# NASCIO EA Development Tool-Kit
# Technology Architecture

Version 3.0

October 2004

# TABLE OF CONTENTS

# TECHNOLOGY ARCHITECTURE

Technology Architecture is a disciplined approach for documenting the enterprise's current, emerging and retiring technologies in order to leverage the investment in those resources and maximize their potential as solutions to business problems. Technology Architecture examines the underlying technologies that are required to run the enterprise and develops a unified vision of the target model of the enterprise's infrastructure and technology platforms.

Documentation of the Technology Architecture facilitates design of flexible, reliable, scalable, and secure systems that will support both known and unforeseen future requirements. Technology Architecture allows the enterprise to add systems and manage the lifecycle of current systems while guiding investment and design decisions. Balancing technology agility with technology efficiency is a challenge for all organizations. The Technology Architecture provides the tools for an organization to achieve the best balance for their state or local governmental body.

Figure 1 shows how Technology Architecture fits within the overall Enterprise Architecture Framework. The Technology Architecture is designed to support the strategic and operational requirements of the enterprise. It aligns with the Business and Information Architectures and supports Implementation Planning and Solution Architecture.

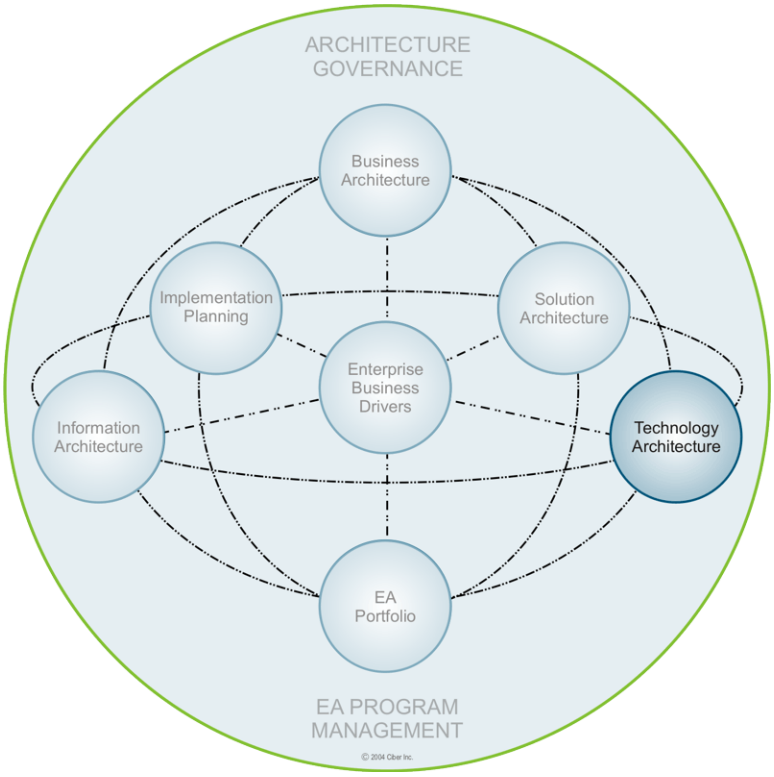



*Figure 1. Technology Architecture Touch-points*

State and local governments continually face mandates for inter-agency Information Technology system interoperability. Technology Architecture provides an adaptable framework for developing solutions that operate across agencies and within the lines of business of state and local governments. The pursuit of formal Enterprise Architecture Programs within organizations contributes to interoperability across enterprises. This is depicted in Figure 2.

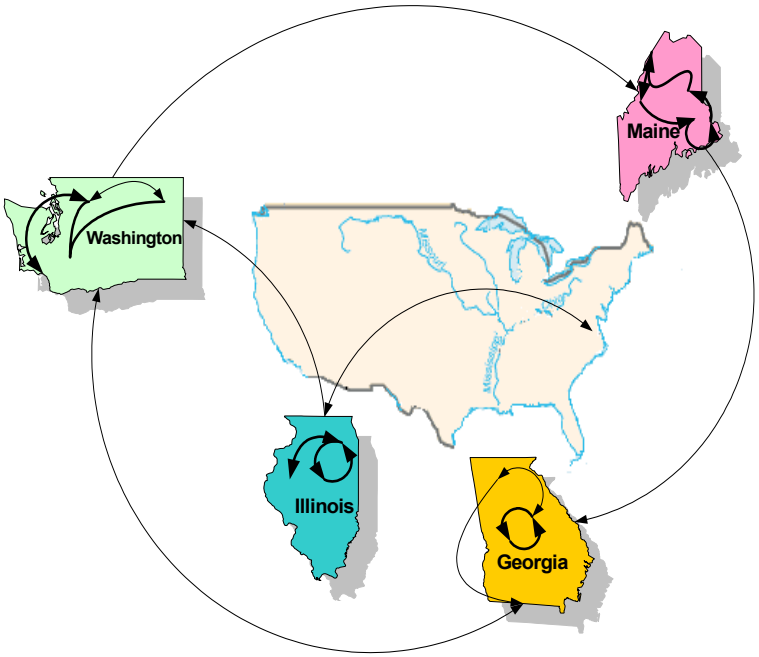



*Figure 2. EA enhances interoperability between all government bodies.*

## Definitions

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

- *Adaptive:* Able to support a wide variety of applications and evolve as technology changes.
- *Agency:* A governmental unit; in the narrowest sense, a governmental unit of the executive branch.
- *Best Practices:* Trends and approaches that have successfully provided services and information over time.
- *Blueprint:* The dynamic, detailed information about a specific enterprise that is captured using standardized, structured processes and templates (the framework). The Technology Architecture Blueprint records the present direction of the enterprise and the direction the enterprise intends to pursue from a perspective of technology products and standards.
- *Business Drivers:* Global influences on business and technology that are captured within the architecture to show their acceptance and adoptability into the environment.

- *Component:* Within this Tool-Kit, component refers to a level of architectural detail. Within each of the constituent architectures, the component level detail is captured utilizing a respective template. Technology Architecture addresses Product Components and Compliance Components.
- *Current Technologies:* Technologies that are the current standard for use within the enterprise, and tested and generally accepted as standard within the industry. These items comply with or support the principles listed for the discipline.
- *Discipline:* Logical functional areas to address when building the architecture blueprint. The descriptions of the disciplines used in this document are found in Appendix B.
- *Domain:* High-level logical groupings of functional or topical operations that form the main building blocks within the architectural framework.
- *Emerging Technologies:* Technologies that, while possibly accepted and well utilized throughout the industry, are new to the enterprise. It is generally understood that emerging technologies be considered carefully before implementing in an enterprise-wide architecture. It is therefore recommended that, for initial implementation, emerging technologies be limited to smaller, non-mission-critical projects until it is proven that they can be integrated successfully into the existing enterprise architecture.
- *Framework:* The combination of the structure, processes, and templates that facilitate the documentation of the architecture in a systematic and disciplined manner. Use of the framework guides the documentation of the enterprise detail, which becomes the architecture blueprint.
- *Gap:* The difference between the "baseline" business environment and the "target" environment.
- *Infrastructure:* The basic, fundamental architecture of the system that supports the flow and processing of information, and that determines how the system functions and how flexible it is to meet future requirements.
- *Integration:* The ability to access and exchange critical information electronically at key decision points throughout the enterprise.
- *Interoperability:* The ability of a system or a product to work with other systems or products without special effort on the part of the customer, either by adhering to published interface standards or by making use of a "broker" of services that can convert one product's interface into another product's interface "on the fly"[1]
- *Legacy systems* An automated system built with older technology that may be unstructured and lacking in modularity, documentation and even source code.
- *Migration:* The evolution from the baseline to the target state.
- *Principle:* A statement of preferred direction or practice. Principles constitute the rules, constraints and behaviors that a bureau, agency or organization will abide by in its daily activities over a long period of time. Principles are business practices and approaches that the organization chooses to institutionalize to better provide services and information.
- *Repository:* An information system used to store and access architectural information, relationships among the information elements, and work products[2].
- *Scalability:* The ability to use the same applications and application systems on all classes of computers from personal computers to supercomputers.
- *Sunset Technologies:* Technologies that have been phased out and cannot be used within the organization past a specified date.

[1] http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci212372,00.html
[2] A Practical Guide to Federal Enterprise Architecture v1.0, CIO Council, February 2001

- *System:* A set of different elements so connected or related as to perform a unique function not performable by the elements alone (Rechtin 1991).
- *Target:* The desired future or "to be" state of the environment, captured in a set of target models.
- *Technology:* Tools or tool systems by which we transform parts of our environment and extend our human capabilities (Tornatzky and Fleischer 1990).
- *Technology Architecture Framework:* the combination of structures, templates and structured processes that facilitates the documentation of the enterprise's technology artifacts (e.g., products, standards) in a systematic and disciplined manner.
- *Template*: The empty form that serves as a guide for documenting the architecture detail. The resulting dynamic content captured using the template is referred to as the "blueprint" and ultimately resides in an Enterprise Architecture repository.
- *Trends:* Emerging patterns of operation within the business world that are impacting how services and information will be provided. Trends include governmental trends as well as architecture specific tends, i.e. technology trends, information management trends, etc.
- *Twilight Technologies:* Technologies being phased out by the enterprise but not yet having an established end date.

A sound Technology Architecture Framework is needed to support implementation of the architecture blueprint. The Technology Architecture Framework shows the relationship of the business drivers to the IT portfolio. The technology model must be flexible enough to provide the processes and templates to document any number of technology solutions to address business needs and problems.

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

## Technology Architecture Framework

The Technology Architecture Framework includes the templates and processes of the Enterprise Architecture Framework that will structure technology direction and existing IT services (Figure 3). This portion of the Tool-Kit documents the semi-static information, i.e. information that changes only when a major shift in the business or technology occurs. The following resources are available:

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

### BUSINESS DRIVERS

The identification and development of Business Drivers is an important part of developing Enterprise Architecture. Business Drivers refer to the global influences on business that drive government and are captured within the architecture to show their acceptance and adoptability into the environment. Though these global influences can be of numerous types, three common categories of Business Drivers are Principles, Best Practices and Trends.

*Principles:* Principles are statements of preferred direction or practice. Principles constitute the rules, constraints and behaviors that a bureau, agency or organization will abide by in its daily activities over a long period of time. Principles are business practices and approaches that the organization chooses to institutionalize to better all provided services and information.

*Best Practices:* Best practices are behaviors and approaches that have proven successful at providing services and information over time.

*Trends:* Trends are emerging influences within the business world that are impacting how services and information will be provided. Trends include governmental trends, as well as architecture specific trends, i.e. technology trends, information management trends, etc.

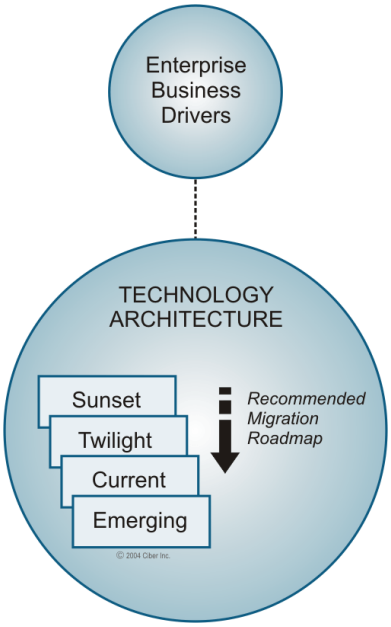



*Figure 3. Technology Architecture Flow*

## TECHNOLOGY ARCHITECTURE BLUEPRINT STRUCTURE

The Technology Architecture Blueprint Framework consists of:

- The Technology Architecture Blueprint Documentation Processes
- The Technology Architecture Blueprint Templates

In order to discuss the Technology Architecture Blueprint Documentation Process, it is first necessary to become familiar with the various levels of the Technology Architecture Blueprint and get an overall picture of how the pieces fit together.

There are five technology architecture blueprint levels:

- Domains
- Disciplines
- Technology Areas
- Product Components
- Compliance Component

As can be seen from the graphic in Figure 4, these pieces work together to ensure the complete documentation of the Domains that form the Technology Architecture Blueprint.

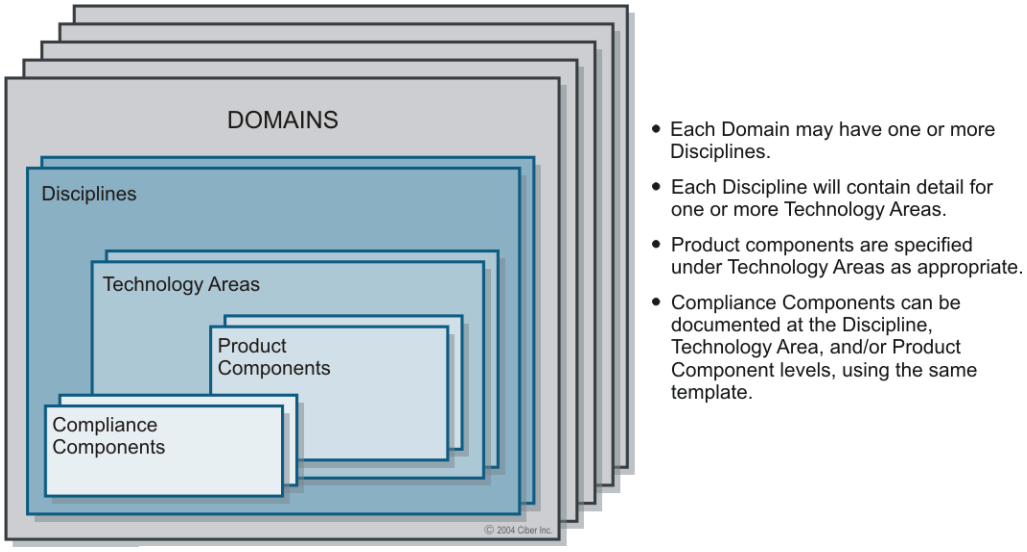



*Figure 4. Blueprint Structure*

**Domains** are the natural divisions of the technology architecture and, as seen in Figure 5, form the main building blocks of the technology architecture blueprint.

A Domain is simply a category that is used to group related topics, similar to the way a library groups related topics (Biographies, Art, History, etc.). Each Domain identified will be developed and documented by a team made up of subject matter experts who are familiar with the organization's IT environment.

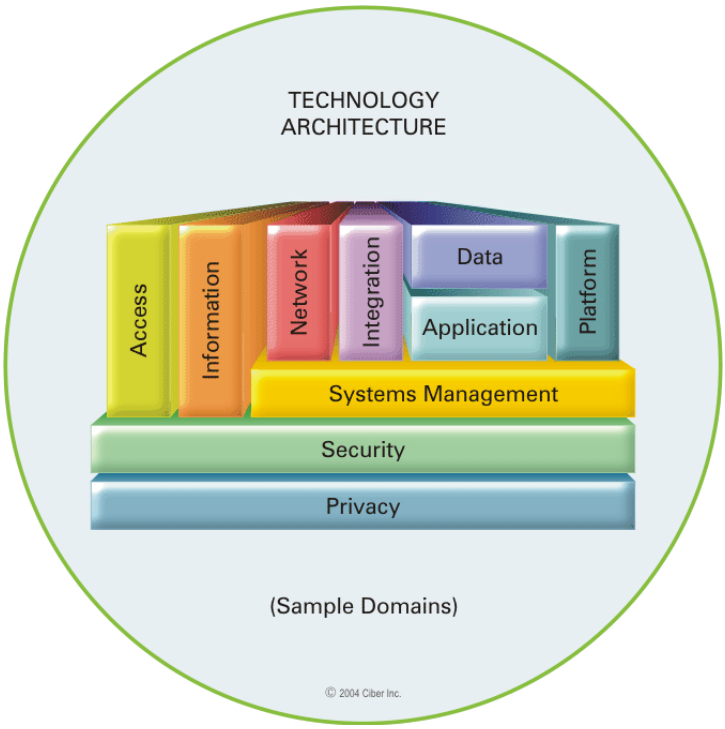



*Figure 5. Sample Technology Architecture Domains*

The logical functional subsets of a Domain are called **Disciplines**. Disciplines allow further breakdown of the Domain into manageable pieces, especially for Domains that cover large and/or diverse topics. Each Discipline is a cohesive unit with regard to its subject areas and stakeholders.

The Systems Management Domain provides a good example of a Domain with multiple Disciplines:

| *Domain* | *Disciplines* |
|---|---|
| Systems Management | • Asset Management<br>• Change Management<br>• Console/Event Management<br>• Help Desk/Problem Management<br>• Business Continuity |

Each Domain will have one or more Disciplines. As with Domains, additional Disciplines may be identified during the development or evolution of the enterprise architecture

**Technology Areas** are those technical topics that support the technology functional areas of the architecture blueprint.

A few examples of technology areas from within the Database Management Discipline of the Information Domain are:

- Relational Database
- Flat File Systems
- Desktop Database
- Data Models

Each of these technology areas will have products, protocols or configurations associated with it. These are documented at the Product Component level.

Technology Areas are identified and addressed within each Discipline. At this level, the technical details of the Technology Architecture Blueprint start to form.

**Product Components** include the protocols, products (families) and configurations that are specific to a technology area. Examples of Product Components identified within the technology area of Data Models include ERWin, Visio, Rational Rose, System Architect and Designer 2000.

The documentation of each Product Component includes the evaluation criteria used by the Documenter to determine the component's acceptance as part of the technology architecture blueprint.

**Compliance Components** identify guidelines, standards and legislative mandates associated with a Discipline, Technology Areas, and/or Product Components as appropriate.

Compliance Components provide the basis for making important decisions about new products, protocols, configurations, etc. The same template for evaluation, classification, and documentation may be used for Compliance Components at all three levels. Guidelines, standards and legislative mandates differ primarily in the degree of compliance prescribed by each.

| *Domain* | *Discipline* | *Technology Area* | *Product Component* | *Compliance Component* |
|---|---|---|---|---|
| Information | Data Management | • Relational Database<br>• Flat File Systems<br>• Desktop Database<br>• Data Models | • Oracle<br>• Sybase<br>• DB2<br>• ERWin<br>• Designer 2000 | • Data Model Denotations- Crows Feet<br>• Normalization<br>• Column Naming Standards |

Each sub-process in the Technology Architecture Documentation Process describes the documentation of one level of the Blueprint, with one additional sub-process to cover the evaluation and classification of the Product and Compliance Components.

Each sub-process will have a process model and narrative section. Where a template is introduced within a process model, the template and its detail follow the process narrative. The Technology Architecture Documentation Process includes the following Sub-processes and Templates.

- Document/Update Domain Blueprint Process
- Domain Blueprint Template
- Document/Update Discipline Blueprint Process
- Discipline Blueprint Template
- Document/Update Technology Area Blueprint Process
- Technology Area Blueprint Template
- Document/Update Product Component Blueprint Process
- Product Component Blueprint Template
- Document/Update Compliance Component Blueprint Process
- Compliance Component Blueprint Template
- Evaluate Compliance/Product Components

# TECHNOLOGY ARCHITECTURE DEVELOPMENT

The process of developing the Technology Architecture begins with initiating the Technology Architecture Documentation Process. This documentation process allows the architecture teams to capture, analyze, and document details about the products and standards, which will be included in the Technology Architecture Blueprint.

Figure 6 provides a graphical representation of the workflow path for the architecture team as it moves through the processes and sub-processes of the Technology Architecture Documentation Process.

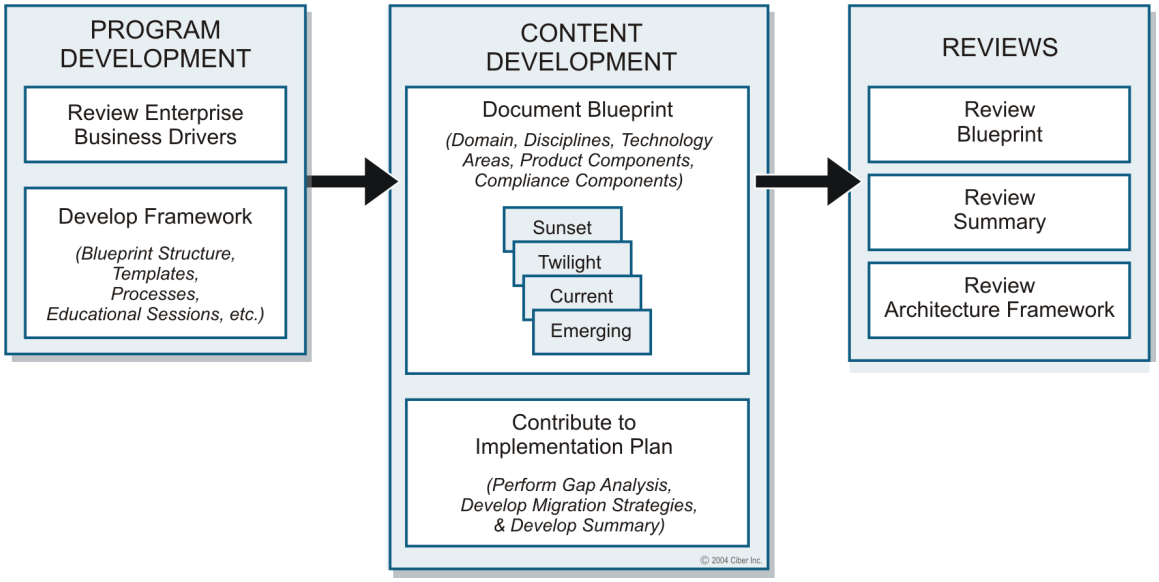



*Figure 6. Technology Architecture Development Work Flow*

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

- Initiate Technology Architecture Documentation Process
- Develop Enterprise Drivers
- Develop Technology Architecture Framework
- Conduct Technology Architecture Work Sessions
- Create/Update Technology Architecture Blueprint Items
- Complete/Update Domain Blueprint
- Complete/Update Discipline Blueprint
- Complete/Update Technology Area Blueprint
- Complete/Update Product Component Blueprint
- Complete/Update Compliance Component Blueprint
- Evaluate Product/ Compliance Component

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

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

# Initiate Technology Architecture Documentation Process

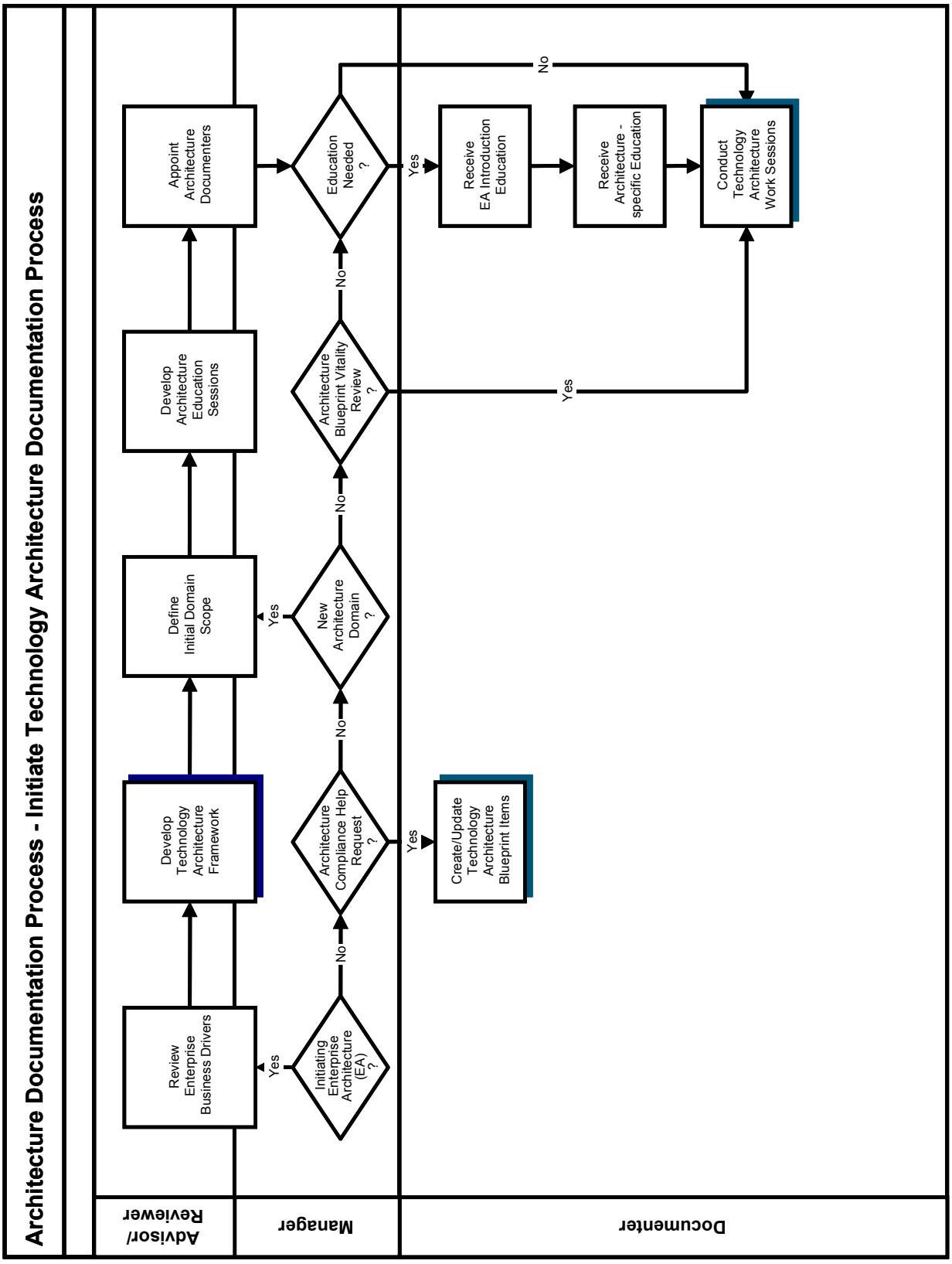
## PROCESS OVERVIEW

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

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

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

- *Enterprise Architecture Initiation Trigger* – The first time the Architecture Blueprint is documented, the Documenters are supplied with basic information for each of the Domains and Disciplines, such as definition, rationale, benefits, boundary statements and an initial set of technology areas to be covered within each. Also, the Documenters are trained on the various enterprise architecture processes and templates. The Documenters are then prepared to develop the detail that will become the EA Blueprint.
- *Architecture Blueprint Vitality Process Trigger* – This periodic process verifies that the Architecture Blueprint is staying current with the changes in the business and in the technology world. Vitality can impact the Architecture Blueprint from the Domain level down.
- *Compliance Process Trigger* – The Compliance Process is the point where IT groups outside of the Architecture group interact with the various Architecture processes and blueprints. This process is initiated from an Architecture Help Request. Compliance can impact the Architecture Blueprint from the Technology Area down


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

## PROCESS DETAIL

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

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

**Define Initial Domain Scope** – Develop the definition of the Technology Domains and add any detail that will be helpful in identifying the documentation team members. Also, add any information that will help the team develop the appropriate level of documentation for these domains.

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

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

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

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

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

**Receive Architecture-specific Education** – After receiving initial enterprise architecture training, the Documenters will receive specialized instruction addressing the business, information or technology

architecture documentation templates and respective architecture documentation processes that they will use to document the Architecture Blueprint.

