Adaptive Enterprise Architecture Development Program

NASCIO

Enterprise Architecture Development Tool-Kit

July 2002 v2.0

National Association of State Chief Information Officers

NASCIO

Enterprise Architecture Development Tool-Kit

July 2002 v2.0

Acknowledgements

NASCIO would like to thank the members of the Architecture Working Group for their contributions to this effort. NASCIO would also like to thank the practitioners from our member states who participated in the regional workshops and various other review activities. Your ideas and suggestions are the driving force behind Tool-Kit v2.0.

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: 859.231.1971
Fax: 859.231.1928
Email: nascio@amrinc.net
Website: www.nascio.org

NASCIO
Representing Chief Information Officers of the States

July 10, 2002

Enterprise architecture enjoys a national momentum fueled by many sources. Mandates of the federal government drive architecture development, as does the recognition by municipal, county and state leaders of the need for increased efficiency in deployment of technology solutions aligned with the business of the enterprise. These same leaders also acknowledge the critical need for timely, accurate information sharing horizontally between departments within the enterprise and vertically with agencies of different governmental levels. The NASCIO Enterprise Architecture Development Tool-Kit is structured to address those needs at each level.

Process models accompanied by explanatory narrative allow the user to customize the tool to fit their specific agency needs. Process diagrams are included for the governance, business and technology architectures. Architecture lifecycle processes are illustrated to encourage the user to address the recurring needs for architecture updates as business processes and technology drivers change. In addition, the Tool-Kit contains sample blueprints for the security and application domains. The fully populated samples were compiled from the input of several state and county representatives.

On behalf of NASCIO, we would like to thank the members of the Architecture Working Group (AWG) for their contributions of time and expertise to enhancing the content of the Tool-Kit for this release. The AWG spent countless hours reviewing and commenting on the Tool-Kit content and process maps. Only with the support and proficiency of our volunteers is NASCIO able to continue to gather content to keep this tool viable.

Lastly, we would like to encourage all who have not yet done so to put architecture on your "To Do List." Once architecture is on the agenda, utilize the wealth of knowledge collected in this resource to begin making information architecture an integral part of your enterprise.

Gerry Wethington, chair AWG
Chief Information Officer
Office of Information Technology
State of Missouri

Doug Robinson, vice-chair AWG
Executive Director
Governor's Office for Technology
Commonwealth of Kentucky

167 West Main Street, Suite 600 Lexington, Kentucky 40507-1324 **P:** 859-231-1971 **F:** 859-231-1928 **E:** nascio@amrinc.net www.nascio.org

TABLE OF CONTENTS

PREFACE 1

About NASCIO 1
Mission 1
History of the Association 1
About the Architecture Program 1
NASCIO Officers and Directors 2001-2002 2
Architecture Working Group Members 2001-2002 4
Architecture Working Group Associate Members 2001-2002 5
Architecture Working Group Consultants 6
NASCIO Staff 6
NASCIO Headquarters 6
Audience for Tool-Kit Sections 7
Executive Summary 8
NASCIO's Current Situation 8
NASCIO's Solution 9

INTRODUCTION 11

Concept - Why Architecture? 11
Overview of Enterprise Architecture Terms & Concepts 15
Architecture Analogy 15
Framing the Enterprise Architecture 16
Breaking Things Down Into Workable Parts 18
Conclusion 21
Overview of Tool-Kit Structure 22
Governance Architecture 23
Business Architecture 23
Technology Architecture 24
Appendix 24

GOVERNANCE ARCHITECTURE 25

Architecture Governance Framework 26
Enterprise & Architecture Governance Elements 26
Governance Approach 26
Enterprise Elements 26
Enterprise Element Relationships 29
Enterprise Architecture Framework Elements 30
Architecture Governance Roles 31

Primary Roles 33
Supportive roles 38
Governance Samples 41
Applicability In The Judicial Environment 41
Governance Models 42
Architecture Governance Process 63
Determine Architecture Governance 65
Create Architecture Governance Structure 68
Document/Update Architecture Lifecycle Processes 70
Confirm Architecture Governance Structure 74
Architecture Lifecycle Processes 77
Architecture Documentation Process 80
Initiating Documentation Process 81
Conduct Documenter Work Sessions 84
Architecture Review Process 86
Propose Architecture Change 87
Determine Review Decision 90
Document Architecture Review Decision 92
Architecture Communication Process 95
Communicate Architecture Information 96
Architecture Compliance Process 99
Request Architecture Help 100
Determine Technology Options 103
Create Architecture Variance Business Case 105
Architecture Framework Vitality Process 107
Determine Architecture Framework Changes 108
Architecture Blueprint Vitality Process 112
Determine Architecture Blueprint Changes 113

TECHNOLOGY ARCHITECTURE 117

Technology Architecture Framework 118
Technology Drivers 118
IT Principles 119
IT Best Practices 119
Technology Trends 119
Technology Architecture Blueprint Framework 120

Architecture Blueprint Structure Overview 120
Complete/Update Domain Blueprint 123
Domain Template 126
Complete/Update Discipline Blueprint 131
Discipline Template 136
Document/Update Technology Areas 142
Technology Area Template 145
Document/Update Product Components 149
Product Component Template 154
Document/Update Compliance Components 160
Compliance Component Template 164
Evaluate Compliance/Product Components 170
Technology Architecture Samples 174
Technology Driver Samples 174
IT Principles 174
IT Best Practices 174
Technology Trends 174
Technology Architecture Blueprint Samples 174
Technology Architecture Communications Document Samples 224
Application Development Classification Report 224
Electronic Collaboration Classification Report 225
Security Classification Report 226
Technology Architecture Miscellaneous Samples 229
Domain/Discipline - Combinations 229
Domain/Discipline – Intersections 230

APPENDIX A - LEXICON 233

APPENDIX B - SAMPLE DISCIPLINE DESCRIPTIONS 237

APPENDIX C: ROLES & RESPONSIBILITIES MATRIX 241

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 to shape national IT policy.

MISSION

The mission of the association is to shape national IT policy through collaborative partnerships, information sharing, and knowledge transfer across jurisdictional and functional boundaries.

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.

NASCIO OFFICERS AND DIRECTORS 2001-2002

OFFICERS			
President	Rock Regan Chief Information Officer State of Connecticut	Department of IT 101 East River Dr East Hartford, CT 06108	Tel: 860-622-2419 Fax: 860-291-8665 rock.regan@po.state.ct.us
Vice 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
Secretary/Treasurer	Bob Stafford Chief Information Officer State of New Mexico	IT Management Office 404 Montezuma Ave Santa Fe, NM 87501	Tel: 505-476-0409 Fax: 505-476-0401 bob_stafford@state.nm.us
Past President	Aldona Valicenti Chief Information Officer Commonwealth of Kentucky	101 Cold Harbor Dr Frankfort, KY 40601	Tel: 502-564-1201 ext. 447 Fax: 502-564-6856 avalicenti@mail.state.ky.us

DIRECTORS		
Bob Feingold Chief Information Officer State of Colorado	225 E. 16th Ave, Suite 900 Denver, CO 80203	Telephone: 303-866-6314 bob.feingold@state.co.us
Anthony Herbert Deputy CIO State of Montana	Department of Administration 125 N. Roberts Helena, MT 59620	Telephone: 406-444-2700 therbert@state.mt.us
Greg Jackson Chief Information Officer State of Ohio	Office of IS Policy & Planning 30 E. Broad St 40th Floor, Suite 4040 Columbus, OH 43215	Telephone: 614-466-6511 greg.jackson@das.state.oh.us

DIRECTORS		
Harry Lanphear Chief Information Officer State of Maine	Department of Administrative and Financial Services 173 State House Station Augusta, ME 04333-0173	Telephone: 207-624-7568 harry.lanphear@state.me.us
Mary Barber Reynolds Chief Technology Officer State of Illinois	Office of the Governor 2 ½ State House Springfield, IL 62706	Telephone: 217-557-3508 mary_reynolds@gov.state.il.us
Terry Savage Director State of Nevada	Department of IT 505 E. King St, Suite 403 Carson City, NV 89701	Telephone: 775-684-5800 tsavage@doit.state.nv.us
Larry Singer CIO & Executive Director State of Georgia	Georgia Technology Authority 100 Peachtree St, Suite 2300 Atlanta, GA 30303	Telephone: 404-463-2300 ljsinger@gagta.com
Curtis Wolfe Chief Information Officer State of North Dakota	IT Department 600 E. Boulevard Ave Department 112 Bismarck, ND 58505-0100	Telephone: 701-328-1000 cwolfe@state.nd.us

CORPORATE LEADERSHIP COUNCIL REPRESENTATIVE		
Holli Ploog VP & General Managing Principal	Unisys 8008 West Park Drive McLean, VA 22102	Telephone: 703-556-5209 holli.ploog@unisys.com

FEDERAL CIO COUNCIL REPRESENTATIVE		
Edward Meagher Special Asst. to Sec. for IT	US Veterans Administration 810 Vermont Ave Washington, DC 20420	Telephone: 202-273-8726 edward.meagher@mail.va.gov

ARCHITECTURE WORKING GROUP MEMBERS 2001-2002

Gerry Wethington *Chair*	Chief Information Officer	Office of Information Technology State of Missouri
Doug Robinson V*ice Chair*	Executive Director	Governor's Office for Technology Commonwealth of Kentucky
Stan Jenkins	Deputy Chief Information Officer	Office of IT Services State of North Carolina
Laura Larimer	Director of Information Technology	Department of Administration State of Indiana
David Lewis	Chief Information Officer	Information Technology Division Commonwealth of Massachusetts
Ed Meagher	Special Assistant to the Secretary for IT	US Veterans Administration Washington DC
Dave Molchany	Chief Information Officer	Fairfax County Government Fairfax County, Virginia
Kym Patterson	Manager, Technical Architecture	Shared Technical Architecture Program State of Arkansas
Mike Ryan	Chief Information Architect	Office of Technology State of Minnesota
Terry Savage	Director	Department of Information Technology State of Nevada
Jennifer Witham	Lead IT Planning and Research Analyst	Information Technology Department State of North Dakota
Judi Wood	Chief Information Officer	Department of Public Safety State of Maryland
Don Heiman	Director (retired February 2002)	Division of Information Systems & Communications State of Kansas

ARCHITECTURE WORKING GROUP ASSOCIATE MEMBERS 2001-2002

Val Asbedian	Director of Strategic Planning	Information Technology Division Commonwealth of Massachusetts
Jim Ballard	Vice President of Sales Consulting	State & Local Government & K-12 Education Oracle
Dr. Behnam Bavarian	Vice President of Technology	Integrated Solutions Division Motorola
Chris Braun	Manager	Software Technology Dyncorp Information Systems
John Carey Brown	Information Resource Manager	Information Technology Office State of Kansas
Mark Calem	Vice President, CTO	AMS
Jean Corder	Systems Consultant	Information Technology Oversight State of Indiana
Bob Dill	Information Technology Architect	Architecture Center for Excellence IBM
Marlene Lockard	Vice President	eGovernment Strategy Ezgov
Dorothy Martin	Computer Facility Manager	Department of Information Technology State of Nevada
Bob Meinhardt	Technology Specialist	Office of Information Technology State of Missouri
Laura Metzger	Vice President	Science Applications International Corp.
Richard Ward	Director	State Government Sales Microsoft

ARCHITECTURE WORKING GROUP CONSULTANTS

John Curley	Project Manager	National Systems & Research Co.
Jean Bogue	Senior Architect	National Systems & Research Co.
Dianna Dees	Senior Architect	National Systems & Research Co.
David J. Roberts	Deputy Executive Director	SEARCH, The National Consortium for Justice Information and Statistics

NASCIO STAFF

Elizabeth Miller	Executive Director	Telephone: 859-514-9171 emiller@amrinc.net
Matthew Trail	Assistant Director	Telephone: 859-514-9212 mtrail@amrinc.net
Nancy Howard	Communications & Programs Coordinator	Telephone: 859-514-9213 nhoward@amrinc.net
Beth Roszman	Membership & Development Coordinator	Telephone: 859-514-9167 broszman@amrinc.net
Cheryl Edwards	Enterprise Architecture Program Coordinator	Telephone: 859-514-9215 cedwards@amrinc.net
J. Chris Dixon	Digital Government Issues Coordinator	Telephone: 859-514-9148 cdixon@amrinc.net
Mary Gay Whitmer	Digital Government Issues Coordinator	Telephone: 859-514-9209 mwhitmer@amrinc.net
Deanna Ballard	Project Associate	Telephone: 859-514-9179 dballard@amrinc.net
Chris Walls	Web Site Coordinator	Telephone: 859-514-9174 cwalls@amrinc.net

NASCIO HEADQUARTERS

National Association of State Chief Information Officers	167 West Main Street, Suite 600 Lexington, KY 40507-1324	Telephone: 859-231-1971 Fax: 859-231-1928 www.nascio.org

Audience for Tool-Kit Sections

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 more technical in nature.

The Tool-Kit contains four major sections – Introduction, Architecture Governance, Business Architecture and Technology Architecture.

The section on ***Architecture Governance*** will be of particular interest to those who currently guide or manage the organization's enterprise architecture or will 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 validation and workshop comments indicated an increasing interest in expanding the scope of ***Business Architecture*** in the Tool-Kit. The Business Architecture section currently contains only an outline, but this section is the focus for future updates to the Tool-Kit. This section will cover items of interest to developers of business or technology architecture, providing insight for organizations to establish the business drivers, and processes necessary to ensure that the technical solutions will address the business needs of the organization.

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

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.

NASCIO's goal is a Tool-Kit that a government enterprise might use as a guide to develop their own Enterprise Architecture Framework. 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.

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

"Adaptive" is key because the Enterprise Architecture Framework must be able to support a wide variety of applications, and it must evolve as technology 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 even more critical.

Enterprise Architecture Framework can be described as a methodology for developing an organization's IT support functions. Ideally, when governments establish their infrastructures using common enterprise architecture, making systems work together will be simpler because each would have addressed the items that are crucial to interoperability of systems developed for specific business needs.

Enterprise architecture is critical because it provides the blueprint for the integration of information and services at the design level across agency boundaries. Enterprise architecture is the blueprint for allowing 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 Current Situation

NASCIO's Architecture Working Group is currently in the fourth year of the Adaptive Enterprise Architecture Program. The working group has presented Version 1.0 of its Tool-Kit, which documents enterprise architecture processes and concepts to municipal, county, and state government nationwide, and has contracted with National Systems & Research Co. (NSR) as a technical support partner to support the development of the Adaptive Enterprise Architecture Program. The design and validation of an enterprise architecture Tool-Kit, benchmarking tools, and models to improve implementation are well underway. Its future focus will be educational workshops and technical assistance for government entities in the process of establishing their enterprise architectures.

NASCIO's Solution

NASCIO's solution provides the Enterprise Architecture Development Tool-Kit as a guide in implementing specific Enterprise Architecture Frameworks. NASCIO promotes 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 Frameworks. Specifically, NASCIO has developed a Tool-Kit that guides government enterprises through the 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, made up 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. The additional states and the District of Columbia will participate 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 are being explored. If deemed feasible, NASCIO will pursue the national certification.

Follow-on efforts to keep the Enterprise Architecture Development Tool-Kit viable, to integrate the Adaptive Enterprise Architecture Development program with other national efforts for standardization, and to expand municipal, county and state government participation 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 with emerging technology and government needs. Integration efforts include mapping the enterprise architecture to the Concept of Operations that has been developed by NASCIO, along with integration with other national standards initiatives conducted by organizations such as the NASCIO Digital Government Work Group, the Global Infrastructure/Standards Working Group and 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 that 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.

Adopting enterprise architecture increases the utility of an enterprise's data by facilitating information sharing between data stores. Committing to an ongoing, renewable enterprise architecture process fosters a technology-adaptive enterprise. Enterprise Architecture becomes a road map, guiding all future technology investments and identifying and aiding in the resolution of gaps in the entity's business and IT infrastructures.

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 entity; we understand what it costs to live there. Moving to a new house, though, 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.

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. These categories are defined in the following paragraphs.

Emerging technologies identify those developing or recently released technologies that are projected to become industry standards. Though the items listed may seem to be the latest and greatest, they will generally take some time to be tested and accepted by the industry as standards. It is generally understood that these items should be considered carefully before implementing them within the enterprise architecture.

Current technologies represent items that are current standards for use within the enterprise. They have been tested and are generally accepted as standard by the industry. These are the preferred technologies of the day. These items comply with or support the Technology Drivers listed for the discipline.

Twilight technologies identify technologies that may still be in use, but are not the optimum. They may be a deterrent to reaching the goals of the enterprise and are being phased out.

Sunset technologies identify technologies that are in use but do not conform to the stated technology architecture direction. The sunset component will have a date of discontinuance.

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 need only categorize the existing architecture within the provided templates.

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 discipline 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 Terms & Concepts

This Tool-Kit outlines some of the considerations to address as you develop or move through the process to achieve adaptive enterprise architecture. It is meant to serve as a guide in understanding the enterprise architecture evolution process and provides process models and templates as well as completed examples of several sections populated with appropriate information.

The Architecture Blueprint is a plan and a methodology.

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.

ARCHITECTURE ANALOGY

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 information 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 fix or 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 architectural framework. 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.

Enterprise architecture can be compared to creating a well planned home, but 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.

FRAMING THE ENTERPRISE ARCHITECTURE

There are numerous items to consider when undertaking a construction project like a house, government building or city planning. 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 managing the elements of enterprise architecture.

The ***Enterprise Architecture Framework*** is an overall framework that allows the framing of all of the architecture elements and defines the interrelationships between them in a consistent and organized fashion.

The Enterprise Architecture Framework graphic in Figure 1 provides a pictorial view of how the various elements in the Enterprise Architecture Framework interact and influence each other. The goals and objectives of the adaptive enterprise architecture are represented conceptually in this graphic. Government entities should provide a similar conceptual diagram when implementing their Enterprise Architecture Framework.

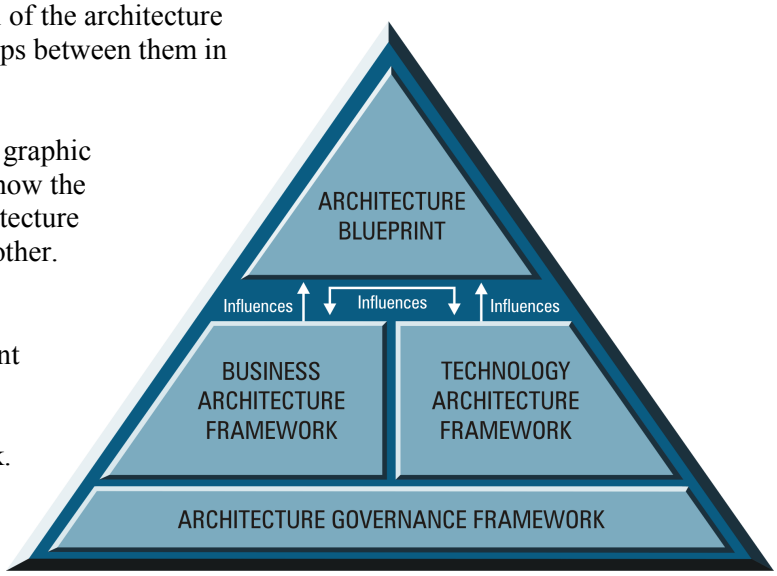


Figure 1. Enterprise Architecture Framework

As can be seen in the pictorial representation of the Enterprise Architecture Framework there are four major Enterprise Architecture Framework Elements:

Architecture Governance Framework

The Architecture Governance Framework includes the governance roles, elements, and processes required in maintaining adaptive enterprise architecture.

The Architecture Governance Framework provides 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. This section of the Tool-Kit supports NASCIO's architecture program by providing municipal, county and state governments a method of establishing effective architecture governance.

Business Architecture Framework

The Business Architecture Framework includes the framing elements required to document the Business Architecture Blueprint. The Business Architecture is broken down into the Business Drivers (Enterprise Business Principles, Business Best Practices, and Industry Trends), as well as Business Architecture Processes and Business Architecture Blueprint Templates. The result of utilizing the Business Architecture Framework is the Business Architecture Blueprint.

The Business Architecture Framework is currently only outlined at this point. In future efforts it will provide:

- Categories for Business Drivers within the Business Principles, Business Best Practices and Industry Trends
- A Business Architecture Blueprint Framework that will include:
  - Business Architecture Processes
  - Business Architecture Blueprint Templates

Technology Architecture Framework

The Technology Architecture Framework includes the framing elements required to document the Technology Architecture Blueprint. The Technology Architecture is broken down into the Technology Drivers (Enterprise IT Principles, IT Best Practices, and Technology Trends), as well as Technology Architecture Processes and Technology Architecture Blueprint Templates. The result of utilizing the Technology Architecture Framework is the Technology Architecture Blueprint.

The Technology Architecture Framework provides a sound set of technology framework elements to support implementation and communication of the technology architecture. The mapping of the IT and Business Strategic Elements with the Technology Drivers is vital in verifying that the architecture is aligned with the enterprise direction. The Technology Blueprint Templates must be concise and consistent to assure uniformed documentation across the enterprise. It is through the completion of these templates that the Technology Architecture Blueprint is communicated throughout the enterprise. Vendors, employees, and business users must all be able to understand the type of information that is provided and where to find it.

Architecture Blueprint

The Architecture Blueprint is the collection of the actual standards and specifications that define how the Business and IT Portfolios are and will be built.

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 structure.

Architecture Blueprints provide the means to implement technology into the enterprise in a timely and efficient manner. The vitality of the architecture provides for information 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 Framework consists of three types of information:

- *Static Information* – Information that changes only on an annual to bi-annual basis. The Architecture Governance Framework is a good example of static information.
- *Semi-Static Information* – Information that changes only when a major shift in the business or technology occurs. The Business and Technology Architecture Frameworks are considered semi-static. Business and Technology Drivers will change as new and improved ways of providing services to the stakeholders are found.
- *Dynamic Information* – Information that is reviewed and updated frequently, typically every four to six months. New information will be added on a monthly basis as various groups in the organization have business or technology solutions added to the Business/IT Portfolio. The Architecture Blueprint (comprised of Business and Technology Architecture Blueprints) is dynamic.

BREAKING THINGS DOWN INTO WORKABLE PARTS

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 more 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.

Architecture Governance Framework

Includes the parts of the Enterprise Architecture Framework that will structure the individuals and groups that are working on the architecture and the processes they will be utilizing.

Four main components of the Architecture Governance Framework are:

- *Enterprise Architecture Framework Elements* – Elements that pertain specifically to the adaptive enterprise architecture. The Enterprise Architecture Framework Elements include:
  - Architecture Governance Framework (including Lifecycle Processes and Templates)
  - Business Architecture Framework
  - Technical Architecture Framework
  - Architecture Blueprint
    - Business Architecture Blueprint
    - Technology Architecture Blueprint
- *Architecture Governance Roles* – Structures of the individuals and groups that are working on the architecture. This is done in a role-based, rather than position-based, view. This allows the various levels of government to decide for themselves the positions and groups that will perform the various roles required to accomplish architecture.
- *Architecture Governance Processes* – Processes that go into setting up the governance and keeping it vital in the organization throughout the architecture process.
- *Architecture Lifecycle Processes* - Definition and flow to show how the various architecture lifecycle processes interact with each other to create a continuous cycle of renewal of the architecture information.

Business Architecture Framework

The Business Architecture Framework includes the parts of the Enterprise Architecture Framework that will structure business direction and existing business services.

Two main components of the Business Architecture Framework are:

- *Business Architecture Blueprint Framework* – Templates on how the business architecture information will be provided and processes on how to document the business architecture information.
- *Business Drivers* – Internal goals and strategies and external trends that influence the business. These are captured in three stages of drivers:
  - *Industry Trends* – Emerging trends within the business world that are impacting how services and information will be provided.
  - *Business Best Practices* – Those trends and approaches that over time have proven to be the most successful at providing the services and information.
  - *Business Principles* – Business practices and approaches that the organization choices to institutionalize to better all services and information provided.

Technology Architecture Framework

***I**ncludes the parts of the Enterprise Architecture Framework that will structure technology direction and existing IT services.*

Two main components of the Technology Architecture Framework are:

- *Technology Architecture Blueprint Framework* – Templates and processes that aid in providing the technology architecture information.

  Architecture Blueprint Template levels include:

  - *Domains* - The natural divisions of the technical architecture and the main building blocks of the technology architecture blueprint
  - *Disciplines* - The logical functional subsets of a Domain. Disciplines allow further breakdown of the Domain into manageable pieces.
  - *Technology Areas* - Those technical topics that support the technology functional areas of the architecture blueprint. Guidelines and standards, which apply to multiple product components, can be addressed at the Technology Area level rather than being repeated for each product at the Product Component level.
  - *Product Components* - The protocols, products (families) and configurations specific to a technology area.
  - *Compliance Components* - The guidelines, standards and legislative mandates associated with a Discipline, Technical Component, and/or Product Component as appropriate.

Figure 2 provides a pictorial view of the relationship between the five technology architecture blueprint templates. As can be seen from the graphic, these pieces work together to ensure the complete documentation of the Domains that form the Technology Architecture Blueprint.

- *Technology Drivers* – Internal business processes and needs and external innovation that influence technology. These are captured in three stages of technology drivers:
  - *Technology Trends* – Emerging trends within the technology world that are impacting how services and the IT Portfolio will be provided.
  - *IT Best Practices* – Those trends and approaches that over time have proven to be the most successful at providing the services and IT Portfolio.
  - *IT Principles* – Those practices and approaches that the organization choices to institutionalize to better all services and IT Portfolio pieces provided.

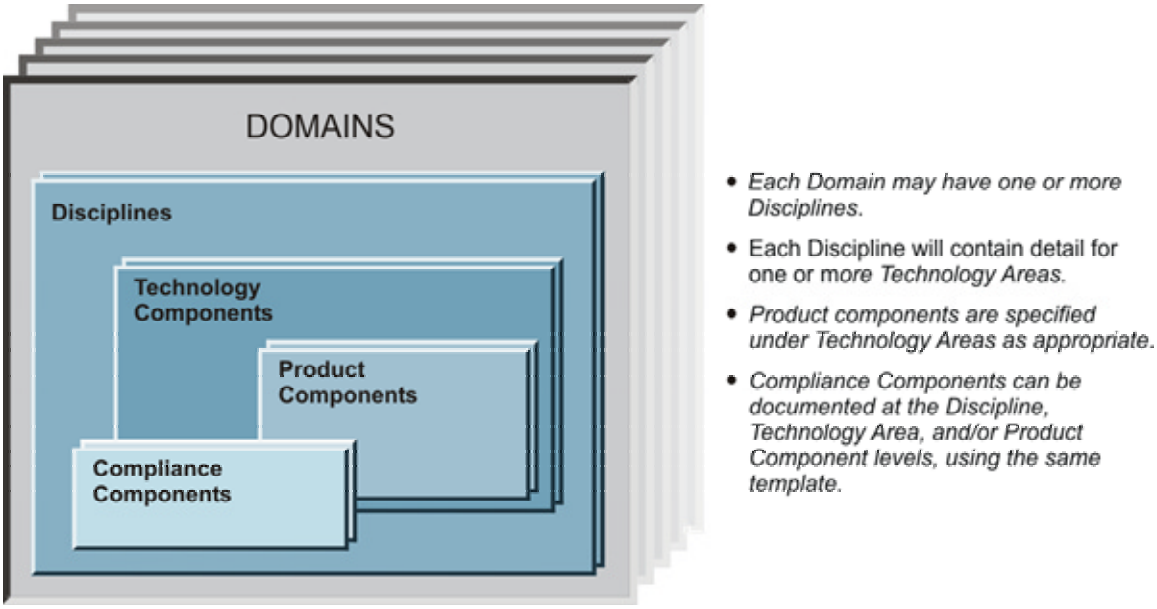


Figure 2. Template Relationships

- *Architecture Blueprint* – The term Architecture Blueprint refers to the dynamic information that is documented for the enterprise utilizing the Business or Technology Architecture Blueprint Templates. This dynamic information becomes the essence of the enterprise architecture, showing exactly how the services, information and Business/IT Portfolio in the organization will be delivered.

CONCLUSION

It is through the enterprise architecture frameworks and framework elements that the NASCIO Tool-Kit provides a governmental enterprise the means to apply adaptive enterprise architecture, which aids in a structured and consistent delivery of services and information.

The architecture blueprint is not a document that you produce once, store on the shelf and reference on occasion. It is a plan and a methodology; it must be both or it has no value. Just as with city plans and building codes, it is constantly being renewed and updated to meet the demands on the organization. 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.

Overview of Tool-Kit Structure

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. As with any map, this section provides an overall view to help you determine where you are and to assist with your navigation through the Tool-Kit.

The Tool-Kit Structure figure provides the map of the Tool-Kit.

