Implementation Plan						P								●					●				
Compile Business Domain Packet						P								●					●				
Review Business Domain Packet							P							●					●				
Summarize Blueprint Changes							P							●					●				
Architecture Review Process							P						S		●				●				
Information Architecture Documentation Process																							
Initiate Information Architecture Documentation Process																							
Review Enterprise Business Drivers	S						P						S		●								●
Develop Information Architecture Framework	S						P						S	●						●			
Review/Update Subject Area Scope	S						P						S	●					●				
Develop Architecture Education Session	S						P						S	●							●		
Appoint Architecture Documenters/Authors	S						P						S	●							●		
Create/Update Information Architecture Blueprint Items						P								●					●				
Receive EA Introduction Education						P										●					●		
Receive Architecture Specific Education						P										●					●		
Conduct Information Architecture Work Sessions						P								●					●				
Develop Information Architecture Framework																							
Develop Information Architecture Processes/Templates	S						P						S	●						●			
Document Information Security Classifications	S						P						S	●					●				
Identify/Define Information Subject Areas (Topical/Functional)	S						P						S	●					●				
Identify Information Subject Area Owners/Stewards	S						P						S	●							●		
Select Initial Information Subject Areas for Documentation	S						P						S	●					●				

Create/Update Information Architecture Blueprint Items																							
Set-up Interview Meetings						P								●					●				
Conduct Interview Meetings						P					S			●					●				
Conduct Follow-up						P					S			●					●				
Produce Meeting Notes						P								●					●				
Document/Update Information Architecture Components						P								●					●				
Create/Update Component Diagrams						P								●					●				
Create Association Matrices						P								●					●				
Perform Quality Assurance						S	P							●					●				
Prepare Confirmation Presentation						P								●					●				
Confirm Diagrams/Documents/Matrices						P	S				S			●					●				
Finalize Documentation						P								●					●				
Conduct Information Architecture Work Sessions																							
Review/Update Subject Area Scope						S	P						S	●					●				
Identify Subject Matter Experts						S	P						S	●					●				
Determine Interview Strategies						S	P						S	●					●				
Create/Update Information Architecture Blueprint Items						P								●					●				
Compile Baseline/Target Packet						P								●					●				
Review Baseline/Target Packet							P						S	●					●				
Contribute to Implementation Plan						P								●					●				
Compile Information Subject Area Packet						P								●					●				
Review Information Subject Area Packet							P							●					●				
Summarize Blueprint Changes							P							●					●				
Architecture Review Process							P						S		●				●				
Technology Architecture Documentation Process																							
Initiate Technology Architecture Documentation Process																							
Review Enterprise Business Drivers	S						P						S		●						●		
Development Technology Architecture Framework	S						P						S	●						●			
Define Initial Domain Scope	S						P						S	●						●			
Develop Architecture Introduction Training	S						P						S	●							●		
Appoint Architecture Documenters/Authors	S						P						S	●							●		
Receive EA Introduction Education						P										●					●		
Receive Architecture Specific Education						P										●					●		
Conduct Technology Architecture Work Sessions						P										●			●				
Create/Update Technology Architecture Blueprint Items						P								●					●				
Develop Technology Architecture Framework																							
Develop Technology Architecture Processes/Templates	S						P						S	●						●			
Identify/Define Domains	S						P						S	●						●			
Identify/Define Disciplines	S						P						S	●						●			
Select Initial Technology Domains for Documentation	S						P						S	●						●			
Create/Update Technology Architecture Blueprint Items																							
Complete/Update Domain Blueprint						P								●					●				
Complete/Update Discipline Blueprint						P								●					●				
Create/Update Technology Area Blueprint						P								●					●				
Create/Update Product Component Blueprint						P								●					●				
Create/Update Compliance Component Blueprint						P								●					●				

Document/Update Domain Blueprint																							
Review/Update Domain Blueprint						P								●					●				
Set Current Status (under review)						P								●					●				
Document Recommended Architecture Domain Changes						P								●					●				
Review Recommended Domain Architecture Changes													P		●				●				
Document Domain IT Contracts						P								●					●				
Update Domain Audit Trail						P								●					●				
Document/Update Discipline Blueprint						P								●					●				
Document/Update Discipline Blueprint																							
Review/Update Discipline Blueprint						P								●					●				
Set Current Status (under review)						P								●					●				
Document Recommended Architecture Changes						P								●					●				
Review Recommended Architecture Changes													P		●				●				
Complete Discipline Blueprint Detail						P								●					●				
Update Discipline Audit Trail						P								●					●				
Conduct Technology Scans						P								●							●		
Document/Update Technology Area Blueprint						P								●					●				
Document/Update Product Component Blueprint						P								●					●				
Document/Update Compliance Component Blueprint						P								●					●				
Document/Update Technology Area Blueprint																							
Complete Technology Area Blueprint Details						P								●					●				
Update Technology Area Audit Trail						P								●					●				
Document/Update Product Component Blueprint						P								●					●				
Document/Update Compliance Component Blueprint						P								●					●				
Document/Update Product Component Blueprints																							
Review/Document Product Component Definition						P								●					●				
Provide Associated Technology Area						P								●					●				
Document Keywords						P								●					●				
Set Current Status (under review)						P								●					●				
Document Vendor Information						P								●					●				
Provide Potential Compliance Organizations						P								●					●				
Identify Compliance Components						P								●					●				
Document Component Review (desirable and undesirable aspects)						P								●					●				
Evaluate Product/Compliance Components						P								●					●				
Create Migration Strategy						P								●					●				
Determine/Document Position Statement on Impact Analysis						P								●					●				
Update Product Component Audit Trail						P								●					●				
Document/Update Compliance Component Blueprint						P								●					●				