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

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

# Develop Technology Architecture Framework

## PROCESS OVERVIEW

Framework refers to the combination of the structure, processes, and templates that facilitate the documentation of the architecture in a systematic and well-disciplined manner. In this Tool-Kit, the term Technology Architecture Framework is used to refer to the combination of the structural elements of the Technology Architecture, including the templates and the structured processes for documenting, reviewing communicating, implementing and maintaining the Technology Architecture.

Each organization should develop a Technology Architecture Framework based on their individual circumstances. The NASCIO Tool-Kit is designed to provide a jumpstart for organizations as they develop their architectures, not to provide a methodology. The framework elements provided in this Tool-Kit represent a sampling of the structural elements an organization should consider as they build their Technology Architecture, and are by no means exhaustive, nor are they intended to be prescriptive There are many methodologies for developing architectures. Regardless of the methodology selected, the structure for capturing Technology Architecture Blueprint detail should be consistent and concise to ensure uniform documentation and communication across the enterprise.

Architecture Documentation Process - Develop Technology Architecture Framework
Advisor/Reviewer
Manager
Documenter
Develop Technology Architecture Processes/ Templates
Identify/Define Domains
Identify/Define Disciplines
Select Initial Technology Domains for Documentation

## PROCESS DETAIL

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

The development of the Technology Architecture processes and templates is a good time to consider the use of a repository or automated tool for the capture and storage of the architecture documentation. The use and maintenance of the Enterprise Architecture is greatly simplified when the information and models are readily available to all stakeholders. There is a large amount of information collected and documented within an EA with many interrelations between the parts of the EA. It is best if all the EA information, models and products are placed in a robust EA repository to maximize the potential for reuse.

**Identify/Define Domains, Identify/Define Disciplines -** Technology Domains provide the natural divisions of the Technology Architecture based on scope and are the main building blocks of the Technology Architecture blueprint. The further breakdown of the Domains into manageable sub-sets, referred to in this Tool-Kit as Disciplines, should also be done as part of the framework development process. Each organization must identify its own Technology Domains and respective Disciplines. Examples of typical Domains and Disciplines with brief descriptions as used in this Tool-Kit can be found in *Appendix B: Sample Domain-Discipline Descriptions*.

**Select Initial Technology Domains for Documentation –** It will not be feasible to attempt to document every Domain at one time. Care should be taken to select a reasonable number of Domains, based on criticality and resources.

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

# Conduct Technology Architecture Work Sessions

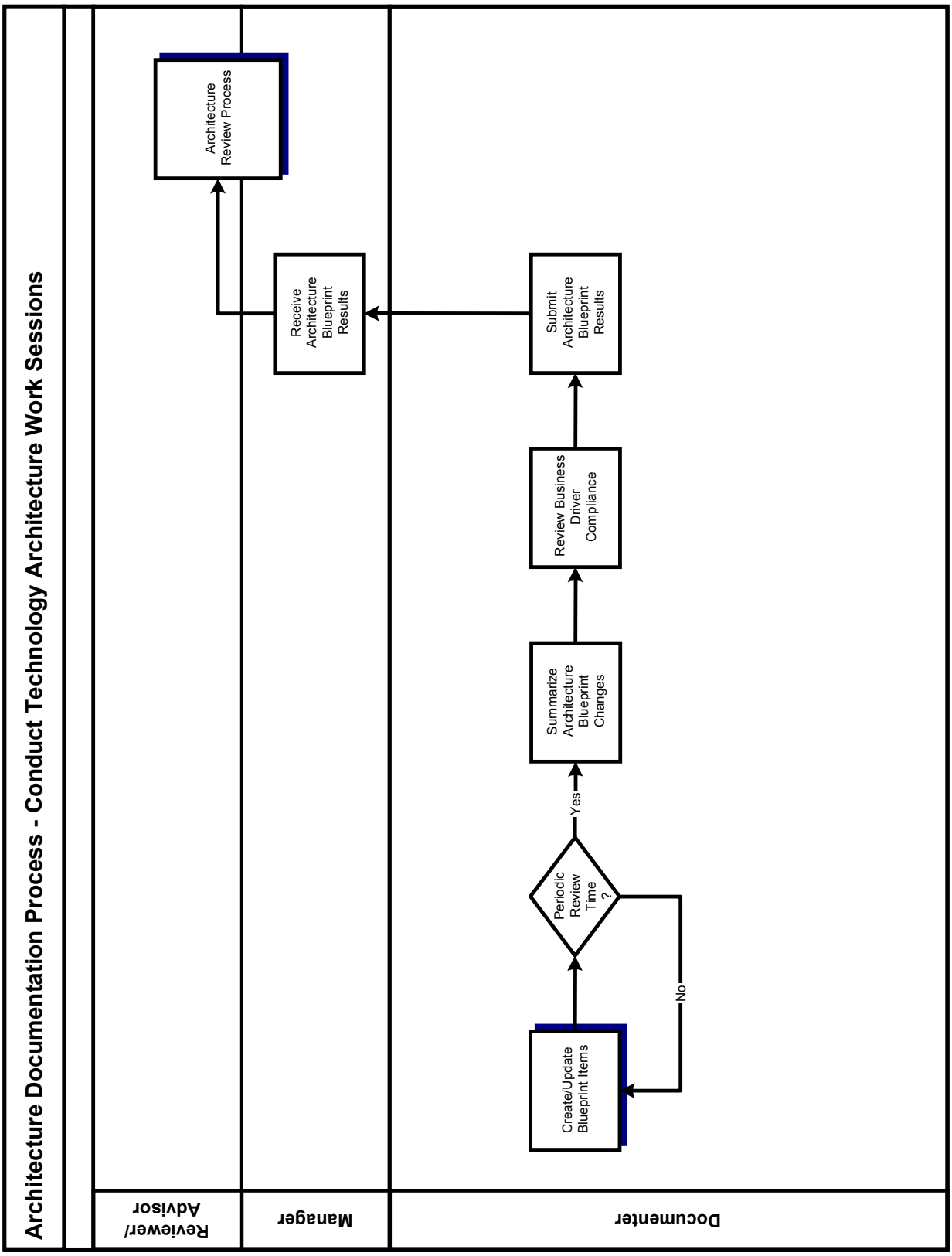
## PROCESS OVERVIEW

The Technology Architecture work sessions are intended to produce the documentation that initially populates the Architecture Blueprint. Ongoing Documenter meetings are required to maintain the vitality of the Domain's architecture blueprint. The first session will include:

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

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

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


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

## PROCESS DETAIL

**Create/Update Blueprint Items** - The primary purpose of the working sessions is to document the Technology Architecture, therefore creating and/or updating the Technology Blueprint items will be on the agenda for most working sessions. The process steps for documentation of the Blueprint items are covered in a separate process step later in this section. (See sub-process - *Create/Update Blueprint Items*)

**Summarize Architecture Blueprint Changes** - Based on changes occurring since the last periodic review, the Documenter will create a summary listing all changes to the Architecture Blueprint for that Domain throughout the five levels.

**Review Business Driver Compliance** - The submitted changes for a specific Domain may cause a conflict with one of the Business Drivers. This process step assures that the Documenter takes a high-level review of the Domain's architecture blueprint to verify that no conflicts exist. Where conflicts exist, the Documenter will provide the proper documentation to the Architecture Manager.

**Submit Architecture Blueprint Results** - Based on time or completion of a documentation process, the Documenter will gather and submit the available Domain blueprint results to the Architecture Manager.

**Review Architecture Blueprint Results** - The Architecture Manager will receive, review, and summarize the Domain results.

**Architecture Review Process** - The prepared Domain Results will be presented and reviewed at the next Architecture Review Meeting.

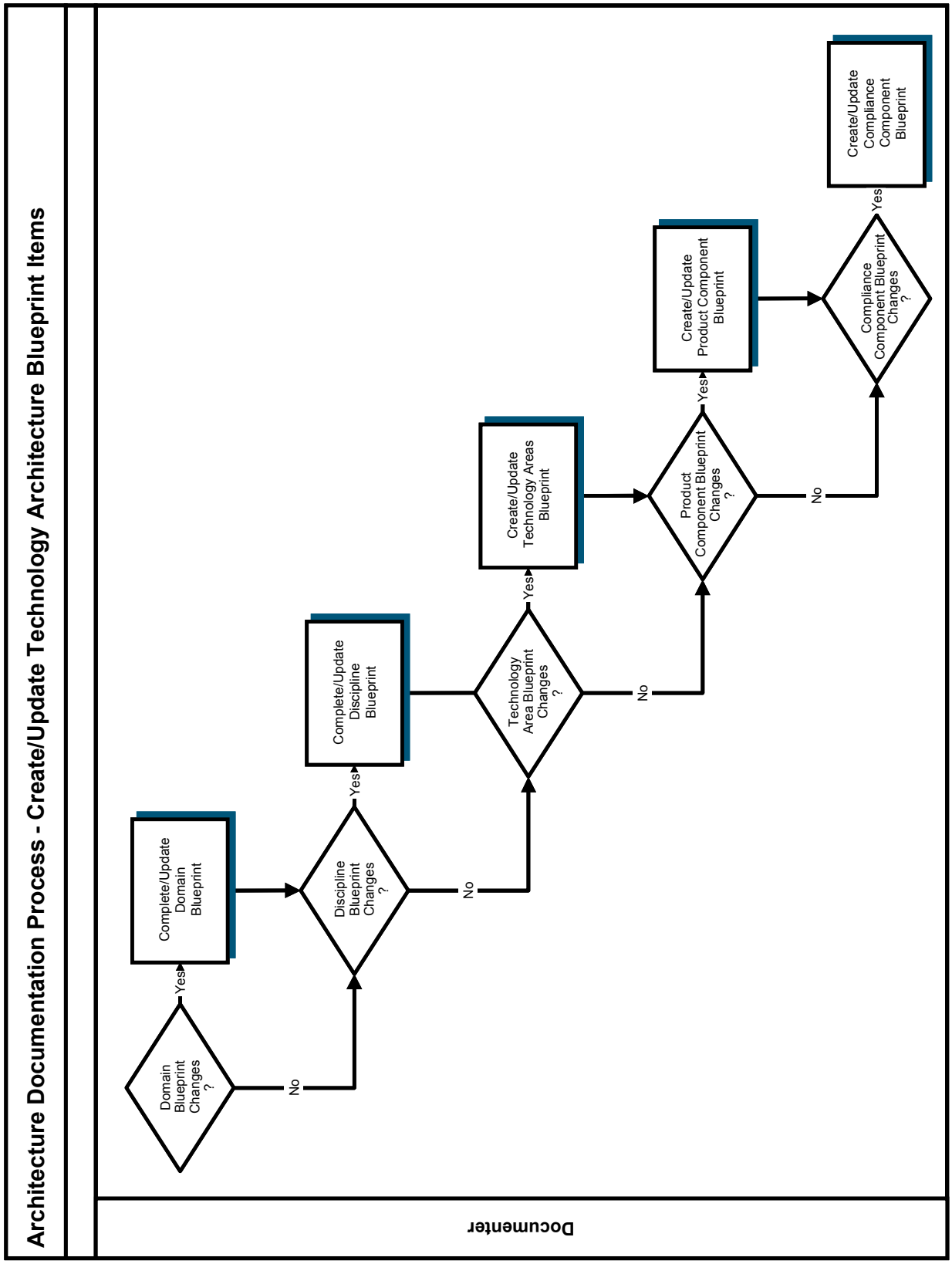
# Create/Update Technology Architecture Blueprint Items

## PROCESS OVERVIEW

Various architecture processes trigger the update of the Technology Architecture Blueprint, including:

- Conduct Technology Work Sessions
- Architecture Review Process
- Architecture Compliance Process
- Architecture Blueprint Vitality Process

The appropriate Technology Architecture Blueprint levels will be updated, based on what triggered the Create/Update Technology Architecture Blueprint Items process.


Architecture Documentation Process - Create/Update Technology Architecture Blueprint Items
Documenter
Domain Blueprint Changes ?
Yes
No
Complete/Update Domain Blueprint
Discipline Blueprint Changes ?
Yes
No
Complete/Update Discipline Blueprint
Technology Area Blueprint Changes ?
Yes
No
Create/Update Technology Areas Blueprint
Product Component Blueprint Changes ?
Yes
No
Create/Update Product Component Blueprint
Compliance Component Blueprint Changes ?
Yes
Create/Update Compliance Component Blueprint

## PROCESS DETAIL

NOTE: The following processes are sub-processes of the Architecture Documentation Process and are used for updating the Architecture Blueprints. Details for each of these sub-processes are provided later in this section.

**Complete/Update Domain Blueprint -** If the accepted change identified a new Domain, the new Domain should be fully documented, including all subordinate levels.

If the change being sought identified changes to an existing Domain, the blueprint for the Domain and the other affected Domains should be updated to reflect the accepted or rejected change.

*For documentation requirements, see Architecture Blueprint Templates – Domain Template*.

**Complete/Update Discipline Blueprint -** If the accepted change identified a new Discipline, fully document the new Discipline, including all subordinate levels. If the requested change identified changes to an existing Discipline, update the blueprint for the Discipline and other affected Disciplines to reflect the accepted or rejected change.

*For documentation requirements, see Architecture Blueprint Templates – Discipline Template.*

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

*For documentation requirements, see Architecture Blueprint Templates – Technology Area Template*.

**Create/Update Product Component Blueprint -** If the accepted change identified a new Product Component, fully document the new Product Component, including all subordinate levels. If the requested change identified changes to an existing Product Component, update the blueprint for the product to reflect the accepted or rejected change.

Conditional use should be documented as well, if it applies.

*For documentation requirements, see Architecture Blueprint Templates – Product Component Template.*

**Create/Update Compliance Component Blueprint -** If the accepted change identified a new Compliance Component, fully document the new Compliance Component. If the requested change identified changes to an existing Compliance Component, update the blueprint for the Compliance Component to reflect the accepted or rejected change.

Conditional use should be documented as well, if it applies.

*For documentation requirements, see Architecture Blueprint Templates – Compliance Component Template.*

# Complete/Update Domain Blueprint

## PROCESS OVERVIEW

The Domain is the highest level of the Technology Architecture Blueprint levels. The definition and development of each Domain is a process that will evolve and change as information is gathered and documented. A domain template is provided to ensure consistent documentation of each Domain.

The NASCIO working group has been involved in a high-level review process to define and document a sample set of Domains. This sample set of Domains includes:

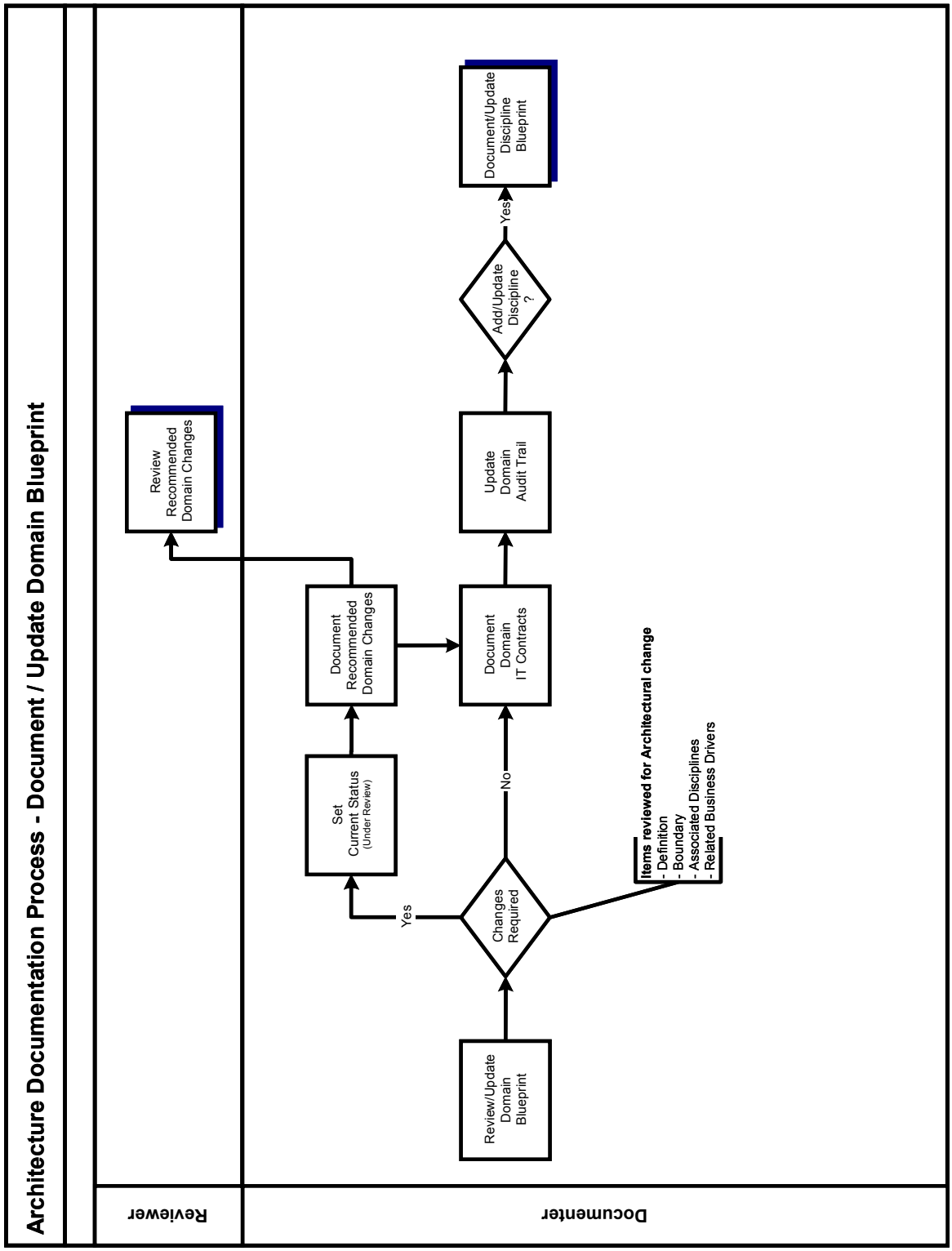
- Access
- Platform
- Network
- Application
- Information
- Integration
- Systems Management
- Security
- Privacy

Each governmental entity must determine the Domain structure that works best for their own organization. Many government entities may identify or define Domains differently during the development or evolution of their own enterprise architecture.

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

- A committee of subject area experts should be established to handle the development and maintenance of each Domain.
- Domains should not be too broad. The scope of each Domain should be reasonable for a committee to handle.
- Domains should not be too narrow. Having Domains that are narrow in scope will cause the creation of many Domains, which in turn results in numerous committees.
- It is best to keep the number of Domains between 5 and 10.

The following information is provided to assist organizations in their efforts to document the items essential to Domain development.


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

## PROCESS DETAIL

The Domain Architecture Blueprint will be completed/updated using the Domain Template as a guide. The following process steps will aid in this documentation:

**Review/Update Domain Blueprint** - The definition of the Domain and the primary Disciplines are provided to the Documenter during the facilitated workshop training. The Documenter will have the responsibility of reviewing:

- Domain definition and Domain boundary
- Associated Disciplines

An Architecture change request should be submitted if additional Disciplines are required.
This request is submitted to the Architecture Manager for validation prior to any further work on that topic.

Conduct a review of the Business Drivers to ensure that the development of the Domain does not conflict with the established Principles, Best Practices and Trends (Industry or Technology). The Documenters should identify the Business Drivers that apply most directly to their Domain and elaborate on (and document) the relationship between their Domain and the Drivers.

**Set Current Status -** Set the Current Status as appropriate. It is important to understand where a given Domain is in the architecture documentation process. Initial statuses identified include:

- *In Development* – The architecture team is currently crafting and/or reviewing the Domain content.
- *Under Review* – The architecture team has completed the Domain content and it is under review by an EA governing body.
- *Accepted* – Indicates the Domain has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Domain was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

**Document Recommended Domain Changes; Review Recommended Domain Changes -** Document and submit to the Architecture Manager any changes to the definition, boundary, or Business Drivers prior to proceeding with the Domain documentation. These types of changes can affect more than just the Documenter requesting the modification.

**Document Domain IT Contracts -** Identify existing or planned state contracts that address the specific Domain technologies. This part of the Domain template should be completed after documenting the Technology Areas, Product Components, and Compliance Components under the Domain.

**Update Domain Audit Trail -** Maintain audit trails for the information provided in the template. During this initial development of the Domain, only information about the creation, accepted/rejected, and date last updated need to be maintained.

**Document/ Update Discipline Blueprint** - If additions or updates to any of the Disciplines are needed, continue with the sub-process Document/ Update Discipline Blueprint, which is described in detail later in this chapter.

# Domain Template

## TEMPLATE OVERVIEW

The Domain Template provides a checklist for documenting the Domain details. A detailed description of each of the content areas follows the visual representation of the Domain Template provided here.

The Domain Template will include the following sections:

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

# Domain

| Definition | |
|---|---|
| *Name* | |
| *Description* | |
| *Rationale* | |
| *Benefits* | |

| Boundary | |
|---|---|
| *Boundary Limit Statement* | |

| Associated Disciplines | |
|---|---|
| *Disciplines under this Domain* | |

| Related Principles | | |
|---|---|---|
| *Reference #s, Statements or Links* | *Conflict* | *Relationship* |
| | ☐ | |
| | ☐ | |

| Related Best Practices | | |
|---|---|---|
| *Reference #s, Statements or Links* | *Conflict* | *Relationship* |
| | ☐ | |
| | ☐ | |

| Related Trends | | |
|---|---|---|
| *Reference #s, Statements or Links* | *Conflict* | *Relationship* |
| | ☐ | |
| | ☐ | |

| State Contracts | |
|---|---|
| *Planned Contracts* | |
| *Existing Contracts* | |

| Current Status | | | | |
|---|---|---|---|---|
| *Domain Status* | ☐ *In Development* | ☐ *Under Review* | ☐ *Rejected* | ☐ *Accepted* |

| Audit Trail | | | |
|---|---|---|---|
| *Creation Date* | | *Date Accepted/Rejected* | |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | |
| *Reason for Update* | | | |
| *Updated By* | | | |

## TEMPLATE DETAIL

### *Definition*

**Name** - Determine an appropriately descriptive name for the Domain.

**Description** - Supply a description of the Domain in a paragraph or two that provides sufficient clarity to reader about the Domain and what it covers.

**Rationale** - Provide a paragraph or two containing the reason or basis for inclusion of this Domain in the technology architecture.

**Benefits** - Provide a paragraph or bulleted statements that supply the benefits associated with the Domain.

### *Boundary*

**Boundary Limit Statement** - The Boundary Limit Statement provides parameters for identifying the boundaries for the Domain. This section should contain statements about what is included, as well as items that are related to, but excluded from, the Domain. If excluded items are identified, it is beneficial to include a reference to the Domain where that information can be found.

### *Associated Disciplines*

**Disciplines under this Domain** - Provide a list of the Disciplines that are covered within this Domain. This provides an index for these Disciplines. The detailed documentation for each Discipline listed will be completed using the Discipline Template.

### *Related Principles*

**References #s, Statements or Links** - Principles identify the overarching general rules that hold true across the enterprise architecture. The principles are developed and documented as Business Drivers at the most global level of the enterprise architecture.

**Conflict** - Verify that the development of the Domain does not conflict with the established Business and Technology Driver Principles. This is a yes/no answer.

**Relationship** - The relationship should be documented for those principles that apply most directly to the Domain. Principles with the relationship left blank will indicate that the principle does not apply to this Domain.

### *Related Best Practices*

**References #s, Statements or Links** – Best practices identify industry processes related to the implementation of the enterprise architecture that will assist in the maintenance and expansion of an adaptive enterprise technology architecture. They are based on experience and proven results. The best practices are documented as Business Drivers, which apply to the enterprise-wide concept of architecture.

**Conflict** - Verify that the development of the Domain does not conflict with the established Business and Technology Driver Best Practices. This is a yes/no answer.

**Relationship** - The relationship should be documented for those best practices that apply most directly to the Domain. Best practices with the relationship left blank will indicate that the best practice does not apply to this Domain.

*NOTE: Best Practices that are identified as specific to the Domain will be defined and documented as Compliance Components (guidelines or standards) at the Discipline level.*

## *Related Trends*

**References #s, Statements or Links -** Industry and technology trends have an effect on the deployment of information technology. Identifying these trends and having an awareness of their impact will allow IT decision makers to develop more informed, effective decisions. The trends are documented as Business Drivers, which apply to the enterprise-wide concept of architecture.

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

**Relationship** - The relationship should be documented for those trends that apply most directly to the Domain. Trends with the relationships left blank will indicate that the trend does not apply to this Domain.

*NOTE: Business and Technology Trends that are identified as specific to the Domain will be further defined and documented at the Discipline level. This will allow the trends to be defined within the Discipline where they most appropriately apply.*

## *State Contracts*

**Planned Contracts -** Provide a list of planned future contracts associated with this Domain.

**Existing Contracts -** Provide a list of existing contracts associated with this Domain

## *Current Status*

**Domain Status -** Document the status of Domain, indicating whether the Domain is in development, under review, rejected, or accepted.

- *In Development* – The architecture team is currently crafting and/or reviewing the Domain content.
- *Under Review* – The architecture team has completed the Domain content and it is under review by an EA governing body.
- *Accepted* – Indicates the Domain has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Domain was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

## *Audit Trail*

The Audit Trail is included at each level of the Architecture Blueprint. It provides the means to track changes made to each of the levels, identifies the date the level was last reviewed to assist in the Vitality Process, and identifies roles and/or individuals involved in the introduction or modification of the Blueprint information for historical purposes.

This information is extremely helpful for the vitality of the Blueprints, as well as invaluable to Project /IT Services Teams in their research when requesting a variance, and to Documenters conducting research on related items across Domains.

**Creation Date -** Provide the date the Domain was created.

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

**Date Accepted/Rejected -** Provide the date the Domain was accepted into the architecture blueprint or rejected.

**Reason for Rejection -** If the Domain was rejected, document the reason for the rejection.

**Last Date Reviewed -** Document the most recent date the Domain was taken through the Architecture Blueprint Vitality Process.

**Last Date Updated** - Document the most recent date that any item in the Domain template was changed.

**Reason for Update** - Document the reason for the update to the Domain. This information should be a detailed description of the change, for future reference.

**Updated By** - Provide the names of the persons responsible for the update to the Domain. This will be helpful information for future reference.

# Complete/Update Discipline Blueprint

## PROCESS OVERVIEW

Disciplines are the second level of the Technology Architecture Blueprint. Disciplines are the technology functional areas within a Domain. The overall structure of the architecture blueprint begins to form at the Discipline level. Each Domain will contain one or more Disciplines. A Discipline template is provided to ensure consistent documentation of each Discipline.

The NASCIO workgroup has been involved in a high-level review process to define and document a sample set of Domains and associated Disciplines for this Tool-Kit. This sample set is intended to provide an example of one way to set up the Domain/Discipline relationships, but is not prescriptive. Descriptions of the sample Domains and Disciplines, as used in this Tool-Kit, can be found in Appendix B.