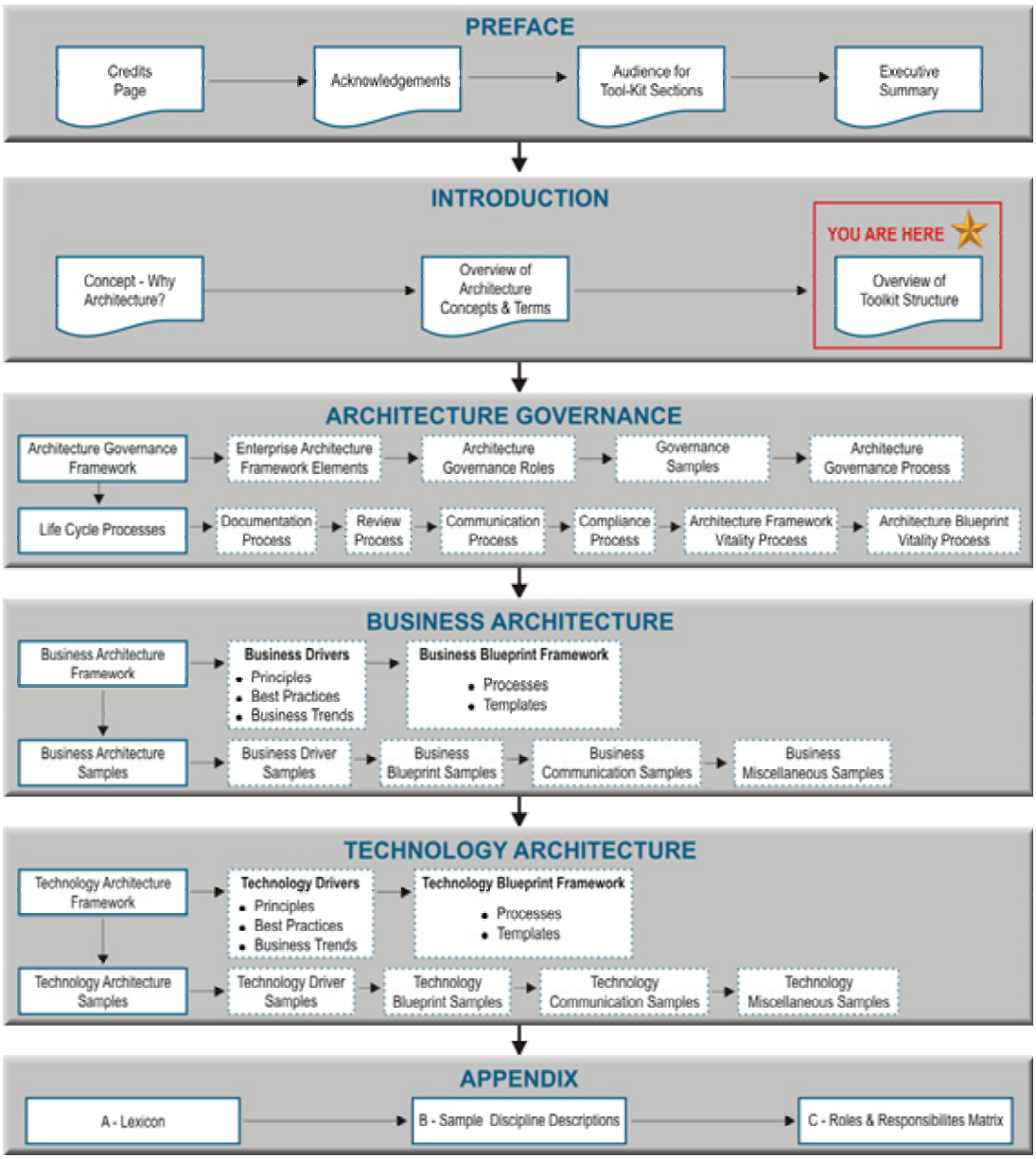


Figure 3. Tool-Kit Structure

The following outline highlights the instructional sections of the Tool-Kit.

GOVERNANCE ARCHITECTURE

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.

Architecture Governance covers the following topics:

- Architecture Governance Framework
  - Enterprise Architecture Framework Elements
  - Architecture Governance Roles
  - Governance Samples, including sample organization charts and mapping to Architecture Governance roles and responsibilities
  - Architecture Governance processes
- Architecture Life Cycle Processes
  - Documentation
  - Review
  - Communication
  - Compliance
  - Architecture Framework Vitality
  - Architecture Blueprint Vitality

BUSINESS ARCHITECTURE

This section will cover items of interest to developers of enterprise architecture, providing insight for organizations to establish the business drivers, and processes necessary to ensure that the technical solutions will address the business needs of the organization.

Business Architecture covers the following topics:

- Business Architecture Framework
  - Business Drivers covering Business Principles, Best Practices and Industry Trends
  - Business Blueprint Framework
    - Business Architecture Processes
    - Business Architecture Blueprint Templates
- Business Architecture Samples
  - Business Driver Samples
  - Business Blueprint Samples

TECHNOLOGY ARCHITECTURE

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

- Technology Architecture Framework
  - Technology Drivers covering Enterprise IT Principles, IT Best Practices and IT Technology Trends
  - Technology Blueprint Framework
    - Technology Architecture Processes
    - Technology Architecture Blueprint Templates
- Technology Architecture Samples
  - Technology Driver Samples
  - Technology Blueprint Samples

APPENDIX

- Lexicon of terms used through the Tool-Kit.
- Sample Discipline Descriptions as used within the Tool-Kit.
- A Role & Responsibility Matrix, which provides an "at-a-glance" reference of the responsibilities of specific role, the items acted upon and the roles that interact regarding the responsibility.

GOVERNANCE ARCHITECTURE

NASCIO has established an Adaptive Enterprise Architecture Program to assist all levels of government with the adoption of adaptive enterprise architecture. The Architecture Program has developed a Tool-Kit identifying an enterprise architecture framework and methodology for developing an adaptive enterprise architecture that effectively aligns information technology with the enterprise business direction.

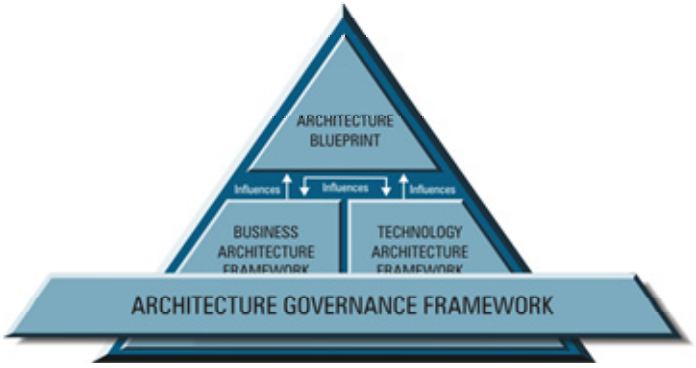
A sound governance framework to support implementation and management of the enterprise architecture is necessary to ensure the enterprise achieves its objectives. The governance framework must be resilient enough to allow for those in primary governance roles to learn and adapt, manage the risks, and appropriately recognize opportunities 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 structures. It effectively supports the gap analysis of existing governance structures, identifying methods to improve governance performance, as well as the development of a governance structure in its entirety.

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

Architecture Governance Framework

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 or governor. Deviations from goals and standards are reported and include recommendations for action requiring endorsement by the governing layer.

Enterprise & Architecture Governance Elements

Governance Approach

The Governance Approach 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 consist of Governance, Business, and Technology Architecture Frameworks, as well as the Architecture Blueprint for the enterprise. These four 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 business needs, technological direction, 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 EA Framework. Some examples of Strategic Enterprise Elements are:

- Enterprise Direction
- Mission Statements
- Organizational Charts
- Operating Budgets
- Strategies, Goals, & Objectives
- Strategic 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 4 illustrates the flow that the Enterprise Elements follow from the enterprise perspective, along with their relationships. .

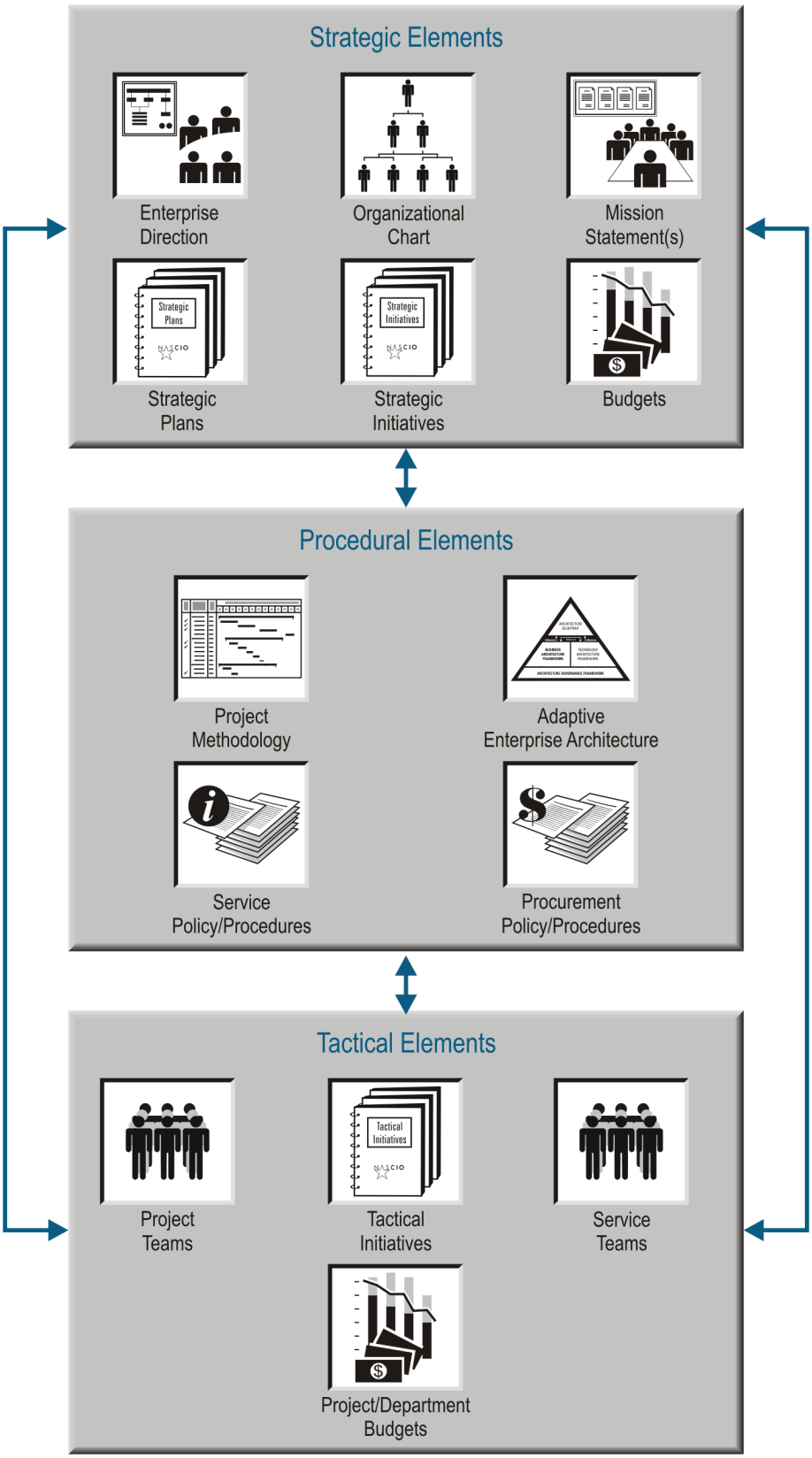


Figure 4. Enterprise Element Relationships

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 Budgets

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 5). 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 and Templates)
- Business Architecture Framework
- Technology Architecture Framework
- Architecture Blueprint

In Figure 5, 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 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 the Business Architecture Framework at the business executive level. The Strategic Elements, focused on Technology Strategies, along with the Business Architecture Framework, aid in establishing and confirming the Technology Architecture Framework.

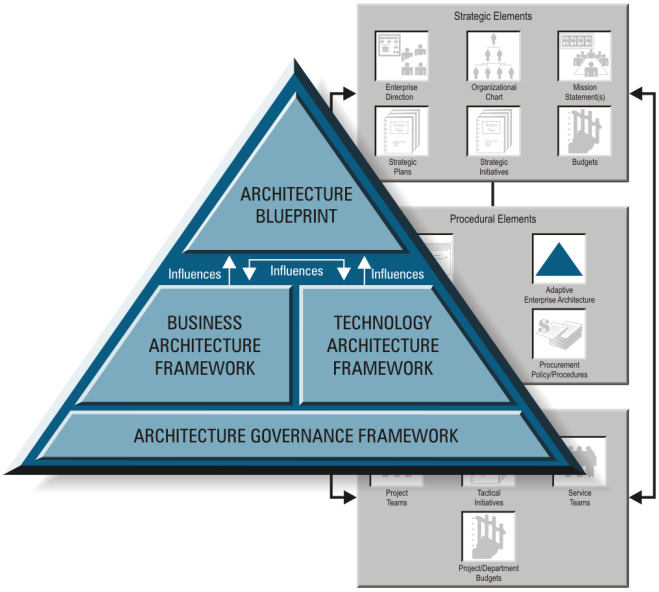


Figure 5. EA Supports Enterprise Elements

The Technology Architecture Framework can also influence the Business Architecture Framework. The affect the Internet has had in changing the way businesses interact with their customers is a good example of how technology can influence business.

The Technology Architecture Framework captures the IT enterprise principles, IT best practices, and IT technology trends.

It is through established processes and templates that the Business Architecture Framework and the Technology Architecture Framework are finalized and maintained. These processes and templates are

discussed in detail later in the Business Architecture and Technology Architecture sections of this Tool-Kit.

Once these foundation pieces of the enterprise architecture are in place, the Architecture Blueprint can be produced. The Technology Architecture Blueprint contains the data on products and compliance criteria that is documented, reviewed, and communicated throughout the enterprise. Technology Architecture Blueprints may differ in the levels and categories of information documented, but at a minimum, they must contain products and compliance criteria. The Architecture Blueprint is utilized by various builders of the Business/IT Portfolio to assure they are meeting the compliance criteria identified by the adaptive enterprise architecture.

ARCHITECTURE GOVERNANCE ROLES

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

- Ensuring the Enterprise 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 Framework and Blueprint.

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

Two types of governance roles are identified in this section: primary roles and supportive roles.

Primary roles are roles that consistently work with the Enterprise Architecture Framework Elements. Supportive roles differ from primary roles in that they work with the Enterprise Architecture Framework Elements on an as-needed basis. Eight primary roles and seven supportive roles are identified to aid in governing the on-going Architecture lifecycle:

ARCHITECTURE GOVERNANCE 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 Methodology Communicator • Special Interest Groups • Enterprise Executive

Figure 6 shows the primary and supportive roles and their close relationships within the Enterprise Architecture Framework.

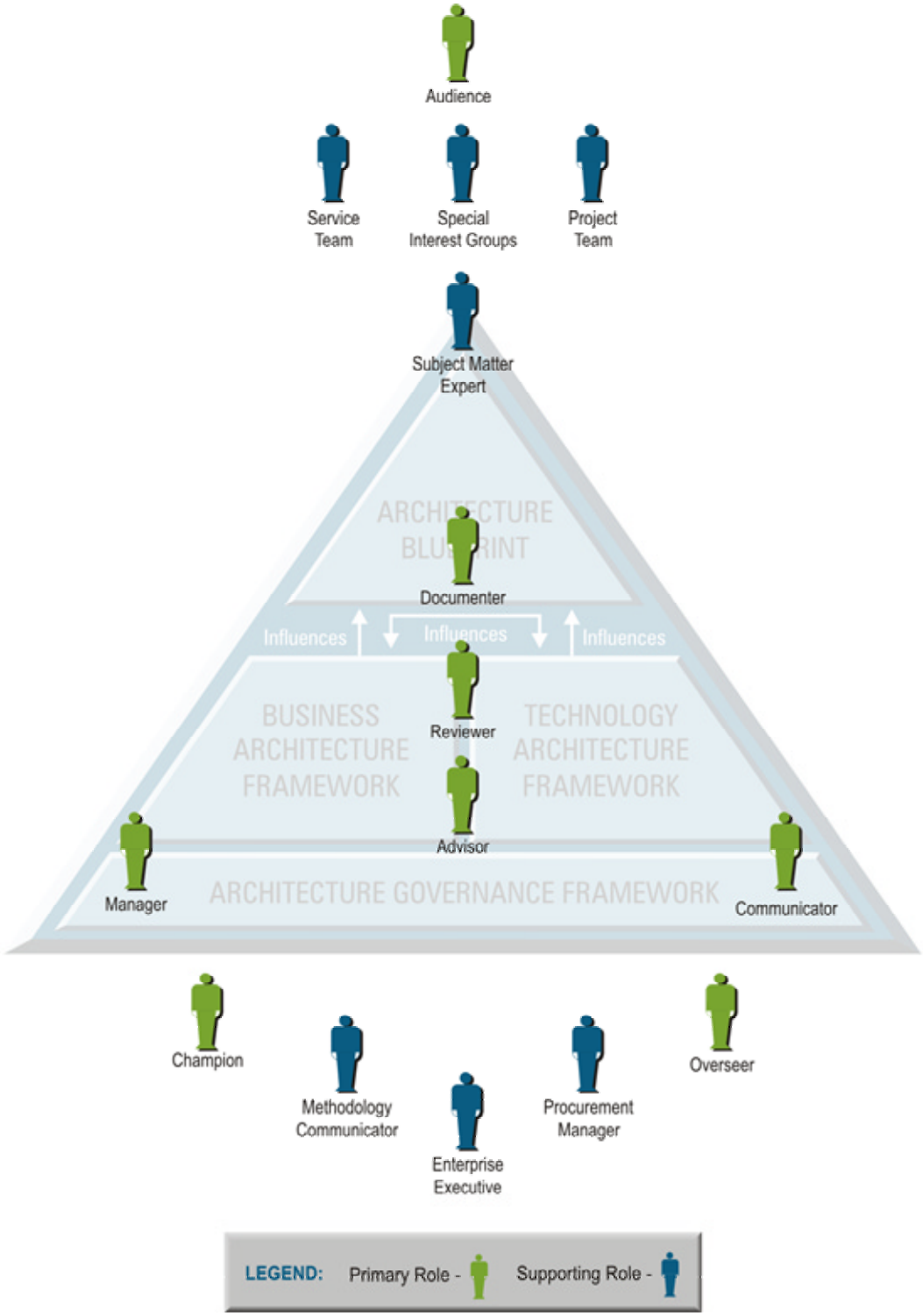


Figure 6. Roles & Responsibilities

Each of the governance roles is described in detail in this section. For each role the following information is provided:

- *Description* – The role and its relationship to other roles.
- *Implementation recommendations* – Is the role better implemented as a committee or as a single position?
- *Checks and Balances* – Should this role be implemented in combination with other roles and what combinations to avoid.
- *Full-time / Part-Time* – Is the role typically considered full-time or part-time.
- *Role Significance* – Is the role critical, necessary, or helpful. If the role is critical or necessary, a comment addressing the risk of non-implementation is provided under "Missing Role Risk".
- *Missing Role Risk* – An explanation of the risk incurred if the role is missing from the governance model. Included only for critical or necessary roles.

Appendix C 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.

PRIMARY ROLES

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 is best implemented as a 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, Communicator, and Subject Matter Expert. 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.
- *Role Significance:* Helpful
- *Missing Role Risk:*

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.
- *Role Significance:* CRITICAL
- *Missing Role Risk:* Lack of executive support and enterprise visibility. Enterprise architecture effort would not be empowered.

Manager

- *Description:* The Manager is an executive that 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 individuals to fulfill enterprise architecture roles 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 approving or rejecting enterprise architecture requests. 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 who can see what 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 Advisor is not recommended.
- *Full-time/ Part-Time:* The Manager role is recommended as full-time.
- *Role Significance:* CRITICAL
- *Missing Role Risk:* Lack of guidance and a single consistent vision.

Documenter

- *Description:* The Documenter can be either a senior and junior level IT staff. A Documenter's primary responsibility is to maintain the various Governance Elements. Based on the Documenter's scope, which is directed by the Manager, the Documenters maintain the following:
  - Architecture Governance Framework
  - Business Architecture Framework
  - Technology Architecture Framework
  - Architecture Blueprint

  The first three 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 is responsible for providing information regarding updates to the various Enterprise Architecture Framework Elements to the Reviewer and the Communicator. After the Documenter receives the results of the evaluation from the Reviewer, the Documenter 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 is best implemented as a committee. A consensus opinion must be put into the documentation. Architecture Blueprint 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 can be combined with the role of Subject Matter Expert, Support Teams, and/or Project Teams. The combination of role of Documenter with the role of Reviewer and/or Communicator is not recommended.
- *Full-time/ Part-time:* The role of Documenter is recommended as part-time. At the start of the Architecture Blueprint documentation period, this may be a full-time role.
- *Role Significance:* CRITICAL
- *Missing Role Risk:* No documented business or technical architecture blueprint 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 roles of:
  – 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 is not recommended.

- *Full-time/ Part-time:* The Communicator role is recommended as part-time.

- *Role Significance:* CRITICAL

- *Missing Role 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 is 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.
- *Role Significance:* Necessary
- *Missing Role Risk:* A well-rounded perspective of the enterprise needs and requirements will be absent**.**

Reviewer

- *Description:* The Reviewer can 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, Subject Matter Expert, Support Teams, and/or Project Teams. The combination of role of Reviewer with the role of Documenter is not recommended.
- *Full-time/ Part-time:* The Reviewer role is recommended as part-time.
- *Role Significance:* CRITICAL
- *Missing Role Risk:* Lacking more than one set of eyes for quality assurance and variety of perspectives.

Audience

- *Description:* The Audience 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:* Please 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.
- *Role Significance:* Necessary
- *Missing Role Risk:* Lack of architecture stakeholders. Must identify those held accountable for compliance and ensure communications are delivered in a timely manner.

SUPPORTIVE ROLES

Subject Matter Experts

- *Description:* An internal or external group that provides knowledge on a given subject. Subject Matter Experts contribute information to the following:
  - Documenter
  - Reviewer
  - Service Teams
  - Project Teams
- *Implementation Recommendation:* This role is best when implemented as a committee or a group. More than one opinion must be put into the expert advice.
- *Checks and Balance:* This role can be combined with the Documenter, Support Teams, and/or Project Teams. The combination of role of Subject Matter Expert with the role of Reviewer of the same effort is not recommended.
- *Full-time/ Part-time:* This Subject Matter Expert role is recommended as part-time.
- *Role Significance:* Necessary
- *Missing Role Risk:* Possible mandate of incorrect product or compliance criteria.

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:* The role of the Services Team is a part-time user of the enterprise architecture.
- *Role Significance:* Necessary
- *Missing Role 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:* The role of Project Team is a part-time user of the enterprise architecture.
- *Role Significance:* Necessary
- *Missing Role 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. The role 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 role of Procurement Manager is a part-time advisor to the enterprise architecture groups.
- *Role Significance:* CRITICAL
- *Missing Role Risk:* This role is critical to the purchasing of new services and technologies for the enterprise. This role is critical to enterprise architecture; to verify 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 role of Project/ Services Methodology Communicator is a part-time advisor to the enterprise architecture groups.
- *Role Significance:* Necessary
- *Missing Role 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:* The role of Special Interest Groups should not be combined with any other role.
- *Full-time/ Part-time:* This Provider role is recommended as part-time.
- *Role Significance:* HELPFUL
- *Missing Role 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 full-time.
- *Role Significance:* CRITICAL
- *Missing Role 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 in 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.

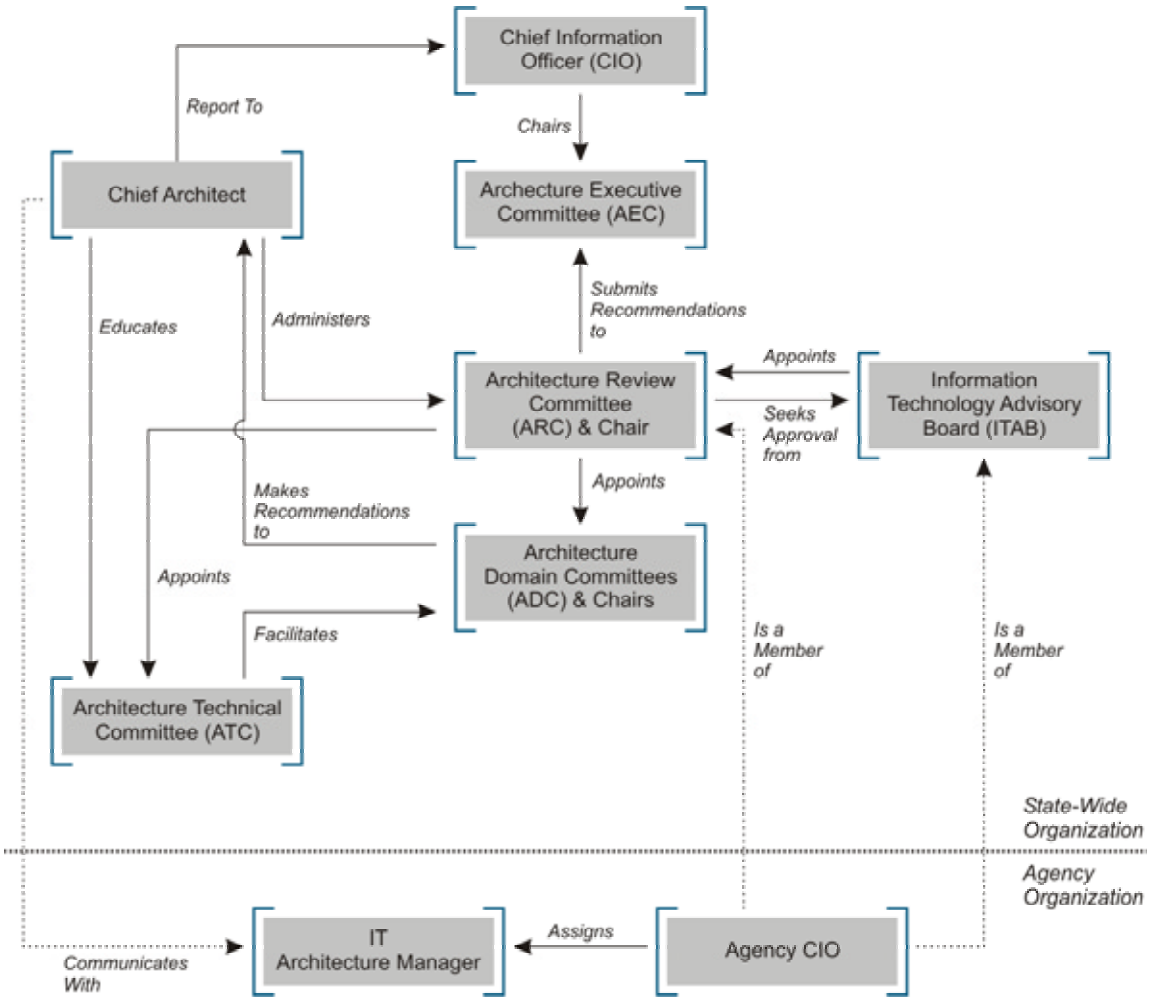
The requirement to keep the three branches of government separate prevents an in-depth involvement and is more strictly enforced in some enterprise environments. Kentucky's illustrated governance model is a good example of this situation. Originally, the judicial branch participated as a voting member 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 the successful Architecture Governance Models that have been 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.



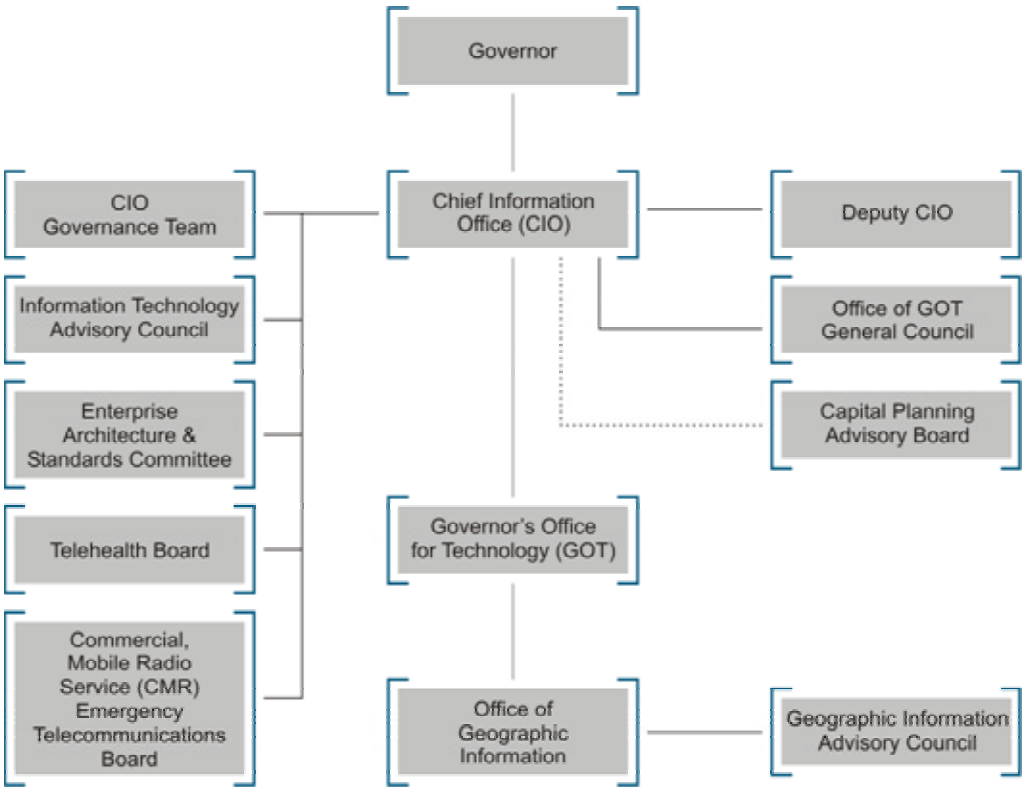
Significant Organizational Functions

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.



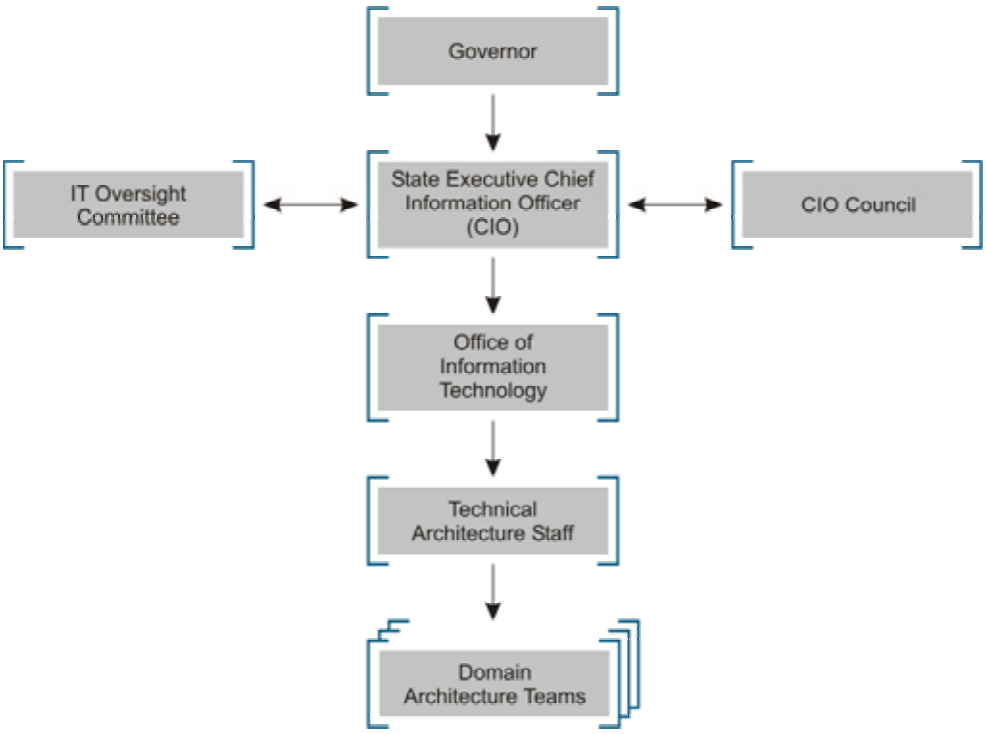
Significant Organizational Functions

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.