Document/Update Compliance Component Blueprints																							
Review/Document Compliance Component Definition						P								●					●				
Document Associated Architecture Levels (e.g., discipline, technology area, product component)						P								●					●				
Document Keywords						P								●					●				
Set Current Status (under review)						P								●					●				
Document Compliance Component Types (e.g., guideline, standard, or legislation)						P								●					●				
Document Compliance Details						P								●					●				
Evaluate Product/Compliance Components						P								●					●				
Create Migration Strategy						P								●					●				
Determine/Document Position Statement on Impact Analysis						P								●					●				
Update Compliance Component Audit Trail						P								●					●				
Evaluate Product/Compliance Components																							
Determine Business Driver Conformance						P								●					●				●
Determine Technology Architecture Conformance						P								●					●				
Determine Business Functionality Fit						P								●					●				
Determine Technology Fit						P								●					●				
Determine Operational Fit						P								●					●				
Evaluate Vendors						P								●					●				
Determine Cost of Ownership						P								●					●				
Set Component Classifications (Emerging, Current, Twilight, Sunset)						P								●					●				
Document Classification Rationale						P								●					●				
Document Conditional Use Restrictions						P								●					●				
Conduct Technology Architecture Work Sessions																							
Create/Update Blueprint Items						P								●					●				
Summarize Architecture Blueprint Changes						P								●					●				
Review Business Driver Compliance						P									●				●				●
Submit Architecture Blueprint Results						P									●				●				
Receive Architecture Blueprint Results							P								●				●				
Architecture Review Process	P						S						P		●				●				
Solution Architecture Documentation Process																							
Initiate Solution Architecture Documentation Process																							
Develop Solution Architecture Framework	S						P						S	●						●			
Develop Solution Architecture Education Session	S						P						S	●							●		
Appoint Solution Set Architect & Documenters	S						P						S	●							●		
Solution Set Vitality Review						P											●		●				
Finalize Documentation						P								●						●	●		
Receive EA Introduction Education						P								●							●		
Receive Solution Architecture Education						P								●							●		
Conduct Solution Set Work Session						P								●					●				

Conduct Solution Architecture Solution Set Work Sessions																							
Review Associated Implementation Plan Items						S				P				●								●	
Identify Solution Set Type						S				P				●								●	
Identify Subject Matter Experts						S				P				●								●	
Determine Interview Strategies						S				P				●								●	
Create/Update Solution Set Items						S				P				●								●	
Review Solution Set Items	S									S			P		●							●	
Compile Solution Set Packet						S				P				●								●	
Review Solution Set Packet with SMEs	S									S	P		S		●							●	
Review for Architecture Compliance	S									S			P		●							●	
Review with Project Stakeholders	S									S			P		●							●	
Coordinate Solution Set with Build Team	S									P			S			●						●	
Summarize EA Blueprint Changes										P				●					●				
Create/Update Solution Architecture Solution Set Items																							
Conduct Interview Meetings						S				P	S			●								●	
Create/Update Solution Set Scope						S				P	S			●								●	
Create/Update Solution Set Requirements						S				P	S			●								●	
Create/Update Solution Set Design Specifications						S				P	S			●								●	
Create/Update Logical Models						S				P	S			●								●	
Perform Quality Assurance						S				P					●							●	
Prepare Confirmation Presentation						S				P				●							●		
Confirm Scope/Requirements/Design Specifications/Models						S				P	S				●							●	
Create/Update BA/IA/TA Blueprint Items						P				S				●					●				
Solution Set Vitality Review										P					●							●	
Finalize Documentation										P				●							●	●	
Solution Architecture Solution Set Vitality Review																							
Review Process Triggers	S									P			S		●							●	
Perform Impact Analysis on Solution Set Items										S					●							●	
Prepare Change Strategy						S				P					●						●		
Identify Subject Matter Experts						S				P					●						●		
Determine Interview Strategies						S				P					●						●		
Create/Update Solution Set Items						S				P				●								●	
Document Results of Vitality Review										P				●							●		
Present Results to Sponsors										P			S			●					●		
Compile Updated Solution Set Packet										P				●								●	
Review Solution Set with SMEs										P	S				●							●	
Review for Architecture Compliance	S									P			S		●							●	
Review with Project Stakeholders	S									P			S		●							●	
Coordinate Solution Set with Build Team	S									P						●						●	
Summarize EA Blueprint Changes										P						●					●		

NASCIO Online
Visit NASCIO on the web for the latest information on the Architecture Program or to download the current version of the Enterprise Architecture Development Tool-Kit.

www.nascio.org