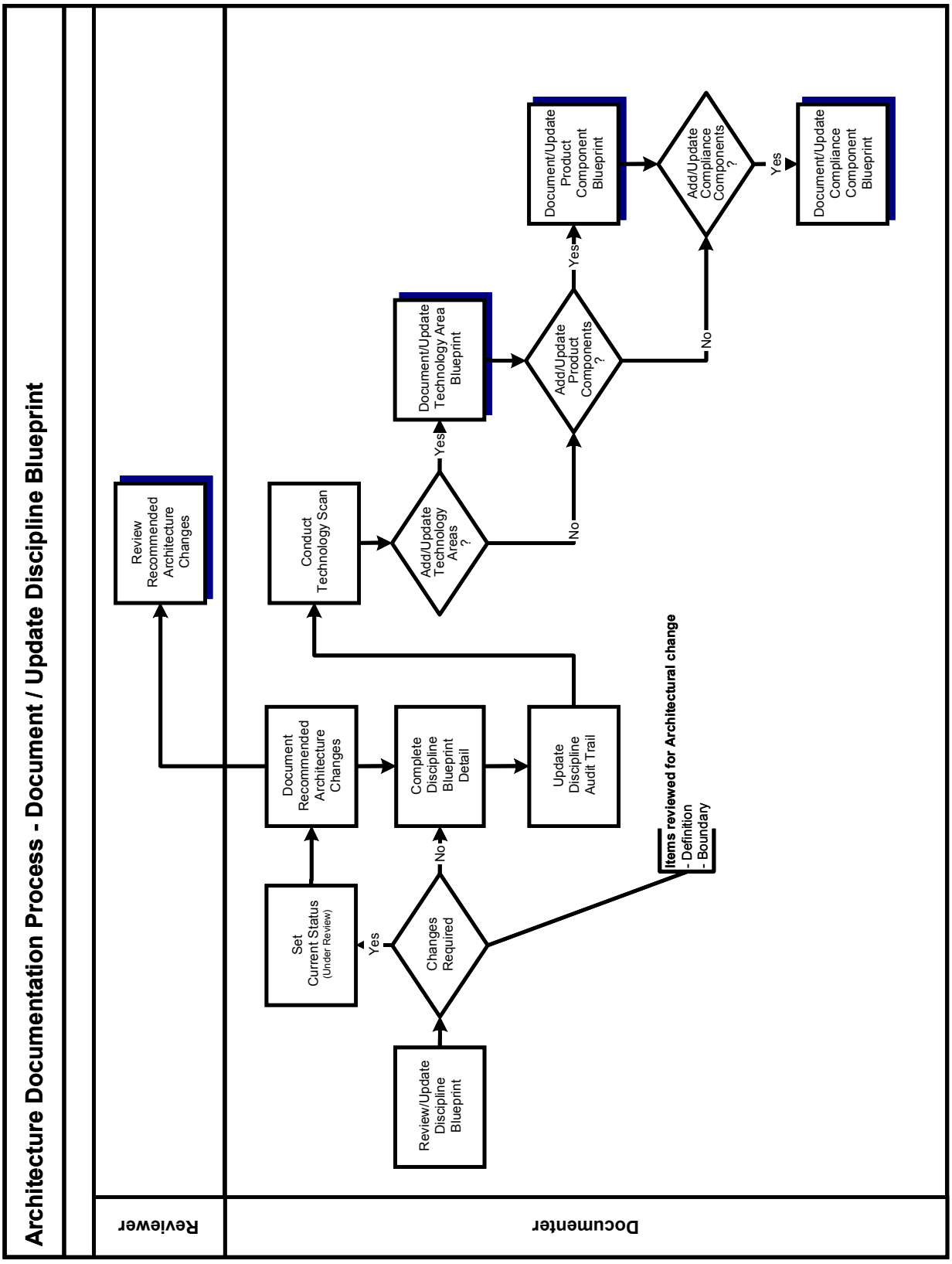
The development of Disciplines within each Domain is the responsibility of the Documenters. This process will evolve and change as information is gathered and documented.

It is anticipated that Documenters may uncover additional information that should be included as part of the Architecture Blueprint and/or Enterprise Architecture Framework. The committees and other enterprise architecture stakeholders are encouraged to provide feedback to the Architecture Manager whenever it is apparent that the feedback will enhance the enterprise architecture.

Important items to keep in mind when determining the creation of Disciplines include:

- Establish Disciplines that include categories of products and services having similar compliances or requiring similar expertise for implementation. This will allow Documenters to document the disciplines in a consistent manner.
- Set up Disciplines based on what will best support your organization's installation base of products and services.
- Avoid spending excessive time determining terminology issues. Just as in metadata documentation, fine-tuning terminology can occupy a majority of the time. Utilize the keywords and boundary statements to assist in identifying various terms that are covered by the discipline.

The first layout of the Disciplines under the Domains may not be the permanent arrangement. The best Discipline/Domain combinations will surface naturally over time during implementation of the Architecture Blueprint within your organization.


Architecture Documentation Process - Document / Update Discipline Blueprint
Reviewer
Documenter
Review Recommended Architecture Changes
Document Recommended Architecture Changes
Complete Discipline Blueprint Detail
Update Discipline Audit Trail
Conduct Technology Scan
Add/Update Technology Areas ?
Yes
No
Document/Update Technology Area Blueprint
Add/Update Product Components ?
Yes
No
Document/Update Product Component Blueprint
Add/Update Compliance Components ?
Yes
Document/Update Compliance Component Blueprint
Set Current Status (Under Review)
Changes Required
Yes
No
Review/Update Discipline Blueprint
Items reviewed for Architectural change
- Definition
- Boundary

## PROCESS DETAIL

The Discipline Blueprint will be completed/updated using the Discipline Template as a guide. The following process steps will aid in this documentation:

**Review/Update Discipline Blueprint** – The Documenter will have the responsibility of reviewing the Discipline definition and Discipline boundary.

An Architecture change request should be submitted if:

- Additional Technology Areas are required
- Changes to the Discipline Definition are made
- Changes to the Discipline Boundary are made.

This request is submitted to the Architecture Manager for validation prior to any further work on that topic and the current status will be set to "Under Review".

**Set Current Status** – Set the Current Status as appropriate. It is important to understand where a given Domain is in the architecture documentation process. Initial statuses identified include:

- *In Development* – The architecture team is currently crafting and/or reviewing the Discipline content.
- *Under Review* – The architecture team has completed the Discipline content and it is under review by an EA governing body.
- *Accepted* – Indicates the Discipline has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Discipline was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

**Document Recommended Architecture Changes; Review Recommended Architecture Changes** – Document and submit to the Architecture Manager any changes to the definition or boundary limit statement prior to proceeding with the Discipline documentation. These types of changes can affect more than just the Documenter requesting the modification.

**Complete Discipline Blueprint Detail** – Critical References can aid in identifying the Technology Areas, Product Components, and/or Compliance Components. The references that are specific for the Discipline include:

- Documentation of Related Disciplines
- Identification of the various Standards Organizations and Government Bodies
- Identification of the Stakeholders/Roles
- Documentation of Discipline-specific Technology Trends

Compliances that are more Discipline-related should be listed at the Discipline level. Each Documenter should evaluate and select Compliance Components that apply to the Discipline. These would include:

- *Guidelines* – General statements of direction or desired future state for this Discipline. These will not be mandated.

- *Standards* – Items set by any generally accepted standards organization appropriate for the Discipline. More than one standard may exist. Variances must be sought if not following one of the existing standards.
- *Legislated* – Items required by law. Only a change in the mandate can allow variances.

The Compliance Component Blueprint details will be captured, using the Compliance Component Template, as described in the sub-process Document/Update Compliance Component Blueprint covered later in this chapter.

Methodologies followed while developing or supporting this Discipline should be documented. This is another place to verify that the deliverables of the methodology do not conflict with the components of the enterprise architecture. Implementation of the selected Technology Areas should be aided by the methodology deliverables.

Technology Areas covered under the Discipline should be listed at this time. The process for deriving and capturing all the remaining levels of the architecture blueprint begins at the Technology Area level, which aids in defining and finding the various products and compliances under a technology. The process steps for documenting the Technology Areas will be covered in detail in Document/Update Technology Area Blueprint process model.

Documentation requirements for the Discipline must be specified, assuring that the quality and level of the documentation intended by the Documenter is maintained. Various subject matter experts will work as Documenters as the architecture blueprint continues to mature. The documentation will preserve the history of the decision-making processes throughout the architecture maturity process. The Documenters can express expectations for how the Discipline is to be maintained within the documentation.

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

- *In Development* – The architecture team is currently crafting and/or reviewing the Discipline content.
- *Under Review* – The architecture team has completed the Discipline content and it is under review by an EA governing body.
- *Accepted* – Indicates the Discipline has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Discipline was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

**Update Discipline Audit Trail** - Audit trails for the information provided in the template must be maintained. During the initial development of the Discipline, only the information regarding creation, accepted/rejected, and date last updated must be maintained.

**Conduct Technology Scan** - At this level, a technology scan of the enterprise should be conducted to determine the existing or proposed products and compliance components used throughout the state as related to this discipline. Based on the technology found, one of the following levels will be documented and/or updated:

- Technology Area Blueprint
- Product Component Blueprint
- Compliance Component Blueprint

One question that arises during the documentation process is how to incorporate the documentation of the existing baseline products and compliance components in the most efficient and effective manner. In reviewing the product and compliance components, select those attributes that provide the most valuable information for your categorization and create a smaller checklist. Send this checklist out to the various subject matter experts in the organization, requesting that they complete the portion that pertains to their area of expertise and return the results within an agreed amount of time (3 – 4 weeks should suffice for most organizations).

Recommended checklist items would include:

*Definition (Name and Description)*

- Keywords
- Vendor Information (Name)
- Required Component
- Audit Trail (Creation Date)

**Document/Update Technology Area Blueprint, Document/Update Product Component Blueprint, and Document/Update Compliance Component Blueprint -** Each of these processes will be executed as needed, based on the results of the technology scan. These processes are covered as independent processes in the remainder of this section.

# Discipline Template

## TEMPLATE OVERVIEW

The Discipline Template provides a checklist for documenting the Discipline details. A detailed description of each of the content areas follows the visual representation of the Discipline Template provided here.

The Discipline Template will include the following sections:

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

# Discipline Template

| Definition | |
|---|---|
| *Name* | |
| *Description* | |
| *Rationale* | |
| *Benefits* | |

| Boundary | |
|---|---|
| *Boundary Limit Statement* | |

| Associated Domain | |
|---|---|
| *Domain Name* | |

## Critical References

*Related Domains/Disciplines*

| | *Domain - Disciplines* | | *Domain - Disciplines* | | *Domain - Disciplines* |
|---|---|---|---|---|---|
| ☐ | | ☐ | | ☐ | |
| ☐ | | ☐ | | ☐ | |
| ☐ | | ☐ | | ☐ | |
| ☐ | | ☐ | | ☐ | |
| ☐ | | ☐ | | ☐ | |
| ☐ | | ☐ | | ☐ | |
| ☐ | | ☐ | | ☐ | |

*Standards Organizations*

| | | | |
|---|---|---|---|
| *Name* | | *Web Address* | |
| *Contact Information* | | | |

*Government Bodies*

| | | | |
|---|---|---|---|
| *Name* | | *Web Address* | |
| *Contact Information* | | | |

*Stakeholders/Roles*

| | |
|---|---|
| *Stakeholders* | |
| *Roles (if stakeholder titles are not known)* | |

*Discipline-Specific Trends*

| | |
|---|---|
| *Trend Statement* | |
| *Trend Source* | |

| Methodologies | |
|---|---|
| *Methodologies Followed* | |

| ASSOCIATED COMPLIANCE COMPONENTS | | | |
|---|---|---|---|
| *Compliance Component Names* | | | |
| **ASSOCIATED TECHNOLOGY AREAS** | | | |
| *Technology Areas* | | | |
| **DISCIPLINE DOCUMENTATION REQUIREMENTS** | | | |
| *Documentation requirements for this Discipline* | | | |
| **CURRENT STATUS** | | | |
| *Discipline Status* | ☐ *In Development* ☐ *Under Review* ☐ *Rejected* ☐ *Accepted* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | | *Date Accepted/Rejected* | |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | |
| *Reason for Update* | | | |
| *Updated By* | | | |

## TEMPLATE DETAIL

### *Definition*

**Name -** Determine an appropriately descriptive name for the Discipline.

**Description** - Supply a description of the Discipline in a paragraph or two that provides sufficient clarity about the Discipline and what it covers.

**Rationale** - Provide a paragraph or two containing the reason or basis for inclusion of this Discipline in the architecture blueprint.

**Benefits** - Provide a paragraph or bulleted statements that supply the benefits associated with the Discipline.

### *Boundary*

**Boundary Limit Statement** - The Boundary Limit Statement provides parameters for identifying the boundaries for the Discipline. This section includes statements about what is included, as well as items that are related to—but excluded from—the Discipline. If excluded items are identified, it is beneficial to include a reference to the Domain and Discipline where that information can be found.

### *Associated Domain*

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

### *Critical References*

**Related Domains/Disciplines** - Provide a list of the Domains and underlying Disciplines that will have an affect on, or be affected by, changes within this Discipline. These references provide coordination points for critical decisions. The Domain-Discipline Intersection Matrix, provided in the Technology Samples section of this Tool-Kit, can be a helpful tool to easily identify these coordination points. If your organization chooses to use such a tool, it should be updated with the new information as well.

In the Discipline template provided, the names of the related Domains/Disciplines have been omitted. Please note that once you have determined the Domains and Disciplines for your organization, the template can be customized to include your information.

**Standards Organizations/Government Bodies** - Provide a list of the various standards organizations and/or government bodies that affect this Discipline. Provide URLs for reference whenever possible. These organizations can affect the Discipline in various ways. Some will have authority to dictate certain decisions, while others may only provide an influence on decisions within the Discipline.

**Stakeholders/ Roles** - Provide a list of Stakeholders for this Discipline. Stakeholders are those who are affected by, or will affect, the Discipline.

If a stakeholder title is not known, provide a description of the role the person or group performs in the roles section. Roles ensure the accountability of all IT components, ensure IT efforts support the needs of the business, and increase quality of IT solutions within the Discipline.

**Discipline-Specific Trends** - Add any Discipline-specific Industry or Technology Trends. Industry and technology trends have an effect on the deployment of information technology. IT decision makers will develop more informed, effective decisions if they are aware of the impact of the trends related to both business and technology.

Some key questions that should be considered when identifying the trends include:

- What trends and events will drive new business investment in IT?
- What technology advances or changes will impact IT deployment decisions?
- How can the organization exploit IT, while facing a complex and volatile environment?

In addition to the trends, provide the source of each trend for reference/historical purposes. This section can include references to organizations like Gartner Group, or they can include the name of the person who proposed the trend. URLs may also be included if applicable.

### *Methodologies*

**Methodologies Followed** - Provide a list of methodologies followed in developing or supporting this Discipline, as appropriate.

### *Associated Compliance Components*

**Compliance Component Names** - Provide a list of Compliance Components that are specific to the Discipline level. The detailed documentation for each component listed will be completed using the Compliance Component Template.

### *Associated Technology Areas*

**Technology Areas** - Provide a list of the Technology Areas that are covered within this Discipline. This provides an index for these Technology Areas. The detailed documentation for each Technology Area listed will be completed using the Technology Area Template.

### *Discipline Documentation Requirements*

**Documentation requirements for this Discipline** - As the enterprise architecture continues to mature, a variety of subject matter experts will serve as Documenters. The transfer of knowledge and the reasoning behind previous additions and modifications can be invaluable to these Documenters, but may not always be obvious.

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

### *Current Status*

**Discipline Status** - Document the status of Discipline, indicating whether it is in development, under review, rejected, or accepted.

- *In Development* – The architecture team is currently crafting and/or reviewing the Discipline content.
- *Under Review* – The architecture team has completed the Discipline content and it is under review by an EA governing body.
- *Accepted* – Indicates the Discipline has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Discipline was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

### *Audit Trail*

**Creation Date** - Provide the date the Discipline was created.

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

**Date Accepted/Rejected** - Provide the date the Discipline was accepted into the architecture blueprint or rejected.

**Reason for Rejection** - If the Discipline was rejected, document the reason for the rejection.

**Last Date Reviewed** - Document the most recent date the Discipline was taken through the Architecture Blueprint Vitality Process.

**Last Date Updated** - Document the most recent date that any item in the Discipline template was changed.

**Reason for Update** - Document the reason for the update to the Discipline.

**Updated By** - Provide the names of the persons responsible for the update to the Discipline. This will be helpful information for future reference.

# Document/Update Technology Area Blueprint

## PROCESS OVERVIEW

Technology Areas are the third level of the Architecture Blueprint. Technology Areas are those technical categories that support the technology functional areas (Disciplines) of the architecture blueprint. Each Discipline will contain one or more Technology Areas. A Technology Area template is provided to ensure consistent documentation of each Technology Area.

Technology Areas allow products for each Discipline to be categorized for:

- Documentation of Compliances
- Research of Architecture Blueprint
- Communication of Architecture Blueprint
- Defining the Discipline Boundaries.

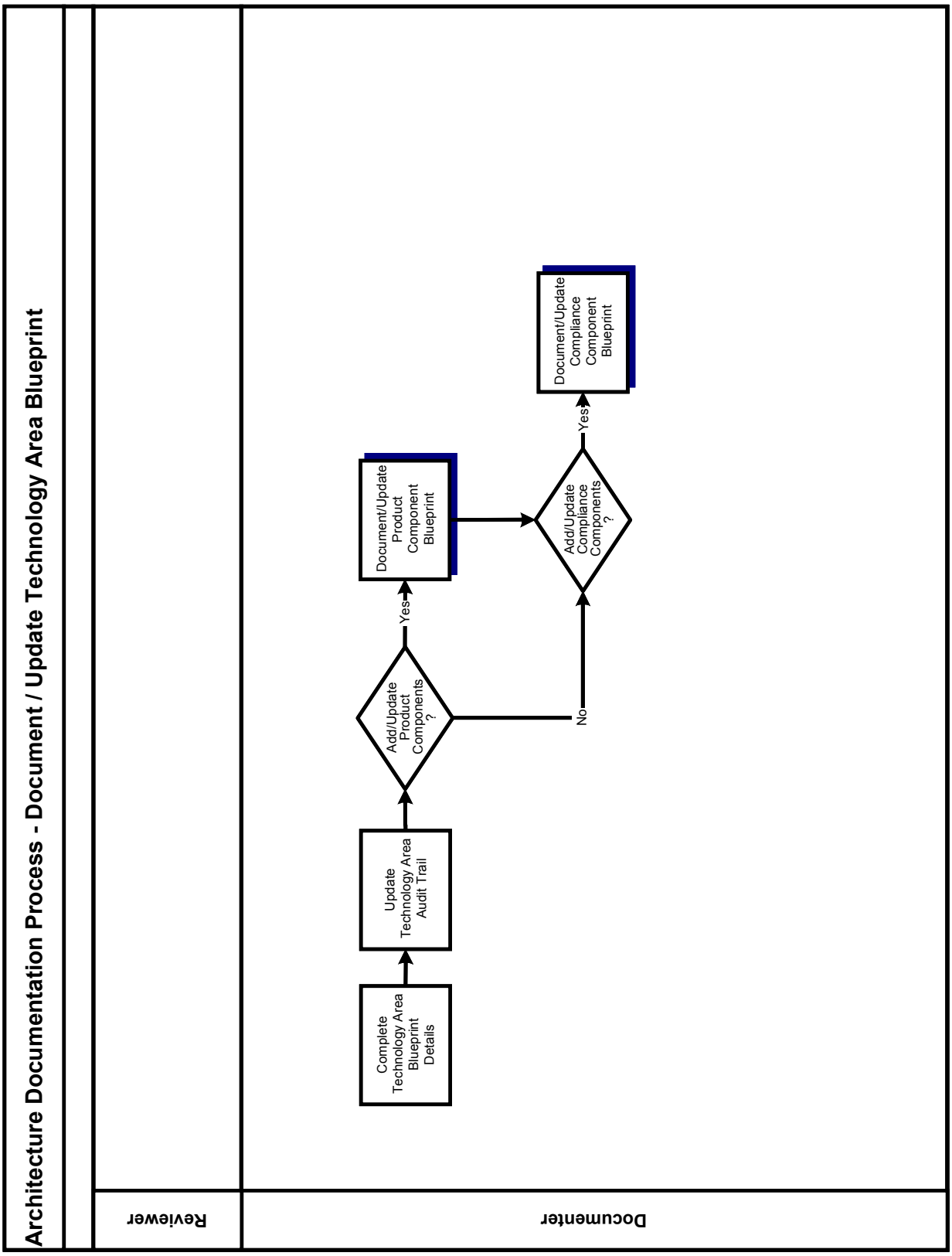
A majority of the Documenters' work will focus on the Technology Areas, Product Components, and Compliance Components including such activities as:

- Documentation
- Vitality of Architecture Blueprint
- Compliance Reviews
- Architecture Help Requests.

Important items to keep in mind when determining the Technology Areas within a Discipline include:

- Technology scans are helpful in capturing information regarding existing products within the organization.
- There is more than one way to determine Technology Areas. Documenters preferring bottom-up analysis will capture the list of products and then categorize these products to determine the Technology Areas. Those preferring top-down analysis will determine and document the Technology Areas first and then proceed to document the products that fall under each of the Technology Areas.
- Create a Technology Area where compliances exist that span products.

- Documentation of products within a Technology Area for a specific Discipline can become an area for boundary debate. A question can arise as to which group is responsible for documenting which products. When certain products span functional areas, a review of the best way to document the product should be discussed. A decision should be made as to whether the product should be documented under multiple Technology Areas, or whether all subject matter experts should come together to document the product once under a specific Technology Area.


Architecture Documentation Process - Document / Update Technology Area Blueprint
Reviewer
Documenter
Complete Technology Area Blueprint Details
Update Technology Area Audit Trail
Add/Update Product Components ?
Yes
No
Document/Update Product Component Blueprint
Add/Update Compliance Components ?
Yes
Document/Update Compliance Component Blueprint

## PROCESS DETAIL

The Technology Area Blueprint should be completed/updated using the Technology Area template as a guide. The following process steps will aid in this documentation:

**Complete Technology Area Blueprint Details -** Review/Document the Technology Areas definition and rationale.

Keywords/nomenclature commonly associated with the Technology Area should be documented to aid in finding various Technology Areas in the architecture blueprint.

Set the Current Status as appropriate. Since so many different Technology Areas go through the Architecture Documentation Process at one time, it is important to understand where a given Technology Area is in the process. Initial statuses identified include:

- *In Development* – The architecture team is currently crafting and/or reviewing the Technology Area content.
- *Under Review* – The architecture team has completed the Technology Area content and it is under review by an EA governing body.
- *Accepted* – Indicates the Technology Area has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Technology Area was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

List the Product and Compliance Components that are associated with this Technology Area. After the technology scan is complete, the Product and Compliance Components can be documented and assigned their classification within the architecture blueprint. The details for documenting the Product and Compliance Components are described in the sub-processes Document/Update Product Component Blueprint and Document/Update Compliance Component Blueprint, which are covered later in this chapter.

If the Technology Area requires a single product solution, the date the determination was made should be documented, along with the rationale for the decision.

**Update Technology Area Audit Trail -** Audit trails for the information provided in the template must be maintained. During the initial development of the Technology Area, only the creation, accepted/rejected, and date last updated will be provided.

**Document/Update Product Component Blueprint -** The details for documenting the Product Components are covered in the sub-process Document/Update Product Components later in this chapter.

**Document/Update Compliance Component Blueprint -** The details for documenting the Compliance Components are covered in the sub-process Document/Update Compliance Components later in this chapter.

# Technology Area Template

## TEMPLATE OVERVIEW

The Technology Area Template provides a checklist for documenting the Technology Area details. A detailed description of each of the content areas follows the visual representation of the Technology Area Template provided here.

The Technology Area Template will include the following sections:

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

# Technology Area Template

| Definition | |
|---|---|
| *Name* | |
| *Description* | |
| *Rationale* | |
| *Benefits* | |
| **Associated Discipline** | |
| *Discipline Name* | |
| **Keywords** | |
| *Keywords/Aliases* | |
| **Associated Compliance Components** | |
| *Compliance Component Names* | |
| **Single Product Solution** | |
| *Date of Single Product Solution Determination* | |
| *Rationale for Decision* | |
| **Associated Product Components** | |
| *Product Component Names* | |
| **Current Status** | |
| *Technology Area Status* | ☐ *In Development* ☐ *Under Review* ☐ *Rejected* ☐ *Accepted* |
| **Audit Trail** | |
| *Creation Date* | *Date Accepted / Rejected* |
| *Created By* | |
| *Reason for Rejection* | |
| *Last Date Updated* | *Last Date Reviewed* |
| *Reason for Update* | |
| *Updated By* | |

## TEMPLATE DETAIL

### *Definition*

**Name** - Determine an appropriately descriptive name for the Technology Area.

**Description** - Supply a description of the Technology Area in a paragraph or two that provides sufficient clarity about the Technology Area and what it covers.

**Rationale** - Provide a paragraph or two containing the reason or basis for inclusion of this Technology Area in the architecture blueprint.

**Benefits** - Provide a paragraph or bulleted statements that supply the benefits associated with the Technology Area.

### *Associated Discipline*

**Discipline Name** - Provide the name of the Discipline with which this Technology Area is associated. This provides the appropriate mapping between Technology Areas and Disciplines.

### *Keywords*

**Keywords/Aliases** - List any keywords/nomenclature and /or aliases that can be used to assist in searching for these Technology Areas. This information will be helpful for anyone looking for information on similar technologies.

### *Associated Compliance Components*

**Compliance Component Names** - List the Compliance Components associated with this Technology Area. The detailed documentation for each component listed will be completed using the Compliance Component Template.

### *Single Product Solution*

For certain Technology Areas, it is essential for an organization to make a determination of a single product solution. E-mail is a good example of a Technology Area that would be a candidate for a single product solution.

**Date of Single Product Solution Determination; Rationale for Decision** - For Technology Areas that require single product solutions, provide the date of the determination, as well as the rationale for the decision.

### *Associated Product Components*

**Product Component Names** - List the Product Components associated with this Technology Area. The detailed documentation for each component listed will be completed using the Product Component Template.

### *Current Status*

**Technology Area Status** - Document the status of Technology Area, indicating whether it is in development, under review, rejected, or accepted.

- *In Development* – The architecture team is currently crafting and/or reviewing the Technology Area content.

- *Under Review* – The architecture team has completed the Technology Area content and it is under review by an EA governing body.
- *Accepted* – Indicates the Technology Area has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Technology Area was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

### *Audit Trail*

**Creation Date** - Provide the date the Technology Area was created.

**Created By** – List all individuals and their titles that helped in the creation of this Technology Area.

**Date Accepted/Rejected** - Provide the date the Technology Area was accepted into the architecture blueprint or rejected.

**Reason for Rejection** - If the Technology Area was rejected, document the reason for the rejection.

**Last Date Reviewed** - Document the most recent date the Technology Area was taken through the Architecture Blueprint Vitality Process.