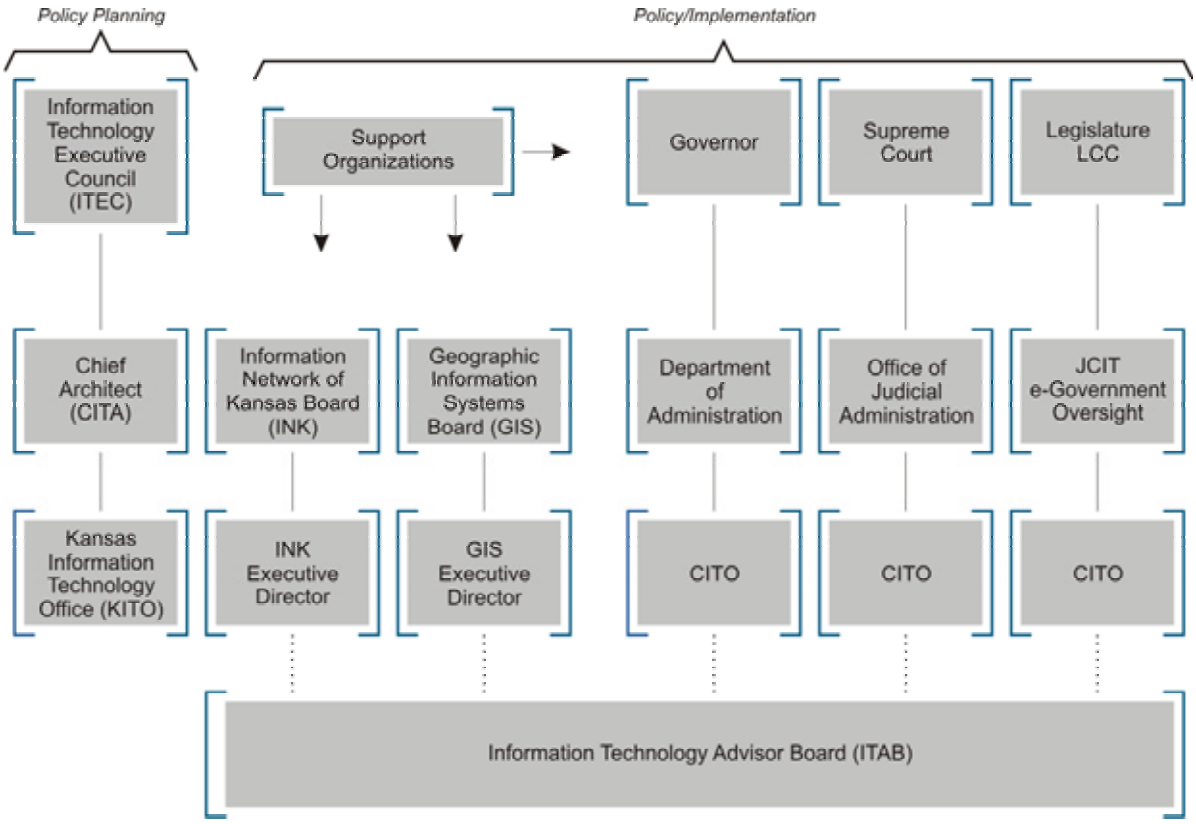
Significant Organizational Functions

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.



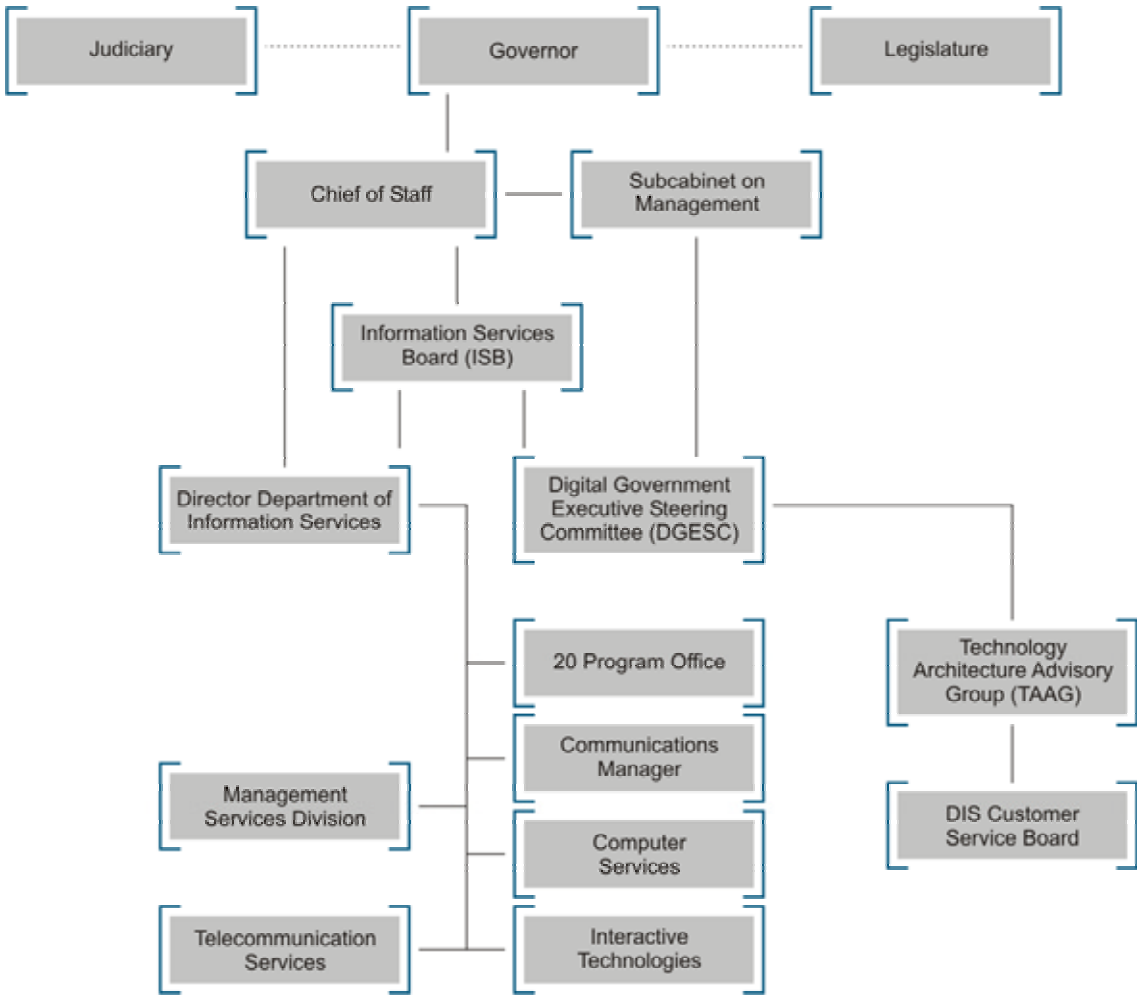
Significant Organizational Functions

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.



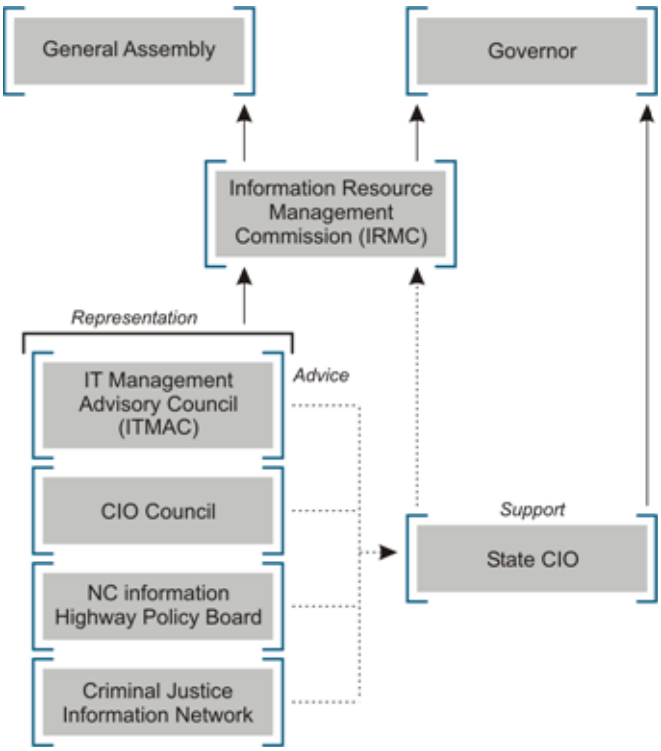
Significant Organizational Functions

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.



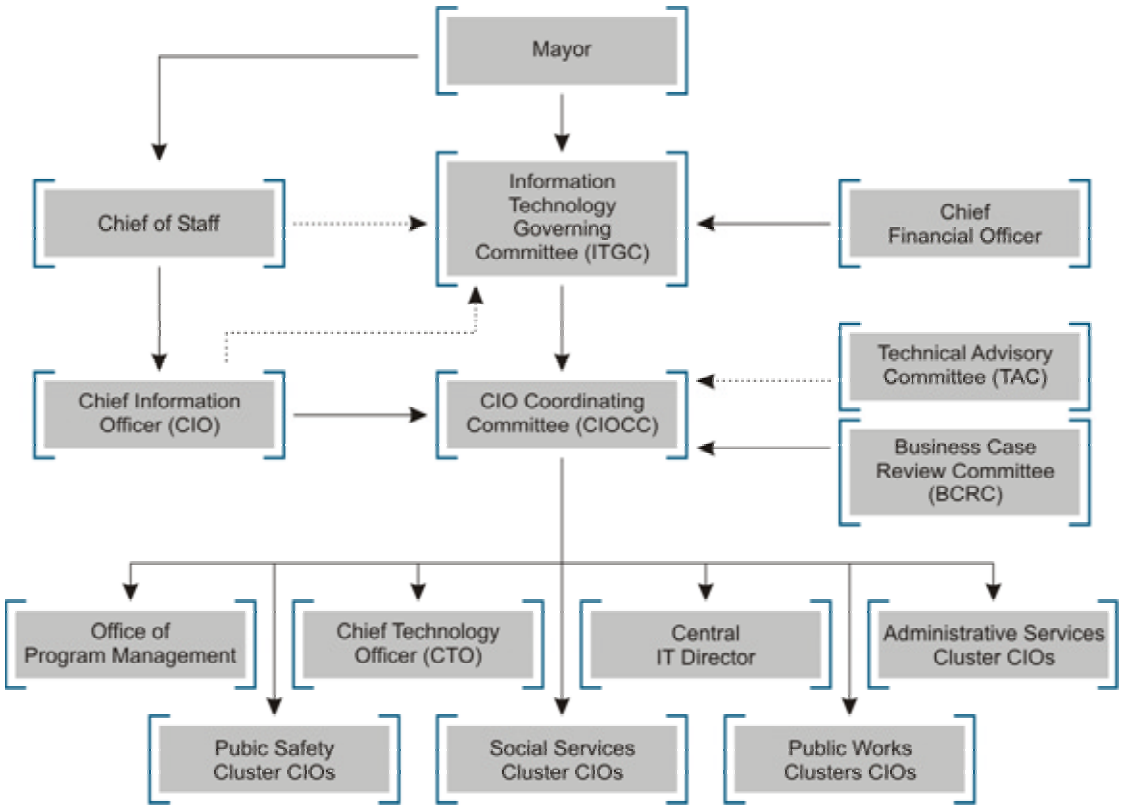
Significant Organizational Functions

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 to Governor and is Secretary of IRMC. Identifies IT polices for IRMC. Provides statewide common IT services – computing, telecommunications, etc. Responsible for statewide IT strategies, initiatives, and QA.	Champion, Manager
Information Resource Management Commission (IRMC)	Top statewide policymaking body, commissions IT committees including the Technical Architecture and Project Certification, Information Privacy and Protection, and E-Government Steering Committees.	Overseer, Documenter, Reviewer, Communicator
IT Management Advisory Council (ITMAC)	Agency business leaders provide representation on the IRMC and advice to the CIO.	Advisor
CIO Council	Agency CIOs provide representation on the IRMC and advice to the CIO.	Subject Matter Expert
NC Information Highway Policy Board	The board provides representation on the IRMC and advice to the CIO.	Subject Matter Expert
Criminal Justice Information Network Board	The board provides representation on the IRMC and advice to the CIO.	Subject Matter Expert

Local Government – Philadelphia, Pennsylvania

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



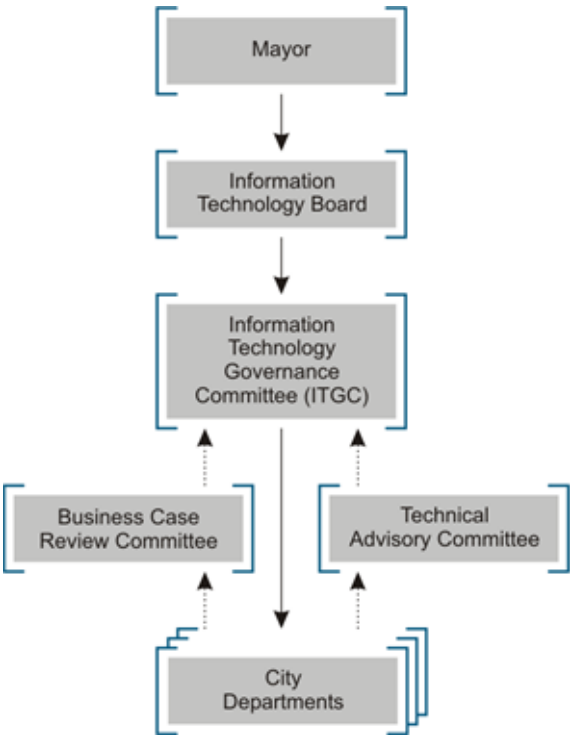
Significant Organizational Functions

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.



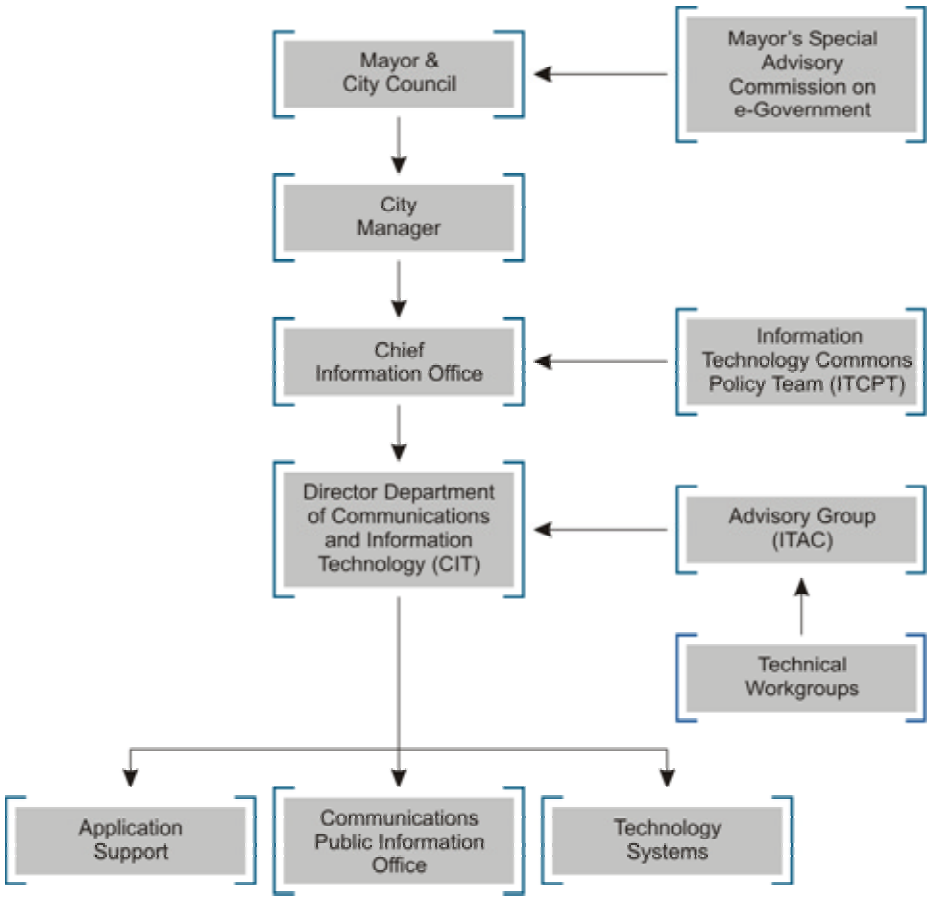
Significant Organizational Functions

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.



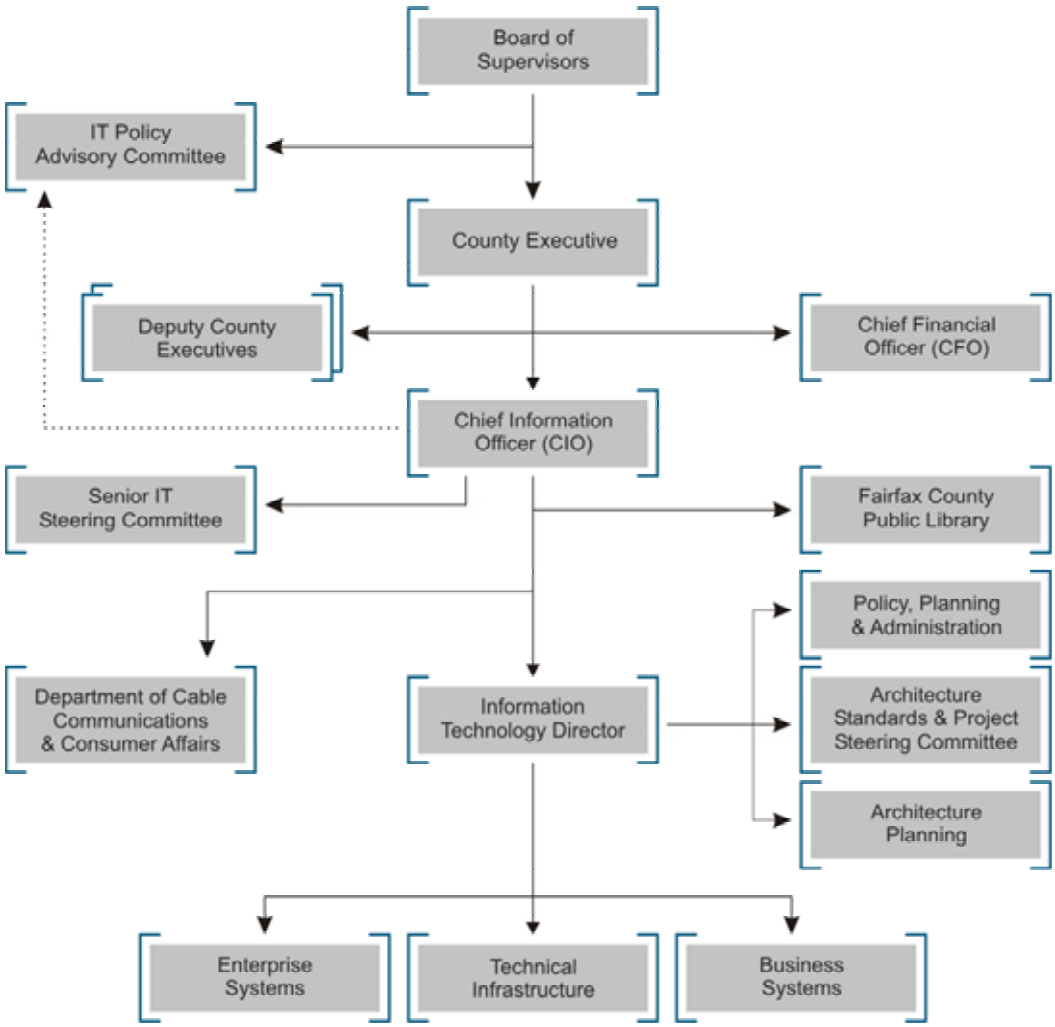
Significant Organizational Functions

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

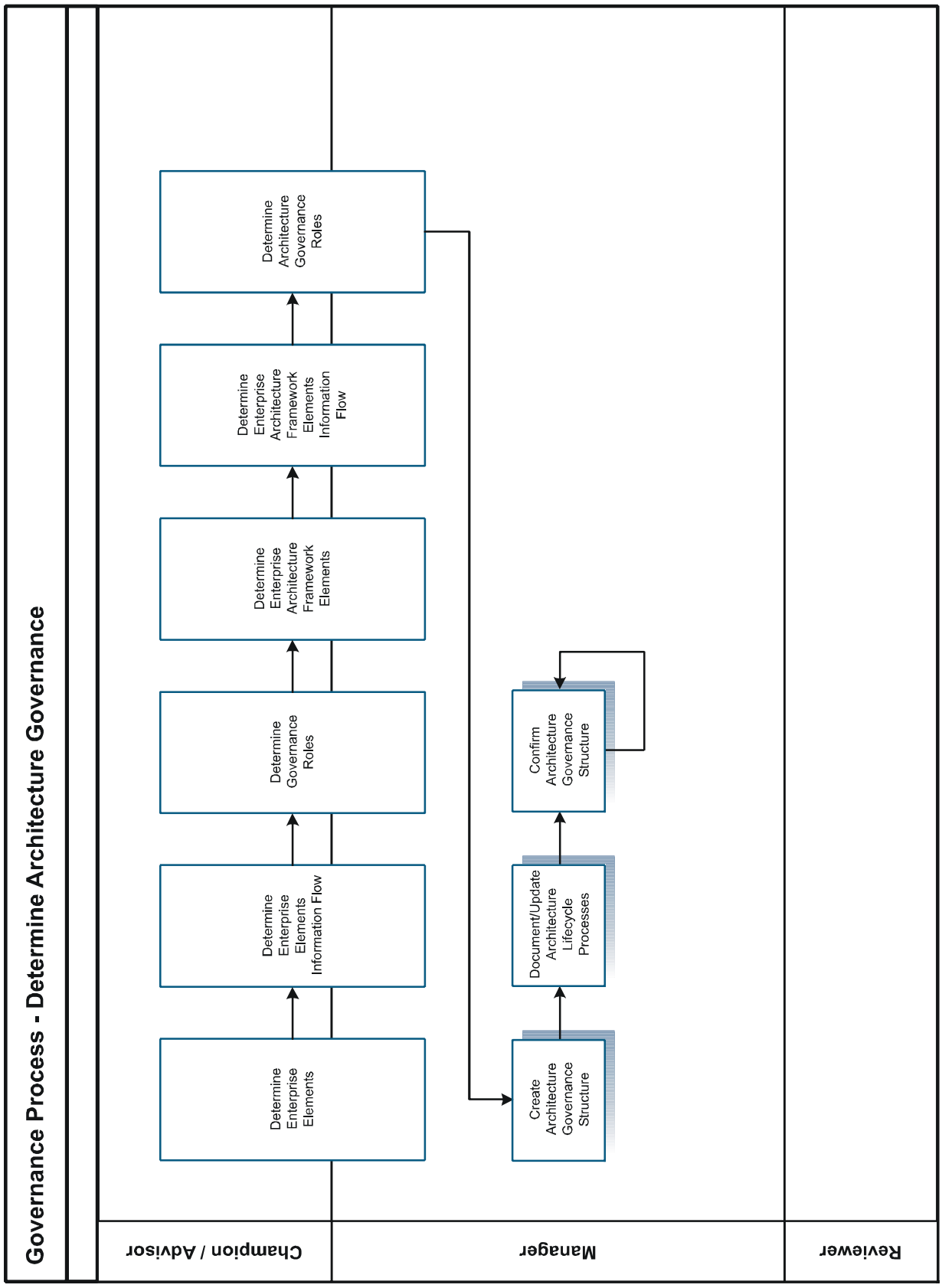
ARCHITECTURE GOVERNANCE PROCESS

This section identifies the process that can be used 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.


Governance Process - Determine Architecture Governance
Champion / Advisor
Manager
Reviewer
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

DETERMINE ARCHITECTURE GOVERNANCE

Define 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.

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

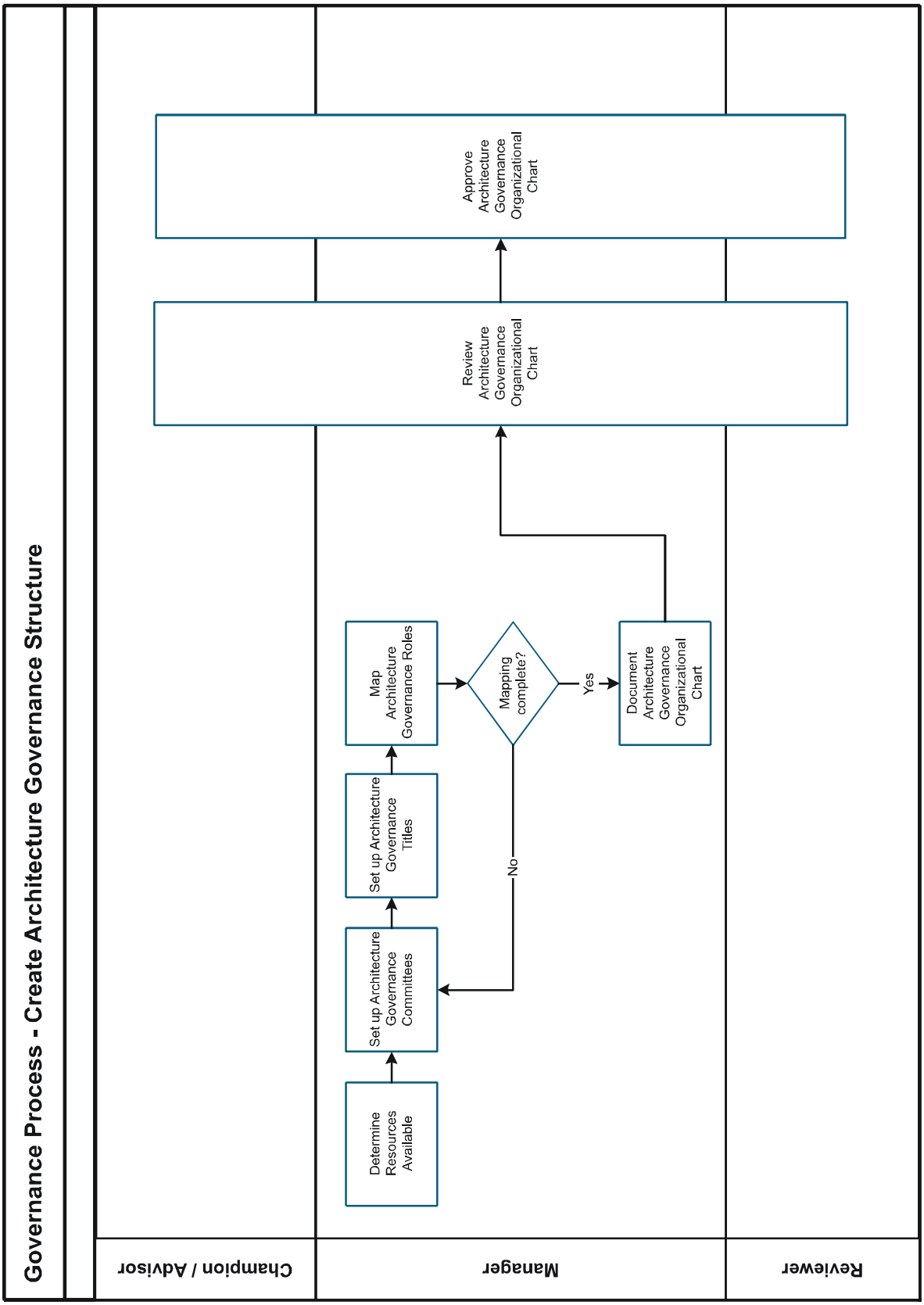
The roles can also play supporting positions such as:

- 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.


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

CREATE ARCHITECTURE GOVERNANCE STRUCTURE

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.

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.

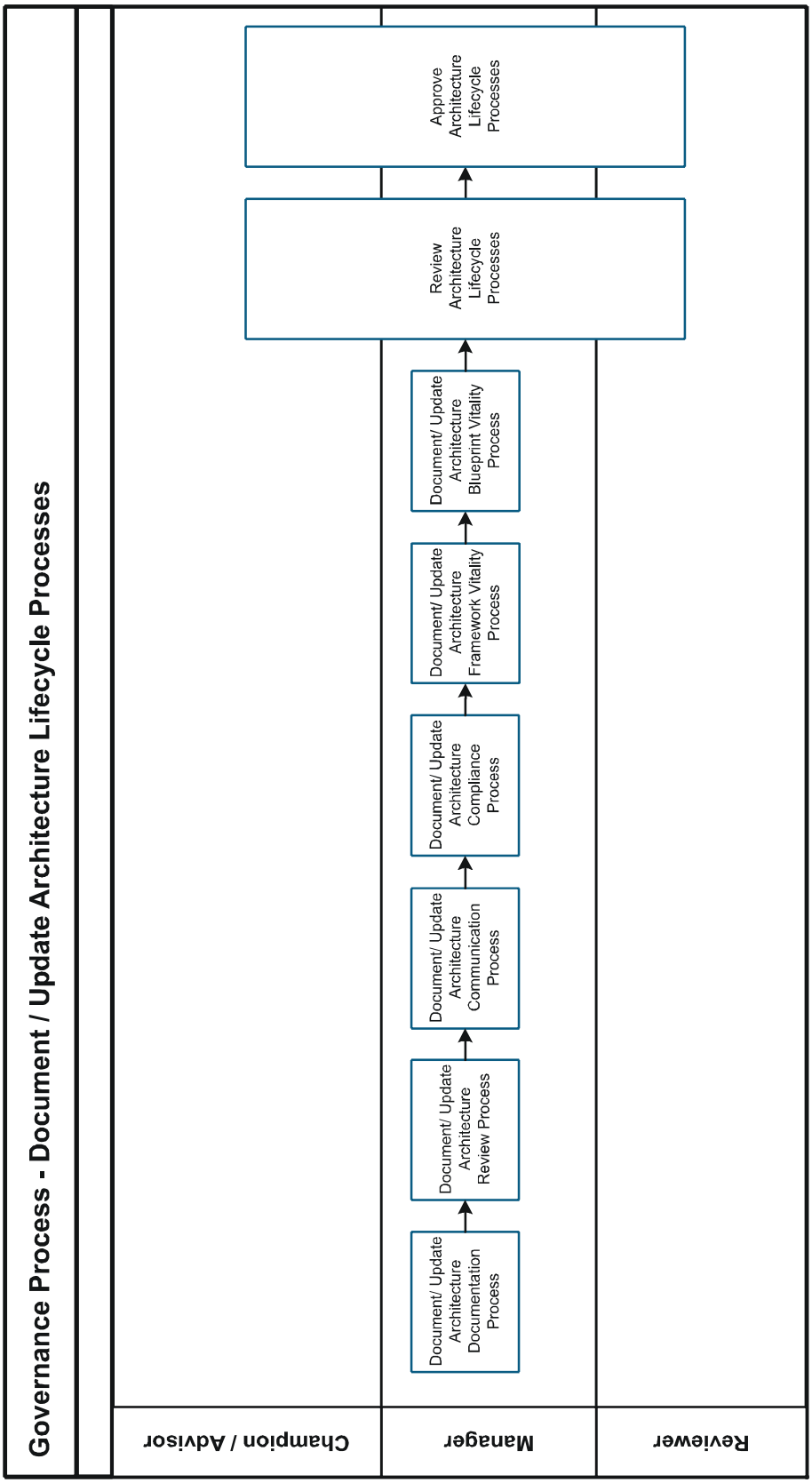
Map Architecture Governance Roles: Map the Architecture Governance Roles to the committees and titles. Document and map any remaining unmapped roles to existing committees or titles.