**Last Date Updated** - Document the most recent date that any item in the Technology Area template was changed.

**Reason for Update** - Document the reason for the update to the Technology Area.

**Updated By** - Provide the names of the persons responsible for the update to the Technology Area. This will be helpful information for future reference.

## Document/Update Product Components

### PROCESS OVERVIEW

The Product Component is the fourth level of the Architecture Blueprint. Product Components include the protocols, products and services that are specific to a Technology Area. Each Technology Area will contain one or more Product Components. A Product Component template is provided to ensure consistent documentation of each Product Component.

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

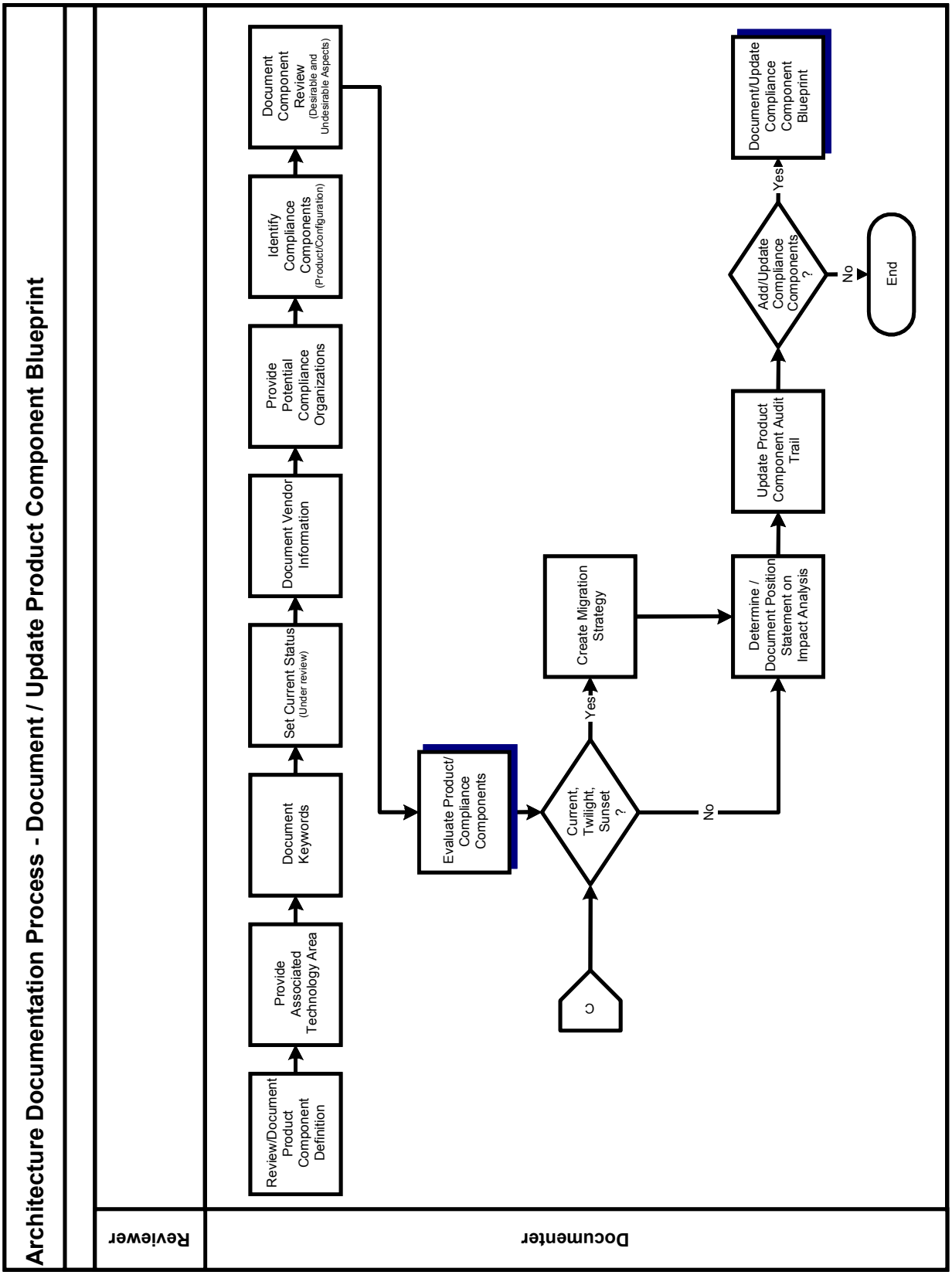
Important items to keep in mind when determining the various product components to document include:

- Is this product in the existing IT portfolio?
- Is this product needed in the next *x* time period to aid in business strategies?
- Is there a request from a project or support team to help find a product to answer a specific business need?
- Has the product already been documented in the Architecture Blueprint under another Domain/Discipline?

  - If this product has been documented elsewhere, did the evaluation of the product include the type of fit criteria needed for classification for your Domain/Discipline?
  - If this product has not been documented previously, is it possible that this product could fall under another Domain/Discipline's boundary?
- Will the product version be captured at the Product Component or the Compliance Component level? The documentation of this information needs to be consistent across the Discipline. (Note: The Discipline template contains a section entitled "Discipline Documentation Requirements" for capturing this type of information.) Examples of this include:
  - Versions captured at the Compliance Component Level:
    - Technology Area: Application Languages
    - Product: Visual Basic
    - Compliance Component: Version 5
    - Compliance Component: Version 6
    - Compliance Component: Visual Basic Standards (regardless of version)
  - Versions captured at the Product Level:
    - Technology Area: Application Languages
    - Product: Visual Basic Version 5
    - Product: Visual Basic Version 6
    - Compliance Components: Visual Basic Standards for Version 5
    - Compliance Components: Visual Basic Standards for Version 6

The Product Components, documented in this sub-process, and the Compliance Components, documented in the Document Compliance Component sub-process, become the essence of the technology architecture for the Architecture Blueprint.

They specifically identify what products, compliances, and recommendations will be used for implementation of the Architecture Blueprint. The levels of the Architecture Blueprint covered to this point are included to aid in bringing subject matter experts together, categorizing products and standards in logical sets, and aiding in concise communication of the Architecture Blueprint.


Architecture Documentation Process - Document / Update Product Component Blueprint
Reviewer
Documenter
Review/Document Product Component Definition
Provide Associated Technology Area
Document Keywords
Set Current Status (Under review)
Document Vendor Information
Provide Potential Compliance Organizations
Identify Compliance Components (Product/Configuration)
Document Component Review (Desirable and Undesirable Aspects)
Evaluate Product/ Compliance Components
Current, Twilight, Sunset ?
Yes
No
C
Create Migration Strategy
Determine / Document Position Statement on Impact Analysis
Update Product Component Audit Trail
Add/Update Compliance Components ?
Yes
No
End
Document/Update Compliance Component Blueprint

## PROCESS DETAIL

The Product Component Blueprint should be completed/updated using the Product Component Template as a guide. The following process steps aid in this documentation:

**Review/Document Product Component Definition -** Review the product component's definition and rationale. Provide updates as necessary.

**Provide Associated Technology Area -** The associated Technology Area should be listed in order to provide the appropriate mapping between Products and Technology Areas.

**Document Keywords -** To aid in finding various products documented in the architecture blueprint, keywords/nomenclature commonly associated with the product will be documented.

**Set Current Status -** Set the Current Status as appropriate. Since so many different Product Components go through the Architecture Documentation Process at one time, it is important to understand where a given Product Component is in the process. Initial statuses identified include:

- *In Development* – The architecture team is currently crafting and/or reviewing the Product Component content.
- *Under Review* – The architecture team has completed the Product Component content and it is under review by an EA governing body.
- *Accepted* – Indicates the Product Component has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Product Component was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

**Document Vendor Information -** Information about the vendor providing the product will be documented, including the name, contact information, and Web site for the vendor. In addition, any evaluation conducted on the vendor should also be documented to aid in future evaluations conducted on the vendor.

**Provide Potential Compliance Organizations -** To assist in the identification of potential Compliance Components for the product, a list of standards organizations and/or government bodies associated with the product will be documented. This list should include:

- Name
- Contact information
- Web site

**Identify Compliance Components -** Compliances that are more product-related should be listed at this level. These might include:

- Guidelines – General statements of direction or desired future states for the product. These will not be mandated.
- Standards – Product releases/versions currently used within the enterprise or proposed for use. More than one standard may exist. A variance must be granted to excuse compliance with an existing standard.

- Legislation – Items required by law. Only a change in the legislation can allow variances to be granted.

The details for documenting the Compliance Components are covered in the sub-process Document/Update Compliance Components covered later in this chapter.

**Document Component Review -** Document both desirable and undesirable aspects of the product. If the undesirable aspects have been discussed with the vendor, summarize the discussion showing the likelihood of vendor redress.

**Evaluate Product/ Compliance Components -** An evaluation of the Product Component is necessary to determine its classification. This will be discussed in detail in the Evaluate Product/Compliance Components sub-process.

**Create Migration Strategy -** For products classified as current, twilight or sunset, a migration strategy must be formulated. This will be done for products migrating from:

- Product Components classified as emerging that are moving to the classification of current.
- Product Components classified as current that are moving to either twilight or sunset.

Migration strategies will identify:

- Impacts on existing components
- Considerations for conversion
- Recommendations for:
  - New development
  - Modifications to existing components (corrections & enhancements)
  - Possibilities for user-base expansion (reuse).

**Determine/Document Position Statement on Impact Analysis -** An impact analysis must be conducted to determine the impact the classification of the product will have on the existing architecture blueprint. Examples of impacts can include:

- Is a product classified as current that is moving to twilight going to cause a software component to go through a release update that may take months to accomplish?
- Support levels may be impacted when choosing not to move a product from current to twilight when a vendor has chosen to no longer support the product.

These are examples of the type of impacts that need a Position Statement on impact.

**Update Product Component Audit Trail -** Audit trails for the information provided in the template must be maintained. During the initial development of the Product Component, only the creation, accepted/rejected, and date last updated must be maintained.

**Document/Update Compliance Component Blueprint -** If new Compliance Components were listed or if updates are needed to existing Compliance Components, the sub-process Document/Update Compliance Component Blueprint will be executed.

# Product Component Template

## TEMPLATE OVERVIEW

The Product Component Template provides a checklist for documenting the Product Component details. A detailed description of each of the content areas follows the visual representation of the Product Component Template provided here.

The Product Component Template will include the following sections:

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

# Product Component Template

| Definition | | | | |
|---|---|---|---|---|
| *Name* | | | | |
| *Description* | | | | |
| *Rationale* | | | | |
| *Benefits* | | | | |
| **Component Classification** | | | | |
| *Classification* | ☐ *Emerging* | ☐ *Current* | ☐ *Twilight* | ☐ *Sunset* |
| *Sunset Date* | | | | |
| *Rationale for Classification* | | | | |
| **Associated Technology Area** | | | | |
| *Technology Area Name* | | | | |
| **Keywords** | | | | |
| *Keywords/Aliases* | | | | |
| **Vendor Information** | | | | |
| *Vendor Name* | | *Web Address* | | |
| *Contact Information* | | | | |
| **Potential Compliance Organizations** | | | | |
| *Standards Organizations* | | | | |
| *Name* | | *Web Address* | | |
| *Contact Information* | | | | |
| *Government Bodies* | | | | |
| *Name* | | *Web Address* | | |
| *Contact Information* | | | | |
| **Associated Compliance Components** | | | | |
| *Product* | | | | |
| *Product-specific Compliance Components* | | | | |
| *Configurations* | | | | |
| *Configuration-specific Compliance Components* | | | | |
| **Component Review** | | | | |
| *Desirable aspects* | | | | |
| *Undesirable aspects* | | | | |

| REQUIRED COMPONENT | | | |
|---|---|---|---|
| *Business Area, Department or Application Name* | | | |
| **CONDITIONAL USE RESTRICTIONS** | | | |
| *Restrictions* | | | |
| **MIGRATION STRATEGY** | | | |
| *Strategy/Source Document* | | | |
| **IMPACT POSITION STATEMENT** | | | |
| *Impact Statement* | | | |
| **CURRENT STATUS** | | | |
| *Product Component Status* | ☐ *In Development* ☐ *Under Review* ☐ *Rejected* ☐ *Accepted* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | | *Date Accepted / Rejected* | |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | |
| *Reason for Update* | | | |
| *Updated By* | | | |

## TEMPLATE DETAIL

### *Definition*

**Name** - Determine an appropriately descriptive name for the Product Component.

**Description** - Supply a description of the Product Component in a paragraph or two that provides sufficient clarity about the Product Component and what it covers.

**Rationale** - Provide a paragraph or two containing the reason or basis for inclusion of this Product Component in the architecture blueprint.

**Benefits** - Provide a paragraph or bulleted statements that supply the benefits associated with the Product Component.

### *Component Classification*

**Classification** - Provide the classification for this Product Component.
(The process for determination is covered under Evaluate Product/Compliance Component Process.)

Classifications include:

- *Emerging:* New technology that has the potential to become current.
- *Current:* Recommended technology that meets the requirements of the enterprise architecture.
- *Twilight:* Items that do not conform to the Technology Drivers and/or Business Drivers.
- *Sunset:* Items that do not conform to the Technology Drivers and/or Business Drivers and have a set discontinuation date.

**Sunset Date** - Document the date for discontinuation of the Product Component.

**Rationale for Classification** - Provide a rationale statement for the chosen classification based on the review of:

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

### *Associated Technology Area*

**Technology Area Name** - Provide the name of the Technology Area with which this Product Component is associated. This will ensure the appropriate mapping of Product Component to Technology Area.

### *Keywords*

**Keywords/Aliases** - List any keywords/nomenclatures and/or aliases that can be used to assist in searching for these Product Components. This information will be helpful for anyone looking for information on similar technologies.

### *Vendor Information*

Provide the following vendor information for the vendor that supplies and or supports the Product Component being documented.

- **Vendor Name**
- **Contact Information**, such as phone number, address, and email address.
- Company **Web Address**, URL, and associated links.

### *Potential Compliance Organizations*

**Standards Organizations -** List all standards organizations that supply standards associated with this Product Component. Provide contact information for each organization, as well as URLs, if available.

**Government Bodies -** List all government bodies that provide policies and/or mandates associated with this Product Component. Provide contact information for each government body, as well as URLs, if available.

These are research references only and are used in identifying standards that may need to be escalated to Compliance Components.

All standards are addressed using the Compliance Component template.

### *Associated Compliance Components*

**Product -** List the product-specific Compliance Components associated with this product. The detailed documentation for each component listed will be completed using the Compliance Component Template.

**Configurations -** List the configuration-specific Compliance Components associated with this product. The detailed documentation for each component listed will be completed using the Compliance Component Template.

### *Component Review*

**Desirable Aspects -** Document the desirable aspects of this Product Component.

**Un-desirable Aspects -** Document the un-desirable aspects of this Product Component.
This information is used to justify recommendations for future use of the component.

### *Required Component*

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

### *Conditional Use Restriction*

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

### *Migration Strategy*

**Strategy/Source Document -** Document Migration Strategy for:

- Product Components classified as emerging that are moving to the classification of current.
- Product Components classified as current that are moving to either twilight or sunset.

These strategies should identify the following items, as applicable:

- Existing user base and technical staff
- Training for existing user base
- Training for existing technical staff
- Impacts on existing Technology Areas
- Considerations for conversion
- Recommendations for the Technology Area in:
  - New development
  - Modifications (corrections & enhancements)
  - Possibilities for user-base expansion (reuse).

**Note**: A link to the source document should be provided if the Migration Strategy is documented as a stand-alone document.

### *Impact Position Statement*

**Impact Statement** - Provide a position statement on the impact of this product on the organization. Consider the follow items when developing the impact position statement:

- The impact on the overall Technology Architecture Blueprint
- The impact on the physical technical environment
- The impact on the business community.

### *Current Status*

**Product Component Status** - Document the status of Product Component, indicating whether the Product Component is in development, under review, rejected, or accepted.

- *In Development* – The architecture team is currently crafting and/or reviewing the Product Component content.
- *Under Review* – The architecture team has completed the Product Component content and it is under review by an EA governing body.
- *Accepted* – Indicates the Product Component has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Product Component was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

### *Audit Trail*

**Creation Date** - Provide the date the Product Component was created.

**Created By** – List all individuals and their titles that helped in the creation of this Product Component

**Date Accepted/Rejected** - Provide the date the Product Component was accepted into the architecture blueprint or rejected.

**Reason for Rejection** - If the Product Component was rejected, document the reason for the rejection.

**Last Date Reviewed** - Document the most recent date the Product Component was taken through the Architecture Blueprint Vitality Process.

**Last Date Updated** - Document the most recent date that any item in the Product Component template was changed.

**Reason for Update** - Document the reason for the update to the Product Component.

**Updated By** - Provide the names of the persons responsible for the update to the Product Component. This will be helpful information for future reference.

# Document/Update Compliance Components

## PROCESS OVERVIEW

Compliance Components are the fifth level of the Architecture Blueprint. Compliance Components are the guidelines, standards and legislative mandates associated with a Discipline, Technology Area, or Product Component, as appropriate. Each Discipline, Technology Area, and/or Product Component will contain one or more Compliance Components. A Compliance Component template is provided to ensure consistent documentation of each Compliance Component.

There are three different types of Compliance Components:

- ***Guidelines*** – General statements of direction or desired future state. Guidelines are highly recommended, but they are not mandated.
- ***Standards*** – Mandated statements. A variance must be granted to excuse compliance with an existing standard. (More than one standard may exist to allow flexibility in the architecture blueprint.)
- ***Legislation*** – Compliance criteria legislated that can be changed only by changing the law. There are numerous types of legislation including, but not limited to, policy, executive order, code of state, federal regulation, or statute.

Compliance Components (guidelines, standards and mandates) documented at the Discipline level provide the basis for making important decisions about new products, protocols, configurations, etc. Compliance Components documented at the Technology Area or Product Component level provide the basis for decisions on which configuration, implementation, or product to utilize. The documentation of Compliance Components provides the information most critical for interoperability.

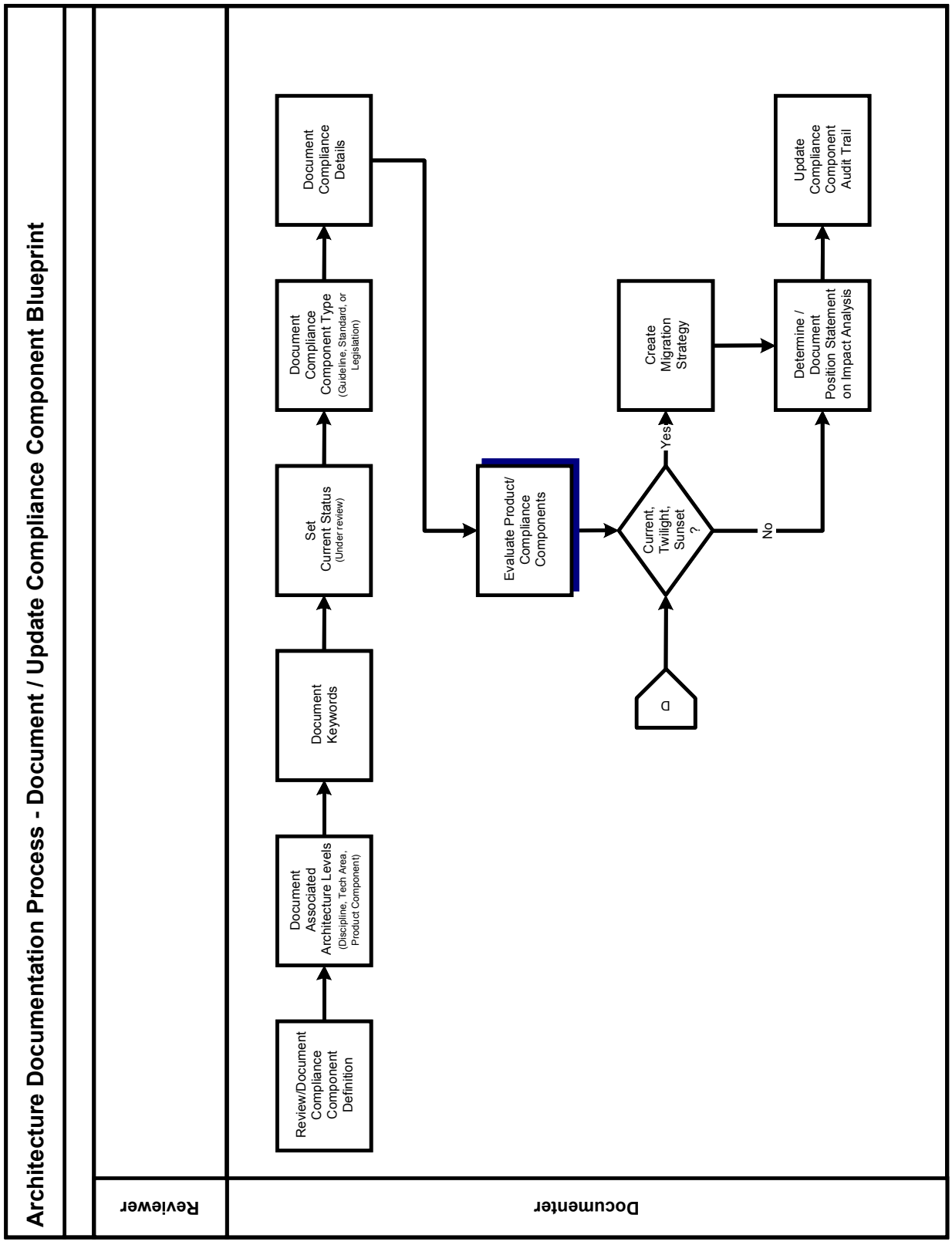
The template for Compliance Components, as well as the process for evaluation and classification, is very similar to that for Product Components. The separation between Product and Compliance Components is necessary for clarity and because the Compliance Components (guidelines, standards and mandates) can be documented at the three levels: Discipline, Technology Area and Product Component level.

Important items to keep in mind when determining the various Compliance Components to document:

- Information captured must be maintainable.
- Overly generic Compliance Components are difficult to enforce.
- Verbose compliance documentation is difficult to understand.
- Utilize standards created in the various standards groups or industry providers.
- When referencing existing compliance documentation from various standards organizations or departments within your organization, be aware of the following:

- Links can become invalid if the original documentation is moved.
- Copies of compliance documentation may no longer be valid if updates are made to the original.

Compliance Components may be guidelines, standards and legislative mandates. The primary difference between the types of Compliance Components lies in the degree of authority as described in the Template Overview. Compliance Components may be associated with a Discipline, Technology Area, and/or a Product Component.


Architecture Documentation Process - Document / Update Compliance Component Blueprint
Reviewer
Documenter
Review/Document Compliance Component Definition
Document Associated Architecture Levels (Discipline, Tech Area, Product Component)
Document Keywords
Set Current Status (Under review)
Document Compliance Component Type (Guideline, Standard, or Legislation)
Document Compliance Details
Evaluate Product/ Compliance Components
Current, Twilight, Sunset ?
Yes
No
Create Migration Strategy
Determine / Document Position Statement on Impact Analysis
Update Compliance Component Audit Trail
D

## PROCESS DETAIL

The Compliance Component Blueprint should be completed/updated using the Compliance Component Template as a guide. The following process steps aid in this documentation:

**Review /Document Compliance Component Definition** - Review the compliance component's definition, rationale, and benefits. Rationale and benefits will be included when the information will aid in the understanding of the compliance component being documented.

**Document Associated Architecture Levels** - Compliances must be defined and associated with the correct levels in the architecture blueprint (Discipline, Technology Area, and/or Product Component).

**Document Keywords** - Keywords or nomenclatures that aid in locating a Compliance Component should be listed. These help identify existing Compliance Components that may already exist for a specific keyword.

**Set Current Status** - Since there will be so many different Compliance Components moving through the Architecture Documentation Process at one time, it is important to understand where a given Compliance Component resides in the process. Initial statuses identified include:

- *In Development* – The architecture team is currently crafting and/or reviewing the Compliance Component content.
- *Under Review* – The architecture team has completed the Compliance Component content and it is under review by an EA governing body.
- *Accepted* – Indicates the Compliance Component has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Compliance Component was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

**Document Compliance Component Type** - Compliances are of three types that describe the level of compliance expected. They include:

- Guidelines – General statements of direction or desired future state for this level of the architecture blueprint (Discipline, Technology Area, or Product Component). These will not be mandated.
- Standards – Specific protocols, product or version statements. More than one standard may exist. Variance must be sought not to follow one of the standards that exist.
- Legislation – Items required by law. Only a change in the legislation will allow variances.

If further clarification of the Component type is needed, the Compliance Component Sub-type is available.

**Document Compliance Details** - The Compliance Component details should be articulated. These include:

- Compliance Statement
- Compliance Referenced Source
  - Standards Organization/Government Body
  - Actual Statue or Standards Document Version

**Evaluate Product/ Compliance Components -** An evaluation of the Compliance Component is necessary to determine its classification. This will be discussed in detail in the Evaluate Product/Compliance Components sub-process.

**Create Migration Strategy** - For a Compliance Component classified as current, twilight, or sunset, a migration strategy must be formulated. This must be done for compliances migrating from:

- Compliance Components classified as emerging that are moving to current.
- Compliance Components classified as current that are moving to either twilight or sunset.

These strategies will identify:

- Impacts on existing components
- Considerations for conversion
- Recommendations for:
  - New development
  - Modifications to existing components (corrections & enhancements)
  - Potential for user-base expansion (reuse).

**Determine/Document Position Statement on Impact Analysis -** An impact analysis must be conducted to determine what impact the most recently determined classification of this Compliance Component will have on the existing architecture blueprint. The analysis must be documented in a Position Statement on impact.

**Update Compliance Component Audit Trail -** Audit trails for the information provided in the template must be maintained. During the initial development of the Compliance Component, only the creation, accepted/rejected, and date last updated must be maintained.

# Compliance Component Template

## TEMPLATE OVERVIEW

The Compliance Component Template provides a checklist for documenting the Compliance Component details. A detailed description of each of the content areas follows the visual representation of the Compliance Component Template provided here.