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.


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 Vitality Process
Document/ Update Architecture Blueprint Vitality Process
Review Architecture Lifecycle Processes
Approve Architecture Lifecycle Processes

DOCUMENT/UPDATE ARCHITECTURE LIFECYCLE PROCESSES

Determine and document the Architecture Lifecycle processes. Figure 7 illustrates the flow of the lifecycle processes over time.

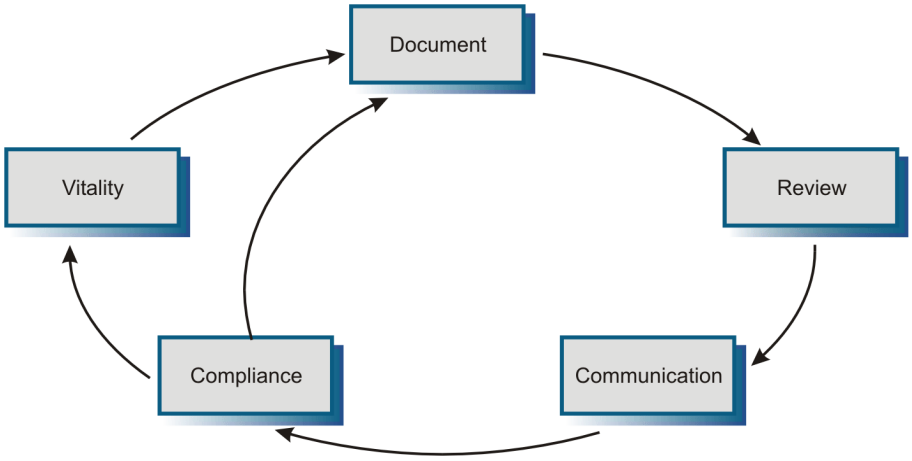


Figure 7. Architecture Lifecycle Process

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. After the policies, procedures, and compliance criteria are finalized and communicated, a variance is required via the Compliance Process for any deviation from the stated compliance criteria. Conduct the Vitality process on the Architecture Blueprint at a recommended minimum of every six months. On a less frequent basis, determined by changes in enterprise direction and technology, the Enterprise Architecture Framework will undergo the compliance 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 following processes must be accomplished in order to set the stage for this lifecycle to begin.

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
    - Technology Architecture Framework
  - Dynamic Information –
    - Technology Architecture Blueprint
      - Technology Architecture Blueprint Levels (Tool-Kit examples are: Domain Discipline, Technology Area, Product Component, and Compliance Component.)
    - Business Architecture Blueprint
      - Business Architecture Blueprint Level (Not determined at this time.)
- 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 Vitality Process: The Framework Vitality 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 Vitality Process must include:

- Events that can trigger changes:
  - New Business Strategic Elements
    - Possible changes in:
      - Business Architecture Framework
      - Technology Architecture Framework
  - New IT Strategic Elements
    - Possible changes in
      - Technology Architecture Framework
  - Modification to Enterprise Architecture Framework Elements (Governance, Architecture Lifecycle Processes, and/or Architecture Blueprint Templates)
    - Possible changes in:
      - Business Architecture Framework
      - Architecture Blueprint
  - Modification to Business Architecture Framework
    - Possible changes in:
      - Technology Architecture Framework
  - Modifications to Technology Architecture Framework
    - Possible changes in:
      - Architecture Blueprint

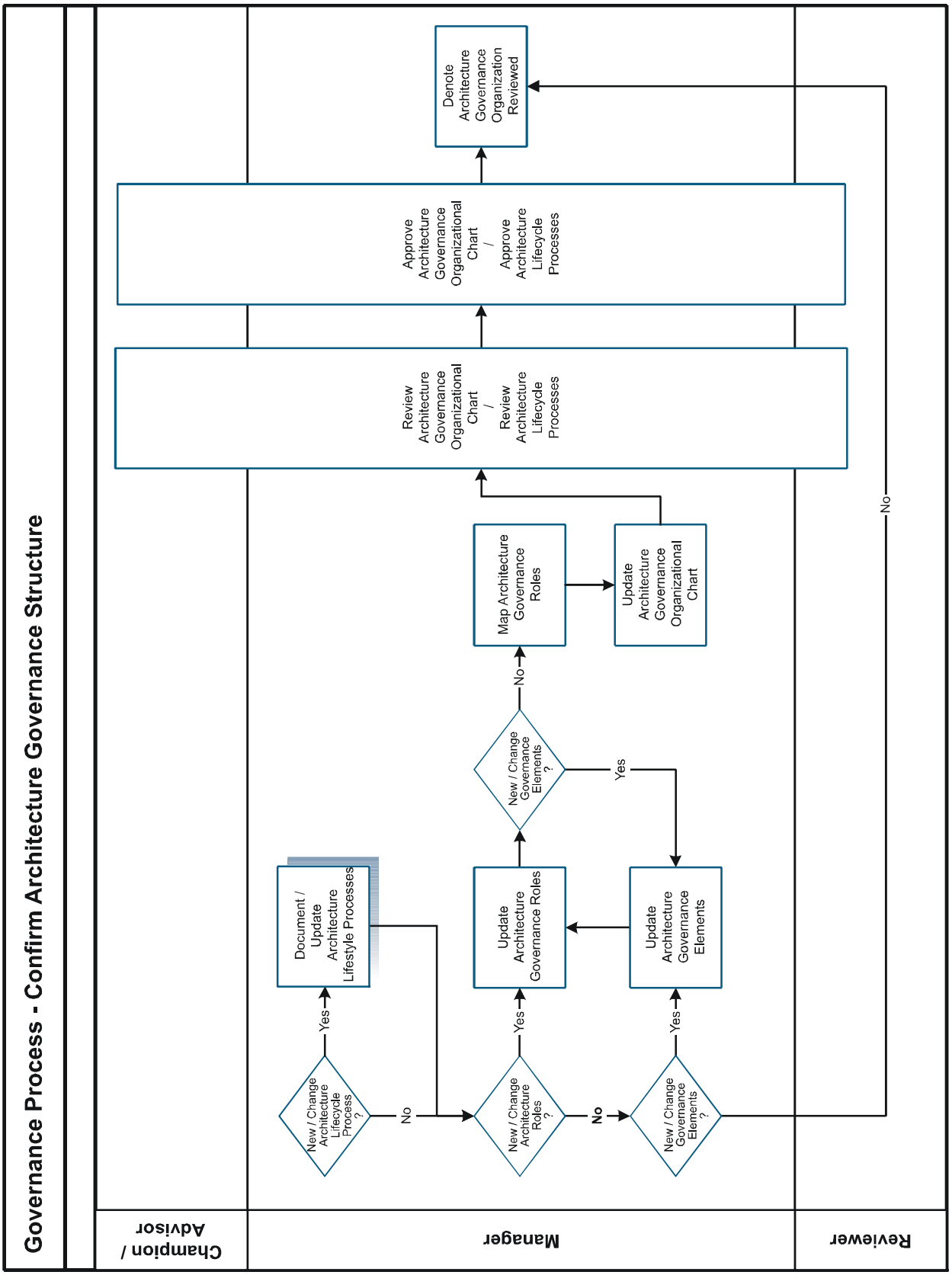
- Best time for initiating periodic reviews.
- Feedback methods to improve the processes, templates, and governance in the adaptive enterprise architecture.
- Training on changes to the Adaptive Enterprise Architecture Framework Manual.

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.


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

CONFIRM ARCHITECTURE GOVERNANCE STRUCTURE

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.

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 enterprise 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 – Shows 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?
- In mapping this role to a specific committee or position will the mapping 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 Process Overview (Figure 8) shows how the architecture lifecycle processes interact with each other to create a continuous cycle of renewal of these dynamic elements.

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

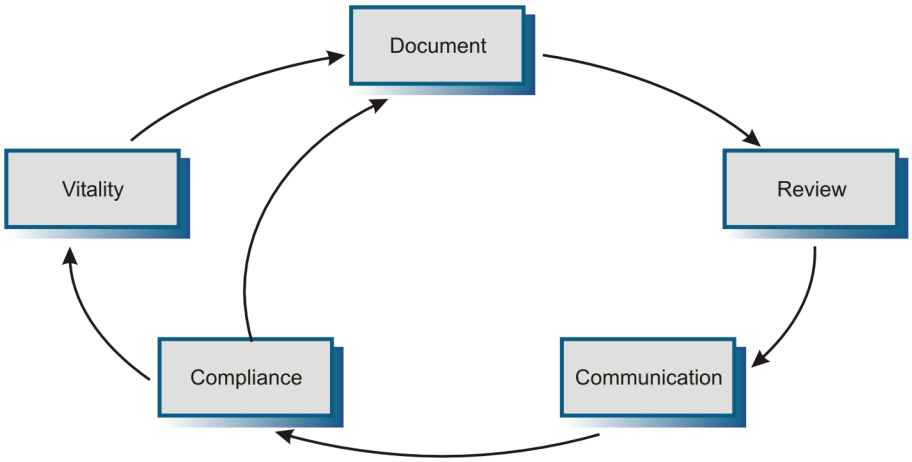


Figure 8. Architecture Life Cycle Process

The cycle of renewal is achieved with a structure of re-usable processes, discussed in detail here.

Architecture Lifecycle Processes Overview: The Architecture Lifecycle Processes are integral pieces of the overall Architecture Governance Framework used to implement technology solutions within government. There are six primary processes:

- Architecture Documentation Process
- Architecture Review Process
- Architecture Compliance Process
- Architecture Communication Process
- Architecture Framework Vitality Process
- Architecture Blueprint Vitality Process

Major deliverables from these processes include:

- Updates to the Adaptive Enterprise Architecture Framework Manual (manual developed by governments for their organization)
- 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.

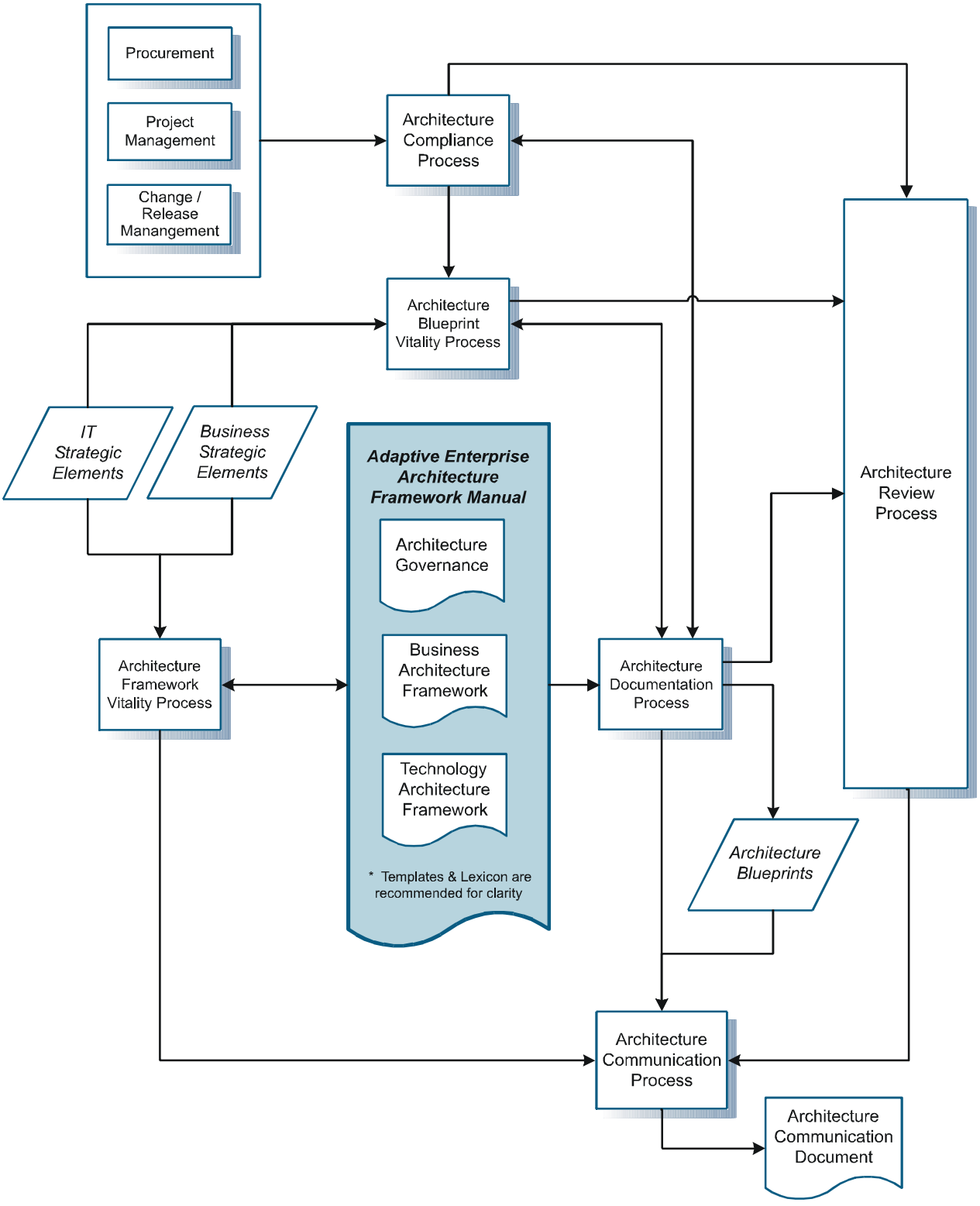


Figure 9. Architecture Lifecycle Processes

ARCHITECTURE DOCUMENTATION PROCESS

The Architecture Blueprint articulates the organization's business and technology architecture, providing classifications for products and compliances as emerging, current, twilight, and sunset. Products and compliances are also denoted as accepted or rejected during the creation and review of the Architecture Blueprint. From this documentation process, a wealth of information will exist to aid agencies in determing technology solutions.

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

Documenters, identified by the Architect 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 Vitality 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.

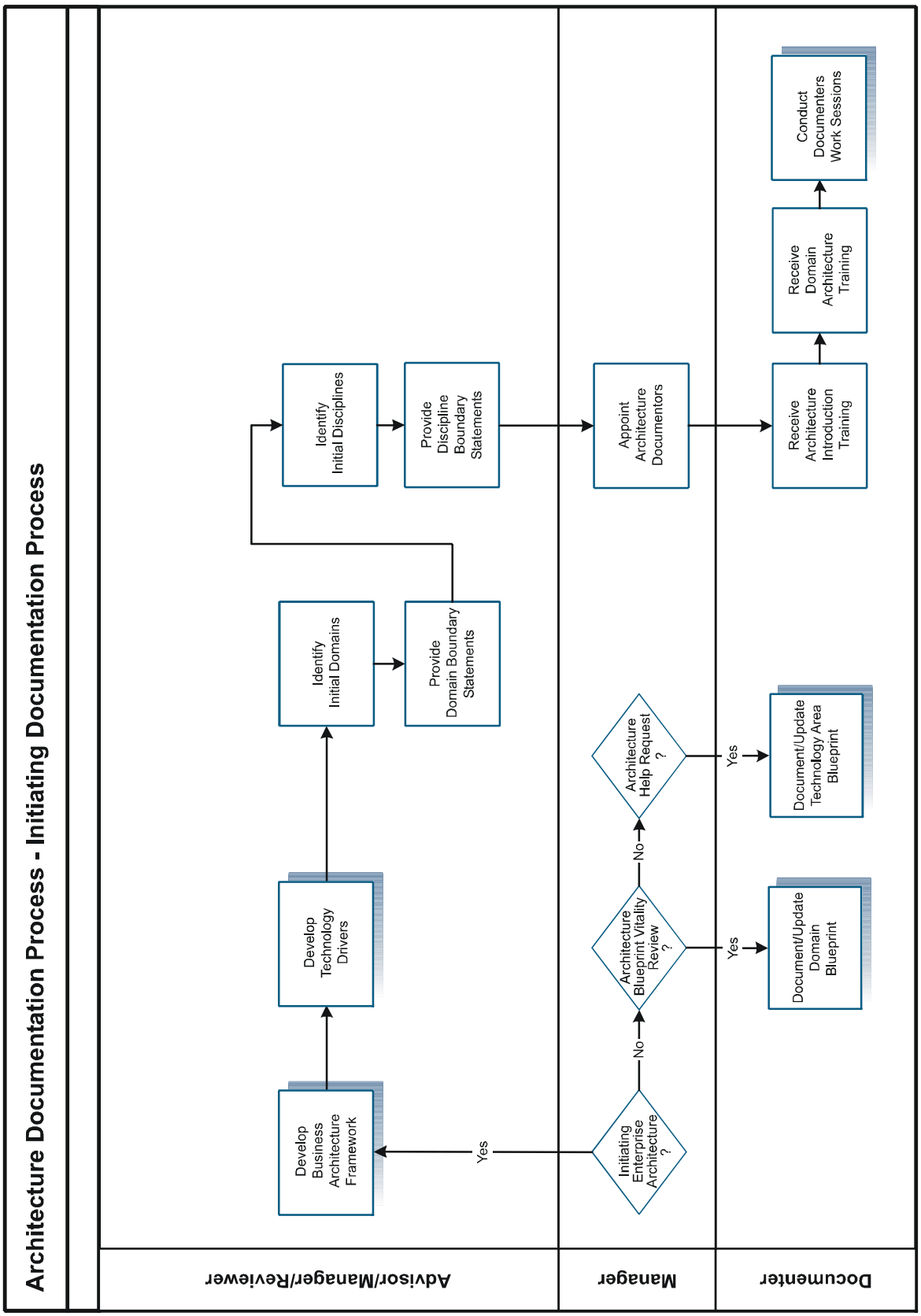
The Architecture Documentation Process applies to both Business and Technology with two sub-processes:

- Outline Domain and train Documenters
- Conduct Documenter work sessions

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

The processes that are specific to business or technology continue in detail within their respective sections of the Tool-Kit:

- Business Architecture Blueprint Framework
- Technology Architecture Blueprint Framework


Architecture Documentation Process - Initiating Documentation Process
Advisor/Manager/Reviewer
Manager
Documenter
Develop Business Architecture Framework
Develop Technology Drivers
Identify Initial Domains
Provide Domain Boundary Statements
Identify Initial Disciplines
Provide Discipline Boundary Statements
Initiating Enterprise Architecture ?
Yes
No
Architecture Blueprint Vitality Review ?
Yes
No
Architecture Help Request ?
Yes
Appoint Architecture Documentors
Document/Update Domain Blueprint
Document/Update Technology Area Blueprint
Receive Architecture Introduction Training
Receive Domain Architecture Training
Conduct Documenters Work Sessions

INITIATING DOCUMENTATION PROCESS

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.

Develop Business Architecture Framework: The information documented within the Business Architecture Framework will play an important role in the development of the Technology Architecture Blueprints and will include items like the creation of the Business Drivers. The processes and templates for development of the Business Architecture Framework are not included in the Tool-Kit at this time; however, they are purposed for future versions of the Tool-Kit.

Develop Technology Drivers, Identify Initial Domains, Provide Domain Boundary Statements, Identify Initial Disciplines, and Provide Discipline Boundary Statements: The Architecture Committee develops and provides:

- Technology Drivers (IT Enterprise Principles, IT Best Practices, and Technology Trends.)
- A definition for each identified Domain and Discipline.
- Parameters for identifying the boundaries of each Domain and Discipline.

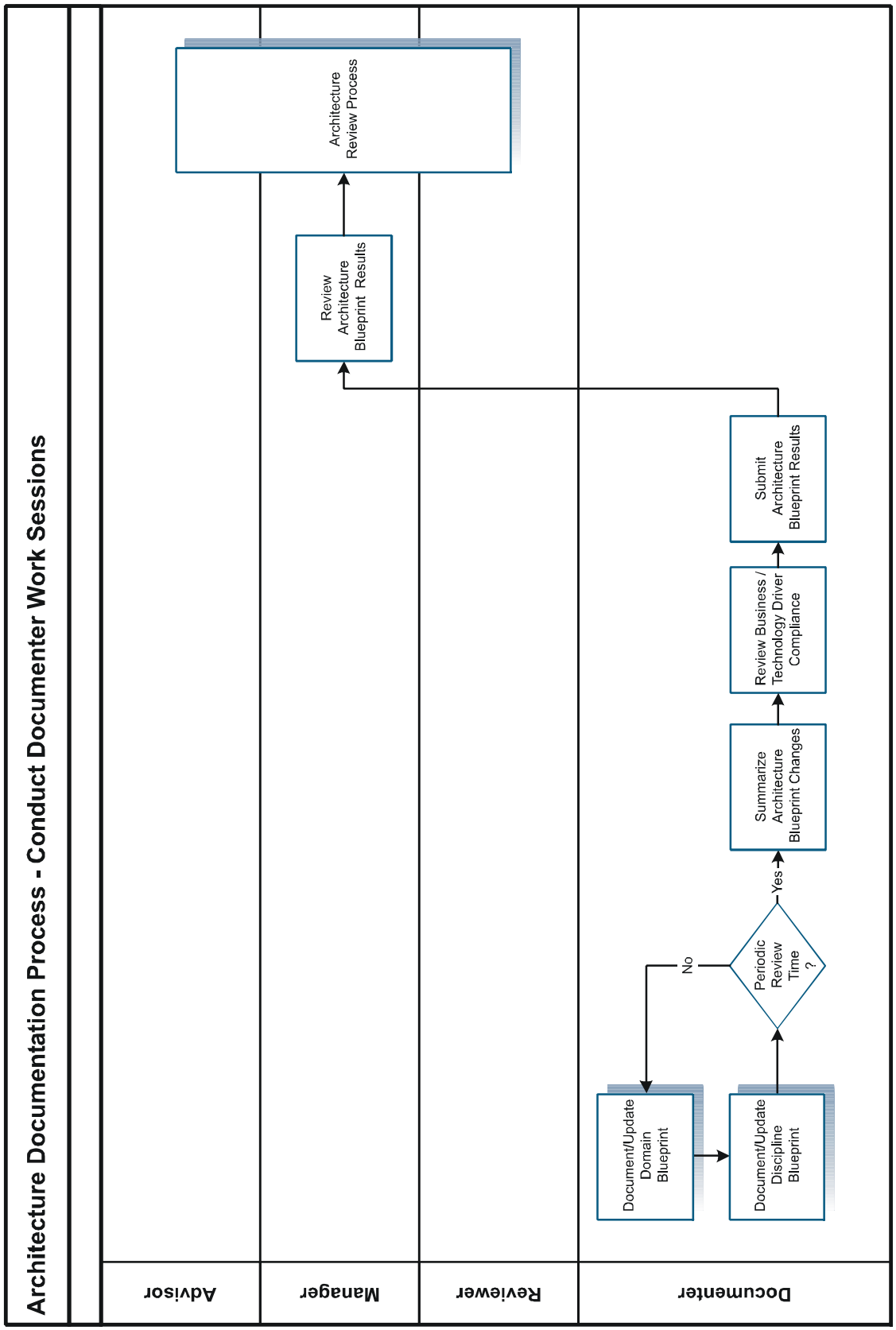
Document Reviewer Domain/Discipline Information: All of the information developed and gathered in the previous processes will be documented and fed into the educational sessions and Documenter working sessions.

Appoint Architecture Documenters: After all of this is developed, the Documenters will be appointed from subject matter experts familiar with the organization's IT environment.

Receive Architecture Introduction Training, Receive Domain Architecture Training, and Conduct Documenter Work Sessions: These committees will receive three progressive educational sessions:

- Architecture Introduction – Covering the overall enterprise architecture and architecture governance.
- Domain Architecture Training – Addressing the technology architecture documentation templates and technology architecture documentation processes.
- Documenter Work Sessions – Applying knowledge gained in first two sessions to begin development of the Domain Architecture Blueprint documentation.

The objective of the Documenters is to develop or select Compliance Components (guidelines, standards, and mandates) for the various levels of the Architecture Blueprint. The level of detail in each Domain's Architecture Blueprint may vary depending on the requirements for specificity. Some may only identify guideline compliances at the Discipline level, while others may have very definitive standards for configurations at the product level. It is the purview of the Documenter to determine the appropriate level of specificity required. This decision should be documented in the Discipline Documentation Requirements section of the Discipline Template.


Architecture Documentation Process - Conduct Documenter Work Sessions
Advisor
Manager
Reviewer
Documenter
Architecture Review Process
Review Architecture Blueprint Results
Document/Update Domain Blueprint
Document/Update Discipline Blueprint
Periodic Review Time ?
No
Yes
Summarize Architecture Blueprint Changes
Review Business / Technology Driver Compliance
Submit Architecture Blueprint Results

CONDUCT DOCUMENTER WORK SESSIONS

These 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.

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

Summarize Architecture Level Changes: Based on changes occurring since the last periodic review, the Documenter will pull together a summary. This summary should list all changes to the Architecture Blueprint for that Domain throughout the five levels.

Review Business/Technology Driver Compliance: The submitted changes for a specific Domain may cause a conflict with one of the Business/Technology 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, provide the proper documentation to the Architecture Manager.

Submit Architecture Blueprint Results: Based on time or completion of a documentation process, pull together 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: Present and review the prepared Domain Results at the next Architecture Review Meeting.

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.

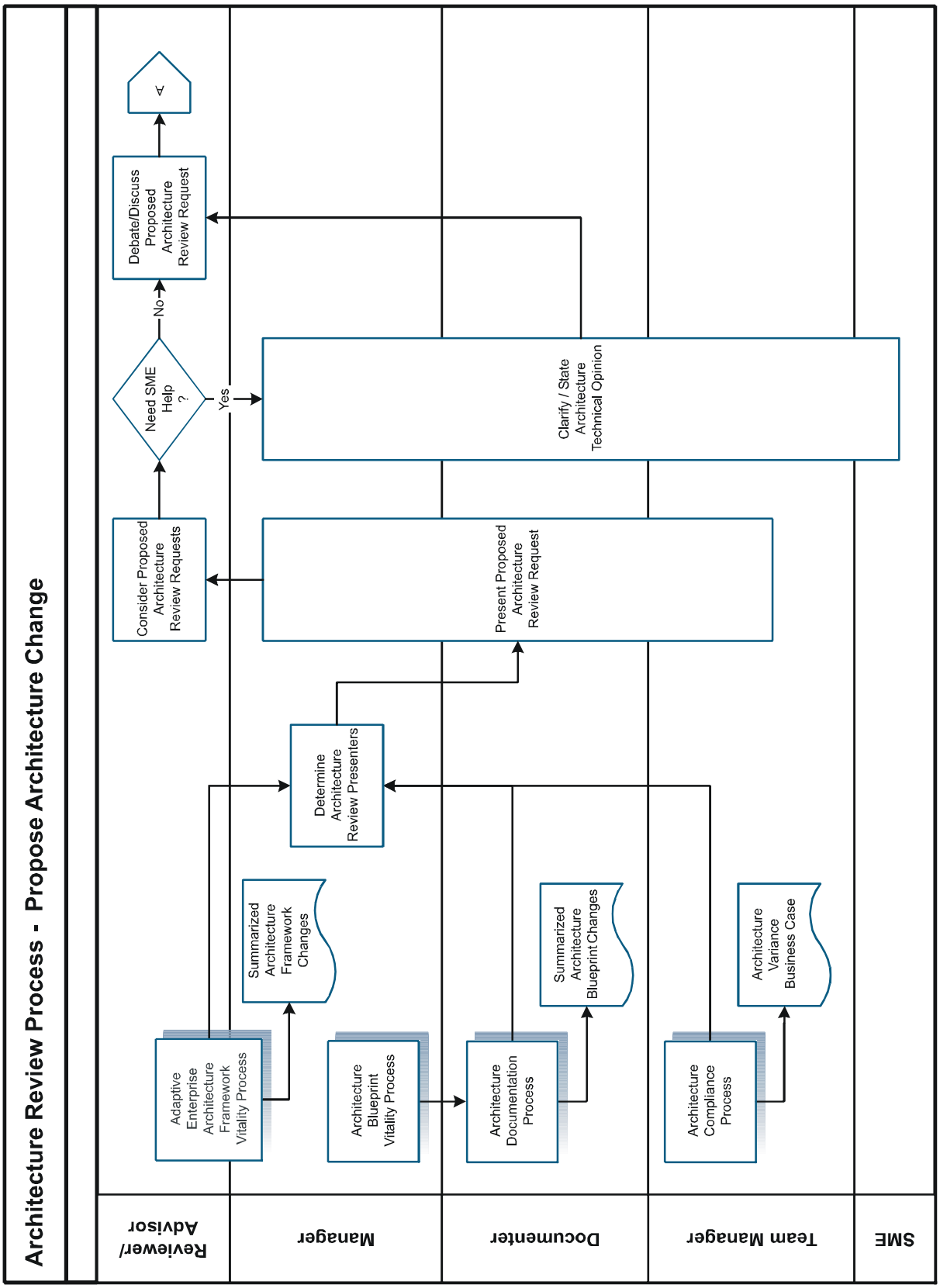
The proposed architecture changes may be triggered from any of the following processes:

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


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

PROPOSE ARCHITECTURE CHANGE

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 Vitality 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 Vitality 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

Determine Architecture Review Presenters, Present Proposed Architecture Review Request: 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.