The Compliance Template will include the following sections:

- Definition
- Component Classification
- Associated Technology Architecture Blueprint Level
- Keywords
- Compliance Component Type
- Compliance Detail
- Conditional Use Restrictions

- Migration Strategy
- Impact Position Statement
- Current Status
- Audit Trail

# Compliance Component

| Definition | |
|---|---|
| *Name* | |
| *Description* | |
| *Rationale* | |
| *Benefits* | |

| Component Classification | | | | |
|---|---|---|---|---|
| *Classification* | ☐ *Emerging* | ☐ *Current* | ☐ *Twilight* | ☐ *Sunset* |
| *Sunset Date* | | | | |
| *Rationale for Classification* | | | | |

| Associated Technology Architecture Blueprint Level | |
|---|---|
| *Discipline Name* | |
| *Technology Area Name* | |
| *Product Component Name* | |

| Keywords | |
|---|---|
| *Keywords/Aliases* | |

| Compliance Component Type | | | |
|---|---|---|---|
| *Component Type* | ☐ *Guideline* | ☐ *Standard* | ☐ *Legislation* |
| *Compliance Sub-type* | | | |

| Compliance Detail | |
|---|---|
| *Statement* | |
| *Source Reference* | |

| *Standards Organization* | | | |
|---|---|---|---|
| *Name* | | *Web Address* | |
| *Contact Information* | | | |

| *Government Body* | | | |
|---|---|---|---|
| *Name* | | *Web Address* | |
| *Contact Information* | | | |

| Conditional Use Restrictions | |
|---|---|
| *Restrictions* | |

| Migration Strategy | |
|---|---|
| *Strategy/Source Document* | |

| IMPACT POSITION STATEMENT | | | |
|---|---|---|---|
| *Impact Statement* | | | |
| **CURRENT STATUS** | | | |
| *Compliance Component Status* | ☐ *In Development* ☐ *Under Review* ☐ *Rejected* ☐ *Accepted* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | | *Date Accepted / Rejected* | |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | |
| *Reason for Update* | | | |
| *Updated By* | | | |

## TEMPLATE DETAIL

### *Definition*

**Name** - Determine an appropriately descriptive name for the Compliance Component.

**Description** - Supply a description of the Compliance Component in a paragraph or two that provides sufficient clarity about the Compliance Component and what it covers.

**Rationale** - Provide a paragraph or two about the reason or basis for inclusion of this Compliance Component in the architecture blueprint.

**Benefits** - Provide a paragraph or bulleted statements that supply the benefits associated with the Compliance Component.

### *Component Classification*

**Classification** - Provide the classification for this Compliance Component.

(The process for determination is covered under Evaluate Product/Compliance Component Process.) Classifications include:

- *Emerging:* New technology, which has the potential to become current
- *Current:* Recommended technology (technology that meets the requirements of the enterprise architecture*.)*
- *Twilight:* Items that do not conform to the Business/Technology Drivers
- *Sunset:* Items that do not conform to the Business/Technology Drivers and have a set discontinuation date

**Sunset Date** - Document the date for discontinuation of the Compliance Component.

**Rationale for Classification** - Provide a rationale statement for the chosen classification based on the review of:

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

### *Associated Technology Architecture Blueprint Level*

**Discipline Name** - Provide the name of the Discipline with which this Compliance Component is associated. This will ensure the appropriate mapping of Compliance Component to Discipline.

**Technology Area Name**- Provide the name of the Technology Area with which this Compliance Component is associated. This will ensure the appropriate mapping of Compliance Component to Technology Area.

**Product Component Name** - Provide the name of the Product Component with which this Compliance Component is associated. This will ensure the appropriate mapping of Compliance Component to Product Component.

### *Keywords*

**Keywords/Aliases** - List any keywords/nomenclature and/or aliases that can be used to assist in searching for these Compliance Components. This information will be helpful for anyone looking for information on similar technologies.

### *Compliance Component Type*

**Component Type** - Denote whether the Compliance Component being considered or documented is a guideline, standard or legislation.

**Compliance Sub-type** - If the component is legislated, provide the type of legislation. Examples include items such as policy, executive order, code of state, federal regulation, or statute. For guidelines or standards, this area is available for instances where a sub-type may need to be included.

### *Compliance Detail*

**Statement** - Provide the compliance statement.

**Source Reference** - Provide source reference for the compliance statement. This will include any reference numbers used for standards and mandates. URLs to web page that contain the full standard or mandate would also be useful.

**Standards Organization** - List the standards organization that supplies the standard. Provide contact information for each organization, as well as URLs, if available.

**Government Body** - List the government body that provides the mandate associated with this Compliance Component. Provide contact information for the government body, as well as URLs, if available.

### *Conditional Use Restrictions*

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

### *Migration Strategy*

**Strategy/Source Document** - Document Migration Strategy for:

- Compliance Components classified as emerging that are moving to current.
- Compliance Components classified as current that are moving to either twilight or sunset.

These strategies should identify the following items, as applicable:

- Existing user base and technical staff
- Training for existing user base
- Training for existing technical staff
- Impacts on existing Technology Areas, Product and Compliance Components
- Considerations for conversion
- Recommendations for the Compliance Component as it applies to:
  - New development
  - Modifications (corrections & enhancements)
  - Possibilities for user-base expansion (reuse).

**Note**: A link to the source document should be provided if the Migration Strategy is documented as a stand-alone document.

### *Impact Position Statement*

**Impact Statement** - Document position statement about the impact of this Compliance Component on the Organization. Consider the follow items when developing the impact position statement:

- The impact on the Technology Architecture Blueprint
- Physical implementation requirements
- The impact on installed applications or services
- The impact on existing installation standards.

### *Current Status*

**Compliance Component Status** - Document the status of Compliance Component, indicating whether the Compliance Component is in development, under review, rejected, or accepted.

- *In Development* – The architecture team is currently crafting and/or reviewing the Compliance Component content.
- *Under Review* – The architecture team has completed the Compliance Component content and it is under review by an EA governing body.
- *Accepted* – Indicates the Compliance Component has been approved and accepted into the architecture blueprint.
- *Rejected* – If the Compliance Component was rejected by any of the governance groups during the various reviews, the reason for the rejection must be documented in the audit trail information.

### *Audit Trail*

**Creation Date** - Provide the date the Compliance Component was created.

**Created By** – List all individuals and their titles that helped in the creation of this Compliance Component.

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

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

**Last Date Reviewed** - Document the most recent date the Compliance Component was taken through the Architecture Blueprint Vitality Process.

**Last Date Updated** - Document the most recent date that any item in the Compliance Component template was changed.

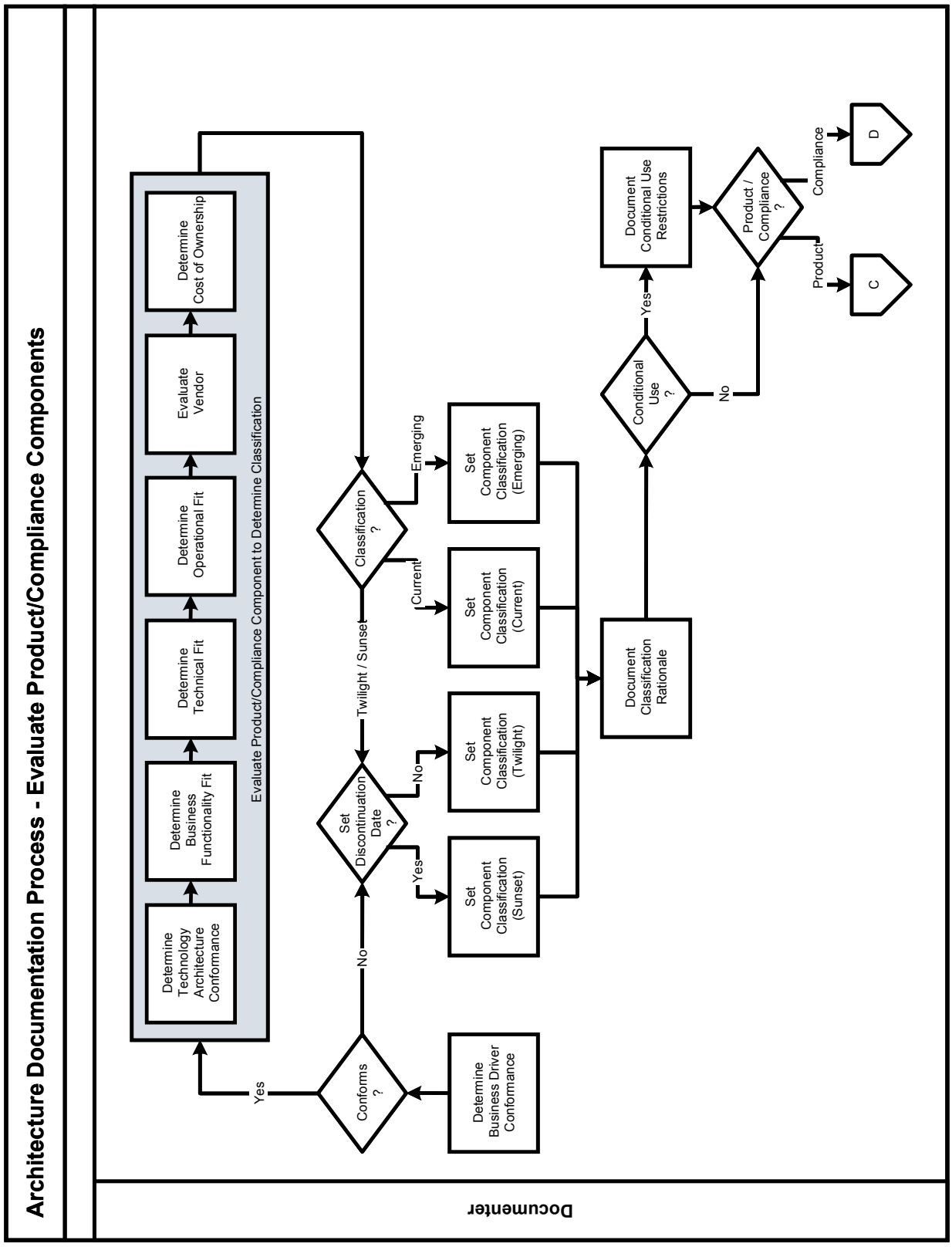
**Reason for Update** - Document the reason for the update to the Compliance Component.

**Updated By** - Provide the names of the persons responsible for the update to the Compliance Component. This will be helpful information for future reference.

# Evaluate Product/Compliance Components

## PROCESS OVERVIEW

In order to develop consistent evaluation of Products and Compliance Components associated with the Technology Architecture Blueprint, there must be objective selection and evaluation criteria.


Architecture Documentation Process - Evaluate Product/Compliance Components
Documenter
Determine Business Driver Conformance
Conforms ?
No
Yes
Determine Technology Architecture Conformance
Determine Business Functionality Fit
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
Classification ?
Current
Emerging
Set Component Classification (Sunset)
Set Component Classification (Twilight)
Set Component Classification (Current)
Set Component Classification (Emerging)
Document Classification Rationale
Conditional Use ?
Yes
No
Document Conditional Use Restrictions
Product / Compliance ?
Product
Compliance
C
D

## PROCESS DETAIL

**Determine Business Driver Conformance** - Components that do not conform to Business Drivers should be classified as either "Twilight" or "Sunset". See further detail for these under Classifications below.

**Evaluate Product/Compliance Component to Determine Classification** - For Components that do conform to the Business Drivers, the following additional evaluation must be performed:

- *Determine Technology Architecture Conformance* – The Component must align with the architecture blueprint. How well does the product comply with the IT principles and standards selected?
- *Determine Business Functionality Fit* – The Component being evaluated must address the functional business requirements. This part of the evaluation should include information on current and pending release levels. Families of products should also be considered when relevant.
- *Determine Technical Fit* – The Component being evaluated must be consistent with the current and planned technical environment.
- *Determine Operational Fit* – The Component being evaluated must meet the systems and other management requirements for operating and supporting the service level agreements in a specific environment.
- *Evaluate Vendor* – The vendor should be evaluated to determine its ability to support the offering, survive in the marketplace, and keep up with changing technology. Market share may be a consideration in determining product viability.
- *Determine Cost of Ownership* – The total cost of ownership must be considered, including acquisition, maintenance, support, integration services, skills, infrastructure, and de-acquisition costs. This should take into account the current organization user base.

**Set Component Classification** - Based on results of the evaluation, classify the Component using the following classifications:

- *Sunset* components are those that are in use but do not conform to the stated Business or Technology Architecture Blueprints. The sunset component will have a date of discontinuance identified, indicating the date that the component will no longer be acceptable for use within the architecture.
- *Twilight* components are those that are in use but do not conform to the stated Business Drivers or Technology Architecture Blueprints. The components have no date of discontinuance identified. These Components should not be used to develop new applications. Extensive modifications to these systems should be reviewed to determine if the system should be redeployed completely using newer technology.
- *Current* components are defined as those having met the requirements of the enterprise architecture. These represent the recommended Components that should be used in deployment of technology solutions.
- *Emerging* products are those that have potential to become current architecture blueprint components. While identified as Emerging, these Components should be used only in pilot or test environments and under highly controlled regulations. After sufficient testing, these Components may become current or may be identified non-compliant or non-functional in the organization's environment. Use of these components requires a variance that must be documented and approved through the compliance process.

**Document Classification Rationale** - Once the classification is known, the rationale for the classification must be documented.

**Document Conditional Use Restrictions** - Occasionally, a component has some characteristic that would limit its usefulness as an enterprise product. For example, some desktop database products may be well suited for a personal desktop application but should never be used for storing, accessing, or maintaining enterprise data.

Document the additional classification of "Conditional" for Components with limited usefulness.

# SAMPLES

## Technology Architecture Samples

This section contains three sets of Blueprint samples, one set of samples from the Application domain and two separate sets of samples from different Security domains. The second set of samples from the Security domain is provided to illustrate that there are many ways to name and group the architectural elements, all of which are correct.

It should be noted that some of the samples were completed using earlier versions of the templates and, while the information that was gathered is the same, it may be presented in a slightly different order or have a slightly different heading or topic title than the latest template versions.

### APPLICATION BLUEPRINT SAMPLES

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

The five levels of the Application Domain are represented starting at the domain level and following a single path throughout the levels as follows:

- Domain – Application
- Discipline – Application Development Management
- Technology Area – Programming Language/Environment
- Product Component - Visual Basic
- Compliance Component - Prefix all constants with c_ and a scope designator

A second example of a Discipline from within the Application Domain includes:

- Discipline – Electronic Collaboration

| *Domain* | *Discipline* | *Technology Area* | *Product Component* | *Compliance Component* |
|---|---|---|---|---|
| Application | Application Development Management | Programming Language / Environment | Visual Basic | Prefix all constants with a c_ and a scope designator |
| | Electronic Collaboration | | | |

# Domain Blueprint

| DEFINITION | |
|---|---|
| *Name* | Domain – Application Architecture |
| *Description* | Defines the roles, policies, standards, and application development methodologies required to bring support the various custom and purchased applications throughout the organization. Disciplines for this domain cover the automation of the workforce, promote group productivity, and provide a set of reusable application components. |
| *Rationale* | The domain of applications has been a stand-alone set of technology experts, tools, and disciplines from the invention of the computer. It is from this base domain that other domains have come in existence and will continue to come as skills and tools become more specialized. Good application architecture enables a high level of system integration, reuse of components, and rapid deployment of applications in response to changing business requirements. |
| *Benefits* | The Application Architecture standardizes the approach to application development and electronic collaboration. This standardization provides a cost effective approach to application development/deployment and minimizes training and retraining requirements. The capability to retain staff will be increased by the simplification of staff retraining and a more effective investment of available project funding. |

| BOUNDARY | |
|---|---|
| *Boundary Limit Statement* | Includes the applications that are developed or deployed to support the business functionality. Subject Areas include:<br>• Business Rules<br>• Development Tools<br>• Coding Standards<br>• Component Object Repositories<br>• Custom Systems<br>• Enterprise wide applications (ex: Electronic Payment Applications, Electronic Benefits Applications, etc.)<br>• Commercial Products<br>• N-Tiered Architecture<br><br>Electronic Collaboration applications are also included:<br>• Email<br>• Calendar<br>• Messenger services<br>• Workgroup<br>• Messaging Boards<br>• Chat rooms |

| ASSOCIATED DISCIPLINES | |
|---|---|
| *Disciplines under this Domain* | Application Development Management<br>Electronic Collaboration |

| RELATED PRINCIPLES | | |
|---|---|---|
| *Reference #s, Statements or Links* | *Conflict* | *Relationship* |
| Business case and metrics for effectiveness of application should accompany automation efforts. (MA-Claudia) | ☐ | Used to verify effectiveness of application pre and post implementation. |
| A business process analysis and review must always accompany automation efforts. Before automating business processes, a demonstrated attempt must be made to eliminate unnecessary processes and to simplify those remaining. | ☐ | Used to verify that automation is done for only critical business functions/processes. |
| Applications should address a business need and requirements for the application should be carefully documented and traced throughout the application development process. | ☐ | Requirements become the basis for the design and testing of the applications. Vital deliverable for making sure the users' needs are met. |
| The order of preference for solution delivery will be to reuse existing, purchase new and tailor, and then build. | ☐ | Use this principle when reviewing new initiatives. |
| Application programs, whether purchased or developed internally, will be deployed with separation of presentation logic, business logic and data access in order to provide modular, reusable functionality. | ☐ | Bases for design and technical fit reviews. |
| New applications will be modular and independent (“atomic”) in nature. They will access common data, use common services and have only inherently essential dependence on other applications (e.g. for provision of up-to-date data). | ☐ | Bases for design and technical fit reviews. |
| New applications will use defined and documented standards-based programming interfaces. | ☐ | Bases for design and code reviews. |
| Long-term plans will be considered when implementing new systems to avoid obsolescence. Agency IT plans need to develop strategies for the removal of non-strategic or retired technologies. | ☐ | IT Portfolio Lifecycle requirements. |
| Vendor neutral standards should be applied to reduce effort required for system integration. Exceptions should be negotiated and mitigated. | ☐ | Architecture Documenters need to adhere to this principle. Exceptions should be noted with rationale. |
| Application configuration decisions should be based on N-tiered and browser-based technologies where appropriate. | ☐ | Bases for design and technical fit reviews. |

| | | |
|---|---|---|
| Hardware and software should comply with industry standards for remote control and monitoring. | ☐ | Bases for design and technical fit reviews. |
| Applications should present a consistent user interface that is adaptable to a particular user's requirement. | ☐ | Bases for design and technical fit reviews. |
| All applications will be built to accessibility standards. (MA-Claudia | ☐ | Bases for design and technical fit reviews. |

## Related Best Practices

| *Reference #s, Statements or Links* | *Conflict* | Relationship |
|---|---|---|
| Business Environment and Organizational Support | ☐ | Include in part of methodologies for projects and IT Services, and implementation plan. |
| Project Preparation | ☐ | Consistent project steps from a business, IT, procurement and architecture view must be created. |
| Project Sequence and Outputs | ☐ | Consistent project steps from a business, IT, procurement and architecture view must be created. |
| Project Tools and Disciplines | ☐ | Education in tools and project roles must be conducted. Their relationship with the Architecture Roles must be specified. |
| Project Organization and Leadership | ☐ | Education of project organization and leadership on Architecture must be conducted prior to project. Project Management Office on large projects should look to having an Architecture representation as part of the project organization. |
| Personnel Management | ☐ | Must work with this management to assure the Architecture Documenters and Subject Matter Experts will be available to aid in documenting the architecture. |
| Interagency Coordination | ☐ | Must be spear headed not only by IT Management but also by the Architecture groups so show benefit of coordination. |
| Operations | ☐ | All groups within IT need to be consulted when creating the Architecture. This group represents the day in and day out activity of supporting the IT operations. This perspective cannot be down played. |

## Related Trends

| *Reference #s, Statements or Links* | *Conflict* | *Relationship* |
|---|---|---|
| | ☐ | |
| | ☐ | |

## State Contracts

| | |
|---|---|
| *Planned Contracts* | None identified |
| *Existing Contracts* | None identified |

## Current Status

| | |
|---|---|
| *Domain Status* | ☐ *In Development* ☐ *Under Review* ☐ *Rejected* ☐ *Accepted* |

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

Click on this link to return to Application Blueprint Samples.

# Discipline Blueprint

| DEFINITION | |
|---|---|
| *Name* | Discipline – Application Development Management |
| *Description* | Defines roles, development methodologies, technology standards, and technologies that define how applications are designed and how they cooperate. It defines how those applications are documented and maintained. The Application Development Management discipline provides criteria, approved methodologies, and technologies that optimize the use and reuse of application components. The discipline includes strategies for the retention of legacy knowledge and the phase out or upgrade of legacy systems. |
| *Rationale* | The Application Development & Management discipline standardizes the methodology, approach, standards and technology components used in application development. The discipline has relationships with but does **not** include database applications and middleware or their associated platforms and operating systems.<br>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.<br>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.<br>Deploy applications systems that are (business) event-driven.<br>Application systems should be engineered or re-engineered to be “highly granular” and “loosely coupled”.<br>Applications systems employ reusable components using a browser-based model.<br>Application systems should share reusable components across the enterprise<br><br>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:<br>• Business Rules<br>• Development Tools<br>• Coding Standards<br>• Component Object Repositories<br>• Custom Systems<br>• Enterprise wide applications (ex: Electronic Payment Applications, Electronic Benefits Applications, etc.)<br>• Commercial Products<br>• N-Tiered Architecture |

| ASSOCIATED DOMAIN | |
|---|---|
| *Domain Name* | Application Architecture |

| CRITICAL REFERENCES | | | | | |
|---|---|---|---|---|---|
| *Related Domains/Disciplines* | | | | | |
| | *Domain – Disciplines* | | *Domain - Disciplines* | | *Domain - Disciplines* |
| ☒ | Access: Internet /Intranet | ☒ | Integration: Functional Integration | ☒ | System Management: Help Desk / Problem Management |
| ☒ | Access: Branding | ☒ | Integration: Middleware | ☒ | System Management: Business Continuity |
| ☒ | Access: Accessibility | ☒ | Application: Application Development Management | ☒ | Security: Enterprise Security |
| ☒ | Information: Data Management | ☒ | Application: Electronic Collaboration | ☒ | Security: Network Security |
| ☒ | Information: Knowledge Management | ☒ | Platform: Platform | ☒ | Security: Host Security |
| ☒ | Information: GIS | ☒ | Platform: Configuration Management | ☒ | Privacy: Profiling |
| ☒ | Information: Data Storage | ☐ | Systems Management: Asset Management | ☒ | Privacy: Personalization |
| ☒ | Network: Physical Network | ☒ | System Management: Change Management | ☒ | Privacy: Privacy |
| ☐ | Network: Network Management | ☒ | System Management: Console / Event Management | ☐ | |

| *Standards Organizations* | | | |
|---|---|---|---|
| *Name* | International Organization for Standardization | *Web Address* | http://www.iso.ch/iso/en/ISOOnline.frontpage |
| *Contact Information* | **ISO Central Secretariat:**<br>International Organization for Standardization (ISO)<br>1, rue de Varembé, Case postale 56<br>CH-1211 Geneva 20, Switzerland<br>Telephone + 41 22 749 01 11; Telefax + 41 22 733 34 30;<br>E-mail: central@iso.org; Web: http://www.iso.org | | |

| *Government Bodies* | | | |
|---|---|---|---|
| *Name* | None Identified | *Web Address* | |
| *Contact Information* | | | |

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

| *Discipline-specific Trends* | |
|---|---|
| *Trend Statement* | Utilizing XML for API calls. Standardize the data types used in the XML.<br>See:<br>XML Schema Part 2: Data types |
| *Trend Source* | http://www.w3.org/TR/xmlschema-2/ |

| METHODOLOGIES | | | |
|---|---|---|---|
| *Methodologies followed* | Rapid Application Development (RAD)<br>Joint Application Development (JAD) | | |
| **ASSOCIATED COMPLIANCE COMPONENTS** | | | |
| *Compliance Component Names* | ANSI/IEEE 1016-1987 (Recommended Practice for Software Design Description) Software design<br>ANSI/IEEE 1016.1 –1993 (Guide for Software Design Descriptions) Software design | | |
| **ASSOCIATED TECHNOLOGY AREAS** | | | |
| *Technology Areas* | Application Development Languages<br>Case Tools<br>Source code repositories | | |
| **DISCIPLINE DOCUMENTATION REQUIREMENTS** | | | |
| *Documentation requirements for this Discipline* | This discipline will be documented to the product level and the compliance components associated with the product version, family etc…) | | |
| **CURRENT STATUS** | | | |
| *Discipline Status* | ☐ *In Development* ☐ *Under Review* ☐ *Rejected* ☐ *Accepted* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | 03/01/02 | *Date Accepted/Rejected* | |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | 03/01/02 |
| *Reason for Update* | | | |
| *Updated By* | | | |

Click on this link to return to Application Blueprint Samples.

# Technology Area Blueprint

| Definition | |
|---|---|
| *Name* | Technology Area – Programming Language / Environment |
| *Description* | Programming Language / Environment includes all the various coding languages and IDE (Integrated Development Environments) utilized within the organization to deliver software applications, components, and objects. |
| *Rationale* | Having a single technology area for all of these allows compliance components that may be applied across all languages to be associated at the Technology Area. |
| *Benefits* | Compliance components will be maintained once for all languages that they apply for thus saving time. This time may be spent in furthering other areas of the architecture blueprint. |

| Associated Discipline | |
|---|---|
| *Discipline Name* | Application Development |

| Keywords | |
|---|---|
| *Keywords/Aliases* | Coding Studios, Programming, Coding Standards, Code Sets, Application Languages |

| Associated Compliance Components | |
|---|---|
| *Compliance Component Names* | Overall Programming Standards |

| Single Product Solution | |
|---|---|
| *Date of Single Product Solution Determination* | |
| *Provide Rationale for Decision* | |

| Associated Product Components | | |
|---|---|---|
| *Product Component Names* | JAVA,<br>COBOL II (MF, AS)<br>C<br>C++ | COBOL (MF, AS)<br>RPG (AS)<br>Pascal<br>Microsoft Visual Basic |

| Current Status | | | | |
|---|---|---|---|---|
| *Technology Area Status* | ☐ *In development* | ☐ *Under Review* | ☐ *Rejected* | ☒ *Accepted* |

| Audit Trail | | | |
|---|---|---|---|
| *Creation Date* | 03/02/02 | *Date Accepted / Rejected* | |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | 03/02/02 |
| *Reason for Update* | | | |
| *Updated By* | | | |

Click on this link to return to Application Blueprint Samples.

# Product Component Blueprint

| Definition | | | |
|---|---|---|---|
| *Name* | Product Component – Visual Basic | | |
| *Description* | Visual Basic programming language. | | |
| *Rationale* | | | |
| *Benefits* | | | |
| **Component Classification** | | | |
| *Classification* | ☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset* | | |
| *Sunset Date* | | | |
| *Rationale for Classification* | Current application language in use in nth architecture for the organization. | | |
| **Associated Technology Area** | | | |
| *Technology Area Name* | Application Languages | | |
| **Keywords** | | | |
| *Keywords/Aliases* | VB, Visual Studio, Client Server language, VBA, | | |
| **Vendor Information** | | | |
| *Vendor Name* | Microsoft | *Web Address* | www.microsoft.com |
| *Contact Information* | **(800) 936-5800** Developers | | |
| **Potential Compliance Organizations** | | | |
| *Standards Organizations* | | | |
| *Name* | ISO | *Web Address* | http://www.iso.ch |
| *Contact Information* | **ISO Central Secretariat:**<br>International Organization for Standardization (ISO)<br>1, rue de Varembé, Case postale 56<br>CH-1211 Geneva 20, Switzerland<br>Telephone + 41 22 749 01 11; Telefax + 41 22 733 34 30;<br>E-mail: central@iso.org; Web: http://www.iso.org | | |
| *Government Bodies* | | | |
| *Name* | | *Web Address* | |
| *Contact Information* | | | |
| **Associated Compliance Components** | | | |
| *Product* | | | |
| *Product-specific Compliance Components* | Practical Standards for Microsoft® Visual Basic®<br>Author James D. Foxall<br>Pages 400<br>Disk 1 CD<br>Level Int/Adv<br>Published 01/26/2000<br>ISBN 0-7356-0733-8 | | |

| Configurations | | | |
|---|---|---|---|
| *Configuration-specific Compliance Components* | Visual Basic 5<br>Visual Basic .nt | | |
| **COMPONENT REVIEW** | | | |
| *Desirable aspects* | | | |
| *Undesirable aspects* | | | |
| **REQUIRED COMPONENT** | | | |
| *Business Area, Department or Application Name* | | | |
| **CONDITIONAL USE RESTRICTIONS** | | | |
| *Restrictions* | | | |
| **MIGRATION STRATEGY** | | | |
| *Strategy/Source Document* | | | |
| **IMPACT POSITION STATEMENT** | | | |
| *Impact Statement* | | | |
| **CURRENT STATUS** | | | |
| *Product Component Status* | ☐ *In development* ☐ *Under Review* ☐ *Rejected* ☒ *Accepted* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | 03/02/02 | *Date Accepted / Rejected* | |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | 03/02/02 |
| *Reason for Update* | | | |
| *Updated By* | | | |

Click on this link to return to the Application Blueprint Samples.

# Compliance Component Blueprint

| Definition | |
|---|---|
| *Name* | Compliance Component – Prefix all constants with c_ and a scope designator |
| *Description* | Naming standard for constants. Includes scope of constant in the name. |
| *Rationale* | Ease of code maintenance and code reviews. |
| *Benefits* | Coding errors are minimized because of consistent naming standards. |
| **Component Classification** | |
| *Classification* | ☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset* |
| *Sunset Date* | |
| *Rationale for Classification* | Visual Basic 5 is current application language used in the organization for client server and nth tier application development. |
| **Associated Technology Architecture Blueprint Level** | |
| *Discipline Name* | Application Development |
| *Technology Area Name* | Application Languages |
| *Product Component Name* | Visual Basic |
| **Keywords** | |
| *Keywords/Aliases* | Constance, Variable, naming, |
| **Compliance Component Type** | |
| *Component Type* | ☐ *Guideline* ☒ *Standard* ☐ *Legislation* |
| *Compliance Sub- Type* | Coding |
| **Compliance Detail** | |
| *Statement* | **5.1 Prefix all constants with c_ and a scope designator**.<br><br>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:<br><br>**Const** COLUMN_INDEX = 7<br><br>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:<br><br>**Const** c_Column_Index = 7<br><br>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.<br><br>**Incorrect:**<br><br>**Const** USDATE = "mm/dd/yyyy"<br>**Const** KEYCONTROL = 17<br><br>**Correct:**<br><br>**Const** c_USDate = "mm/dd/yyyy"<br>**Const** c_KeyControl = 17<br><br>**Also correct:**<br><br>**Const** c_US_Date = "mm/dd/yyyy"<br>**Const** c_Key_Control = 17<br><br>**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.<br><br>**Incorrect (module level or global level):**<br><br>**Private Const** c_US_DATE = "mm/dd/yyyy"<br>**Public Const** c_KeyControl = 17<br><br>**Correct:**<br><br>**Private Const** mc_US_Date = "mm/dd/yyyy"<br>**Public Const** gc_KeyControl = 17 |
| *Source Reference* | Practical Standards for MS Visual Basic - Chapter 5<br>by James D. Foxall<br>ISBN 0-7356-0733-8 |
| *Standards Organization* | |
| *Name* | *Web Address* |
| *Contact Information* | |
| *Government Body* | |
| *Name* | *Web Address* |
| *Contact Information* | |
| CONDITIONAL USE RESTRICTIONS | |
| *Restrictions* | |
| MIGRATION STRATEGY | |
| *Strategy/Source Document* | |
| IMPACT POSITION STATEMENT | |
| *Impact Statement* | |

| CURRENT STATUS | | | | | |
|---|---|---|---|---|---|
| *Compliance Component Status* | ☐ *In development* | ☐ *Under Review* | ☐ *Rejected* | ☒ *Accepted* | |
| **AUDIT TRAIL** | | | | | |
| *Creation Date* | 03/02/02 | | *Date Accepted / Rejected* | | |
| *Created By* | | | | | |
| *Reason for Rejection* | | | | | |
| *Last Date Updated* | | | *Last Date Reviewed* | 03/02/02 | |
| *Reason for Update* | | | | | |
| *Updated By* | | | | | |

Click on this link to return to the Application Blueprint Samples.

# Discipline Blueprint

| DEFINITION | |
|---|---|
| *Name* | Discipline - Electronic Collaboration |
| *Description* | The Electronic Collaboration discipline defines the standards and infrastructure components that facilitate the interaction of the workforce and promote group productivity. These include e-mail, directory services and other person-to-person or group collaboration tools.<br><br>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.<br>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:<br>• Spreadsheets<br>• Business Graphics<br>• Presentation Packages<br>• Personal Data Bases<br>• Word Processing<br>• Time Management and Scheduling<br>• Calendars<br>• Desktop Publishing<br>• Multi-media<br>• Document Imaging<br>• Mail |

| Associated Domain | |
|---|---|
| *Domain Name* | Application Architecture |

| Critical References | | | | | |
|---|---|---|---|---|---|
| *Related Domains/Disciplines* | | | | | |
| *Domain – Disciplines* | | *Domain - Disciplines* | | *Domain - Disciplines* | |
| ☐ | *Access: Internet /Intranet* | ☒ | *Integration: Functional Integration* | ☐ | *System Management: Help Desk / Problem Management* |
| ☐ | *Access: Branding* | ☐ | *Integration: Middleware* | ☒ | *System Management: Business Continuity* |
| ☒ | *Access: Accessibility* | ☒ | *Application: Application Development Management* | ☒ | *Security: Enterprise Security* |
| ☐ | *Information: Data Management* | ☒ | *Application: Electronic Collaboration* | ☒ | *Security: Network Security* |
| ☐ | *Information: Knowledge Management* | ☐ | *Platform: Platform* | ☒ | *Security: Host Security* |
| ☐ | *Information: GIS* | ☒ | *Platform: Configuration Management* | ☐ | *Privacy: Profiling* |
| ☐ | *Information: Data Storage* | ☐ | *Systems Management: Asset Management* | ☐ | *Privacy: Personalization* |
| ☒ | *Network: Physical Network* | ☒ | *System Management: Change Management* | ☒ | *Privacy: Privacy* |
| ☐ | *Network: Network Management* | ☐ | *System Management: Console / Event Management* | | |

| *Standards Organizations* | | | |
|---|---|---|---|
| *Name* | International Organization for Standardization | *Web Address* | http://www.iso.ch/iso/en/ISOOnline.frontpage |
| *Contact Information* | **ISO Central Secretariat:**<br>International Organization for Standardization (ISO)<br>1, rue de Varembé, Case postale 56<br>CH-1211 Geneva 20, Switzerland<br>Telephone + 41 22 749 01 11; Telefax + 41 22 733 34 30;<br>E-mail: central@iso.org; Web: http://www.iso.org | | |

| *Government Bodies* | | | |
|---|---|---|---|
| *Name* | None Identified | *Web Address* | |
| *Contact Information* | | | |

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

| *Discipline-specific Trends* | |
|---|---|
| *Trend Statement* | None identified |
| *Trend Source* | |

| METHODOLOGIES | | | |
|---|---|---|---|
| *Methodologies followed* | | | |
| **ASSOCIATED COMPLIANCE COMPONENTS** | | | |
| *Compliance Component Names* | None identified | | |
| **ASSOCIATED TECHNOLOGY AREAS** | | | |
| *Technology Areas* | e-Mail<br>Calendaring | | |
| **DISCIPLINE DOCUMENTATION REQUIREMENTS** | | | |
| *Documentation requirements for this Discipline* | This discipline will be documented to the product level and the compliance components associated with the product version, family etc…) | | |
| **CURRENT STATUS** | | | |
| *Discipline Status* | ☐ *In development* ☐ *Under Review* ☐ *Rejected* ☒ *Accepted* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | 03/01/02 | *Date Accepted/Rejected* | |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | 03/01/02 |
| *Reason for Update* | | | |
| *Updated By* | | | |

Click on this link to return to Application Blueprint Samples.

## SECURITY BLUEPRINT SAMPLES – SET ONE

The five levels of the first Security Domain sample are represented starting at the domain level and following a single line throughout the levels as follows:

- Domain – Security
- Discipline – Host Security
- Technology Area – Directory Services
- Product Component - OpenLDAP
- Compliance Component – OpenLDAP 2.0 Administrator's Guide

Additional examples of Disciplines and a Discipline-level Compliance Component from within the first sample Security Domain include:

- Discipline – Enterprise Security
- Compliance Component – Workstation Security
- Discipline – Network Security

| *Domain* | *Discipline* | *Technology Area* | *Product Component* | *Compliance Component* |
|---|---|---|---|---|
| Security | Host Security | Directory Services | OpenLDAP | OpenLDAP 2.0 Administrator's Guide |
| | Enterprise Security | | | Workstation Security |
| | Network Security | | | |

# Domain Blueprint

| DEFINITION | |
|---|---|
| *Name* | Domain – Security |
| *Description* | The Security Domain defines the roles, technologies, standards, and policies necessary to protect the information assets of states and their citizenry from vandalism, theft, and any other form of unauthorized access. The Security Domain defines the security and access management principles that are applied to ensure the appropriate level of protection for states' information assets. This Domain facilitates identification, authentication, authorization, administration, audit, and naming services.<br><br>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:<br><br>Physical Security<br><br>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.<br><br>User Security<br><br>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.<br><br>Application Security<br><br>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.<br><br>System Security<br><br>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<br><br>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.<br><br>Network Security<br><br>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.<br><br>Security Administration<br><br>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.<br><br>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.<br><br>Social Engineering/Human Factors<br><br>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.<br><br>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.<br><br>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:<br>• Physical security of the data and resources used to produce the data.<br>• Protection against unauthorized and inappropriate use that could potentially impede authorized and appropriate use of the resource.<br>• Identification and validation of the person who is requesting the information<br>• Control of access involves the ability to read, write, delete or otherwise acquire access to information.<br>• Data Privacy or confidentiality includes protection of information from unauthorized disclosure and interception.<br>• Data integrity or protecting the data from unauthorized modification, including unintentional modifications caused by disk errors, system problems, etc.<br>• Audit trails for accountability.<br>• 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.<br>• Security protects the computing infrastructure from unauthorized access.<br>• A functional, yet non-intrusive, secure architecture ensures enterprise-wide interoperability, as well as connectivity with external stakeholders.<br>• Security, designed into all architectural elements balances accessibility and ease-of-use with protection of data.<br>• Security, based on accepted standards allows the architecture to focus on open systems. |
| **BOUNDARY** | |
| *Boundary Limit Statement* | The Security Domain is associated with virtually all other domains because security needs must be assessed and applied where necessary in all phases of information resource development and management. The Security Domain does not include the privacy aspects associated with deployment of information technologies. |
| **ASSOCIATED DISCIPLINES** | |
| *Disciplines under this Domain* | Enterprise Security<br>Network Security<br>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.<br>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.<br><br>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.<br><br>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.<br>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.<br>When storage media (for example, hard drives or tapes) are no longer usable, all data on the media should be erased before disposal.<br>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.<br>CMOS passwords and file encryption should be employed on portable devices when they contain sensitive information.<br>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.<br>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.<br>Router connectivity should be secured by means of a firewall type device to control any access from outside the LAN, consistent with agency policy.<br>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.<br>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.<br>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.<br>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).<br>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.<br>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.<br>Common functions of the ISA include:<br>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.<br>Enable logging for important system level events and for services and proxies, and set up a log archiving facility. Review the logs.<br>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.<br>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.<br>Scan the network to create and maintain a complete map of systems to which the agency is connected.<br>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.<br>Common functions of the ISO include:<br>Use network-based vulnerability scanners.<br>Implement the latest applicable patches, remove or tighten unnecessary services, and tighten system settings on each host operating system.<br>Establish a host-based perimeter.<br>Implement a file integrity (cryptographic fingerprinting) system to ensure that you can tell which files were changed in an attack.<br>Identify the systems that must be protected for business to continue or trust to be maintained. These are identified as critical servers.<br>Implement instrumentation (such as host-based intrusion detection and cryptographic file fingerprinting) for critical servers to enable immediate response to unauthorized access.<br>Conduct a physical security assessment and correct insecure access and other physical security weaknesses.<br>Implement intrusion detection sensors and analysis stations.<br>Implement audited access using one or more forms of encryption, certificates, or tokens.<br>Assess and strengthen dial-in service configuration. |

| | | |
|---|---|---|
| | | Conduct a modem sweep to search for back doors.<br>Search for and eradicate sniffer programs.<br>Conduct a vulnerability scan, searching for additional vulnerabilities that have been exploited but are more rare and sophisticated.<br>Implement configuration management controls for the introduction of new systems to the network.<br>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.<br>Implement encryption, possibly as a virtual private network, to avoid disclosure of sensitive information traveling over the network.<br>Tighten security of the web server.<br>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.<br>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).<br>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.<br>Administrators should consider using available tools to test such things as the strength of passwords.<br>The security policy should also be reviewed and updated on a regular basis.<br>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.<br>Maintain a list of technical support personnel authorized to request information.<br>Encourage users to have vendors, outside technical support or contractors contact the organization's IT staff support for information pertaining to the network or information access. |
| **RELATED TRENDS** | | |
| *Reference #s, Statements or Links* | *Conflict* | *Relationship* |
| | ☐ | |
| | ☐ | |

| IT CONTRACTS | | | |
|---|---|---|---|
| *Planned Contracts* | | | |
| *Existing Contracts* | | | |
| **CURRENT STATUS** | | | |
| *Domain Status* | ☐ *In development* ☐ *Under Review* ☐ *Rejected* ☒ *Accepted* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | 4/15/2002 | *Date Accepted/Rejected* | |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | |
| *Reason for Update* | | | |
| *Updated By* | | | |

Click on this link to return to the Security Blueprint Samples – Set One.

# Discipline Blueprint

| DEFINITION | |
|---|---|
| *Name* | Discipline - Host Security |
| *Description* | Defines the roles, standards, policies, and tools for monitoring and ensuring the security across the organization's platform infrastructure. The Host Security discipline defines the security and access management principles that are applied to ensure the appropriate level of protection for information assets. |
| *Rationale* | Security of IT systems requires the protection of systems and information, and the assurance that the systems do exactly what they are supposed to do and nothing more. IT security requires management controls to ensure authorized access to the information in the systems and proper handling of input, processing, and output. The confidentiality of information must be assured whether on-site or off-site.<br>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:<br><br>User Security – identification, authentication, and authorization of user, including audit procedures and mechanisms.<br><br>Application Security – security between applications, including impact of distributed traffic, proxy accesses and middleware.<br><br>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)<br><br>Data Security – encompasses both physically protecting the data from unauthorized access as well as loss of data through mechanical/electrical failure or viruses, includes information classification, backup and archive procedures, off-site storage, and audit procedures. |

| ASSOCIATED DOMAIN | |
|---|---|
| *Domain Name* | Security |

## CRITICAL REFERENCES

### *Related Domains/Disciplines*

| *Domain-Disciplines* | | *Domain-Disciplines* | | *Domain-Disciplines* | |
|---|---|---|---|---|---|
| ☐ | *Interface – Branding* | ☐ | *Integration – Functional Integration* | ☐ | *Systems Mgt – Business Continuity* |
| ☒ | *Interface – Access* | ☒ | *Integration – Middleware* | ☐ | *Security – Enterprise Security* |
| ☐ | *Interface – Accessibility* | ☐ | *Application – Application Engineering* | ☒ | *Security – Network Security* |
| ☐ | *Information – Knowledge Mgt* | ☐ | *Application – Electronic Collaboration* | ☒ | *Security – Host Security* |
| ☐ | *Information – Data Mgt* | ☐ | *Systems Mgt – Asset Mgt* | ☐ | *Privacy – Profiling* |
| ☐ | *Information- GIS* | ☐ | *Systems Mgt – Change Mgt* | ☐ | *Privacy – Personification* |
| ☐ | *Infrastructure - Network* | ☐ | *Systems Mgt – Console/Event Mgt* | ☐ | *Privacy – Privacy* |
| ☐ | *Infrastructure - Platform* | ☒ | *Systems Mgt – Help Desk/Problem Mgt* | | |

### *Standards Organizations*

| | | | |
|---|---|---|---|
| *Name* | National Institute of Standards and Technology (NIST) | *Web Address* | http://www.nist.gov/ - NIST Homepage |
| *Contact Information* | **NIST**<br>100 Bureau Drive, Stop 3460<br>Gaithersburg, MD 20899-3460<br>Email: inquiries@nist.gov<br>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**<br>Washington, DC Headquarters<br>1819 L Street, NW, 6th Fl.<br>Washington, DC, 20036<br>Email: info@ansi.org<br>Telephone: 202.293.8020 Fax: 202.293.9287 | | |

### *Government Bodies*

| | | | |
|---|---|---|---|
| *Name* | None Identified | *Web Address* | |
| *Contact Information* | | | |

### *Stakeholders/Roles*

| | |
|---|---|
| *Stakeholders* | |
| *Roles (if stakeholder titles are not known)* | |

### *Discipline-specific Trends*

| | |
|---|---|
| *Trend Statement* | |
| *Trend Source* | |

| METHODOLOGIES | | | |
|---|---|---|---|
| *Methodologies followed* | | | |
| **ASSOCIATED COMPLIANCE COMPONENTS** | | | |
| *Compliance Component Names* | IEEE Std 1363-2000, IEEE Standard Specifications for Public-Key Cryptography<br>FIPS 46-3 October 1999, Data Encryption Standard (DES); specifies the use of Triple DES<br>FIPS 140-2 June 2001, Security requirements for Cryptographic Modules<br>FIPS 186-2 January 2000, Digital Signature Standard (DSS) | | |
| **ASSOCIATED TECHNOLOGY AREAS** | | | |
| *Technology Areas* | User Security<br>Directory Services<br>Application Security<br>System Security<br>Data Security | | |
| **DISCIPLINE DOCUMENTATION REQUIREMENTS** | | | |
| *Documentation requirements for this Discipline* | | | |
| **CURRENT STATUS** | | | |
| *Discipline Status* | ☐ *In development* ☐ *Under Review* ☐ *Rejected* ☒ *Accepted* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | 4/16/2002 | *Date Accepted/Rejected* | |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Reviewed* | | *Last Date Updated* | |
| *Reason for Update* | | | |
| *Updated By* | | | |

Click on this link to return to the Security Blueprint Samples – Set One.

# Technology Area Blueprint

| Definition | |
|---|---|
| *Name* | Technology Area – Directory Services |
| *Description* | A means for managing access to computer resources and keeping track of the users of a network, such as a company's intranet. Directories are repositories of network name knowledge, essential for navigating loosely structured data like the Web. One type of directory common on TCP/IP networks is the Domain Name System (DNS), which is a globally accessible table of domain names and their corresponding IP addresses. |
| *Rationale* | A directory is specialized database optimized for reading, browsing and searching. Directories contain descriptive, attribute-based information and support sophisticated filtering capabilities. Directories are tuned to give quick-response to high-volume lookup or search operations. They may have the ability to replicate information widely in order to increase availability and reliability, while reducing response time. |
| *Benefits* | Applications like e-mail and network management can benefit from more natural directory entries that include, for instance, people's names, type of service, or geographic locale. This is particularly true on the global Internet, where the address space is growing exponentially; but it's increasingly true on wide-area intranets, as well. |
| **Associated Discipline** | |
| *Discipline Name* | Host Security |
| **Keywords** | |
| *Keywords/Aliases* | Authentication, Directory Services |
| **Associated Compliance Components** | |
| *Compliance Component Names* | N/A |
| **Single Product Solution** | |
| *Date of Single Product Solution Determination* | N/A |
| *Rationale for Decision* | N/A |
| **Associated Product Components** | |
| *Product Component Names* | OpenLDAP<br>NDS (Novell Directory Services) |
| **Current Status** | |
| *Technology Area Status* | ☐ *In development* ☐ *Under Review* ☐ *Rejected* ☒ *Accepted* |

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

Click on this link to return to the Security Blueprint Samples – Set One.

# Product Component Blueprint

| DEFINITION | |
|---|---|
| *Name* | Product Component – OpenLDAP |
| *Description* | OpenLDAP Software is an open source implementation of the Lightweight Directory Access Protocol (LDAP).<br><br>The suite includes:<br>• slapd - stand-alone LDAP server<br>• slurpd - stand-alone LDAP replication server<br>• Libraries implementing the LDAP protocol, and<br>• Utilities, tools, and sample clients.<br><br>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.<br><br>Key aspects of LDAP are:<br>• Protocol elements are carried directly over TCP or other transport, bypassing much of the session/presentation overhead.<br>• Many protocol data elements are encoding as ordinary strings (e.g., Distinguished Names).<br>• A lightweight BER encoding is used to encode all protocol elements. |
| *Rationale* | LDAP has been endorsed as the directory protocol of choice by many organizations, including the University of Michigan and Netscape Communications. |
| *Benefits* | LDAP is a lightweight alternative to the X.500 Directory Access Protocol (DAP) for use on the Internet. It uses TCP/IP stack verses the overly complex OSI stack. It also has other simplifications, such as the representing most attribute values and many protocol items as textual strings, which are designed to make clients easier to implement. |

| COMPONENT CLASSIFICATION | | | | |
|---|---|---|---|---|
| *Classification* | ☐ *Emerging* | ☒ *Current* | ☐ *Twilight* | ☐ *Sunset* |
| *Sunset Date* | | | | |
| *Rationale for Classification* | OpenLDAP is currently in use within the organization. | | | |

| ASSOCIATED TECHNOLOGY AREA | |
|---|---|
| *Technology Area* | Directory Services |

| KEYWORDS | |
|---|---|
| *Keywords/Aliases* | LDAP, OpenLDAP, Directory Access, sldap |

| VENDOR INFORMATION | | | |
|---|---|---|---|
| *Vendor Name* | OpenSource | *Web Address* | http://www.openldap.org/ |
| *Contact Information* | Foundation@OpenLDAP.org<br><br>The OpenLDAP Foundation<br>270 Redwood Shores Pkwy, PMB#107<br>Redwood City, California 94065<br>USA | | |
| **POTENTIAL COMPLIANCE ORGANIZATIONS** | | | |
| *Standards Organizations* | | | |
| *Name* | Internet Engineering Task Force (IETF) | *Web Address* | http://www.ietf.org/ |
| *Contact Information* | Contact information is provided per workgroup. See information contained on web site. | | |
| *Government Bodies* | | | |
| *Name* | | *Web Address* | |
| *Contact Information* | | | |
| **ASSOCIATED COMPLIANCE COMPONENTS** | | | |
| *Product* | | | |
| *Product-specific Compliance Components* | OpenLDAP Admin Guide | | |
| *Configurations* | | | |
| *Configuration-specific Compliance Components* | OpenLDAP Admin Guide – 5. The slapd Configuration File | | |
| **COMPONENT REVIEW** | | | |
| *Desirable aspects* | slapd is an LDAP directory server that runs on many different platforms. Some of slapd's features and capabilities include:<br><br>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.<br><br>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.<br><br>Transport Layer Security: slapd provides privacy and integrity protections through the use of TLS (or SSL). slapd's TLS implementation utilizes OpenSSL software.<br><br>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.<br><br>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.<br><br>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.<br><br>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).<br><br>Threads: slapd is threaded for high performance. A single multi-threaded slapd process handles all incoming requests, reducing the amount of system overhead required.<br><br>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.<br><br>Configuration: slapd is highly configurable through a single configuration file, which allows a wide range of change. Configuration options have reasonable defaults, which also makes configuration easier. |
| *Undesirable aspects* | Limitations – The main LDBM database backend does not handle range queries or negation queries very well. These features and more will be coming in a future release. |
| **REQUIRED COMPONENT** | |
| *Business Area, Department or Application Name* | N/A |
| **CONDITIONAL USE RESTRICTIONS** | |
| *Restrictions* | N/A |
| **MIGRATION STRATEGY** | |
| *Strategy/Source Document* | |

| IMPACT POSITION STATEMENT | | | |
|---|---|---|---|
| *Impact Statement* | | | |
| **CURRENT STATUS** | | | |
| *Product Component Status* | ☐ *In development* ☐ *Under Review* ☐ *Rejected* ☒ *Accepted* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | 5/21/2002 | *Date Accepted / Rejected* | |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | |
| *Reason for Update* | | | |
| *Updated By* | | | |

Click on this link to return to the Security Blueprint Samples – Set One.

# Compliance Component Blueprint

| Definition | |
|---|---|
| *Name* | Compliance Component – OpenLDAP Administrator's Guide |
| *Description* | This document describes how to build, configure, and operate OpenLDAP software to provide directory services. |
| *Rationale* | This includes details on how to configure and run the stand-alone LDAP daemon, slapd(8) and the stand-alone LDAP update replication daemon, slurpd(8). |
| *Benefits* | Provides information including, but not limited to:<br>Configuration Choices<br>Building and Installing OpenLDAP Software<br>slapd Configuration<br>Database Creation and Maintenance Tools<br>Schema Specification |

| Component Classification | | | | |
|---|---|---|---|---|
| *Classification* | ☐ *Emerging* | ☒ *Current* | ☐ *Twilight* | ☐ *Sunset* |
| *Sunset Date* | | | | |
| *Rationale for Classification* | Configurations as documented within the Administrator's Guide are currently in use within the organization. | | | |

| Associated Technology Architecture Blueprint Levels | |
|---|---|
| *Discipline Name* | |
| *Technology Area Name* | |
| *Product Component Name* | OpenLDAP |

| Keywords | |
|---|---|
| *Keywords/Aliases* | LDAP, OpenLDAP, sldap |

| Compliance Component Type | | | |
|---|---|---|---|
| *Component Type* | ☒ *Guideline* | ☐ *Standard* | ☐ *Legislation* |
| *Compliance Sub-type* | | | |

| Compliance Detail | | | |
|---|---|---|---|
| *Statement* | OpenLDAP 2.0 Administrator's Guide | | |
| *Source Reference* | http://www.openldap.org/doc/admin/index.html | | |
| *Standards Organization* | | | |
| *Name* | Internet Engineering Task Force (IETF) | *Web Address* | http://www.ietf.org/ |
| *Contact Information* | Contact information is provided per workgroup. See information contain ed on web site. | | |
| *Government Body* | | | |
| *Name* | | *Web Address* | |
| *Contact Information* | | | |

| CONDITIONAL USE RESTRICTIONS | | | |
|---|---|---|---|
| *Restrictions* | N/A | | |
| **MIGRATION STRATEGY** | | | |
| *Strategy/Source Document* | | | |
| **IMPACT POSITION STATEMENT** | | | |
| *Impact Statement* | | | |
| **CURRENT STATUS** | | | |
| *Compliance Component Status* | ☐ *In development* ☐ *Under Review* ☐ *Rejected* ☒ *Accepted* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | 5/20/2002 | *Date Accepted / Rejected* | |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | |
| *Reason for Update* | | | |
| *Updated By* | | | |

Click on this link to return to the Security Blueprint Samples – Set One.