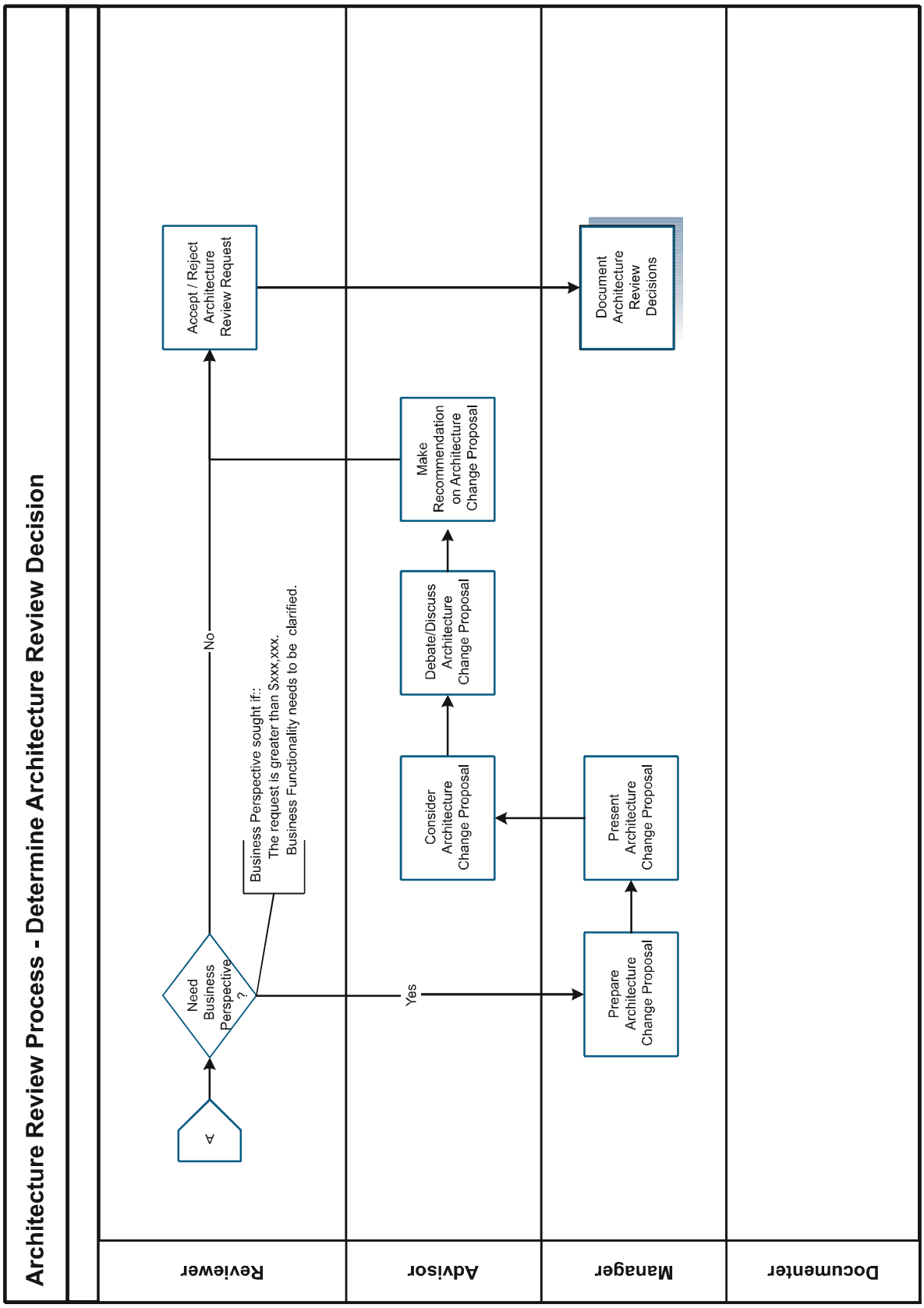
Consider Proposed Architecture Review Requests: For each proposed change the Reviewers should consider:

- Impact on the Technology 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 Technical 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.


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 needs to be 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

DETERMINE REVIEW DECISION

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.

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.

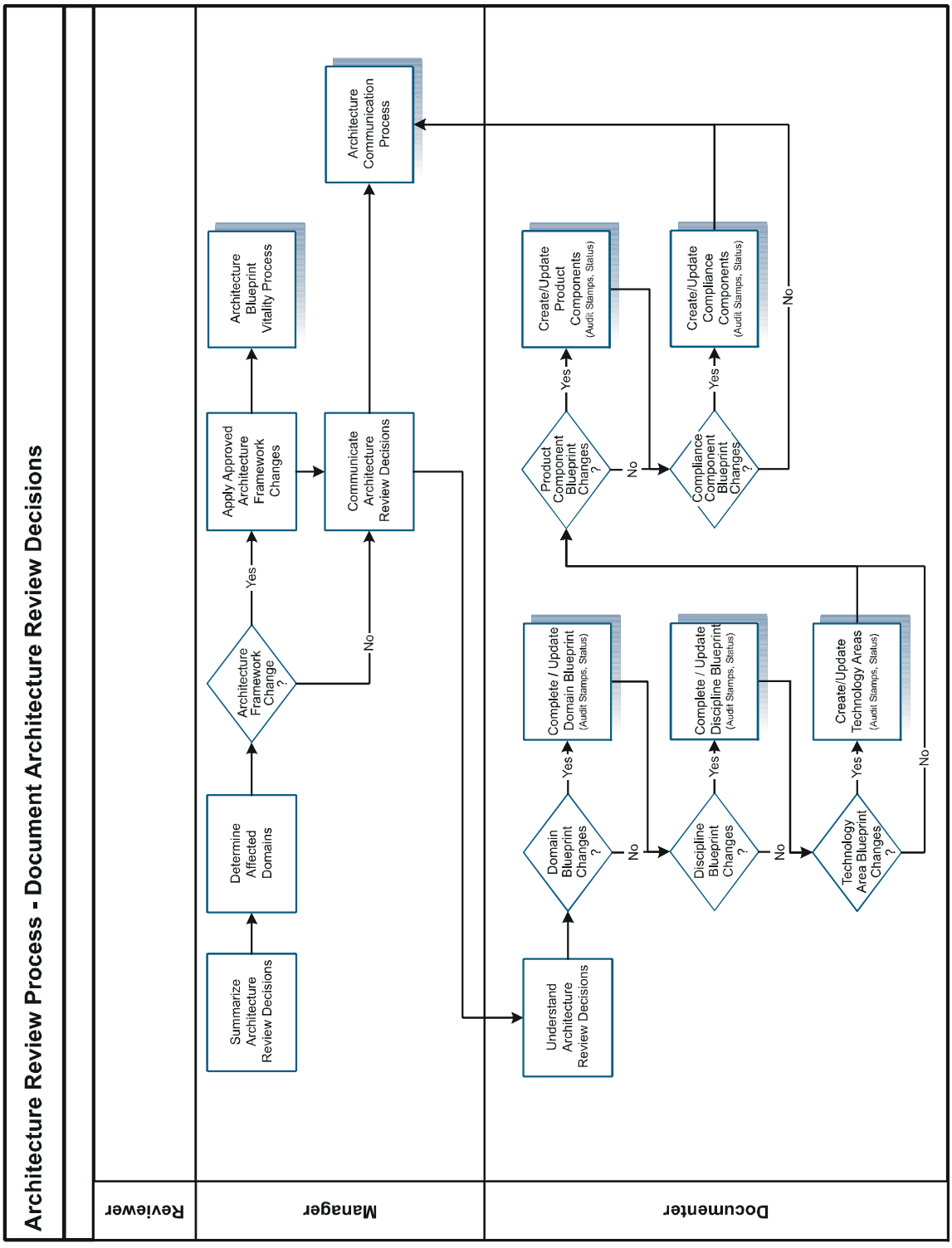
Debate/Discuss Architecture Change Proposal: The Advisors weigh the pros and cons from the business perspective to make a determination toward accepting or rejecting the change. As with the Reviewers, the Advisors will also consider the immediate, as well as the long-term needs of the organization.

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.


Architecture Review Process - Document Architecture Review Decisions
Reviewer
Manager
Documenter
Summarize Architecture Review Decisions
Determine Affected Domains
Architecture Framework Change ?
Yes
No
Apply Approved Architecture Framework Changes
Architecture Blueprint Vitality Process
Communicate Architecture Review Decisions
Architecture Communication Process
Understand Architecture Review Decisions
Domain Blueprint Changes ?
Yes
No
Complete / Update Domain Blueprint (Audit Stamps, Status)
Discipline Blueprint Changes ?
Yes
No
Complete / Update Discipline Blueprint (Audit Stamps, Status)
Technology Area Blueprint Changes ?
Yes
No
Create/Update Technology Areas (Audit Stamps, Status)
Product Component Blueprint Changes ?
Yes
No
Create/Update Product Components (Audit Stamps, Status)
Compliance Component Blueprint Changes ?
Yes
No
Create/Update Compliance Components (Audit Stamps, Status)

DOCUMENT ARCHITECTURE REVIEW DECISION

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 Vitality 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.

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

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.

See Architecture Blueprint Templates – Domain Template for documentation requirements.

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 identifies changes to an existing Discipline, update the blueprint for the Discipline and other affected Disciplines to reflect the accepted or rejected change.

See Architecture Blueprint Templates – Discipline Template for documentation requirements.

Create/Update Technology Areas: If the accepted change identifies a new technology area, fully document the new technology area, including all subordinate levels. If the requested change identifies changes to an existing technology area, update the blueprint for the area to reflect the accepted or rejected change.

See Architecture Blueprint Templates – Technology Area Template for documentation requirements.

Create/Update Product Components: If the accepted change identified a new Product Component, fully document the new Product Component, including all subordinate levels. If the requested change identifies 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.

See Architecture Blueprint Templates – Product Component Template for documentation requirements.

Create/Update Compliance Components: If the accepted change identified a new Compliance Component, fully document the new Compliance Component. If the requested change identifies 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.

See Architecture Blueprint Templates – Compliance Template for documentation requirements.

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.

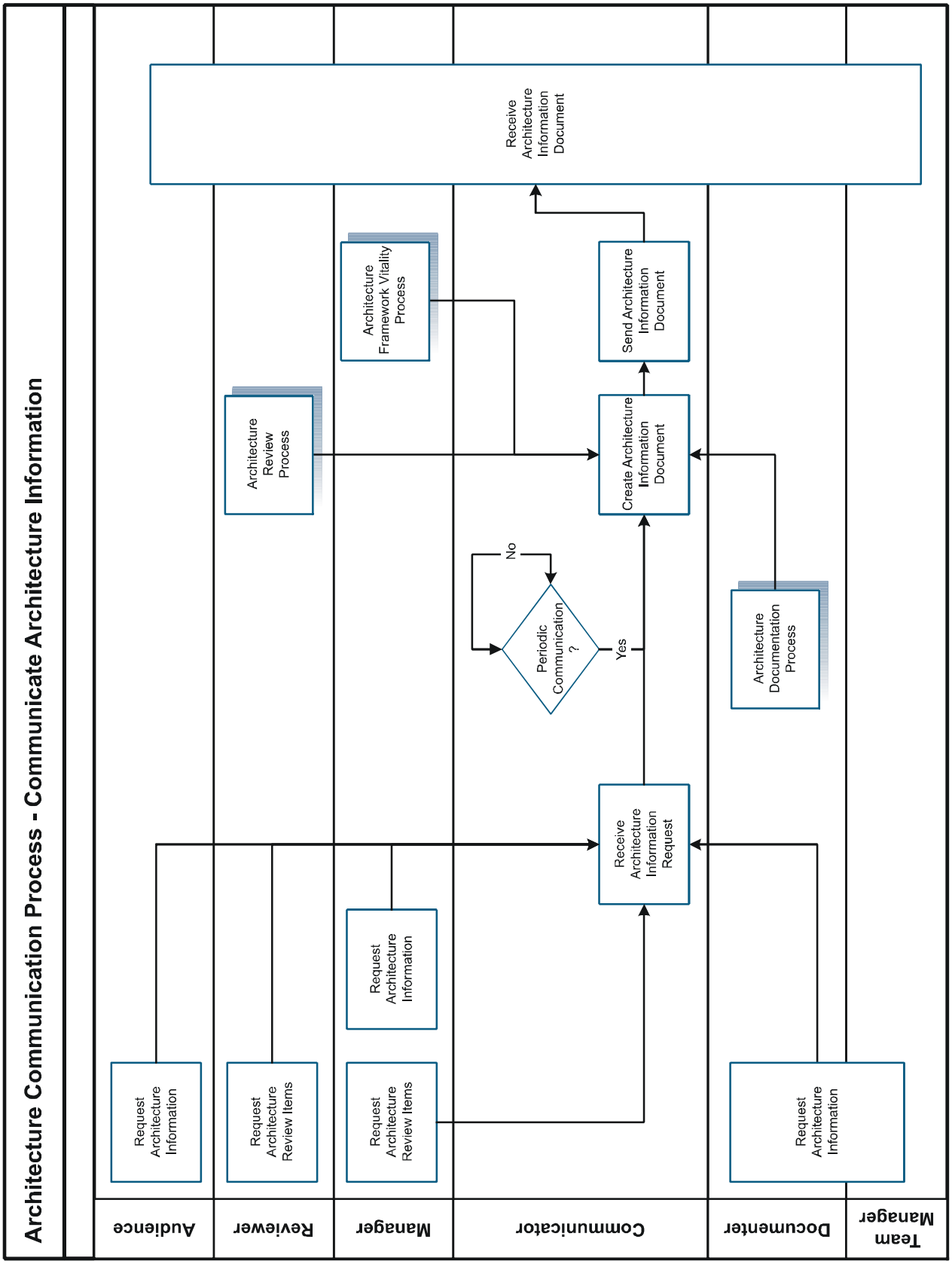
All users must have access to the latest version of the enterprise architecture documents and blueprints. A mechanism must exist to communicate the status and updated documentation to all users. Adequate communication of the enterprise architecture plays a vital role in ensuring that enterprise activities 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.


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

COMMUNICATE ARCHITECTURE INFORMATION

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.

Request Architecture Information: The Architecture Audience, Architecture Manager, and/or Architecture Documenter 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 Vitality 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 Vitality 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 product or compliance 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.

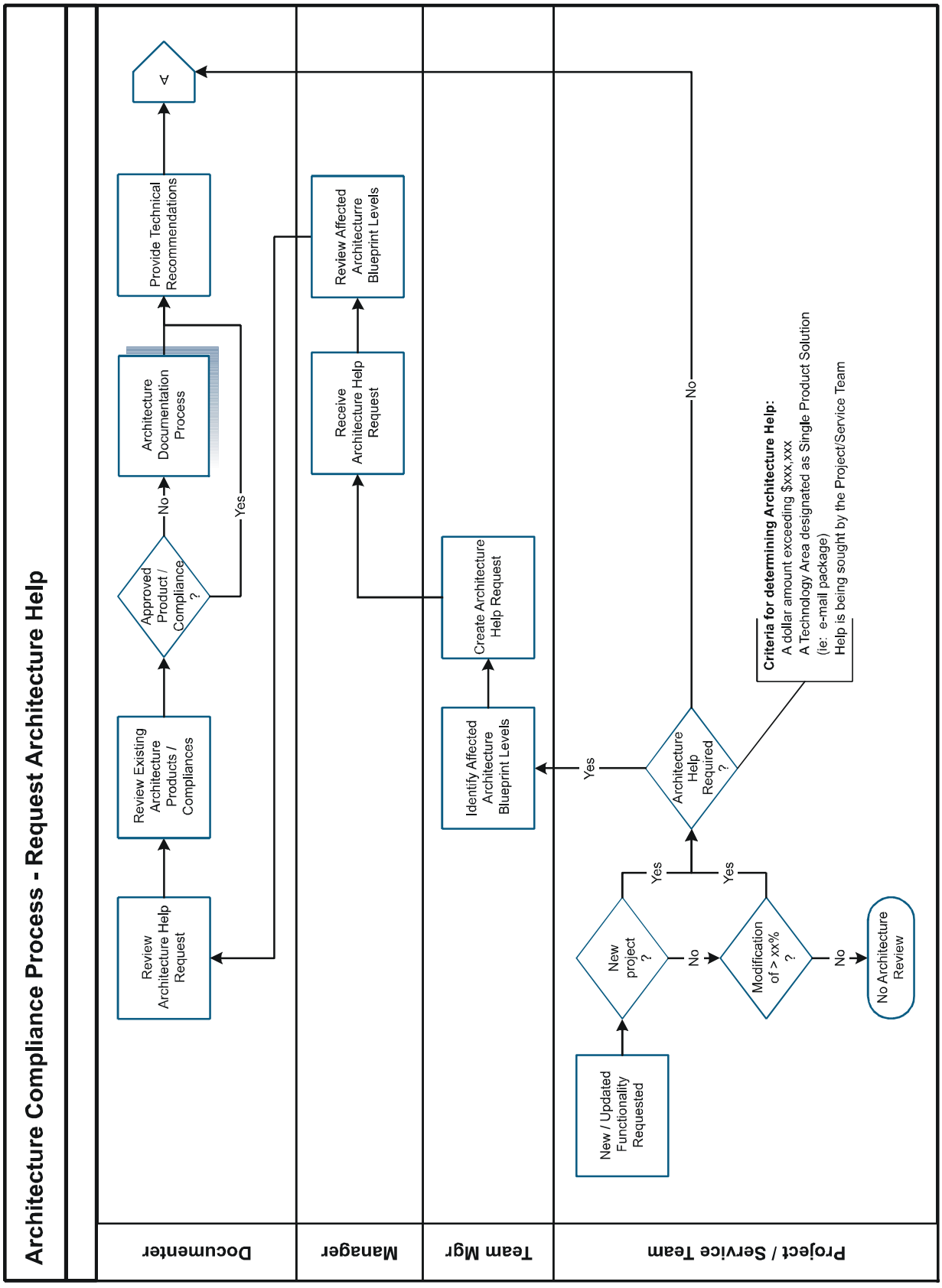
In every organization, there will be circumstances that will preclude the use of the documented standards. A formal compliance process is essential to allow for the review and acceptance of variances from the enterprise-wide architecture standards. Members of the organization will be allowed to submit 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 Technology Options
- Create Architecture Variance Business Case

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


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

REQUEST ARCHITECTURE HELP

New/Updated Functionality Requested: When there is a request to create or update functionality in the organization's information technology areas, first determine the scope of the request and then document the requirements. 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 technology 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 Levels: 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:

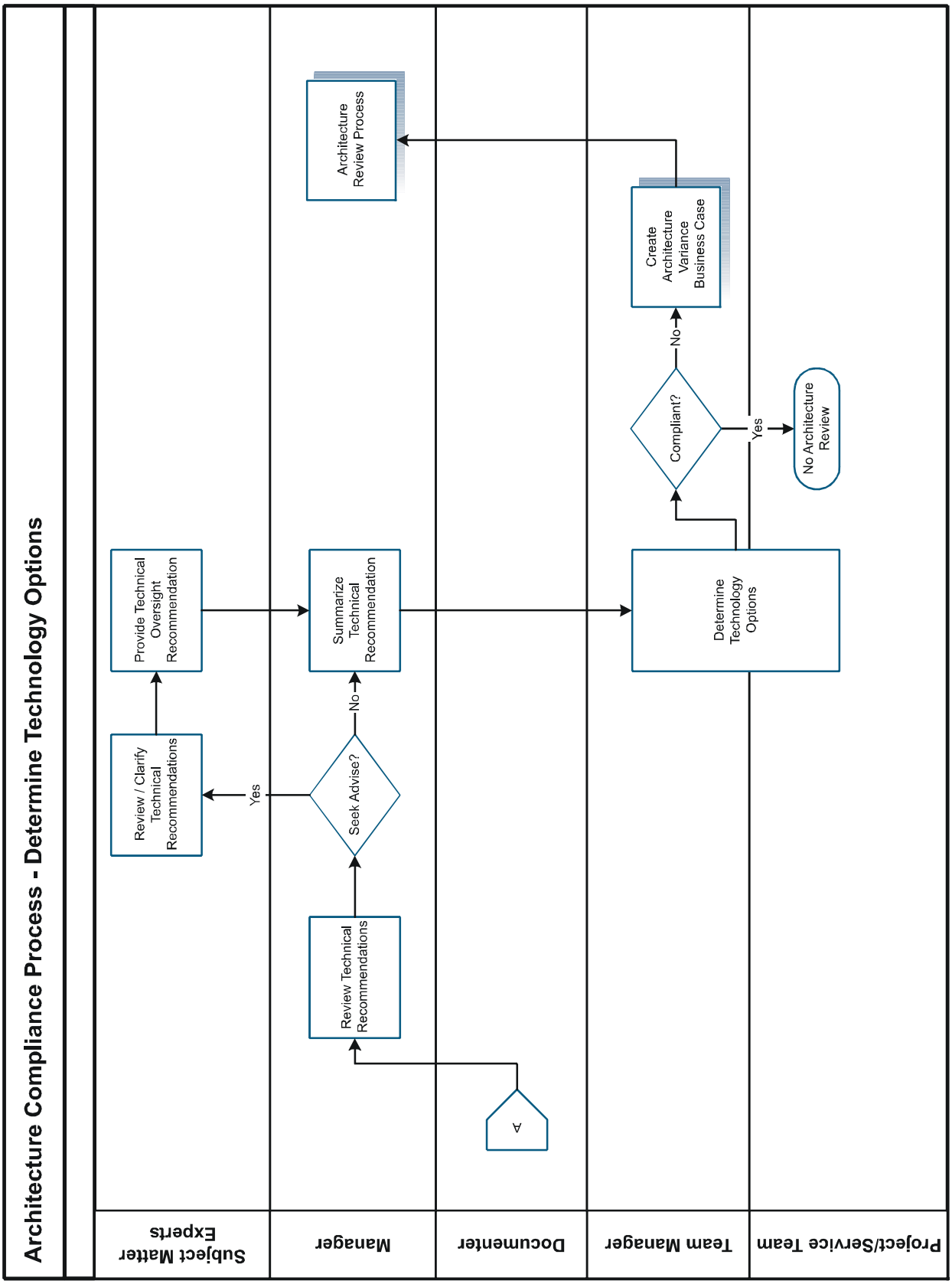
- Is there enough information to determine possible solutions?
- Has contact information for the person requesting been supplied?
- Has the resolution date been communicated?

Review Affected Architecture Blueprint Levels: The Architecture Manager, with help from the Reviewers and Advisors, will ensure that all affected Domains 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 Products/Compliances, and Document Architecture 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 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, executing 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 Technical Recommendations: Based on the reviews and evaluations conducted, the Documenters will make technical 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.


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

DETERMINE TECHNOLOGY OPTIONS

Review Technical 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 Technical Recommendations: The Subject Matter Experts aid the Compliance Process by reviewing and clarifying the recommendations provided by the Documenters.

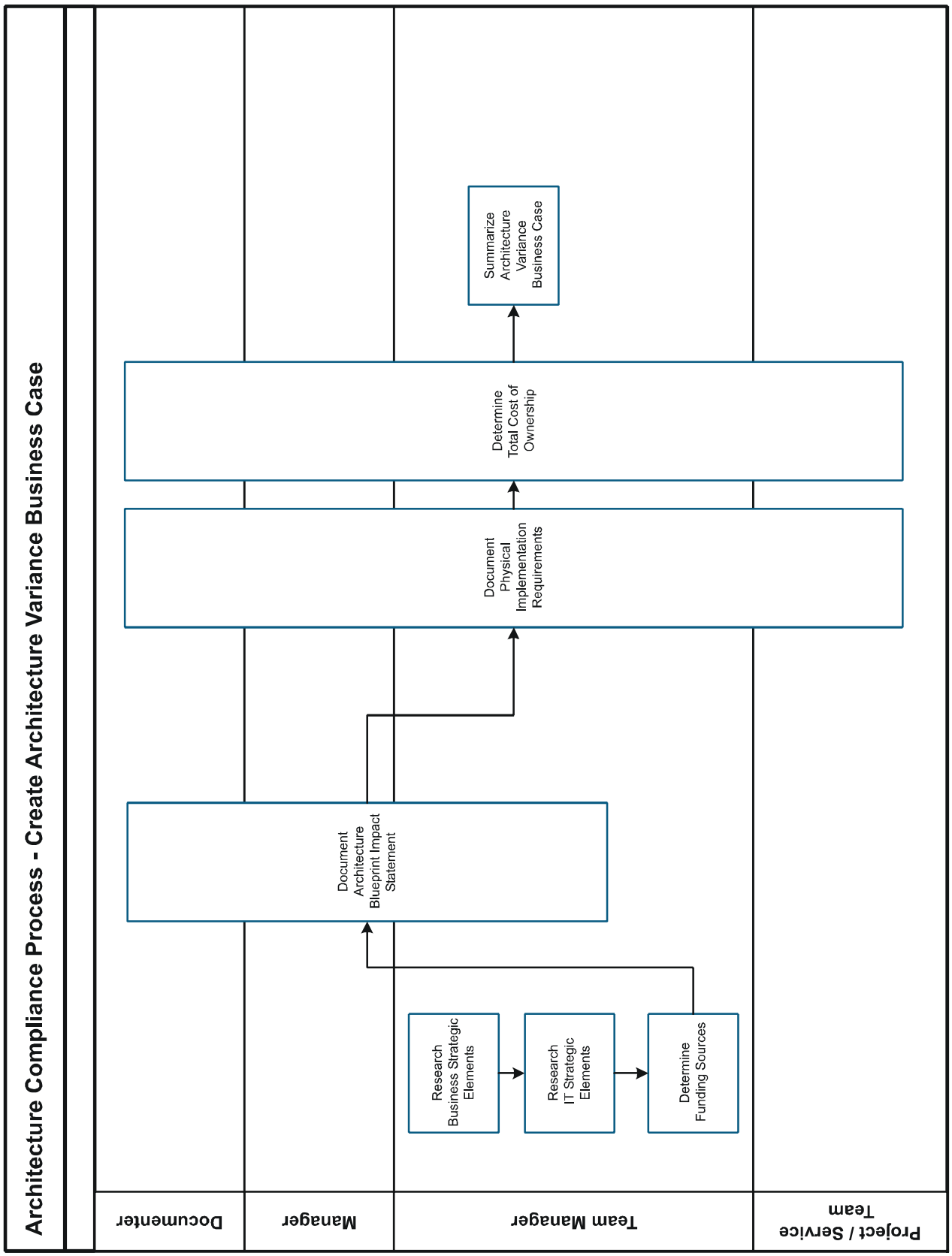
Provide Technical Oversight Recommendation: Once the Subject Matter Experts have reviewed and clarified the Technical Recommendations, they provide their recommendation.

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

Determine Technology Options: Various options for solving the functional requirements will be reviewed and a technology 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 technology 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.


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

CREATE ARCHITECTURE VARIANCE BUSINESS CASE

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 Sources: 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.

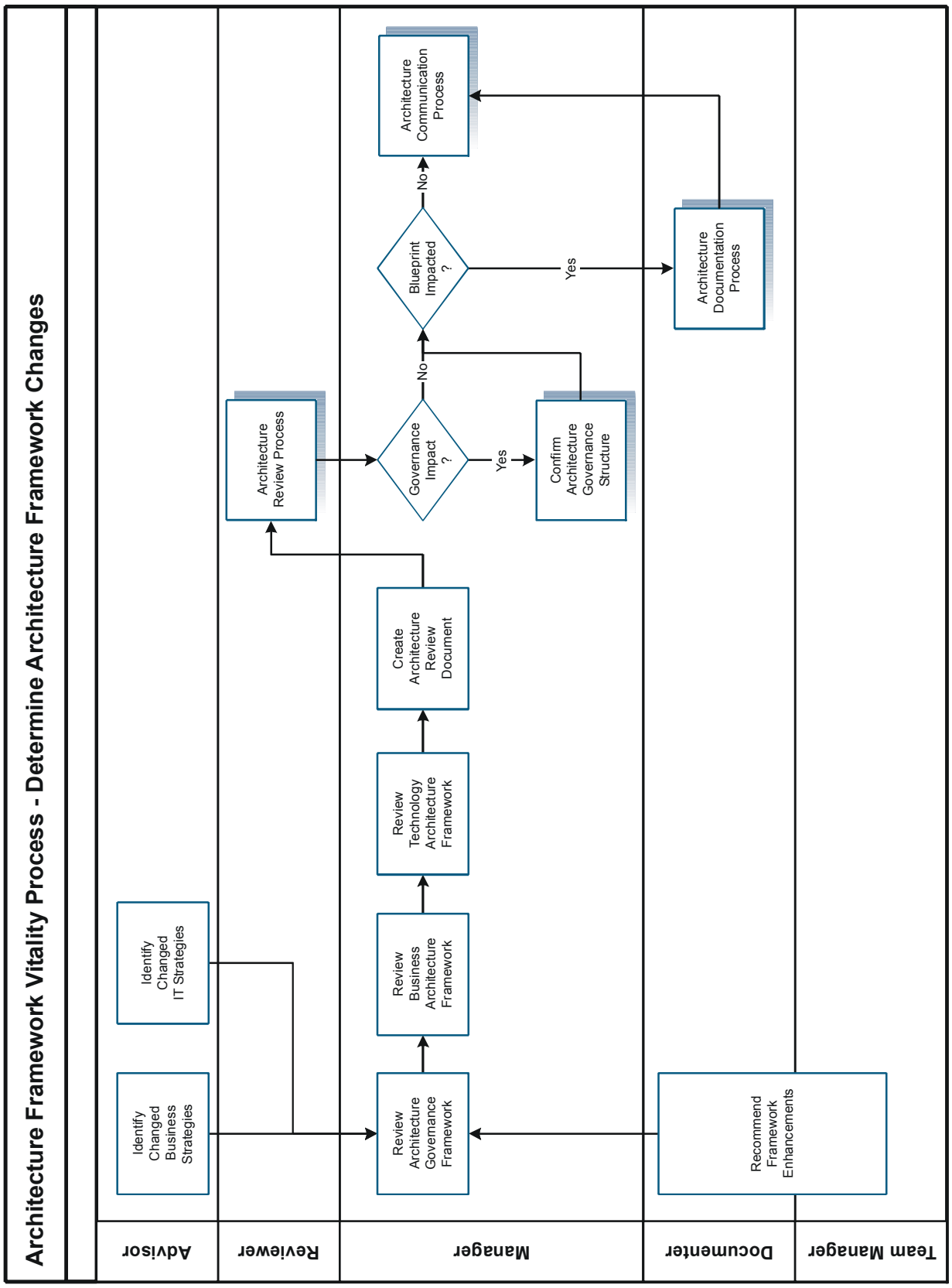
ARCHITECTURE FRAMEWORK VITALITY PROCESS

Architecture Framework Vitality 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 vitality, 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.


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

DETERMINE ARCHITECTURE FRAMEWORK CHANGES

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.

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 Business Architecture Framework: Changes in the Business and IT Strategies may cause the Business Architecture Framework Business Drivers to change. If the Strategy changes have caused changes to the Business Drivers, there will be a rippling effect. Review the Architecture Documentation Process for Domains and Disciplines having relationships with the changed Business Drivers to verify continued validity.