# Discipline Blueprint

| DEFINITION | |
|---|---|
| *Name* | Discipline – Enterprise Security |
| *Description* | Defines the roles, standards, policies, audits, and business process reviews for monitoring and ensuring the security across the organization's enterprise. Includes securing the physical assets from theft and vandalism. |
| *Rationale* | Enterprise security can be an issue with State agencies. Due to lack of proper office space, sensitive equipment is often located outside secured areas. Some of the smaller computer rooms are left unlocked and untended. Take steps to place business critical equipment in secure areas.<br>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.<br>Enterprise Security also covers:<br>• Security Administration – setting, periodic review and testing of policies and the design and analysis of the proposed or existing security systems<br>• Social Engineering/Human Factors – prevent the release of sensitive infrastructure details by employees to unauthorized sources. |

| ASSOCIATED DOMAIN | |
|---|---|
| *Domain Name* | Security Domain |

| CRITICAL REFERENCES | | | | | |
|---|---|---|---|---|---|
| *Related Domains/Disciplines* | | | | | |
| *Domain-Disciplines* | | *Domain-Disciplines* | | *Domain-Disciplines* | |
| ☐ | *Interface – Branding* | ☐ | *Integration – Functional Integration* | ☒ | *Systems Mgt – Business Continuity* |
| ☐ | *Interface – Access* | ☐ | *Integration – Middleware* | ☒ | *Security – Enterprise Security* |
| ☐ | *Interface – Accessibility* | ☐ | *Application – Application Engineering* | ☐ | *Security – Network Security* |
| ☐ | *Information – Knowledge Mgt* | ☐ | *Application – Electronic Collaboration* | ☐ | *Security – Host Security* |
| ☐ | *Information – Data Mgt* | ☒ | *Systems Mgt – Asset Mgt* | ☐ | *Privacy – Profiling* |
| ☐ | *Information- GIS* | ☐ | *Systems Mgt – Change Mgt* | ☐ | *Privacy – Personification* |
| ☐ | *Infrastructure - Network* | ☐ | *Systems Mgt – Console/Event Mgt* | ☐ | *Privacy – Privacy* |
| ☐ | *Infrastructure - Platform* | ☒ | *Systems Mgt – Help Desk/Problem Mgt* | | |

| *Standards Organizations* | |
|---|---|
| *Name* | |
| *Contact Information* | |

| *Government Bodies* | |
|---|---|
| *Name* | |
| *Contact Information* | |

| *Stakeholders/Roles* | |
|---|---|
| *Stakeholders* | Security Personnel<br>Help Desk Personnel<br>Operations Staff<br>Users |
| *Roles (if stakeholder titles are not known)* | |

| *Discipline-specific Trends* | |
|---|---|
| *Trend Statement* | |
| *Trend Source* | |

| METHODOLOGIES | |
|---|---|
| *Methodologies followed* | |

| ASSOCIATED COMPLIANCE COMPONENTS | |
|---|---|
| *Compliance Component Names* | |

| ASSOCIATED TECHNOLOGY AREAS | |
|---|---|
| *Technology Areas* | Physical Security<br>Security Administration<br>Social Engineering/Human Factors |

| DISCIPLINE DOCUMENTATION REQUIREMENTS | |
|---|---|
| *Documentation requirements for this Discipline* | |

| CURRENT STATUS | | | |
|---|---|---|---|
| *Discipline Status* | ☐ *In development* ☐ *Under Review* ☐ *Rejected* ☒ *Accepted* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | 4/15/2002 | *Date Accepted/Rejected* | |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Reviewed* | | *Last Date Updated* | |
| *Reason for Update* | | | |

Click on this link to return to the Security Blueprint Samples – Set One.

# Compliance Component Blueprint

| Definition | |
|---|---|
| *Name* | Work Station Security Policy |
| *Description* | Policies regarding work station security |
| *Rationale* | Guidelines are provided in order to maintain enterprise wide security related to work stations and work station use. |
| *Benefits* | Increased security awareness, protection of enterprise assets include intellectual capital |
| **Associated Architecture Levels** | |
| *Domain Name* | Security |
| *Discipline Name* | Enterprise Security |
| *Technology Area Name* | |
| *Product Component Name* | |
| **Compliance Component Type** | |
| *Component Type* | Policy |
| *Component Sub-type* | |
| **Compliance Detail** | |
| *Policy, Guideline, Standard or Legislation* | 1.0 Overview<br><br>All programmable workstations equipped with fixed storage devices, e.g., hard disks, shall have security policies established and implemented to restrict unauthorized individuals and programs from accessing information and software stored in the workstation and associated peripherals.<br><br>2.0 Mandatory Protection for all Workstations<br><br>All workstations must have adequate controls to provide continued confidentiality, integrity, and availability of data stored on the system. Critical business functions must not reside on workstations unless specifically authorized for that environment. All workstations must employ an approved access control mechanism (e.g., software or hardware) to restrict access to authorized users. Workstations must be configured with screen savers to blank the screen and require a password to resume operation whenever the workstations are unattended. GOT employees and contractors must not leave their workstation unattended without first shutting down the workstation, logging out, or invoking a password-protected screen saver. Unless otherwise notified by systems administrators or the Division of Security Services, GOT employees and contractors are required to shut down and power off their workstation at the end of the workday. The owner of the workstation has ultimate responsibility for the security of the information on their workstation.<br><br>2.1 Protection for Sensitive Workstations<br><br>In addition to the protection required for all workstations, workstations that access sensitive data must use password protection which prevents the rebooting or powering on of the workstation without authentication. Furthermore, workstation equipment must be physically protected to lessen the risks of theft, destruction, and unauthorized access to data. |

| | |
|---|---|
| | 2.2 Resident Protection from Malicious Software<br><br>Workstations must employ approved virus screening programs at all times. If the screening program detects a virus, the users must immediately notify the LAN administrator. Users will NOT attempt to eradicate a virus or use the affected machine until trained personnel have been notified so they may document and address the problem.<br><br>2.3 Erasure of Restricted/Confidential Information<br><br>Sensitive data must be electronically erased from media or overwritten with approved software before the media leaves the business environment. This does not apply to confidential data written to media as part of scheduled backup processes. Due to the wide availability of programs to restore files that were "accidentally" deleted, the erasure of sensitive data must be accomplished by means other than "deleting" the file and as authorized by the Director, Division of Security Services.<br><br>2.4 Workstation/Server/Device Equipped with Modems<br><br>Workstations/servers/devices with modems are not permitted unless approved by the Director, Division of Security Services. For those workstations authorized to have modems, the modem and telecommunication line must be configured to permit outbound dialing only. An auto-answering modem attached to a workstation is an easy target and method to subvert perimeter security (modem banks, Firewalls, etc.) and gain unauthorized access to internal networks.<br><br>2.5 Unattended Workstation Processing<br><br>If workstations are connected to a network and are not performing specialized approved background functions such as monitoring or logging, when unattended, they must always be logged out. Workstation must be shut down and powered off at the end of the day. For specialized workstations that cannot be logged off, measures such as screensavers or physical security access to keyboards must be employed.<br><br>2.6 Supplemental Encryption<br><br>Data that has been identified to be sensitive in nature by the data owner must be encrypted with the aid of approved encryption programs when stored on disks, tapes, or other media. Potential standards and tools are currently under review.<br><br>2.7 Authorized Applications<br><br>Only GOT authorized applications and utilities may be loaded on user workstations. Installing unauthorized applications can impact the performance of the workstation and potentially circumvent security controls implemented by GOT. Unauthorized applications will be removed and the user will be subject to possible disciplinary actions.<br><br>2.8 Workstations that Employ Password Controls<br><br>For workstations that employ operating systems software that have the capability to enact password restrictions, such as Microsoft Windows NT, those capabilities must be configured and enabled. |

| | | | |
|---|---|---|---|
| *Source Reference* | http://csrc.nist.gov/fasp/FASPDocs/security-ate/ISSO-participant-book.doc | | |
| *Standards Organizations* | | | |
| *Name* | National Institute of Standards and Technology (NIST) http://csrc.nist.gov/ | *Website* | csrc.nist.gov |
| *Contact Information* | cert@cert.org | | |
| *Government Body* | | | |
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) | *Website* | http://csrc.nist.gov/ |
| *Contact Information* | inquiries@nist.gov | | |
| KEYWORDS | | | |
| *Keywords/Aliases* | Workstation, security, policy, | | |
| COMPONENT CLASSIFICATION | | | |
| *Classification* | ☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset* | | |
| *Rationale for Component Classification* | | | |
| *Rationale for Component Classification* | | | |
| *Conditional Use Restrictions* | | | |
| *Restrictions* | | | |
| *Migration Strategy* | | | |
| *Migration Strategy* | | | |
| *Impact Position Statement* | | | |
| *Position Statement on Impact* | | | |
| CURRENT STATUS | | | |
| *Current Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |
| AUDIT TRAIL | | | |
| *Creation Date* | 5/19/2004 | *Date Accepted / Rejected* | 5/19/2004 |
| *Reason for Rejection* | | | |
| *Last Date Reviewed* | | *Last Date Updated* | |
| *Reason for Update* | | | |

Click on this link to return to the Security Blueprint Samples – Set One.

# Discipline Blueprint

| Definition | |
|---|---|
| *Name* | Discipline – Network Security |
| *Description* | Defines the roles, standards, policies, and tools for monitoring and ensuring the security across the organization's network. |
| *Rationale* | As enterprise information systems become increasingly decentralized, the responsibility for security becomes distributed across the various operating locations. Therefore, it is essential that all aspects of security, including security policies, procedures, information-system-based controls and network security be coordinated, monitored, audited and enforced. |
| *Benefits* | |

| Boundary | |
|---|---|
| *Boundary Limit Statement* | Network security includes the physical/electrical links between the desktop client and the host computer. This responsibility is generally split between agencies with the user agency and DISC performing part of the functions. In view of this, maintain close cooperation between these groups. The LAN and WAN links must be reviewed and evaluated for security needs. The use of the Internet and dial-up connections to facilitate traveling staff places an additional burden on this analysis; since those links can not be controlled and therefore carry a greater risk of being compromised.<br>The following areas are also covered under Network Security:<br>• Web security – covers firewalls, DMZs, etc.<br>• Electronic Transaction Security- the transmissions into and out of the State's host computers. Includes all types of information sharing: e-mail, file transfer, electronic data interchange, etc. |

| Associated Domain | |
|---|---|
| *Domain Name* | Security |

## Critical References

*Related Domains/Disciplines*

| *Domain-Disciplines* | | *Domain-Disciplines* | | *Domain-Disciplines* | |
|---|---|---|---|---|---|
| ☐ | *Interface – Branding* | ☒ | *Integration – Functional Integration* | ☒ | *Systems Mgt – Business Continuity* |
| ☒ | *Interface – Access* | ☒ | *Integration – Middleware* | ☐ | *Security – Enterprise Security* |
| ☐ | *Interface – Accessibility* | ☐ | *Application – Application Engineering* | ☒ | *Security – Network Security* |
| ☒ | *Information – Knowledge Mgt* | ☐ | *Application – Electronic Collaboration* | ☒ | *Security – Host Security* |
| ☒ | *Information – Data Mgt* | ☐ | *Systems Mgt – Asset Mgt* | ☐ | *Privacy – Profiling* |
| ☒ | *Information- GIS* | ☒ | *Systems Mgt – Change Mgt* | ☐ | *Privacy – Personification* |
| ☒ | *Infrastructure - Network* | ☒ | *Systems Mgt – Console/Event Mgt* | ☐ | *Privacy – Privacy* |
| ☐ | *Infrastructure - Platform* | ☒ | *Systems Mgt – Help Desk/Problem Mgt* | | |

| | | | |
|---|---|---|---|
| *Standards Organizations* | | | |
| *Name* | International Organization for Standardization | *Web Address* | http://www.iso.ch/iso/en/ISOOnline.frontpage |
| *Contact Information* | **ISO Central Secretariat:**<br>International Organization for Standardization (ISO)<br>1, rue de Varembé, Case postale 56<br>CH-1211 Geneva 20, Switzerland<br>Email: central@iso.org<br>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**<br>100 Bureau Drive, Stop 3460<br>Gaithersburg, MD 20899-3460<br>Email: inquiries@nist.gov<br>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**<br>1828 L Street, N.W., Suite 1202<br>Washington, D.C. 20036-5104<br>Email: ieeeusa@ieee.org<br>Tel: +1 202 785 0017 Fax: +1 202 785 0835 | | |
| *Government Bodies* | | | |
| *Name* | None Identified | *Web Address* | |
| *Contact Information* | | | |
| *Stakeholders/Roles* | | | |
| *Stakeholders* | Systems Analysts, Network Personnel, Applications Developer, Applications Testing Team, Third-Party Network Vendors, System Administrators, Security Personnel, Configuration Management Team, Help Desk Personnel | | |
| *Roles (if stakeholder title is not known)* | | | |
| *Discipline-specific Trends* | | | |
| *Trend Statement* | | | |
| *Trend Source* | | | |
| METHODOLOGIES | | | |
| *Methodologies Followed* | | | |
| ASSOCIATED COMPLIANCE COMPONENTS | | | |
| *Compliance Component Names* | Secure Sockets Layer (SSL)<br>Electronic Communications Privacy Act of 1986 (Public Law 99-508)<br>IEEE 802.10-1998, IEEE Standard for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS)<br>IEEE 802.10a-1999, Supplement to 802.10-1998, Standard for Interoperable LAN/MAN Security (SILS) - Security Architecture Framework<br>IEEE 802.10c-1998, Supplement to 802.10-1998, Key management (Clause 3)<br>FIPS 146-2, TCP/IP for wide-area network transmission.<br>RFC 791 as the definition of IP for wide area network transmission.<br>Open Systems Interconnection (OSI) Reference Model (ISO/DIS 7498)<br>Telecommunications Security: Electronic Signature Standardization Report European Telecommunications Standards Institute | | |

| ASSOCIATED TECHNOLOGY AREAS | | | |
|---|---|---|---|
| *Technology Areas* | Network Security<br>Web security<br>Electronic Transaction Security | | |
| **DISCIPLINE DOCUMENTATION REQUIREMENTS** | | | |
| *Documentation requirements for this Discipline* | (This discipline will be documented to the product level and the compliance components associated with the product version, family etc…) | | |
| **CURRENT STATUS** | | | |
| *Discipline Status* | ☐ *In development* ☐ *Under Review* ☐ *Rejected* ☒ *Accepted* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | 4/16/2002 | *Date Accepted/Rejected* | |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | |
| *Reason for Update* | | | |
| *Updated By* | | | |

Click on this link to return to the Security Blueprint Samples – Set One.

## SECURITY BLUEPRINT SAMPLES – SET TWO

The second set of sample Blueprints from a Security Domain represent an additional set of Discipline, Technology Areas and Compliance Components. This sample addresses the Disciplines of Management, Operational and Technical Controls. The Security Domain Blueprint has not been repeated.

- Discipline – Management Controls
- Discipline – Operational Controls
- Technology Area – Incident Response
- Compliance Component – Incident Response Reporting
- Compliance Component – Risk Level Awareness & Countermeasures
- Discipline – Technical Controls
- Technology Area – Identification/Authentication
- Compliance Component – Password Controls
- Technology Area – Virus Detection & Elimination
- Compliance Component – Criteria for E-Mail
- Compliance Component – Criteria for Gateways
- Compliance Component – Criteria for Server
- Compliance Component – Criteria for Workstation
- Compliance Component – Criteria for Wireless
- Technology Area – Intrusion Detection Systems
- Compliance Component – Network Based IDS
- Compliance Component – Host Based IDS
- Compliance Component – Application Based IDS
- Technology Area – Logical Access Controls
- Compliance Component – Date/Time Controls
- Compliance Component – Inactivity Controls
- Compliance Component – Logon Banners

| *Domain* | *Discipline* | *Technology Area* | *Product Component* | *Compliance Component* |
|---|---|---|---|---|
| Security | Management Controls | | | |
| | Operational Controls | Incident Response | | • Incident Response Reporting<br>• Risk Level Awareness & Countermeasures |
| | Technical Controls | Identification / Authentication | | • Password Controls |
| | | Virus Detection & Elimination | | • Criteria for E-Mail<br>• Criteria for Gateways<br>• Criteria for Server<br>• Criteria for Workstation<br>• Criteria for Wireless |
| | | Intrusion Detection Systems | | • Network Based IDS<br>• Host Based IDS<br>• Application Based IDS |
| | | Logical Access Controls | | • Date/Time Controls<br>• Inactivity Controls<br>• Logon Banners |

Again, a reminder that some of the sample Blueprints were completed using earlier versions of the templates and, while the information that was gathered is the same, it may be presented in a slightly different order or have a slightly different heading or topic title than the latest template versions, which were presented earlier within this document.

# Discipline Blueprint

| Definition | |
|---|---|
| *Name* | Discipline – Management Controls |
| *Description* | Management Controls are techniques and concerns, normally addressed by management, regarding the organization's computer security strategy. It includes the mitigation of risk within the organization. |
| *Rationale* | Addresses security within a business context and provides implementation authority. |
| *Benefits* | Promotes trust, maintains continuous business flow, provides guidance |
| **Boundary** | |
| *Boundary Limit Statement* | Security controls that focus on the management of the enterprise security programs and managing security risks. |
| *Boundary Topics* | Life Cycle Management;<br>Risk Management;<br>Review of Security Controls;<br>System Certification and Accreditation;<br>System Security Planning;<br>Personnel Security |
| **Associated Domain** | |
| *Domain Name* | Security |

## Critical References

*Related Domains/Disciplines*

| | | | | | |
|---|---|---|---|---|---|
| ☐ | *Interface – Branding* | ☐ | *Integration – Functional Integration* | ☐ | *Systems Mgt – Business Continuity* |
| ☐ | *Interface – Access* | ☐ | *Integration – Middleware* | ☒ | *Security – Management Controls* |
| ☐ | *Interface – Accessibility* | ☐ | *Application – Application Engineering* | ☒ | *Security – Operational Controls* |
| ☐ | *Information – Knowledge Mgt* | ☐ | *Application – Electronic Collaboration* | ☒ | *Security – Enterprise Security* |
| ☐ | *Information – Data Mgt* | ☐ | *Systems Mgt – Asset Mgt* | ☒ | *Security – Network Security* |
| ☐ | *Information- GIS* | ☐ | *Systems Mgt – Change Mgt* | ☒ | *Security – Host* |
| ☐ | *Infrastructure - Network* | ☐ | *Systems Mgt – Console/Event Mgt* | ☐ | *Privacy – Profiling* |
| ☐ | *Infrastructure - Platform* | ☐ | *Systems Mgt – Help Desk/Problem Mgt* | ☐ | *Privacy – Personification* |
| | | | | ☐ | *Privacy – Privacy* |

*Standards Organizations/Government Bodies*

| | | | |
|---|---|---|---|
| *Standards Organizations* | National Institute of Standards & Technology (NIST) Computer Security Resource Center<br><br>International Organization for Standardization (ISO) | *Web Address* | http://csrc.nist.gov/<br><br>http://www.iso.ch/iso/en/ISOOnline.frontpage |
| *Government Bodies* | NSA, FBI, Department of Homeland Security | | |

| Stakeholders/Roles | | | |
|---|---|---|---|
| *Stakeholders* | Executive Management – Department Director, Department CIO, Department CFO, etc. | | |
| *Roles* | Decision makers; administrative authority | | |
| *Discipline-specific Trends* | | | |
| *Trend Statement* | | | |
| *Trend Source* | | | |
| METHODOLOGIES | | | |
| *Methodologies followed* | National Institute of Standards and Technologies (NIST), Computer Security Resource Center | | |
| ASSOCIATED COMPLIANCE COMPONENTS | | | |
| *Compliance Component Names* | | | |
| ASSOCIATED TECHNOLOGY AREAS | | | |
| *Technology Areas* | Information Classification;<br>Personnel Security;<br>Security Risk Management;<br>Vulnerability Testing | | |
| DISCIPLINE DOCUMENTATION REQUIREMENTS | | | |
| *Documentation requirements for this Discipline* | | | |
| CURRENT STATUS | | | |
| *Discipline Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |
| AUDIT TRAIL | | | |
| *Creation Date* | 12-19-2002 | *Date Accepted / Rejected* | 01-21-2003 |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | |
| *Reason for Update* | | | |
| *Updated By* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

# Discipline Blueprint

| Definition | |
|---|---|
| *Name* | Discipline – Operational Controls |
| *Description* | Operational Controls are procedures implemented and executed by people, as opposed to systems, to improve the security of a system or group of systems. They often require technical or specialized expertise and may rely upon management activities as well as technical controls. |
| *Rationale* | Provides consistent controls to secure the enterprise. |
| *Benefits* | Promotes standardization, structure, and consistent behavior;<br>Defines responsibilities related to security operations. |
| **Boundary** | |
| *Boundary Limit Statement* | Controls implemented and executed by people, including policies and procedures |
| *Boundary Topics* | Physical Security;<br>Production, Input/Output Controls;<br>Contingency Planning;<br>Hardware & Systems Security Software Maintenance;<br>Data Verification;<br>Security Documentation;<br>Security Awareness, Training & Education;<br>Incident Response Capability |
| **Associated Domain** | |
| *Domain Name* | Security |

## Critical References

*Related Domains/Disciplines*

| | | | | | |
|---|---|---|---|---|---|
| ☐ | *Interface – Branding* | ☐ | *Integration – Functional Integration* | ☐ | *Systems Mgt – Business Continuity* |
| ☐ | *Interface – Access* | ☐ | *Integration – Middleware* | ☒ | *Security – Management Controls* |
| ☐ | *Interface – Accessibility* | ☐ | *Application – Application Engineering* | ☒ | *Security – Operational Controls* |
| ☐ | *Information – Knowledge Mgt* | ☐ | *Application – Electronic Collaboration* | ☒ | *Security – Enterprise Security* |
| ☐ | *Information – Data Mgt* | ☐ | *Systems Mgt – Asset Mgt* | ☒ | *Security – Network Security* |
| ☐ | *Information- GIS* | ☐ | *Systems Mgt – Change Mgt* | ☐ | *Security – Host* |
| ☐ | *Infrastructure – Network* | ☐ | *Systems Mgt – Console/Event Mgt* | ☐ | *Privacy – Profiling* |
| ☐ | *Infrastructure – Platform* | ☐ | *Systems Mgt – Help Desk/Problem Mgt* | ☐ | *Privacy – Personification* |
| | | | | ☐ | *Privacy – Privacy* |
| | | | | | |

*Standarda Organizations*

| | | | |
|---|---|---|---|
| *Name* | National Institute of Standards & Technology (NIST)<br>Computer Security | *Web Address* | http://csrc.nist.gov/ |

| | | | |
|---|---|---|---|
| | Resource Center | | |
| *Name* | International Organization for Standardization (ISO) | *Web Address* | http://www.iso.ch/iso/en/ISOOnline.frontpage |
| *Name* | SysAdmin, Audit, Network, Security (SANS) | *Web Address* | http://www.sans.org/newlook/home.php |
| *Government Bodies* | | | |
| *Government Bodies* | HIPPA, DOT, local government | | |
| *Stakeholders/Roles* | | | |
| *Stakeholders* | System Administrators; security officers; facility managers | | |
| *Roles* | Implementers | | |
| *Discipline-specific Trends* | | | |
| *Trend Statement* | | | |
| *Trend Source* | | | |
| METHODOLOGIES | | | |
| *Methodologies followed* | National Institute of Standards & Technology (NIST), Computer Security Resource Center | | |
| ASSOCIATED COMPLIANCE COMPONENTS | | | |
| *Compliance Component Names* | | | |
| ASSOCIATED TECHNOLOGY AREAS | | | |
| *Technology Areas* | Authorization;<br>Data Verification;<br>Event Monitoring/Analysis;<br>Fire/Safety Factors / Supporting Utilities;<br>Incident Response;<br>Message Authentication;<br>Password Policy Controls;<br>Penetration Testing;<br>Physical Access Control;<br>Portable System Controls (Phys Access);<br>Security Awareness;<br>Security Education;<br>Security Skills Training / Certification;<br>Virus Detection & Elimination | | |
| DISCIPLINE DOCUMENTATION REQUIREMENTS | | | |
| *Documentation requirements for this Discipline* | | | |
| CURRENT STATUS | | | |
| *Discipline Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |

| AUDIT TRAIL | | | |
|---|---|---|---|
| *Creation Date* | 12-19-2002 | *Date Accepted / Rejected* | 01-21-2003 |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | |
| *Reason for Update* | | | |
| *Updated By* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

# Technology Area Blueprint

| Definition | | | |
|---|---|---|---|
| *Name* | Technology Area - Incident Response | | |
| *Description* | Incident Response capability is a combination of technically skilled people, policies, procedures, and techniques that constitute a proactive approach to handling computer security incidents. | | |
| *Rationale* | Provides a consistent approach to handling security incidents. | | |
| *Benefits* | Consistent method of evaluation and associate metrics; decrease spread; minimize damage; fulfills risk mitigation; limits impacts; promotes awareness; proactively improves network assurance; increases communication | | |
| **Associated Dicipline** | | | |
| *Discipline Name* | Operational Controls | | |
| **Keywords** | | | |
| *Keywords/Aliases* | Incident reporting; intrusion detection; exposure; vulnerability; INFOCON; attack; incident impacts; defense; threat; risk; alerts; countermeasure; communication; denial of service | | |
| **Associated Compliance Components** | | | |
| *Compliance Component Names* | ❑ Incident Reporting Procedures<br>❑ Incident Risk Level Assessment and Countermeasures | | |
| **Associated Product Components** | | | |
| *Product Component Names* | | | |
| **Technology Area Detail** | | | |
| *Supporting Documentation* | NIST Special Publication: SP-800-3 Establishing a Computer Security Incident Response Capability (CSIRC) – November 1991 | | |
| *Source Reference* | http://csrc.nist.gov/publications/nistpubs/800-3/800-3.pdf | | |
| *Standards Organization / Government Body* | | | |
| *Name* | NIST | *Website* | http://www.nist.gov/ |
| *Contact Information* | National Institute of Standards and Technology<br>(301) 975-NIST | | |
| **Current Status** | | | |
| *Technology Area Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |
| **Audit Trail** | | | |
| *Creation Date* | 12-19-2002 | *Date Accepted / Rejected* | 01-21-2003 |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | |
| *Reason for Update* | | | |
| *Updated By* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