Review the Business Drivers to determine if any of them need to be more strongly emphasized in the Business Architecture Framework. For example, due to the change, an item currently stated as a Best Practice may be elevated to a Principle, or a Business Trend may be elevated to Best Practice.

These types of changes will also affect the Domains and Disciplines that are related to or conflicted with the changed business drivers.

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

Review Technology Architecture Framework: Changes in the Business and IT Strategies may cause the Technology Architecture Framework Technology Drivers to change. A rippling effect occurs if the Strategy changes cause changes to the Technology Drivers. Domains and Disciplines having a relationship with the changed Technology Drivers must revisit the Architecture Documentation Process to verify their validity and update as needed.

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

These types of changes will also affect the Domains and Disciplines that are related to or conflicted with the changed technology drivers.

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

Create Architecture Review Document: The Architecture Manager summarizes the technical and business 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 technical inputs come from:

- Technology Architecture Framework Review Results
- Updated IT Strategic Elements

The business inputs come from:

- Business Architecture Framework Review Results
- Updated Business 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 levels of the architecture blueprint to be reviewed will be determined as follows:

- Changes to the overarching Business and Technology Drivers will cause review of the Architecture Blueprint from the Domain 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 or Domains?

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

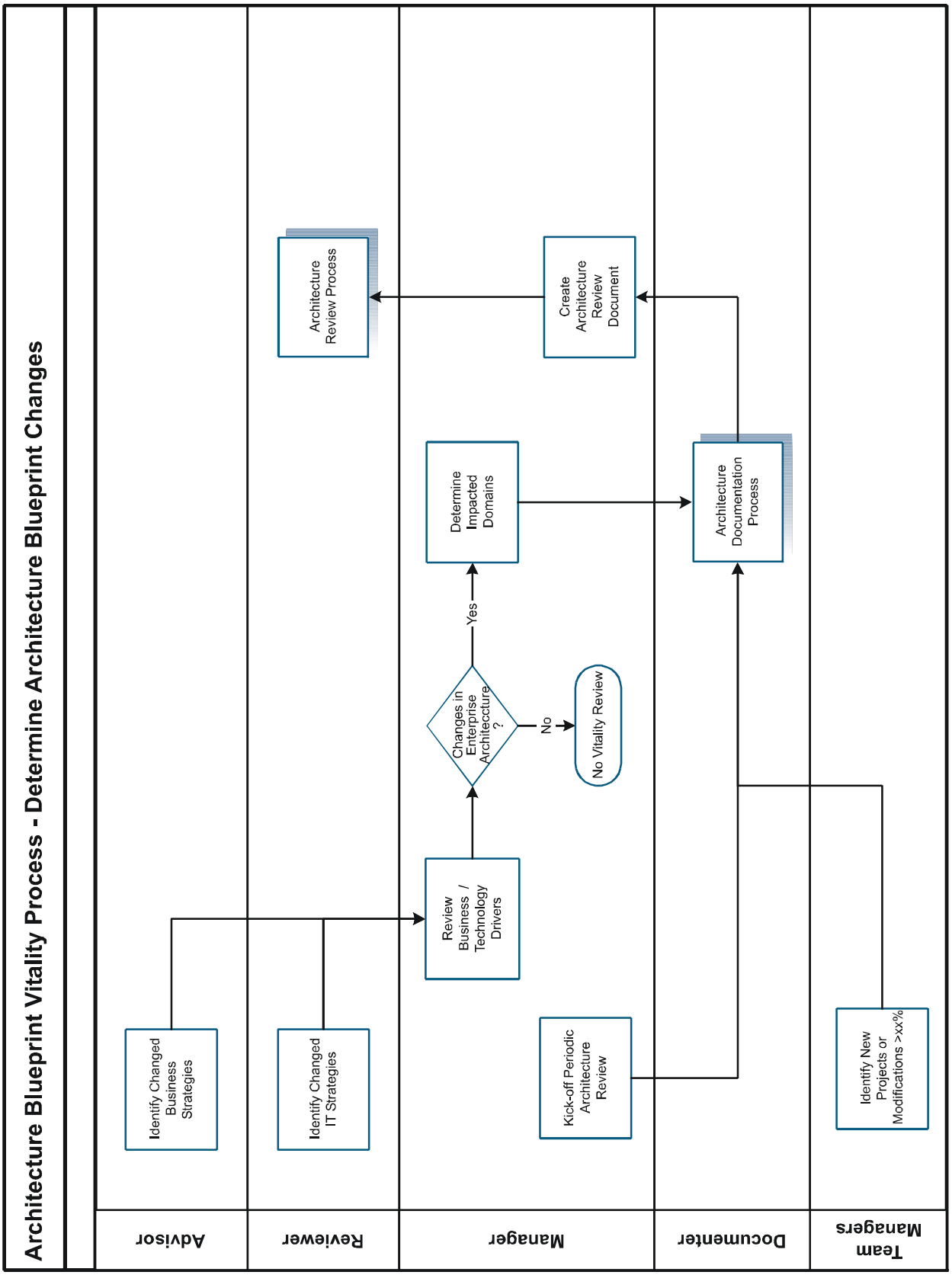
Architecture Blueprint Vitality Process is the process that insures the architecture blueprint content remains current and accurate. This is a major requirement of the overall architecture lifecycle processes. To ensure Architecture Blueprint vitality, the Architecture Blueprint must be reviewed from 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.

The process follows the format of a process model followed by the process detail.


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

DETERMINE ARCHITECTURE BLUEPRINT CHANGES

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/Technology Drivers: Changes in the Business and IT Strategic Elements may cause the Business/Technology 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/Technology Drivers should be taken through the Architecture Documentation Process to verify they are still valid and updated as needed.

Review the Business/Technology Drivers to determine whether any of the drivers require stronger emphasis in the Business or Technology Architecture Frameworks. 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 and Disciplines that are related to or conflicted with the changed Business/Technology Drivers.

Determine Impacted Domains: Based on additions or changes to the overarching Technology Architecture Framework, the Domains that are impacted need to be identified 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 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/Technology Drivers or Periodic Architecture Review cycles will cause the Architecture Blueprint to be reviewed from the Domain level down.
- 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 or Domains?

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.

TECHNOLOGY ARCHITECTURE

A sound Technology Architecture Framework is needed to support implementation of the architecture blueprint. The Technology Architecture Framework shows the relationship of the business and technology 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.

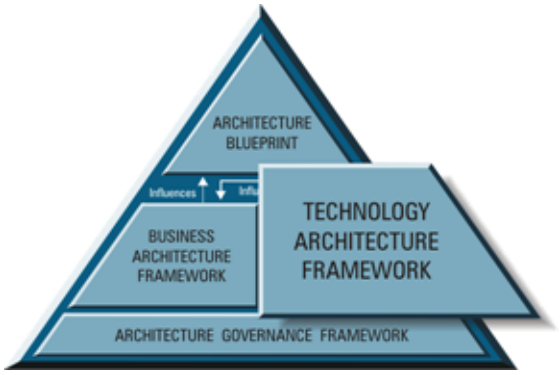
This section of the Tool-Kit, which focuses on technology, supports NASCIO's architecture program by providing government entities a method of establishing effective architecture technology models. It effectively supports the gap analysis of existing technology documentation, identifying methods to improve technology documentation performance, as well as the development of a Technology Architecture Blueprint in its entirety.

This part of the Tool-Kit contains two pieces of the Enterprise Architecture Framework:

- Technology Architecture Framework – Portion of the Enterprise Architecture Framework Elements that provides:
  - Technology Drivers
  - Technology Architecture Blueprint Framework
- Technology Architecture Blueprint – The technology portion of the Architecture Blueprint.

Technology Architecture Framework

Technology Architecture Framework includes the parts of the Enterprise Architecture Framework that will structure technology direction and existing IT services. This portion of the Tool-Kit provides the semi-static information, information that changes only when a major shift in the business or technology occurs. The following resources are available:



- Place to capture the Technology Drivers that are a result of the business and IT strategies. These Technology Drivers are then mapped to the IT portfolio in the Architecture Blueprint.
- Processes for documentation of the Technology Architecture Blueprint levels.
- Templates for the capturing of information requested during the Technology Architecture Processes.

TECHNOLOGY DRIVERS

This portion of the Tool-Kit covers the Technology Drivers: IT Principles, IT Best Practices, and Technology Trends. These Technology Drivers are related. The relationship has two aspects:

- The migration between the three drivers.
- The compliance requirements against which the documentation of the Architecture Blueprint are compared.

The migration occurs when:

- A Technology Trend is proven over time, and re-categorized as an IT Best Practice.
- An IT Best Practice is reviewed by the organization and approved to become an IT Principle, which requires adherence at each of the Technology Architecture Blueprint Levels.

Thus, the three Technology Drivers can have an upward migration. The process for comparing each of these drivers with the Technology Architecture Blueprint will be similar, but the compliance requirements differ for each.

Technology Driver Compliance requirements are as follows:

- IT Principles - Architecture Blueprint levels cannot be in conflict with this driver. If a conflict is found, it must be documented and submitted to the Architect Manager along with the recommendation to change the principle. The Architecture Reviewers need to reevaluate the IT Principle and possibly change it.
- IT Best Practices – Architecture Blueprint levels can be in conflict with this driver. If a conflict is found, it must be documented and submitted to the Architect Manager for review.

- Technology Trend – Architecture Blueprint levels can be in conflict with this driver. In the Architecture Template denote that a conflict exist and explain what the conflict entails in a comment.

IT PRINCIPLES

Processes and templates for this section are identified for inclusion in a subsequent version of the NASCIO Tool-Kit.

IT BEST PRACTICES

Processes and templates for this section are identified for inclusion in a subsequent version of the NASCIO Tool-Kit.

TECHNOLOGY TRENDS

Processes and templates for this section are identified for inclusion in a subsequent version of the NASCIO Tool-Kit.

TECHNOLOGY ARCHITECTURE BLUEPRINT FRAMEWORK

ARCHITECTURE BLUEPRINT STRUCTURE OVERVIEW

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 10, these pieces work together to ensure the complete documentation of the Domains that form the Technology Architecture Blueprint.

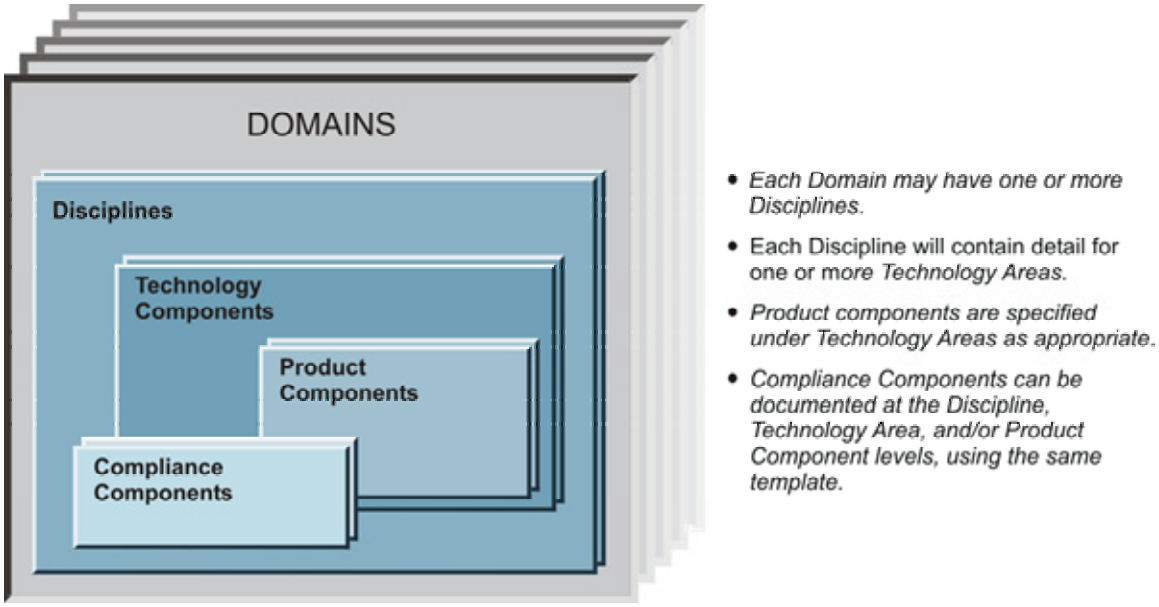


Figure 10. Template Relationships

Domains are the natural divisions of the technical architecture and as seen in Figure 10, form the main building blocks of the technology architecture blueprint.

Each Domain identified will be developed and documented by a Documenter made up of subject matter experts who are familiar with the organization's IT environment.

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 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 as appropriate for the 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, 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 identifies guidelines, standards and legislative mandates associated with a Discipline, Technology Areas, and/or Product Component as appropriate.

Compliance Components (guidelines, standards and mandates) may be documented at the Discipline, Technology Area, and/or Product Component level and 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 covers 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

COMPLETE/UPDATE DOMAIN BLUEPRINT

Domain 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 include:

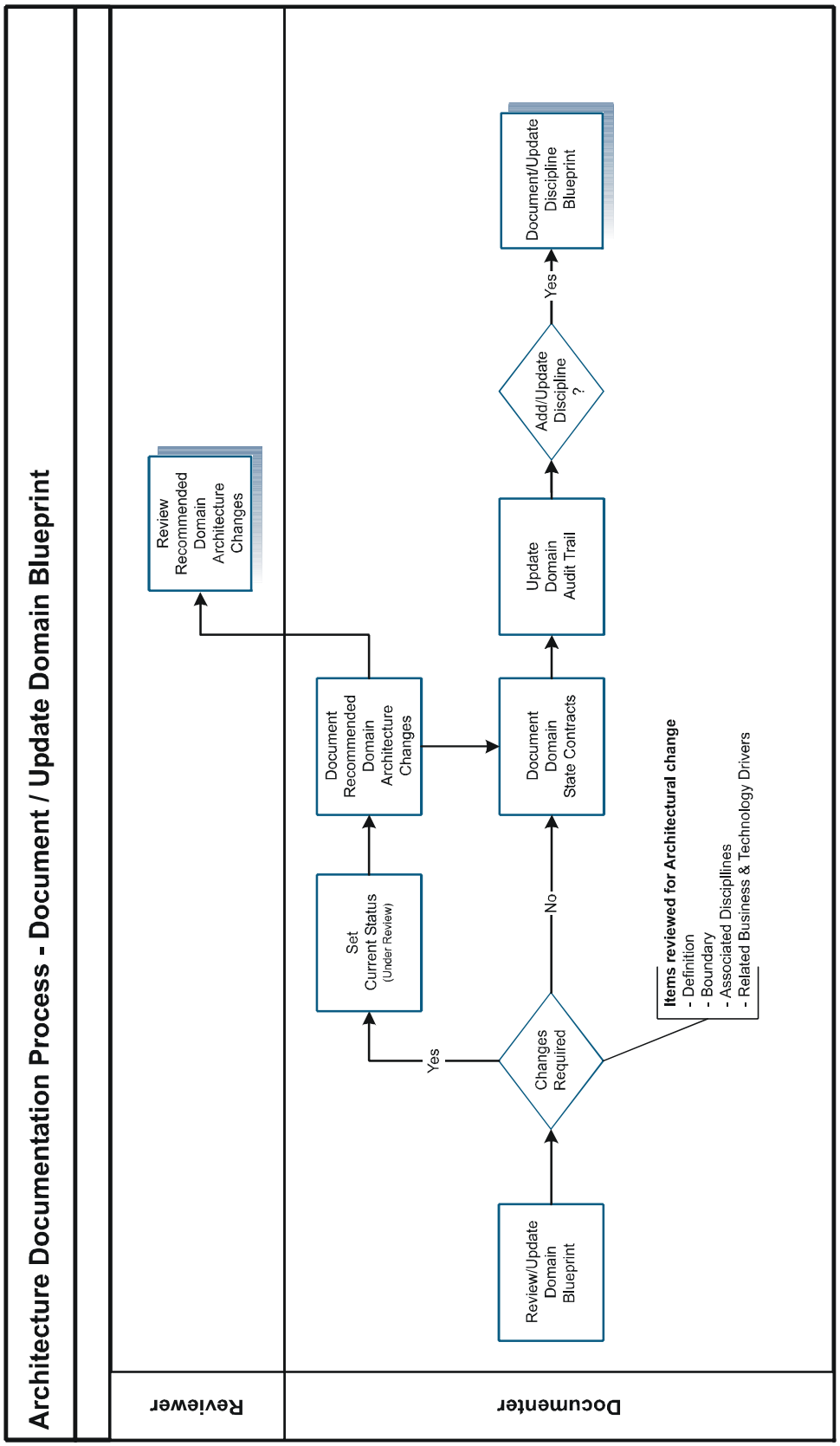
- Access
- Platform
- Network
- Application
- Information
- Integration
- Systems Management
- Security
- Privacy

The 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 Recommended Domain Architecture Changes
Review/Update Domain Blueprint
Changes Required
Yes
No
Set Current Status (Under Review)
Document Recommended Domain Architecture Changes
Document Domain State Contracts
Update Domain Audit Trail
Add/Update Discipline ?
Yes
Document/Update Discipline Blueprint
Items reviewed for Architectural change
- Definition
- Boundary
- Associated Disciplines
- Related Business & Technology Drivers

Using the Domain Template as a guide, the Domain Architecture Blueprint will be completed/updated. Follow the following process steps to aid in this documentation:

Review/Update Domain Blueprint: The definition of the Domain and the primary subject areas 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 and Technology 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 and Technology 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 process. Initial statuses identified include:

- Under Review – Represents when a Domain is being defined and reviewed.
- 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 Architecture Changes and Review Recommended Architecture Changes: Document and submit to the Architecture Manager any changes to the definition, boundary, or Business/Technology Drivers prior to proceeding with the Domain documentation. These types of changes can affect more than just the Documenter requesting the modification.

Document Domain State 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.

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 Sections

The Domain Template will include the following sections:

- Definition
- Boundary
- Current Status
- Associated Disciplines
- Related Principles
- Related Best Practices
- Related Trends
- State Contracts
- Audit Trail

Template Form Sample

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.

Domain Template

DEFINITION	
Name	
Description	
Rationale	
Benefits	

BOUNDARY	
Boundary Limit Statement	

CURRENT STATUS			
Provide the status of this Domain	☐ *Under Review*	☐ *Rejected*	☐ *Accepted*

ASSOCIATED DISCIPLINES	
List 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	

AUDIT TRAIL			
Creation Date		*Date Accepted/Rejected*	
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 information can be found.

- Current Status

  Document the status of Domain, indicating whether the Domain is under review, rejected, or accepted.

  Upon identifying changes to the Domain, the Current Status should be set to "Under Review." After the suggested updates/modifications have been reviewed, the status will be updated to "Rejected" or "Accepted," as appropriate.

- Associated Disciplines

  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, Statements or Links: The overarching general rules that hold true across the enterprise architecture. The principles are developed and documented as Business and Technology 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

  Best Practices – 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 technical 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 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

  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 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.

  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.

- 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 Documenters conducting research on related items across Domains.

  Creation Date: Provide the date the Domain was created.

  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

Discipline 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 B.

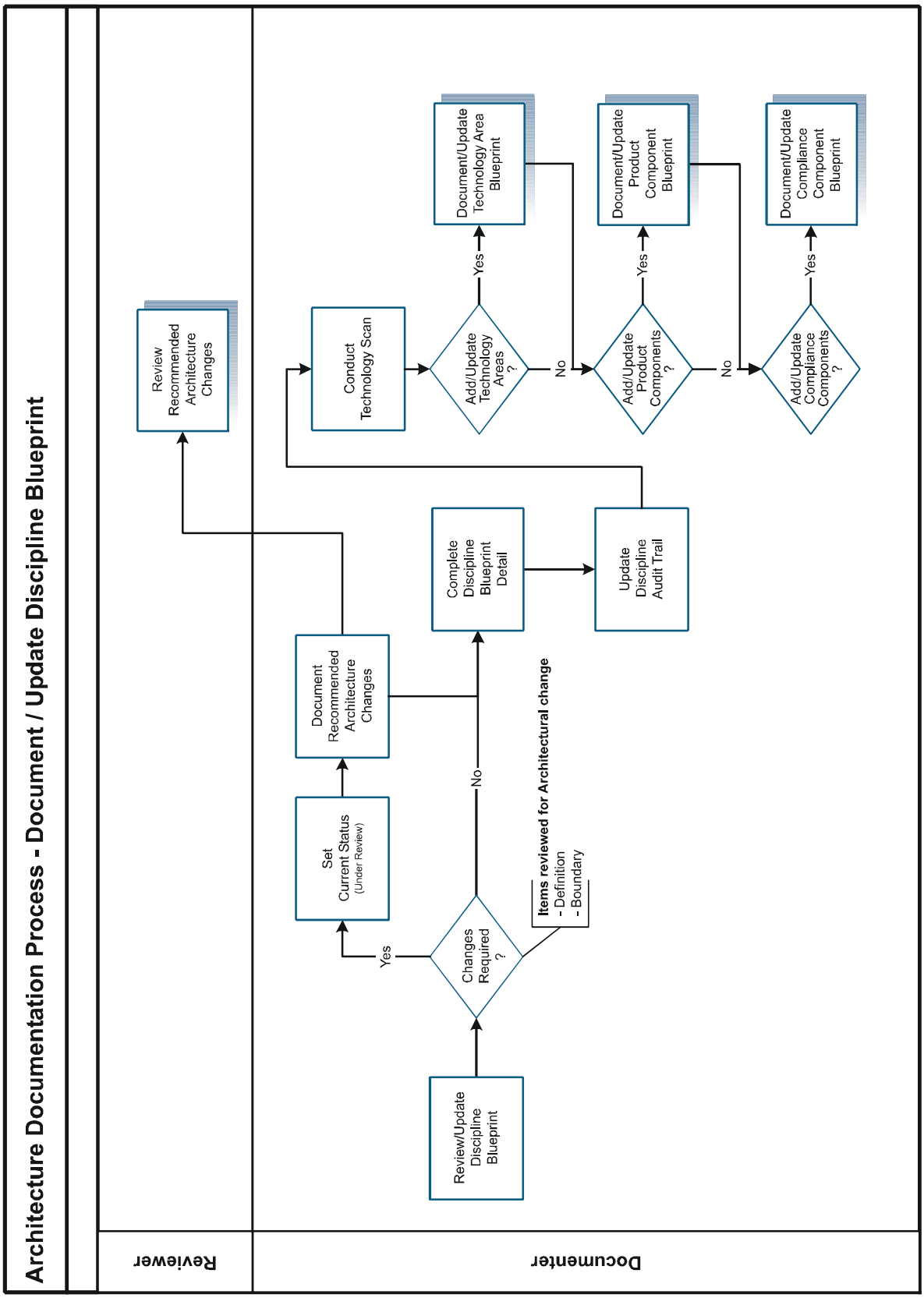
The development of Disciplines within each Domain is the responsibility of the Documenter. This process will evolve and change as information is gathered and documented.

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 lay out 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/Update Discipline Blueprint
Changes Required ?
Yes
No
Items reviewed for Architectural change
- Definition
- Boundary
Set Current Status (Under Review)
Document Recommended Architecture Changes
Review 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

Using the Discipline Template as a guide, the Discipline Blueprint will be completed/updated. The following process steps must be followed to 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 subject 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".

Complete Discipline Blueprint Details: Set the Current Status as appropriate. It is important to understand where a given Discipline is in the process. Initial statuses identified include:

- Under Review – Represents when a Discipline is first being defined and reviewed.
- 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.

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 documented 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.

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 Sections

The Discipline Template will include the following sections:

- Definition
- Boundary
- Associated Domain
- Current Status
- Critical References
- Methodologies
- Associated Compliance Components
- Associated Technology Areas
- Discipline Documentation Requirements
- Audit Trail

Template Form Sample

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.

Discipline Template

DEFINITION	
Name	
Description	
Rationale	
Benefits	

BOUNDARY	
Boundary Limit Statement	

ASSOCIATED DOMAIN	
List the Domain Name	

CURRENT STATUS			
Provide the status of this Discipline	☐ *Under Review*	☐ *Rejected*	☐ *Accepted*

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

List Stakeholders	
List Roles (if stakeholder titles are not known)	

Discipline-Specific Trends			
List Discipline-specific Trends			
Trend Source			
METHODOLOGIES			
List methodologies followed			
ASSOCIATED COMPLIANCE COMPONENTS			
List Discipline-specific Compliance Component Names			
ASSOCIATED TECHNOLOGY AREAS			
List the Technology Areas associated with this Discipline			
DISCIPLINE DOCUMENTATION REQUIREMENTS			
Provide documentation requirements for this Discipline			
AUDIT TRAIL			
Creation Date		*Date Accepted/Rejected*	
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 information can be found.

- Associated Domain

  Provide the name of the Domain with which this Discipline is associated. This provides the appropriate mapping between Domain and Disciplines.

- Current Status

  Document the status of Discipline, indicating whether it is under review, rejected, or accepted.

  Upon identifying changes to the Discipline, the Current Status should be set to "Under Review." After the suggested updates/modifications have been reviewed, the status will be updated to "Rejected" or "Accepted," as appropriate.

- 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.

  Standard Organization/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 to decision 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 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

  Provide a list of methodologies followed in developing or supporting this Discipline as appropriate.

- Associated Compliance Components

  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

  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

  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, which is not always obvious, can be invaluable to them.

  The Documenters should use this section to document the quality assurance criteria for the Discipline and express their expectations for how the Discipline is to be maintained.

- Audit Trail

  Creation Date: Provide the date the Discipline was created.

  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 AREAS

Technology Area Overview

Technology Area is 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

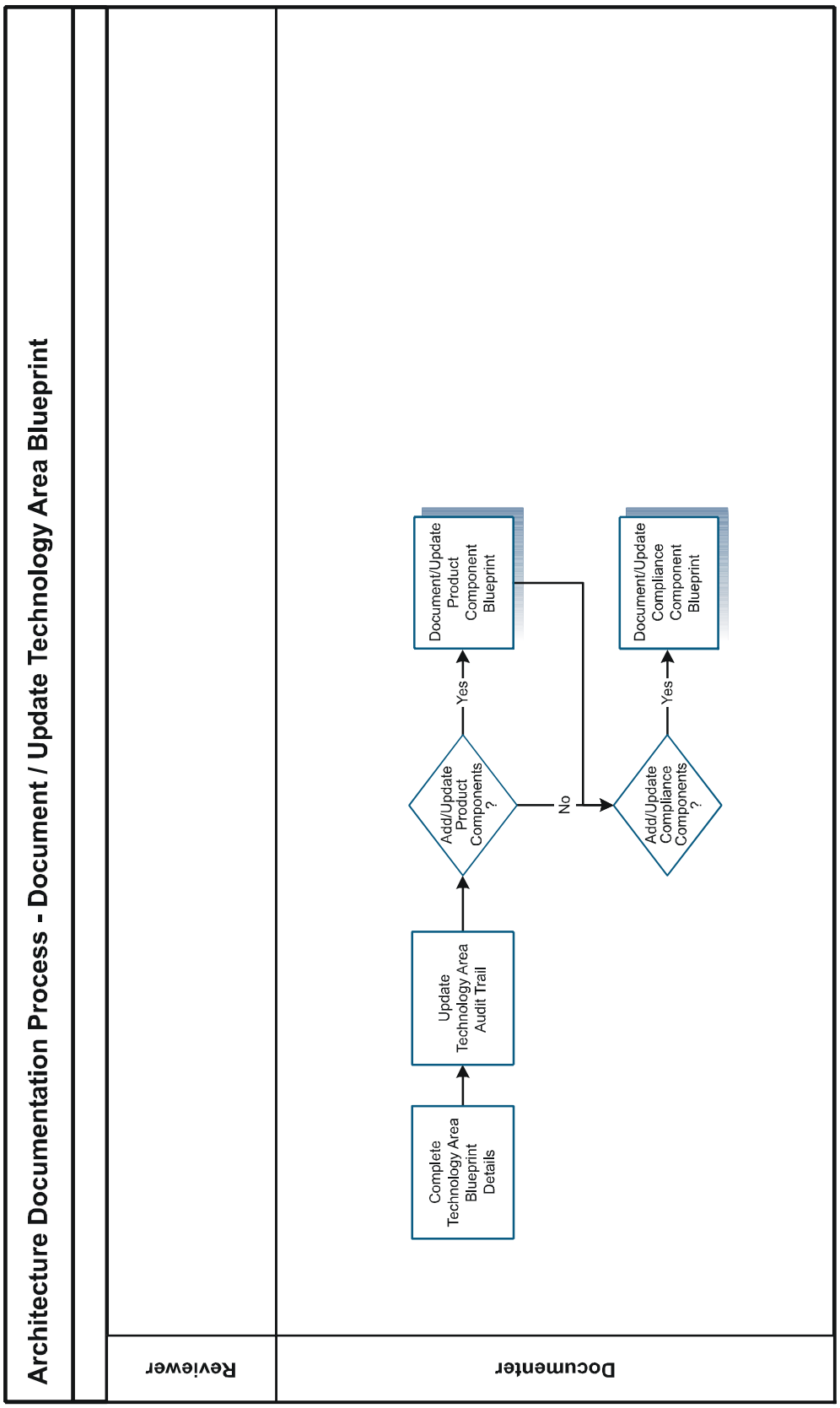
A majority of the Documenters' work will focus on the Technology Areas, Product Components, and Compliance Components including such activities as:

- 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
Document/Update Product Component Blueprint
No
Add/Update Compliance Components ?
Yes
Document/Update Compliance Component Blueprint

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:

- Under Review – Represents when a technology area is being defined and reviewed.
- 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

TECHNOLOGY AREA TEMPLATE

Template Sections

The Technology Area Template will include the following sections:

- Definition
- Associated Discipline
- Keywords
- Current Status
- Associated Compliance Components
- Single Product Solution
- Associated Product Components
- Audit Trail

Template Form Sample

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.

Technology Area Template

DEFINITION	
Name	
Description	
Rationale	
Benefits	

ASSOCIATED DISCIPLINE	
List the Discipline Name	

KEYWORDS	
List Keywords	

CURRENT STATUS			
Provide the status of this Technology Area	☐ *Under Review*	☐ *Rejected*	☐ *Accepted*

ASSOCIATED COMPLIANCE COMPONENTS	
List the Compliance Component Names	

SINGLE PRODUCT SOLUTION	
Date of Single Product Solution Determination	
Provide Rationale for Decision	

ASSOCIATED PRODUCT COMPONENTS	
List the Product Component Names	

AUDIT TRAIL			
Creation Date		*Date Accepted / Rejected*	
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

  Provide the name of the Discipline with which this Technology Area is associated. This provides the appropriate mapping between technology area and Discipline.

- Keywords

  List any keywords/nomenclature 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.

- Current Status

  Document the status of technology area, indicating whether the technology area is under review, rejected, or accepted.

  Upon identifying changes to technology area, the Current Status should be set to "Under Review." After the suggested updates/modifications have been reviewed, the status will be updated to "Rejected" or "Accepted," as appropriate.

- Associated Compliance Components

  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.

  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

  List the Product Components associated with this technology area. The detailed documentation for each component listed will be completed using the Product Component Template.

- Audit Trail

  Creation Date: Provide the date the technology area was created.

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

Product Component Overview

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.

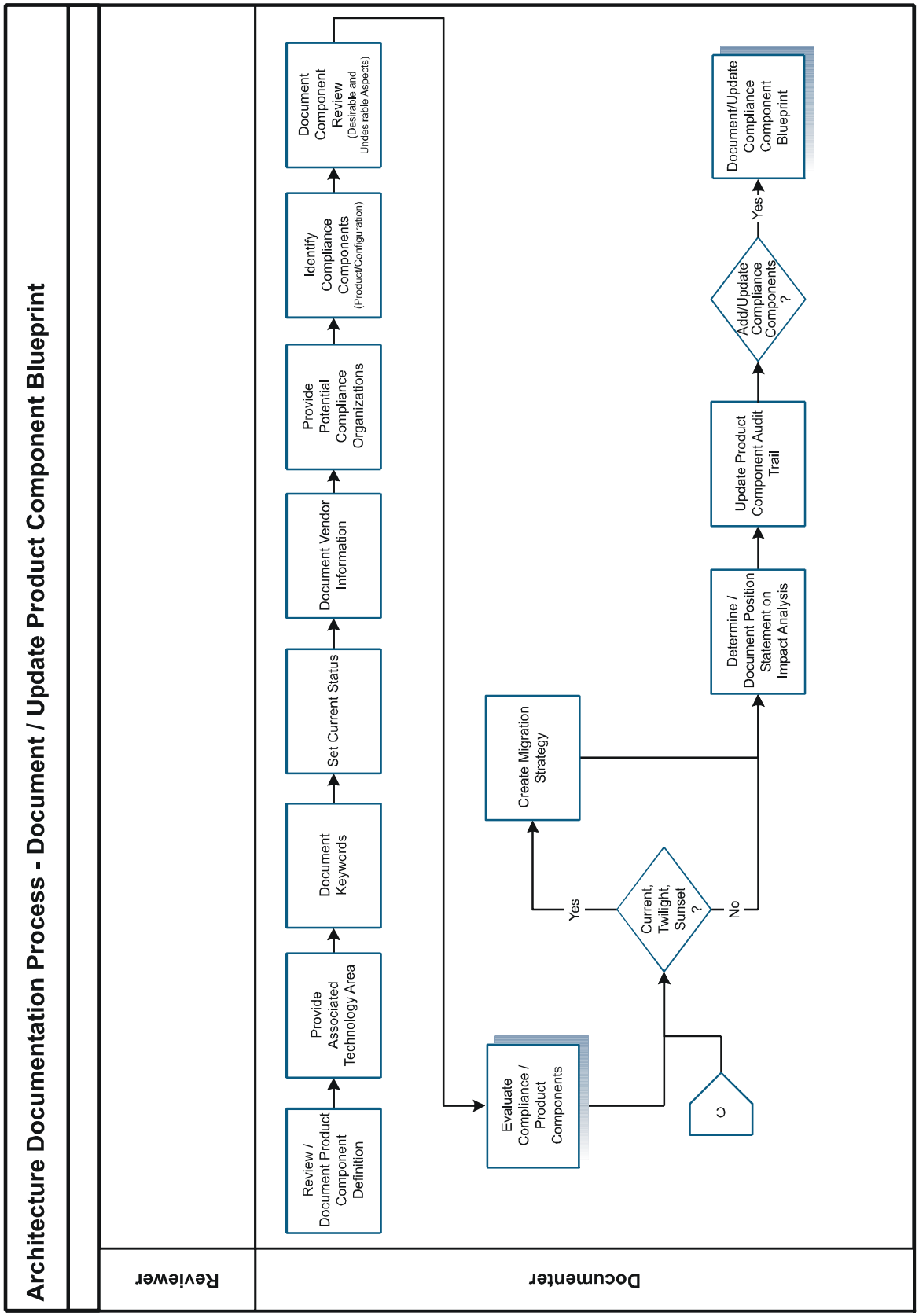
The Documenter will evaluate each Product Component identified to determine its applicability. Document each Product Component reviewed in a Product Component Template, whether accepted or rejected.

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 implementation 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
Document Vendor Information
Provide Potential Compliance Organizations
Identify Compliance Components (Product/Configuration)
Document Component Review (Desirable and Undesirable Aspects)
Evaluate Compliance / Product Components
C
Current, Twilight, Sunset ?
Yes
No
Create Migration Strategy
Determine / Document Position Statement on Impact Analysis
Update Product Component Audit Trail
Add/Update Compliance Components ?
Yes
Document/Update Compliance Component Blueprint

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 Areas: The associated technology area should be listed in order to provide the appropriate mapping between Domain and Disciplines.

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:

- Under Review – Represents when a Product Component is being defined and reviewed.
- 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

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.

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.

Evaluate Compliance/Product Components: Once the product is documented, an evaluation of the product to determine its classification must occur. This will be discussed in detail in the Evaluate Compliance/Product 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:

- 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.

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 Sections

The Product Component Template will include the following sections:

- Definition
- Associated Technology Area
- Keywords
- Current Status
- Vendor Information
- Potential Compliance Organizations
- Associated Compliance Components
- Component Review
- Component Classification
- Required Component
- Conditional Use Restrictions
- Migration Strategy
- Impact Position Statement
- Audit Trail

Template Form Sample

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.

Product Component Template

DEFINITION	
Name	
Description	
Rationale	
Benefits	

ASSOCIATED TECHNOLOGY AREA	
List the name of the associated Technology Area	

KEYWORDS	
List all Keywords	

CURRENT STATUS	
Provide the Current Status of this Product Component	☐ *Under Review* ☐ *Rejected* ☐ *Accepted*

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	
List the Product-specific Compliance Component Names	
Configurations	
List the Configuration-specific Compliance Component Names	

COMPONENT REVIEW	
List Desirable aspects	
List Undesirable aspects	

COMPONENT CLASSIFICATION				
Provide the Classification	☐ *Emerging*	☐ *Current*	☐ *Twilight*	☐ *Sunset*
Provide the Rationale for Component Classification				
REQUIRED COMPONENT				
List Business Area, Department or Application for which this is a required item				
CONDITIONAL USE RESTRICTIONS				
Document the Conditional Use Restrictions				
MIGRATION STRATEGY				
Document the Migration Strategy				
IMPACT POSITION STATEMENT				
Document the Position Statement on Impact				
AUDIT TRAIL				
Creation Date		*Date Accepted / Rejected*		
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.

- Associated Technology Area

  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

  List any keywords/nomenclatures 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.

- Current Status

  Document the current status of Product Component, indicating whether the Product Component is under review, rejected, or accepted.

  Upon identifying changes to the Product Component, the Current Status should be set to "Under Review."

  After the suggested updates/modifications have been reviewed, the status will be updated to "Rejected" or "Accepted," as appropriate.

- 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 site, 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 Component

  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.

  Configuration: 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.

- Component Classification

  Component 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 has a set discontinuation date.

  Sunset Date: Document the date for discontinuation of the Product Component.

- Rationale for Component Classification

  Provide a rationale statement for the chosen classification based on the on review of:

  - Technology Architecture Blueprint Conformance
  - Business Functionality Fit
  - Technical Fit
  - Operational Fit
  - Vendor Evaluation
  - Cost of Ownership

- Required Component

  If this Product Component is specifically required, specify the Business Area, Department or Application for which the product is a requirement.

- Conditional Use Restriction

  Document any specialized circumstances and requirements associated with the use of this Product Component.

- Migration Strategy

  Document Migration Strategy 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)

- Impact Position 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

- Audit Trail

  Creation Date: Provide the date the Product Component was created.

  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 Domain. This will be helpful information for future reference.

DOCUMENT/UPDATE COMPLIANCE COMPONENTS

Compliance Component Overview

Compliance Component is 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.

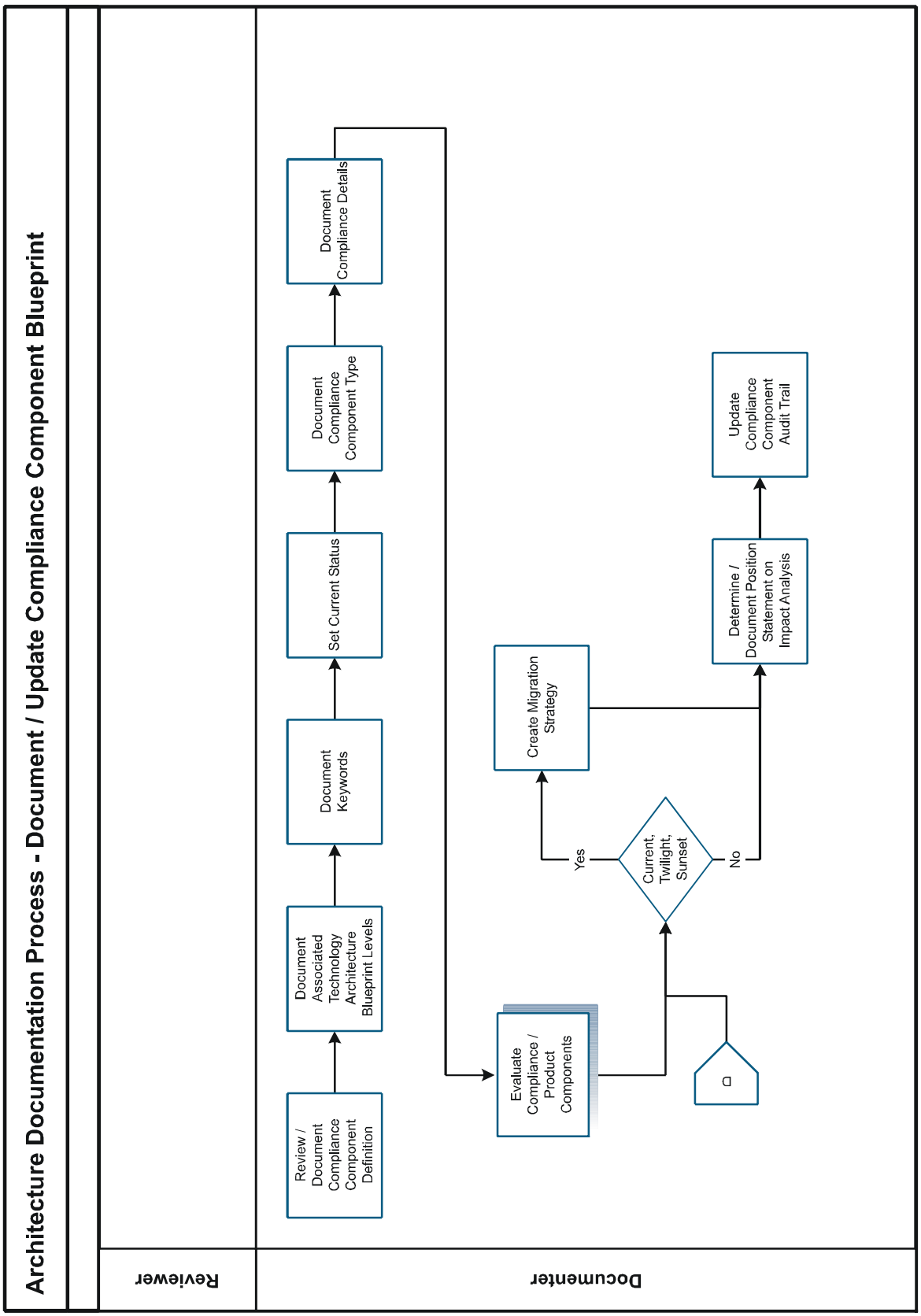
Compliance Components (guidelines, standards and mandates) documented at the Discipline level provide the basis for making important decisions about new products, protocols, configurations, etc. Compliance Components documented at the Technology Area or Product Component level provide the basis for decisions 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 Technology Architecture Blueprint Levels
Document Keywords
Set Current Status
Document Compliance Component Type
Document Compliance Details
Evaluate Compliance / Product Components
Current, Twilight, Sunset
Yes
No
Create Migration Strategy
Determine / Document Position Statement on Impact Analysis
Update Compliance Component Audit Trail

This section provides the process steps necessary for documenting the Compliance Components, as well as the sample template with details.

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 Technology Architecture Blueprint 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 Component 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:

- Under Review – Represents a component that is being defined and reviewed.
- Accepted – Indicates the component has been approved and accepted into the architecture blueprint.
- Rejected – If the 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.

Determine 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 Compliance/Product Components: Once the Compliance Component is documented, an evaluation of the product must be done to determine its classification. This classification process will be discussed in detail in the Evaluate Compliance/Product 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:

- Existing Compliance Components classified as emerging that are moving to current.
- Existing 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 Domain, only the creation, accepted/rejected, and date last updated must be maintained.

COMPLIANCE COMPONENT TEMPLATE

Template Sections

The Compliance Template will include the following sections:

- Definition
- Associated Technology Architecture Blueprint Level
- Keywords
- Current Status
- Compliance Component Type
- Compliance Detail
- Component Classification
- Conditional Use Restrictions
- Migration Strategy
- Impact Position Statement
- Audit Trail

Template Form Sample

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.

Compliance Component Template

DEFINITION	
Name	
Description	
Rationale	
Benefits	

ASSOCIATED TECHNOLOGY ARCHITECTURE BLUEPRINT LEVEL	
List the Discipline Name	
List the Technology Area Name	
List the Product Component Name	

KEYWORDS	
List all Keywords	

CURRENT STATUS			
Provide the status of this Compliance Component	☐ *Under Review*	☐ *Rejected*	☐ *Accepted*

COMPLIANCE COMPONENT TYPE			
Document the Compliance Component Type	☐ *Guideline*	☐ *Standard*	☐ *Legislation*
Compliance Sub-type (Executive Order, Federal Regulation, Statute, etc.)			

COMPLIANCE DETAIL	
Provide the Guideline, Standard or Legislation statement	
Document Source Reference #	

Standards Organization			
Name		*Web Address*	
Contact Information			

Government Body			
Name		*Web Address*	
Contact Information			

COMPONENT CLASSIFICATION				
Provide the Classification	☐ *Emerging*	☐ *Current*	☐ *Twilight*	☐ *Sunset*
Provide the Rationale for Classification				

CONDITIONAL USE RESTRICTIONS			
Document the Conditional Use Restrictions			
MIGRATION STRATEGY			
Document the Migration Strategy			
IMPACT POSITION STATEMENT			
Document the Position Statement on Impact			
AUDIT TRAIL			
Creation Date		*Date Accepted / Rejected*	
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.

- Associated Technology Architecture Blueprint Level

  Discipline - 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 - 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 - 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

  List any keywords/nomenclature 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.

- Current Status

  Document the current status of Compliance Component, indicating whether the Compliance Component is under review, rejected, or accepted.

  Upon identifying changes to the Compliance Component, the Current Status should be set to "Under Review." After the suggested updates/modifications have been reviewed, the status will be updated to "Rejected" or "Accepted," as appropriate.

- 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.

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.

- Component Classification

  Component 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 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 has a set discontinuation date.

  Sunset Date: Document the date for discontinuation of the Product Component.

- Rationale for Component 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

- Conditional Use Restrictions

  Document any specialized circumstances and/or requirements associated with the use of this Compliance Component.

- Migration Strategy

  Document Migration Strategy for:

  - Existing Compliance Components classified as emerging that are moving to current.
  - Existing 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)

- Impact Position 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

- Audit Trail

  Creation Date: Provide the date the Compliance Component was created.

  Date Accepted/Rejected: Provide the date the Compliance Component was accepted into the architecture blueprint or rejected.

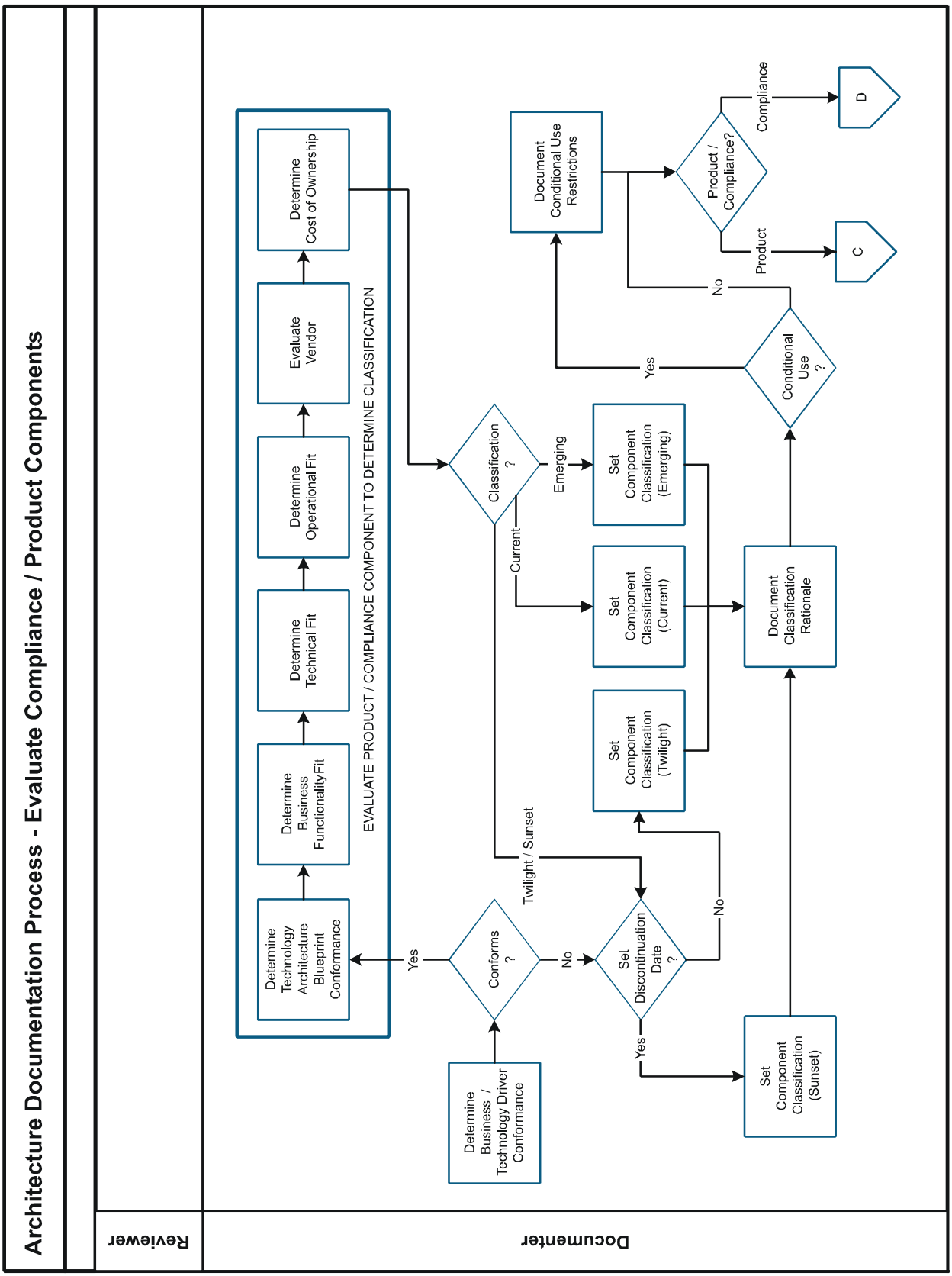
  Reason for Rejection: If the Compliance Component was rejected, document the reason for the rejection.

  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 Domain. This will be helpful information for future reference.


Architecture Documentation Process - Evaluate Compliance / Product Components
Reviewer
Documenter
Determine Business / Technology Driver Conformance
Conforms ?
Yes
No
Determine Technology Architecture Blueprint Conformance
Determine Business FunctionalityFit
Determine Technical Fit
Determine Operational Fit
Evaluate Vendor
Determine Cost of Ownership
EVALUATE PRODUCT / COMPLIANCE COMPONENT TO DETERMINE CLASSIFICATION
Set Discontinuation Date ?
Yes
No
Twilight / Sunset
Set Component Classification (Sunset)
Classification ?
Current
Emerging
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

EVALUATE COMPLIANCE/PRODUCT COMPONENTS

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.

Determine Business /Technology Driver Conformance: The following areas should be used as selection guidelines for each Product or Compliance Component.

Components that do not conform to Business and Technology 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 and Technology Drivers, the following additional evaluation must be performed:

- ***Determine Technology Architecture Blueprint 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 Product Component using the following classifications:

- ***Sunset*** components are those that are in use but do not conform to the stated Business/Technology Drivers 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/Technology 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.

Technology Architecture Samples

Technology Driver Samples

Samples are provided as models to help articulate the Tool-Kit – not as the solution.

IT Principles

IT Best Practices

Technology Trends

Technology Architecture Blueprint Samples

This section contains Blueprint samples from the Application and Security domains.

The five levels of the Application Domain are represented starting at the domain level and following a single line 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 from within the Application Domain includes:

- Discipline – Electronic Collaboration

The five levels of the Security Domain 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 from within the Security Domain include:

- Discipline – Enterprise Security
- Discipline – Network Security

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

CURRENT STATUS			
Provide the status of this Domain	☒ *Under Review*	☐ *Rejected*	☐ *Accepted*

ASSOCIATED DISCIPLINES	
List 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 meet.
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

AUDIT TRAIL			
Creation Date	03/01/02	*Date Accepted/Rejected*	
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	03/06/02
Reason for Update			
Updated By			

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	
List the Domain Name	Application Architecture

CURRENT STATUS			
Provide the status of this Discipline	☒ *Under Review*	☐ *Rejected*	☐ *Accepted*

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

List Stakeholders	Business Analyst, Systems Analyst, Business Functional Users, Quality Assurance Testers, IT Operations Staff, Developers, Software Vendors, Outsource Development Vendors, Data Analyst, etc…
List Roles (if stakeholder titles are not known)	

Discipline-specific Trends			
List Discipline-specific Trends	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			
List methodologies followed	Rapid Application Development (RAD) Joint Application Development (JAD)		
ASSOCIATED COMPLIANCE COMPONENTS			
List Discipline-specific 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			
List the Technology Areas associated with this Discipline	Application Development Languages Case Tools Source code repositories		
DISCIPLINE DOCUMENTATION REQUIREMENTS			
Provide 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…)		
AUDIT TRAIL			
Creation Date	03/01/02	*Date Accepted/Rejected*	
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	03/01/02
Reason for Update			
Updated By			

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	
List the Discipline Name	Application Development

KEYWORDS	
List Keywords	Coding Studios, Programming, Coding Standards, Code Sets, Application Languages

CURRENT STATUS			
Provide the status of this Technology Area	☐ *Under Review*	☐ *Rejected*	☒ *Accepted*

ASSOCIATED COMPLIANCE COMPONENTS	
List the Compliance Component Names	Overall Programming Standards

SINGLE PRODUCT SOLUTION	
Date of Single Product Solution Determination	
Provide Rationale for Decision	

ASSOCIATED PRODUCT COMPONENTS		
List the Product Component Names	JAVA, COBOL II (MF, AS) C C++	COBOL (MF, AS) RPG (AS) Pascal Microsoft Visual Basic

AUDIT TRAIL			
Creation Date	03/02/02	*Date Accepted / Rejected*	
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	03/02/02
Reason for Update			
Updated By			

Product Component Blueprint

DEFINITION	
Name	**Product Component - Visual Basic**
Description	Visual Basic programming language.
Rationale	
Benefits	

ASSOCIATED TECHNOLOGY AREA	
List the name of the associated Technology Area	Application Languages

KEYWORDS	
List all Keywords	VB, Visual Studio, Client Server language, VBA,

CURRENT STATUS	
Provide the Current Status of this Product Component	☐ *Under Review* ☐ *Rejected* ☒ *Accepted*

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	
List the Product-specific Compliance Component Names	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			
List the Configuration-specific Compliance Component Names	Visual Basic 5 Visual Basic .nt		
COMPONENT REVIEW			
List Desirable aspects			
List Undesirable aspects			
COMPONENT CLASSIFICATION			
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Provide the Rationale for Component Classification	Current application language in use in nth architecture for the organization.		
REQUIRED COMPONENT			
List Business Area, Department or Application for which this is a required item			
CONDITIONAL USE RESTRICTIONS			
Document the Conditional Use Restrictions			
MIGRATION STRATEGY			
Document the Migration Strategy			
IMPACT POSITION STATEMENT			
Document the Position Statement on Impact			
AUDIT TRAIL			
Creation Date	03/02/02	*Date Accepted / Rejected*	
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	03/02/02
Reason for Update			
Updated By			

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.

ASSOCIATED TECHNOLOGY ARCHITECTURE BLUEPRINT LEVEL	
List the Discipline Name	Application Development
List the Technology Area Name	Application Languages
List the Product Component Name	Visual Basic

KEYWORDS	
List all Keywords	Constance, Variable, naming,

CURRENT STATUS			
Provide the status of this Compliance Component	☐ *Under Review*	☐ *Rejected*	☒ *Accepted*

COMPLIANCE COMPONENT TYPE			
Document the Compliance Component Type	☐ *Guideline*	☒ *Standard*	☐ *Legislation*
Compliance Sub- Type (Executive Order, Federal Regulation, Statute, etc.)	Coding		

COMPLIANCE DETAIL	
Provide the Guideline, Standard or Legislation 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
Document Source Reference #	Practical Standards for MS Visual Basic - Chapter 5 by James D. Foxwell ISBN 0-7356-0733-8
Standards Organization	
Name	*Web Address*
Contact Information	
Government Body	
Name	*Web Address*
Contact Information	
COMPONENT CLASSIFICATION	
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*
Provide the Rationale for Classification	Visual Basic 5 is current application language used in the organization for client server and nth tier application development.
CONDITIONAL USE RESTRICTIONS	
Document the Conditional Use Restrictions	

MIGRATION STRATEGY			
Document the Migration Strategy			
IMPACT POSITION STATEMENT			
Document the Position Statement on Impact			
AUDIT TRAIL			
Creation Date	03/02/02	*Date Accepted / Rejected*	
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	03/02/02
Reason for Update			
Updated By			

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	
List the Domain Name	Application Architecture

CURRENT STATUS			
Provide the status of this Discipline	☒ *Under Review*	☐ *Rejected*	☐ *Accepted*

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

List Stakeholders	Business Analyst, Systems Analyst, Business Functional Users, Software Vendors, and, Data Analyst, etc…
List Roles (if stakeholder titles are not known)	

Discipline-specific Trends			
List Discipline-specific Trends	None identified		
Trend Source			
METHODOLOGIES			
List methodologies followed			
ASSOCIATED COMPLIANCE COMPONENTS			
List Discipline-specific Compliance Component Names	None identified		
ASSOCIATED TECHNOLOGY AREAS			
List the Technology Areas associated with this Discipline	e-Mail Calendaring		
DISCIPLINE DOCUMENTATION REQUIREMENTS			
Provide 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…)		
AUDIT TRAIL			
Creation Date	03/01/02	*Date Accepted/Rejected*	
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	03/01/02
Reason for Update			
Updated By			

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. 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.
CURRENT STATUS	
Provide the status of this Domain	☒ Under Review ☐ Rejected ☐ Accepted
ASSOCIATED DISCIPLINES	
List 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	

AUDIT TRAIL			
Creation Date	4/15/2002	*Date Accepted/Rejected*	
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

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	
List the Domain Name	Security

CURRENT STATUS			
Provide the status of this Discipline	☒ *Under Review*	☐ *Rejected*	☐ *Accepted*

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

List Stakeholders	
List Roles	

Discipline-specific Trends

List Discipline-specific Trends	
Trend Source	

ASSOCIATED COMPLIANCE COMPONENTS	
List Discipline-specific 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)
METHODOLOGIES	
List methodologies followed	
DISCIPLINE DOCUMENTATION REQUIREMENTS	
Provide documentation requirements for this Discipline	
ASSOCIATED TECHNOLOGY AREAS	
List the Technology Areas associated with this Discipline	User Security Directory Services Application Security System Security Data Security

AUDIT TRAIL			
Creation Date	4/16/2002	*Date Accepted/Rejected*	
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			
Updated By			

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	
List the Discipline Name	Host Security

KEYWORDS	
List Keywords	Authentication, Directory Services

CURRENT STATUS			
Provide the status of this Technology Area	☒ *Under Review*	☐ *Rejected*	☐ *Accepted*

ASSOCIATED COMPLIANCE COMPONENTS	
List the Compliance Component Name(s)	N/A

SINGLE PRODUCT SOLUTION	
Date of Single Product Solution Determination	N/A
Provide Rationale for Decision	N/A

ASSOCIATED PRODUCT COMPONENTS	
List the Product Component Name(s)	OpenLDAP NDS (Novell Directory Services)

AUDIT TRAIL			
Creation Date	5/12/2002	*Date Accepted / Rejected*	
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

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.

ASSOCIATED TECHNOLOGY AREA	
List the name of the associated Technology Area	Directory Services

KEYWORDS	
List all Keywords	LDAP, OpenLDAP, Directory Access, sldap

CURRENT STATUS			
Provide the Current Status of this Product Component	☒ *Under Review*	☐ *Rejected*	☐ *Accepted*

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			
List the Product-specific Compliance Component Names	OpenLDAP Admin Guide		
Configurations			
List the Configuration-specific Compliance Component Names	OpenLDAP Admin Guide – 5. The slapd Configuration File		
COMPONENT REVIEW			
List 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.
List 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.
COMPONENT CLASSIFICATION	
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*
Provide the Rationale for Component Classification	OpenLDAP is currently in use within the organization.
REQUIRED COMPONENT	
List Business Area, Department or Application for which this is a required item	N/A
CONDITIONAL USE RESTRICTIONS	
Document the Conditional Use Restrictions	N/A

MIGRATION STRATEGY			
Document the Migration Strategy			
IMPACT POSITION STATEMENT			
Document the Position Statement on Impact			
AUDIT TRAIL			
Creation Date	5/21/2002	*Date Accepted / Rejected*	
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

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

ASSOCIATED TECHNOLOGY ARCHITECTURE BLUEPRINT LEVELS	
List the Discipline Name	
List the Technology Area Name	
List the Product Component Name	OpenLDAP

KEYWORDS	
List all Keywords	LDAP, OpenLDAP, sldap

CURRENT STATUS			
Provide the status of this Compliance Component	☒ *Under Review*	☐ *Rejected*	☐ *Accepted*

COMPLIANCE COMPONENT TYPE			
Document the Compliance Component Type	☒ *Guideline*	☐ *Standard*	☐ *Legislation*
Compliance Sub-type (Executive Order, Federal Regulation, Statute, etc.)			

COMPLIANCE DETAIL	
Provide the Guideline, Standard or Legislation statement	OpenLDAP 2.0 Administrator's Guide
Document 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			

COMPONENT CLASSIFICATION			
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Provide the Rationale for Classification	Configurations as documented within the Administrator's Guide are currently in use within the organization.		
CONDITIONAL USE RESTRICTIONS			
Document the Conditional Use Restrictions	N/A		
MIGRATION STRATEGY			
Document the Migration Strategy			
IMPACT POSITION STATEMENT			
Document the Position Statement on Impact			
AUDIT TRAIL			
Creation Date	5/20/2002	*Date Accepted / Rejected*	
Reason for Rejection			
Last Date Updated		*Last Date Reviewed*	
Reason for Update			
Updated By			

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	
List the Domain Name	Security Domain

CURRENT STATUS			
Provide the status of this Discipline	☒ *Under Review*	☐ *Rejected*	☐ *Accepted*

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/Government Bodies

List Standards Organizations	
List Government Bodies	

Stakeholders/Roles

List Stakeholders	Security Personnel Help Desk Personnel Operations Staff Users
List Roles	

Discipline-specific Technology Trends

List Discipline-specific Technology Trends	
Technology Trend Source	

ASSOCIATED COMPLIANCE COMPONENTS

List Discipline-specific Compliance Component Names	

METHODOLOGIES

List methodologies followed	

DISCIPLINE DOCUMENTATION REQUIREMENTS

Provide documentation requirements for this Discipline	

ASSOCIATED TECHNOLOGY AREAS

List the Technology Areas associated with this Discipline	Physical Security Security Administration Social Engineering/Human Factors

AUDIT TRAIL			
Creation Date	4/15/2002	*Date Accepted/Rejected*	
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			
Subject Matter Expert(s)			

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	
List the Domain Name	Security

CURRENT STATUS			
Provide the status of this Discipline	☒ *Under Review*	☐ *Rejected*	☐ *Accepted*

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

List Stakeholders	Systems Analysts, Network Personnel, Applications Developer, Applications Testing Team, Third-Party Network Vendors, System Administrators, Security Personnel, Configuration Management Team, Help Desk Personnel
List Roles	

Discipline-specific Technology Trends			
List Discipline-specific Technology Trends			
Technology Trend Source			
ASSOCIATED COMPLIANCE COMPONENTS			
List Discipline-specific 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		
METHODOLOGIES			
List methodologies followed			
DISCIPLINE DOCUMENTATION REQUIREMENTS			
Provide 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…)		
ASSOCIATED TECHNOLOGY AREAS			
List the Technology Areas associated with this Discipline	Network Security Web security Electronic Transaction Security		
AUDIT TRAIL			
Creation Date	4/16/2002	*Date Accepted/Rejected*	
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			
Updated By			

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	

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	

Domain: Application Architecture | *Discipline:* Electronic Collaboration

Technology Area	*Emerging Technologies*	*Current Technologies*	*Twilight Technologies*	*Sunset Technologies*
Network Security	• AES (encryption)	• Firewalls/router ACL • IPSEC • Encryption (3 DES/RSA) • Encrypted VPN • Intrusion Detection • Vulnerability Scanners	• Dedicated lines	
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 B.

Each government entity should define the disciplines as appropriate for its enterprise. The descriptions provided in Appendix B 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 11 provides a pictorial view of the sample Domains that make up the Technology Architecture in this Tool-Kit.

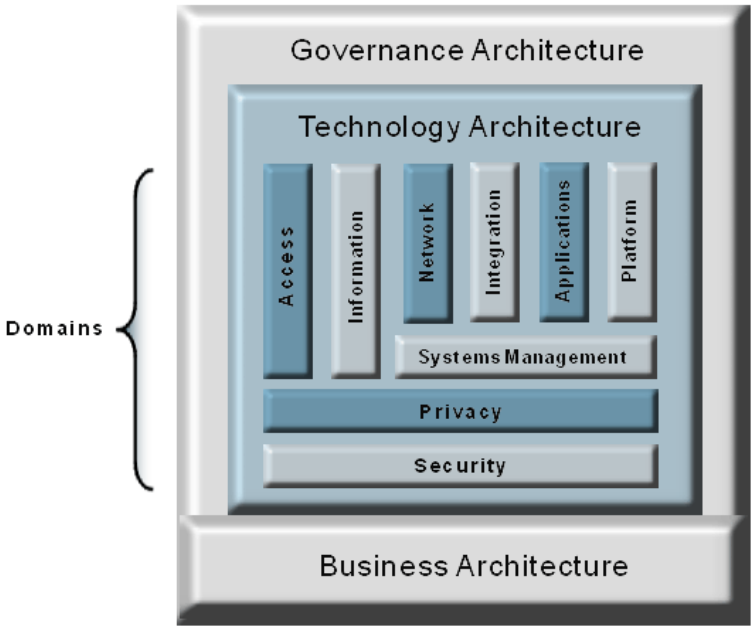


Figure 11. Domains Comprising the Technology

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.

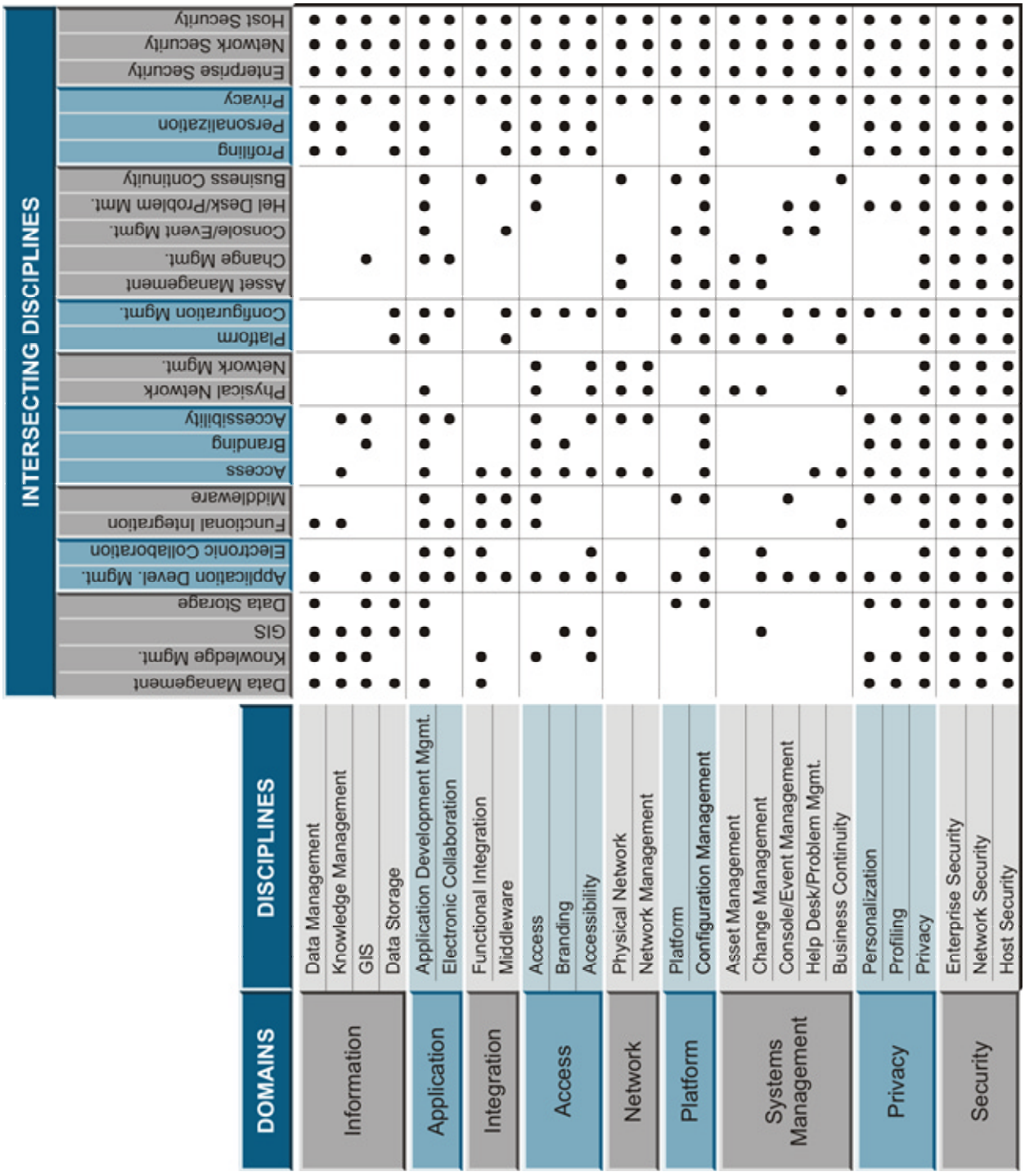


Table 2. Domain-Discipline Intersection Matrix

APPENDIX A - LEXICON

The Lexicon defines critical terminology. New items are added as identified.

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.
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.
Blueprint	Plan or guide, commonly used in construction, laid out logically and including essential elements to address and follow as building progresses.
Business Drivers	Internal goals and strategies and external trends that influence the business. These are captured in three stages of drivers: • Industry Trends – Emerging trends within the business world that are impacting how services and information will be provided. • Business Best Practices – Trends and approaches that are most successful at providing services and information over time. • Business Principles – Business practices and approaches that the organization chooses to institutionalize to better all provided services and information.
Component	In object-oriented programming and distributed object technology, a component is a reusable program building block that can be combined with other components in the same or other computers in a distributed network to form an application.
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.
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.
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.

Term	Definition
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	Logical groupings of disciplines that form the main building blocks within the architectural framework.
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	An overall plan for designing, implementing and maintaining the infrastructure to support the enterprises business functions and underlying networks and systems.
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.
Entity	An information-sharing unit. All agencies (see definition above) are entities; so are courts and legislative bodies. Private organizations that share governmental information are also entities, as are private persons.
Framework	Illustration of the various architecture elements, used as a guide for assisting governments as they create enterprise architectures for their organizations. Currently in the NASCIO Tool-Kit there are four Frameworks: • Enterprise Architecture Framework • Architecture Governance Framework • Business Architecture Framework • Technology Architecture Framework
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.

Term	Definition
HIPAA	Acronym for the Health Insurance Portability and Accountability Act of 1996, which addresses such items as privacy and electronic sharing of information.
Industry Trends	Emerging trends within the business world that impact the provision of services and information.
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	The capability to allow users to readily share data among applications residing on varying combinations of hardware and software within and between existing networks.
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.
Lexicon	Provides a glossary and cross-reference for words that may have multiple meanings. The purpose is to create common definitions to allow for clearer understanding.
Mandate	An authoritative command or instruction.
Middleware	Systems integration software for distributed processing and database and user interfaces.
Models	Representations of information, activities, relationships and constraints.
NASCIO	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.
NSR	National Systems & Research Co. is the contracted company, working with NASCIO as a technical partner, to support the development of a model adaptive enterprise-wide architecture template for municipal, county and state government use in establishing enterprise architecture.

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 of time.
Proprietary	Owned by a private individual or corporation.
Protocol	Rules governing transmitting and receiving of data.
Scalability	The ability to use the same applications and systems on all classes of computers from personal computers to supercomputers.
Standard	Sets of criteria, voluntary guidelines and best practices. Some may be mandatory.
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).
Technology	Tools or tool systems by which we transform parts of our environment and extend our human capabilities (Tornatzky and Fleischer 1990).
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.
Technology Drivers	Internal business processes or needs and external innovation that influence technology. These are captured in three stages: • Technology Trends – Emerging trends within the technology world that are impacting how services and the IT portfolio will be provided. • IT Best Practices – Trends and approaches that are most successful at providing services and IT portfolio. • IT Principles – Those practices and approaches that the organization chooses to institutionalize to better all provided services and IT portfolio pieces.
Template	A form used as a guide, such as a document in which the standard parts are already included and the variable parts are completed as appropriate.
Twilight Technologies	Technologies being phased out by the enterprise.

APPENDIX B - SAMPLE DISCIPLINE DESCRIPTIONS

The following information provides descriptions of the disciplines used in this document.
As governments develop enterprise architecture they may use or modify the disciplines in this document or create their own. In any case, it will be important for agencies to provide a description, as well as the purpose of each discipline as they apply to the organization.

Information Domain	
Data Management	Defines the roles, policies, standards and technologies for data definition, design, management and administration as a recognized enterprise resource. The Data Management discipline provides a process-independent view of all enterprise data stored and housed in a manner that enables data sharing while adhering to all Security and Privacy domain requirements.
Knowledge Management	Defines the roles, standards, and decision-making criteria for the acquisition and deployment of the components that perform the systematic process of finding, selecting, organizing and distilling information in a way that provides internal, as well as external users easy access to information. (Examples include Document Management, Data Warehousing, Data-marts, and Metadata).
GIS	Defines the standards and technologies for implementation of Geographic Information Systems.
Data Storage	Defines the roles, policies, standards and decision-making criteria for the acquisition and deployment of data storage media, as well as the policies governing archiving of data and the use of storage facilities.

Application Domain	
Application Development Management	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.
Electronic Collaboration	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.

Integration Domain	
Functional Integration	Defines the roles, standards, and technologies responsible for the conceptual and logical models, both current and proposed, which show how each of the functional areas, various application systems, and business information requirements tie together. Two perspectives should be considered: a high-level business perspective along with major system components and a high-level information model.
Middleware	Defines the components that create an integration environment between the user workstations and legacy and server environments to improve the overall usability of the distributed infrastructure. Middleware provides interfaces between applications and network communications mechanisms. Middleware functions to create uniform mechanisms for application integration independent of network and platform technologies.

Access Domain	
Access	Defines the roles, policies, standards and technologies that provide the framework for the electronic delivery of information and services to every government agency, business or citizen as deemed permissible under privacy and other mandated regulations.
Branding	Branding defines the "look and feel" for government Web sites.
Accessibility	Defines the roles, policies, standards, and technologies as they apply to tool sets used to facilitate the accessing of information and services by disabled citizens, assuring equal access to electronic technology and automated systems for all Americans.

Network Domain	
Physical Network	Includes network infrastructure for the computing environment. It provides reliable communication for the organization's distributed information processing environment. The Physical Network discipline consists of infrastructure elements, physical components (i.e. wiring, LANS, hubs), carrier services (i.e. frame relay, leased channels, ATM) and protocols (i.e. access routing and naming). It does not include user workstations, server platforms, or their operating systems.
Network Management	Defines the roles, policies, standards and technologies that manage the communications infrastructure for the organization's distributed computing environment. It defines the structure, topologies, bandwidth management, carrier services and protocols necessary to facilitate the interconnection of the organization's information resources, including those facilitating e-government initiatives. This includes consideration for public access from private and kiosk workstations, wireless devices and PCs.

Platform Domain	
Platform	Defines the roles, policies, standards and decision-making criteria for the acquisition and deployment of computing and data storage hardware. The Platform discipline provides for the inclusion of industry standard platforms in use by the citizenry to enable e-government access. Components of the Platform discipline range from enterprise class servers to workstations and hand held computing devices.
Configuration Management	Defines the roles, policies, standards and decision-making criteria for the set-up and provisioning of computing and data storage hardware specifications and its operating software and systems. The Configuration Management discipline provides for the inclusion of industry standard operating systems and utility systems running on the platforms covered under the Platform discipline. Standard configuration for each platform aids in maintainability of the various platforms.

Systems Management Domain	
Asset Management	Defines the policies, procedures, standards and systems required for the tracking and reporting of assets owned by the government entity including software licensing, metering, asset tracking, asset replacement, asset retirement, software distribution and inventory. Other tasks associated with asset management include, but are not limited to, the tracking of service level agreements, capacity management, cost management and personnel skills inventory.
Change Management	Defines the roles, policies, standards and technologies for version control of all IT assets.
Console/Event Management	Defines the roles, standards, policies and technologies for monitoring and controlling components of all collective hardware and software within the entity's data center, including large and mid-range systems.
Help Desk / Problem Management	Defines the roles, standards, policies and technologies for monitoring and controlling problem reporting and resolution.
Business Continuity	Defines the roles, standards, policies and technologies for disaster recovery and restoring the enterprise to full functionality.

Privacy Domain	
Profiling	Defines the roles, standards, policies, audits, and tools used for creating, maintaining, and utilization of profiles for the various stakeholders of the organization services.
Personalization	Defines the roles, standards, policies, audits, and tools used for creating, maintaining and implementing personalization of services and information.
Privacy	Addresses the privacy concerns of citizens and agencies with well-defined roles, policies, procedures and technologies. In addition, the Privacy domain addresses all state and federal laws related to privacy issues such as the distribution, availability, notification or permission to distribute and privacy violation notification. The Privacy discipline focuses on the prevention of unauthorized viewing and/or acquisition of information about a person, case, or other classified activity.

Security Domain	
Enterprise Security	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.
Network Security	Defines the roles, standards, policies, and tools for monitoring and ensuring the security across the organization's network.
Host Security	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.

APPENDIX C: ROLES & RESPONSIBILITIES MATRIX

This matrix 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.

Level	*Responsibility Definition*	*Element Acted upon*	*Interacts with*
		Responsible Role: CHAMPION	
All	Promoting, advertising, marketing, participating in Architecture efforts.	Adaptive Enterprise Architecture Framework	All
Executive	Assuring enterprise goals and objectives for Architecture are met.	Strategic Elements	Enterprise Executives, Overseers, Managers, Audience
All	Cheerleading and public relationship for success.	Communication Documents	All
		Responsible Role: MANAGER	
Executive	Responsible for the coordination of the overall Architecture effort.	Adaptive Enterprise Architecture Framework	All
Executive	Seeks guidance and support for the Architecture effort.	Adaptive Enterprise Architecture Framework	Champion
Executive	Gets clarity and support for the Architecture effort.	Strategic Elements	Advisor, Enterprise Executives
Executive	Chairs and directs the Architecture Review efforts.	Adaptive Enterprise Architecture Framework	Reviewer, Advisor, Subject Matter Expert, Documenter, Manager (Team)
Executive	Receive and evaluate recommendations regarding to Architecture effort.	Adaptive Enterprise Architecture Framework	Reviewer, Documenters, Advisors, Manager (Team)
Executive	Approve/Reject Architecture Requests.	Architecture Review Requests	Reviewer, Documenters, Advisors, Manager (Team)
Executive	Appoint Architecture Documenters.		Documenters, Champion
Executive	Direct Architecture Documenters on process and scope of work.		Documenters
Executive	Provide information to the Communicator about the Architecture pieces.	Adaptive Enterprise Architecture Framework	Communicator, Audience
Executive	Create and Maintain Architecture Governance Framework.	Architecture Governance Framework	Reviewer, Advisor
Executive	Create and Maintain Business Architecture Framework.	Business Architecture Framework	Reviewer, Advisor

Level	*Responsibility Definition*	*Element Acted upon*	*Interacts with*
Executive	Create and Maintain Technology Architecture Framework.	Technology Architecture Framework	Reviewer, Advisor
Executive	Initially set up Architecture Blueprint (Domain / Disciplines).	Architecture Blueprint	Reviewer, Advisor
Executive	Receive Architecture Documentation Results.	Architecture Blueprint	Documenter
Executive	Determine Architecture Review Presenters.	Architecture Lifecycle Process	Documenter, Reviewer, Manager (Team)
Executive	Prepare Architecture Change Request for Business Advisors.	Architecture Lifecycle Process	Advisor, Reviewers
Executive	Direct the Architecture Review Decision Documentation / Communication.	Architecture Lifecycle Process	Reviewer, Documenters, Communicators
Executive	Responsible for the vitality of the Adaptive Enterprise Architecture Framework.	Adaptive Enterprise Architecture Framework	Advisor, Reviewers, Documenters, Manager (Team)
Executive	Review Architecture Help Request and determine affected Architecture Blueprint levels.	Architecture Help Request, Architecture Blueprint	Manager (Team), Documenter
Executive	Review and summarize Technical Advise.	Summarized Technical Advise	Documenter, Advisor, Manager (Team)
Executive	Help create Architecture Variance Business Case.	Architecture Variance Business Case	Manager (Team), Documenter, Project Teams, Service Teams
Executive	Coordinate Architecture Blueprint Vitality Process.	Architecture Blueprint Vitality Process	Manager (Team), Documenter, Advisor, Reviewer
Team	Adhere to Architecture Compliance Process.	Architecture Compliance Process	Manager (Executive), Documenter, Reviewer
Team	Create Architecture Variance Business Case.	Architecture Variance Business Case	Manager (Executive), Documenter, Project Teams, Service Teams
Team	Request Architecture Information for the Architecture Framework and Architecture Blueprint.	Architecture Communication Process	Communicator
Team	Create Architecture Help Request with initial identification of affected Architecture Blueprint levels.	Architecture Compliance Process	Manager (Executive), Documenter, Service Teams, Project Teams
Team	Work with Project and Service Teams to determine recommended Technology Option for implementation.	Architecture Compliance Process	Service Teams, Project Teams
Team	Recommend Architecture Framework enhancements.	Architecture Framework Vitality Process	Manager (Executive), Service Team, Project Team
Team	Help with Architecture Blueprint Vitality process based on technology solutions from IT projects or major enhancements.	Architecture Blueprint Vitality Process	Manager (Executive), Service Team, Project Team

Level	*Responsibility Definition*	*Element Acted upon*	*Interacts with*
	Responsible Role: DOCUMENTER		
Blueprint	Receive Architecture Educational Training.	Architecture Documentation Process	Manager (Executive)
Blueprint	Facilitate and conduct Domain working sessions.	Architecture Documentation Process	Manager (Executive), Subject Matter Experts
Blueprint	Document/Update Architecture Blueprint.	Architecture Documentation Process	Manager (Executive), Subject Matter Experts
Blueprint	Summarize Architecture Blueprint Changes.	Architecture Documentation Process, Architecture Review Process	Manager (Executive)
Blueprint	Review Architecture Blueprint changes to Technology Drivers for conflicts.	Architecture Documentation Process	Manager (Executive)
Blueprint	Document Architecture Review Decisions in the various Architecture Blueprint levels.	Architecture Review Process	Manager (Executive)
Blueprint	Request Architecture Information for the Architecture Framework and Architecture Blueprint.	Architecture Communication Process	Communicator
Blueprint	Develop a through knowledge of the Architecture Framework.	Adaptive Enterprise Architecture Framework	Manager (Executive)
Blueprint	Help with Architecture Help Requests responses.	Architecture Compliance Process	Manager (Executive), Manager (Team), Subject Matter Experts, Project Teams, Service Teams
Blueprint	Help with Creating Architecture Variance Business Case.	Architecture Compliance Process	Manager (Executive), Manager (Team), Project Teams, Service Teams
Blueprint	Recommend Architecture Framework enhancements.	Architecture Framework Vitality Process	Manager (Executive), Subject Matter Experts
Blueprint	Document and Recommend Domain Architecture Changes (such as domain boundary limits, associated disciplines, and technology drivers).	Architecture Documentation Process	Subject Matter Experts, Reviewer
Blueprint	Document and Recommend Discipline Architecture Changes (such as discipline boundary limits).	Architecture Documentation Process	Subject Matter Experts, Reviewer
Blueprint	Conduct Technology Scan.	Architecture Documentation Process	Subject Matter Experts
Blueprint	Evaluate Product and Compliance Components for classification in the Architecture Blueprint.	Architecture Documentation Process	Subject Matter Experts

Level	*Responsibility Definition*	*Element Acted upon*	*Interacts with*
	Responsible Role: COMMUNICATOR		
All	Conduit for Architecture Information into the enterprise.	Architecture Communication Process	Audience, Manager (Executive), Documenter
All	Create a specific Communication Document based upon a request for information.	Architecture Communication Process	Audience
All	Create a routine Communication Document based upon the completion of a process or period timing.	Architecture Communication Process	Audience
	Responsible Role: ADVISOR		
Executive	Provide clarity and support to the Manager of the Architecture.	Strategic Elements	Manager (Executive)
Executive	Represent the Strategic Elements based on their background IT and/or Business.	Strategic Elements	Manager (Executive)
Executive	Provide guidance on Architecture Variance Requests from a business and economical perspective.	Architecture Compliance Process	Manager (Executive), Reviewer
Executive	Create the Adaptive Enterprise Architecture Framework (including identifying Enterprise Elements, creation of Architecture Governance Roles, definition of Architecture Elements).	Adaptive Enterprise Architecture Framework	Manager (Executive), Champion
Executive	Review and approve the Architecture Governance Organization Structure.	Governance Processes	Manager (Executive), Champion
Executive	Review and approve the Architecture Lifecycle processes.	Governance Processes	Manager (Executive), Champion
Executive	Develop Technology Drivers.	Architecture Documentation Process	Manager (Executive), Reviewer
Executive	Create initial Architecture Blueprint (Domain /Disciplines).	Architecture Blueprint	Manager (Executive), Reviewer
Executive	Consider proposed Architecture Review Request and Architecture Change Request.	Architecture Review Process	Manager (Executive), Reviewer
Executive	Offer recommendations based on the consideration of the Architecture Review Request and Architecture Change Request.	Architecture Review Process	Manager (Executive), Reviewer
Executive	Provide changed Strategic Elements.	Architecture Framework Vitality Process and Architecture Blueprint Vitality Process	Manager (Executive)

Level	*Responsibility Definition*	*Element Acted upon*	*Interacts with*
	Responsible Role: REVIEWER		
Framework	Review the various Architecture Governance Element Changes.	Architecture Documentation Process, Architecture Review Process	Manager (Executive), Documenter
Framework	Review and approve the Architecture Governance Organization Structure.	Governance Processes	Manager (Executive), Advisor
Framework	Review and approve the Architecture Lifecycle processes.	Governance Processes	Manager (Executive), Advisor
Framework	Develop Technology Drivers.	Architecture Documentation Process	Manager (Executive), Advisor
Blueprint	Create initial Architecture Blueprint (Domain / Disciplines).	Architecture Blueprint	Manager (Executive), Advisor
Blueprint	Review and approve Architecture Blueprint changes and additions.	Architecture Review Process	Subject Matter Experts, Advisors, Manager (Executive), Documenter, Manager (Team)
Framework	Review and approve Architecture Framework changes and additions.	Architecture Review Process	Subject Matter Experts, Advisors, Manager (Executive), Documenter
All	Request Architecture Information and Architecture Review items for the Architecture Framework and Architecture Blueprint.	Architecture Communication Process	Communicator
Blueprint	Review and approve Architecture Domain and Discipline scope changes.	Architecture Documentation Process	Documenter
	Responsible Role: AUDIENCE		
All	Review and receive Architecture information.	Architecture Communication Process	Communicator
	Responsible Role: OVERSEER		
Executive	Ensure that IT plans follow the proper direction for the enterprise and IT budgets are well spent.	Strategic Elements	Manager (Executive), Champion, Advisor
	Responsible Role: SUBJECT MATTER EXPERT		
All	Clarify and state technical opinions during Architecture Review Process.	Architecture Review Process	Documenter, Manager (Executive), Manager (Team)
Blueprint	Review Technical Recommendations during Architecture Compliance Process.	Architecture Compliance Process	Manger (Executive)
Blueprint	Provide Technical Oversight opinion during Architecture Compliance Process.	Architecture Compliance Process	Manger (Executive)
Blueprint	Help Documenters to create the Architecture Blueprint.	Architecture Documentation Process	Documenter

Level	*Responsibility Definition*	*Element Acted upon*	*Interacts with*
Blueprint	Determine if existing technology can support requested services.	Architecture Blueprint	Documenter, Manager (Executive), Manager (Team)
Blueprint	Communicate new compliances or technology needs to Manager. (This can include version updates.)	Architecture Blueprint	Documenter, Manager (Executive), Manager (Team)
All	Request Architecture Information for the Architecture Framework and Architecture Blueprint.	Architecture Communication Process	Communicator
Blueprint	Request Architecture Help.	Architecture Compliance Process	Manager (Team), Manager (Executive)
Blueprint	Help Team Manager determine recommended Technology Option for implementation.	Architecture Compliance Process	Manager (Team)
Blueprint	Help document the Physical Implementation Requirements for the Architecture Variance Business Case.	Architecture Compliance Process	Manager (Team), Manager (Executive), Documenter
Blueprint	Help create the Total Cost of Ownership for the Architecture Variance Business Case.	Architecture Compliance Process	Manager (Team), Manager (Executive), Documenter
	Responsible Role: PROJECT TEAMS		
Blueprint	Seek further technology scans to extend the Architecture Blueprint.	Architecture Blueprint	Documenter, Manager (Executive), Manager (Team)
Blueprint	Request Architecture Information for the Architecture Framework and Architecture Blueprint.	Architecture Communication Process	Communicator
Blueprint	Request Architecture Help.	Architecture Compliance Process	Manager (Team), Manager (Executive)
Blueprint	Help Team Manager determine recommended Technology Option for implementation.	Architecture Compliance Process	Manager (Team)
Blueprint	Help document the Physical Implementation Requirements for the Architecture Variance Business Case.	Architecture Compliance Process	Manager (Team), Manager (Executive), Documenter
Blueprint	Help create the Total Cost of Ownership for the Architecture Variance Business Case.	Architecture Compliance Process	Manager (Team), Manager (Executive), Documenter

Level	*Responsibility Definition*	*Element Acted upon*	*Interacts with*
	Responsible Role: PROCUREMENT MANAGER		
Executive	Develop procurement policies and procedures.	Procedural Elements	Manager (Executive)
Blueprint	Verify purchase requests have the appropriate Architecture compliance review sign off.	Procedural Elements, Architecture Compliance Process	Manager (Executive)
	Responsible Role: PROJECT/SERVICE METHODOLOGY COMMUNICATOR		
Executive	Develop project and service methods, policies and procedures.	Procedural Elements	Manger (Executive)
Blueprint	Verify projects and service plans include the appropriate Architecture Compliance review steps.	Procedural Elements, Architecture Compliance Process	Manager (Executive)
	Responsible Role: SPECIAL INTEREST GROUP		
All	Provide advisory input into the Enterprise Architecture by identifying special needs, interests, or considerations as well as architecture compliance requirements specific to the group.	Architecture Blueprint, Business Drivers, Technology Drivers	Manager (Executive)
	Responsible Role: ENTERPRISE EXECUTIVE		
Executive	Provide the Strategic Elements that give direction, goals and objectives to the enterprise.	Strategic Elements	Manager (Executive), Overseer, Advisor

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

Notes

Notes

Notes