# Compliance Component Blueprint

| Definition | |
|---|---|
| *Name* | Compliance Component - Incident Response Reporting |
| *Description* | Plan and procedures to help ensure the State's IT community is aware of information security threats and concerns. Plan and Procedures should record and document the following:<br>• Attempts (failed or successful) to gain unauthorized access to systems or data;<br>• Unwanted disruption or denial of service;<br>• The unauthorized use of a system for the transmission, processing or storage of data;<br>• Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction or consent. |
| *Rationale* | Minimizes the damage from security incidents and facilitates communication throughout State agencies. |
| *Benefits* | Promotes awareness of incidents; allows for monitoring; builds knowledge base – collecting the right information enables the creation of useful reports (big picture/patterns); standardization |

| Associated Architecture Levels | | | |
|---|---|---|---|
| *Domain Name* | Security | | |
| *Discipline Name* | Operational Controls | | |
| *Technology Area Name* | Incident Response | | |
| *Product Component Name* | | | |

| Compliance Component Type | | | |
|---|---|---|---|
| *Component Type* | Guideline | | |
| *Component Sub-type* | | | |

| Compliance Detail | | | |
|---|---|---|---|
| *Guideline, Standard or Legislation* | State Incident Response Plan and Procedures | | |
| *Source Reference* | | | |
| *Standards Organization* | | | |
| *Name* | OA Information Security Management Office (ISMO) | *Website* | |
| *Contact Information* | | | |
| *Government Body* | | | |
| *Name* | Information Technology Advisory Board (ITAB) | *Website* | |
| *Contact Information* | Security Committee | | |

| Keywords | |
|---|---|
| *Keywords/Aliases* | INFOCON; intrusion detection; exposure; vulnerability; attack; incident impacts; defense; threat; risk; alerts; communication; denial of service |

| Component Classification | | | | |
|---|---|---|---|---|
| *Classification* | ☐ *Emerging* | ☒ *Current* | ☐ *Twilight* | ☐ *Sunset* |

| Rationale for Component Classification | | | |
|---|---|---|---|
| *Rationale for Component Classification* | Currently the active plan and procedures authorized by Information Technology Advisory Board. | | |
| *Conditional Use Restrictions* | | | |
| *Restrictions* | | | |
| *Migration Strategy* | | | |
| *Migration Strategy* | | | |
| *Impact Position Statement* | | | |
| *Position Statement on Impact* | | | |
| CURRENT STATUS | | | |
| *Current Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |
| AUDIT TRAIL | | | |
| *Creation Date* | 12-19-2002 | *Date Accepted / Rejected* | 01-21-2003 |
| *Reason for Rejection* | | | |
| *Last Date Reviewed* | | *Last Date Updated* | |
| *Reason for Update* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

# Compliance Component Blueprint

| DEFINITION | |
|---|---|
| *Name* | Compliance Component - Incident Risk Level Awareness, Assessment and Countermeasures |
| *Description* | Actions to uniformly heighten or reduce defensive posture, to defend against computer network attacks, and to mitigate sustained damage to the State information infrastructure, including computer and telecommunications networks and systems. This is a comprehensive defense posture and protocol based on the status of information systems, sustaining operations, and intelligence assessments of adversary capabilities and intent. |
| *Rationale* | Incidents impact all personnel who use State information systems. Awareness, assessment, and countermeasures protect systems while supporting mission accomplishment, and coordinate the overall effort through adherence to guidelines. |
| *Benefits* | The State gains standard processes for assessing threats to the information infrastructure, and prescribes predictable responsive actions. When implemented consistently, each member of the State's enterprise will have reasonable assurance that other members of the network present no greater vulnerability than the defined baseline standards.<br><br>Provides an opportunity for the technology community to make senior management aware there is a constant battle to maintain network security, and that the entire State government is moving proactively to improve network assurance. |

| ASSOCIATED ARCHITECTURE LEVELS | | | |
|---|---|---|---|
| *Domain Name* | Security | | |
| *Discipline Name* | Operational Controls | | |
| *Technology Area Name* | Incident Response | | |
| *Product Component Name* | | | |
| **COMPLIANCE COMPONENT TYPE** | | | |
| *Component Type* | Standard | | |
| *Component Sub-type* | | | |
| **COMPLIANCE DETAIL** | | | |
| *Guideline, Standard or Legislation* | INFOCON (INFormation Operations CONdition) System for State Agencies -- Nov 19, 2002 | | |
| *Source Reference* | | | |
| *Standards Organization* | | | |
| *Name* | Information Technology Advisory Board (ITAB) | *Website* | |
| *Contact Information* | Security Committee | | |
| *Government Body* | | | |
| *Name* | | *Website* | |
| *Contact Information* | | | |
| **KEYWORDS** | | | |
| *Keywords/Aliases* | INFOCON; countermeasure; incident reporting; intrusion detection; exposure; vulnerability; attack; incident impacts; defense; threat; risk; alerts; risk level | | |

| COMPONENT CLASSIFICATION | | | |
|---|---|---|---|
| *Classification* | ☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset* | | |
| *Rationale for Component Classification* | | | |
| *Rationale for Component Classification* | Established by the State Office of Information Technology (OIT), with the consensus of the Office of Homeland Security (OHS), at the recommendation of the Information Technology Advisory Board (ITAB). | | |
| *Conditional Use Restrictions* | | | |
| *Restrictions* | N/A | | |
| *Migration Strategy* | | | |
| *Migration Strategy* | N/A | | |
| *Impact Position Statement* | | | |
| *Position Statement on Impact* | | | |
| CURRENT STATUS | | | |
| *Current Status*) | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |
| AUDIT TRAIL | | | |
| *Creation Date* | 12-19-2002 | *Date Accepted / Rejected* | 01-21-2003 |
| *Reason for Rejection* | | | |
| *Last Date Reviewed* | | *Last Date Updated* | |
| *Reason for Update* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

# Discipline Blueprint

| DEFINITION | |
|---|---|
| *Name* | Discipline - Technical Controls |
| *Description* | Technical Controls are security controls executed by computer systems, as opposed to people. The implementation of technical controls requires significant operational consideration and should be consistent with the management of security within the organization. |
| *Rationale* | Identifies automated controls that improve system security. |
| *Benefits* | Promotes standardization, trust, interoperability, connectivity, automation, and increased efficiency. |
| **BOUNDARY** | |
| *Boundary Limit Statement* | Security controls implemented and executed by systems and/or machines. |
| *Boundary Topics* | Identification and Authentication;<br>Logical Access Controls;<br>Audit Trails |
| **ASSOCIATED DOMAIN** | |
| *Domain Name* | Security |

**CRITICAL REFERENCES**

*Related Domains/Disciplines*

| | | | | | |
|---|---|---|---|---|---|
| ☐ | *Interface – Branding* | ☐ | *Integration – Functional Integration* | ☐ | *Systems Mgt – Business Continuity* |
| ☐ | *Interface – Access* | ☐ | *Integration – Middleware* | ☒ | *Security – Management Controls* |
| ☐ | *Interface – Accessibility* | ☐ | *Application – Application Engineering* | ☒ | *Security – Operational Controls* |
| ☐ | *Information – Knowledge Mgt* | ☐ | *Application – Electronic Collaboration* | ☒ | *Security – Technical Controls* |
| ☐ | *Information – Data Mgt* | ☐ | *Systems Mgt – Asset Mgt* | ☐ | *Privacy – Profiling* |
| ☐ | *Information- GIS* | ☐ | *Systems Mgt – Change Mgt* | ☐ | *Privacy – Personification* |
| ☐ | *Infrastructure - Network* | ☐ | *Systems Mgt – Console/Event Mgt* | ☐ | *Privacy – Privacy* |
| ☐ | *Infrastructure - Platform* | ☐ | *Systems Mgt – Help Desk/Problem Mgt* | | |

| *Standards Organizations/Government Bodies* | |
|---|---|
| *Standards Organizations* | National Institute of Standards & Technology (NIST)<br>Computer Security Resource Center<br>http://csrc.nist.gov/<br>International Organization for Standardization (ISO)<br>http://www.iso.ch/iso/en/ISOOnline.frontpage<br>SysAdmin, Audit, Network, Security (SANS)<br>http://www.sans.org/newlook/home.php |
| *Government Bodies* | |
| *Stakeholders/Roles* | |
| *Stakeholders* | Network Administrators, CIT, CIS, etc. |
| *Roles* | Technical personnel |

| Discipline-specific Trends | | | |
|---|---|---|---|
| *Trend Statement* | | | |
| *Trend Source* | | | |
| **METHODOLOGIES** | | | |
| *Methodologies followed* | National Institute of Standards & Technology (NIST), Computer Security Resource Center | | |
| **ASSOCIATED COMPLIANCE COMPONENTS** | | | |
| *Compliance Component Names* | | | |
| **ASSOCIATED TECHNOLOGY AREAS** | | | |
| *Technology Areas* | Access Controls;<br>Cryptography;<br>Date / Time Controls;<br>Entity Authentication;<br>Intrusion Detection Systems;<br>Inactivity Controls;<br>Log-on Banners;<br>Remote Access;<br>Secure Gateways / Firewalls | | |
| **DISCIPLINE DOCUMENTATION REQUIREMENTS** | | | |
| *Documentation requirements for this Discipline* | | | |
| **CURRENT STATUS** | | | |
| *Discipline Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | 12-19-2002 | *Date Accepted / Rejected* | 01-21-2003 |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | |
| *Reason for Update* | | | |
| *Updated By* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

# Technology Area Blueprint

| Definition | |
|---|---|
| *Name* | Technology Area - Identification and Authentication |
| *Description* | Identification and Authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system.<br><br>Identification is a unique way of identifying each individual (e.g., a unique user name or ID).<br><br>Authentication is the mechanism that verifies that an individual is who they claim to be. Verification is based on one or more of the following:<br>• Something known (e.g., a password or pin);<br>• Something carried (e.g., a smart card or a token);<br>• Something the individual is (e.g., biometrics – like a fingerprint). |
| *Rationale* | Hardware platforms, operating systems, application-specific constraints, and overall financial or confidentiality risk are factors that influence the need for identification and authentication controls.<br><br>System and application developers are responsible for designing strong authentication into the systems they build, and individual users are responsible for assisting in the protection of the systems they use.<br><br>Identification and Authentication are the first lines of defense to protect enterprise system assets from unauthorized access, destruction or theft. |
| *Benefits* | • If identification and authentication are not handled correctly, they are the weakest link in the protection of enterprise systems and data.<br>• Identification and authentication provides user accountability and auditable trails of user access.<br>• Identification and authentication helps prevent unauthorized persons from entering enterprise IT systems. |
| **Associated Discipline** | |
| *Discipline Name* | Technical Controls |
| **Keywords** | |
| *Keywords/Aliases* | Passwords, password controls, digital signatures, access cards, smart cards, tokens, biometrics, user name, user ID, PIN, logon ID |
| **Associated Compliance Components** | |
| *Compliance Component Names* | • Password Controls |
| **Associated Product Components** | |
| *Product Component Names* | |
| **Technology Area Detail** | |
| *Supporting Documentation* | NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems |
| *Source Reference* | www.csrc.nist.gov/publications/nistpubs |
| *Standards Organization / Government Body* | |

| | | | |
|---|---|---|---|
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) | *Website* | http://csrc.nist.gov/ |
| *Contact Information* | inquiries@nist.gov | | |
| *Name* | National Security Agency (NSA), Security Recommendation Guides | *Website* | http://nsa2.www.conxion.com/index.html |
| *Contact Information* | W2KGuides@nsa.gov | | |
| **CURRENT STATUS** | | | |
| *Technology Area Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | 02/13/2003 | *Date Accepted / Rejected* | 03/24/2003 |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | |
| *Reason for Update* | | | |
| *Updated By* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

# Compliance Component Blueprint

| Definition | |
|---|---|
| *Name* | Compliance Component - Password Controls |
| *Description* | Password Controls apply to information technology systems and processes that create, modify, or use information that is private/confidential or of significant value to the organization. All such systems shall adhere to the minimum acceptable standards for system authentication by means of a password.<br><br>A password is a sequence of characters obtained by a selection or generation process from a set of acceptable controls. |
| *Rationale* | A login ID with a secret password is the most common method of authenticating users to a computer system or application, and often the only technical control employed.<br><br>For systems that rely upon password protection, system administrators shall institute strong password controls, and users shall be responsible for creating strong passwords and keeping them secret. |
| *Benefits* | • Password controls provide a method to authenticate users.<br>• Passwords represent a first line of defense, and if not handled correctly, they can be the weakest link in the enterprise.<br>• Strong password controls reduce the threat of password compromise as an avenue of attack on computer resources.<br>• Password controls help prevent unauthorized persons from entering IT systems.<br>• Password Controls provide user accountability. |

| Associated Architecture Levels | |
|---|---|
| *Domain Name* | Security |
| *Discipline Name* | Technical Controls |
| *Technology Area Name* | Identification and Authentication |
| *Product Component Name* | |

| Compliance Component Type | |
|---|---|
| *Compliance Component Type* | Guideline |
| *Component Sub-type* | |

| Compliance Detail | |
|---|---|
| *Guideline, Standard or Legislation* | **Password Control Guidelines**<br>Systems that do not support external identification and authentication via an application-programming interface, or do not natively support the minimum password controls outlined in these guidelines, shall be considered candidates for upgrade or replacement.<br><br>**General Password Requirements**<br>• All enterprise systems and applications shall utilize, as a minimum form of security, a unique user identifier and a secret password as a means of authentication.<br>• Internal network devices (routers, firewalls, access control servers, etc.) shall be password protected.<br>• Default system or device passwords must be changed.<br>• Passwords shall not be hard coded into software unless they are encrypted. |

- All enterprise systems should provide automated support of password controls.
- Passwords issued initially or reset by systems or administrators shall be uniquely defined for each user.
- Proof of identity shall be presented to the administrator for user password resets, such as photo ID, supervisor verification, or knowledge of a shared secret.
- If intervention is required, only administrators are authorized to reset, change or disable user passwords.
- Password resets or changes shall be promptly confirmed with the user. The confirmation method is at the discretion of each agency (e.g., phone, e-mail, registered mail, etc.).
- Passwords shall be changed after a system compromise or after the threat of a system compromise, such as the termination of a system administrator, security level change, etc.
- Users shall promptly change all passwords if they suspect or know unauthorized parties received the passwords or they have shared it in the course of getting help with a problem.
- Passwords shall be different for State (internal) and non-State (external) networks and systems, such as local ISP.
- Restricted public access systems or machines that have no access to critical State systems or data are exemptions to State password controls.

**Password Composition Requirements**

*Passwords are made up of various characters, which can be broken down into four character groups. These are uppercase alphabetic, lowercase alphabetic, numeric, and special characters. Requiring complex passwords also increases the time necessary to crack passwords exponentially.*

- Passwords for all systems are subject to the following password composition rules:
  - Password shall contain characters from at least three of the following four categories:
    - English Uppercase Alphabetic (A - Z)
    - English Lowercase Alphabetic (a - z)
    - Numeric Base-ten digits (0 – 9)
    - Special characters (e.g., exclamation point [!], dollar sign [$], pound sign [#], percent sign [%], asterisk [*], etc.)
    - Passwords are not to be your name, address, date of birth, username, nickname, or any term that could be easily guessed by someone who is familiar with you.
    - Passwords are not to be related to the job or personal life, e.g., not a license plate number, spouse's name, telephone number, etc.
    - Passwords are not to be dictionary words or proper names, places or slang.
    - Passwords may not contain all or part (3 or more sequential characters) of the user's account or login name.
    - Passwords shall not contain characters that do not change combined with characters that predictably change when changing passwords upon expiration. For example, users may not choose passwords like "x345JAN" in January, "x345FEB" in February, etc., or identical or substantially similar to passwords the user previously chose.

**Password Lifetime Requirements**

The purpose for requiring password lifetime restrictions is to prevent users from using their favorite password until it expires, and changing their password more

| | |
|---|---|
| | times than the system remembers, and cycling back to their favorite password, thus circumventing the system.<br><br>• Passwords for all systems are subject to the following password aging and history rules:<br>– Password age shall not exceed 90 days. However, passwords should be changed on a more frequent basis commensurate with the sensitivity, criticality and value of the information it protects.<br>– Administrator password age shall not exceed 60 days.<br>– Any default or initial password issued by a security administrator shall be valid only for the user's first logon session.<br>– Systems shall maintain an encrypted history of previously used passwords per logon ID.<br>– Password history files should contain, at a minimum, the last 24 passwords particular to a logon ID to ensure that users do not cycle through regular passwords.<br>– The minimum password age is 1 day (24 hours).<br><br>**Password Length Requirements**<br>*A 7-character password made up of only lowercase characters has $26^7$ possible passwords. A 7 character password made up of uppercase, lowercase, and special characters (on a standard 104 key keyboard) has 95 possible keys (excluding control characters) that make for $95^7$ possible password combinations. That's nearly the "simple" set of passwords to the power of four!*<br><br>• All passwords shall be at least 7 characters in length.<br>• Passwords that do not comply with the frequency portion of the Password Lifetime Requirements above, such as system service passwords, shall be at least 14 characters in length.<br><br>**Password Source Requirements**<br>• Only end-users or automated processes shall generate passwords.<br><br>**Password Ownership Requirements**<br>• Passwords for all systems are subject to the following password ownership rules:<br>– Users shall not disclose their password to anyone.<br>– No passwords are to be spoken, written, e-mailed, hinted at, shared, or in any way known to anyone other than the user involved.<br>– User-initiated password changes shall be supported on enterprise networks and systems.<br><br>**Password Storage Requirements**<br>• Passwords for all State IT systems are subject to the following password storage rules:<br>– Personnel shall not record their passwords unless they have a secure method of storing them, such as saving them in an encrypted file or storing them in a locked safe.<br>– Passwords area not to be displayed or concealed at the user's workspace.<br>– Passwords shall not be stored in dial-up communications programs or Internet browsers.<br>– Passwords stored and transmitted over open networks shall be encrypted.<br><br>**Password Entry Requirements**<br>*One method of gaining access to a computer system is to continuously access systems, using common account names, and different passwords until one works.* |

| | | | |
|---|---|---|---|
| | *Dictionary attacks use lists of common words as passwords in attempts to logon to a system. They are often successful against weak passwords. Brute force attacks attempt to use every possible character combination as a password, and will always be successful given enough time.*<br><br>*In order to combat these attacks, password entry requirements are established to disable an account after a specified number of failed logins occurs during a defined period of time. That account will remain locked out for a defined period of time. Enabling lockout policies make these attacks mathematically infeasible.*<br><br>• After a maximum of five invalid password or unsuccessful access attempts, one of the following actions shall be enforced:<br>– Disable or revoke the account until intervention by a system administrator.<br>– Suspend the account for at least 30 minutes.<br>– Disconnect if dial-up or other external network connection.<br><br>**Password Auditing Requirements**<br>• An authorized system administrator shall audit all passwords to ensure compliance with password guidelines. | | |
| *Source Reference* | N/A | | |
| *Standards Organizations* | | | |
| *Name* | | *Website* | |
| *Contact Information* | | | |
| *Government Body* | | | |
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) | *Website* | http://csrc.nist.gov/ |
| *Contact Information* | inquiries@nist.gov | | |
| *Name* | National Security Agency (NSA), Security Recommendation Guides | *Website* | http://nsa2.www.conxion.com/index.html |
| *Contact Information* | W2KGuides@nsa.gov | | |
| KEYWORDS | | | |
| *Keywords/Aliases* | Passwords, password controls, digital signatures, access cards, smart cards, tokens, biometrics, user name, user ID, PIN, logon ID, dial-up, lost, forgotten | | |
| COMPONENT CLASSIFICATION | | | |
| *Classification* | ☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset* | | |
| *Rationale for Component Classification* | | | |
| *Rationale for Component Classification* | | | |
| *Conditional Use Restrictions* | | | |
| *Restrictions* | | | |
| *Migration Strategy* | | | |
| *Migration Strategy* | | | |
| *Impact Position Statement* | | | |

| | | | |
|---|---|---|---|
| *Position Statement on Impact* | | | |
| **CURRENT STATUS** | | | |
| *Current Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | 02-13-2003 | *Date Accepted / Rejected* | 03-24-2003 |
| *Reason for Rejection* | | | |
| *Last Date Reviewed* | | *Last Date Updated* | |
| *Reason for Update* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

| Definition | |
|---|---|
| *Name* | Technology Area - Virus Detection and Elimination |
| *Description* | Virus Detection and Elimination addresses those policies, methods and tools associated with detecting, combating, reporting and eradicating malicious program code (e.g., worms, Trojan horse, malware).<br><br>A virus usually has a destructive or disruptive effect on the executable program or system component that it affects. |
| *Rationale* | Provide a scalable multi-tiered defense to fend off virus threats and prevent loss of time and money. |
| *Benefits* | Protect assets (i.e., data and resources) from corruption, disruption, destruction, and unavailability. Can assist in the system quarantine, repair and clean-up virus damage. |
| **Associated Discipline** | |
| *Discipline Name* | Technical Controls |
| **Keywords** | |
| *Keywords/Aliases* | virus, zoo, trojan horse, backdoor, worm, stealth, blended threat, boot sector infector, companion, denial of service, dropper, file infector, logic bomb, malware, multi-partite, overwriting, parasitic, polymorphic, tunneling, variant, terminate and stay resident (tsr), management; boot sector infector |
| **Associated Compliance Components** | |
| *Compliance Component Names* | • Virus Detection and Elimination Policies and Best Practices<br>• Virus Detection and Elimination Criteria for Anti-Virus Management Tools<br>• Virus Detection and Elimination Criteria for Gateways<br>• Virus Detection and Elimination Criteria for E-mail/Groupware<br>• Virus Detection and Elimination Criteria for Servers<br>• Virus Detection and Elimination Criteria for Workstations<br>• Virus Detection and Elimination Criteria for Wireless |
| **Associated Product Components** | |
| *Product Component Names* | • McAfee<br>– VirusScan (workstation)<br>– NetShield (server)<br>– Groupshield (e-mail)<br>– WebShield Appliances(gateway)<br>– EPolicy Orchestrator (management tool)<br>– VirusScan Wireless Devices (wireless)<br>• Symantec<br>– AntiVirus Corporate Edition (workstation)<br>– AntiVirus Corporate Edition (server)<br>– AntiVirus Corporate Edition (e-mail)<br>– AntiVirus Corporate Edition (gateway)<br>– AntiVirus Corporate Edition (management tool)<br>• Sybari Software Inc.<br>– Antigen for Microsoft Exchange (e-mail)<br>– Antigen for Lotus Notes/Domino (e-mail)<br>○ Antigen for Microsoft Exchange (gateway)<br>• Computer Associates<br>– InoculateIT (workstation) |

| | | | |
|---|---|---|---|
| | - InoculateIT (server)<br>- InoculateIT (management tool) | | |
| **TECHNOLOGY AREA DETAIL** | | | |
| *Supporting Documentation* | • NIST 800-5 and 500-1166<br>• Gartner Research Group – Enterprise Anti-Virus product evaluation. Release Note 22 May 2002 | | |
| *Source Reference* | | | |
| *Standards Organizations / Government Body* | | | |
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) | *Website* | http://csrc.nist.gov/ |
| *Contact Information* | inquiries@nist.gov | | |
| *Name* | ICSA Labs | *Website* | www.icsalabs.com |
| *Contact Information* | ICSA Labs is a division of TruSecure Corporation and can be reached at 1-888-396-8348 (info@trusecure.com) | | |
| **CURRENT STATUS** | | | |
| *Technology Area Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | 02-06-03 | *Date Accepted / Rejected* | 02-27-2003 |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | |
| *Reason for Update* | | | |
| *Updated By* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

# Compliance Component Blueprint

| Definition | |
|---|---|
| *Name* | Compliance Component - Virus Detection and Elimination Criteria for E-Mail |
| *Description* | To make available to the State Enterprise a set of minimum criteria for the selection of anti-virus software and products for security protection of E-mail and Groupware applications. |
| *Rationale* | All E-mail and Groupware applications within the State computer environment shall execute an anti-virus security product that conforms to a minimum set of compliance criteria. These criteria shall serve as a checklist to help administrators choose the appropriate anti-virus solution for their environment. |
| *Benefits* | To significantly improve E-mail and Groupware trust and security through a set of criteria for the following security services:<br>1. Protection to E-mail and Groupware application systems from computer virus intrusion.<br>2. Detection of computer viruses on an infected E-mail or Groupware applications.<br>3. E-mail and Groupware application recovery from a computer virus infection. |
| **Associated Architecture Levels** | |
| *Domain Name* | Security |
| *Discipline Name* | Technical Controls |
| *Technology Area Name* | Virus Detection and Elimination |
| *Product Component Name* | |
| **Compliance Component Type** | |
| *Component Type* | Guideline |
| *Component Sub-type* | |
| **Compliance Detail** | |
| *Guideline, Standard or Legislation* | **Virus Detection and Elimination Criteria for E-Mail and Groupware Applications**<br><br>State E-mail and Groupware applications shall be protected with anti-virus software and procedures that meet the checklist of criteria detailed in the following service areas.<br><br><u>General E-mail and Groupware Anti-Virus Criteria</u><br>• Virus scanner software shall be run on all E-mail and Groupware applications even if the networks perimeter devices are scanning for viruses.<br>• Anti-virus software shall use a separate and configurable agent specifically designed to protect E-mail and Groupware applications.<br>• All E-mail and Groupware applications shall be scanned for viruses at least once a day.<br>• E-mail and Groupware anti-virus software shall provide integration capabilities with an enterprise anti-virus policy management suite.<br>• All State E-mail and Groupware applications shall execute a virus scan product certified by the ICSA Labs (http://www.icsalabs.com). ICSA Labs certification requires anti-virus products to detect 100% of all viruses "in the wild" as captured by the WildList Organization International (http://www.wildlist.org). |

| | |
|---|---|
| | Virus Detection/Scanning Capabilities<br>• Anti-virus software shall be capable of detecting malicious software before it is executed.<br>• Shall support both On-Access (real-time) and On-Demand (flexible) scanning capabilities.<br>• Shall provide detection for all "in the wild" virus types (boot viruses, file viruses, macro viruses, and script viruses).<br>• Shall provide detection for Zoo type viruses (file viruses, macro viruses, script viruses, polymorphic viruses, other malware, false positives).<br>• Shall provide detection for archived and compressed file types (ZIP, TAR, LZH, recursive and self-extracting archives, runtime-compressed files).<br>• Shall provide scanning capabilities for all standard office file formats (including embedded OLE objects and password protected files).<br>• Shall provide for flexible configuration to include/exclude file types, drives and directories from scans.<br>• Shall support both Inbound and Outbound real-time scan protection of E-mail.<br>• Shall support customizable e-mail message and attachment scanning, blocking and quarantine.<br>• Shall provide Heuristic-scanning capabilities (intelligent analysis of unknown or suspicious sections of messages, attachments and code).<br>• Shall support multi-mode scanning (Windows platforms only) to protect Windows API, ESE, and MAPI.<br><br>E-mail Content Filtering<br>• E-Mail and Groupware anti-virus products shall support the filtering of e-mail messages for tailored anti-viral support including filtering on items such as:<br>– E-mail file size<br>– Sender name (virus@malicious.com)<br>– DNS extension name (@dns.com)<br>– Subject line<br>– Message body context<br>– Attachment name<br>– Multiple criteria<br><br>Virus Reporting Capabilities<br>• Anti-virus software shall provide the ability for detection notification via both audio and visual alerts.<br>• Anti-Virus software must provide remote notification of administrative alerts via the following methods:<br>– SMTP/E-Mail<br>– SNMP Alerts<br>– Log to a file<br>– Log to an Enterprise Repository<br><br>Post-Detection Anti-Virus Action Capabilities<br>• It is highly desirable that anti-virus software be able to eradicate malicious software and viruses detected through the following means:<br>– Quarantine – moving the infected file into an area where it cannot cause more harm.<br>– Virus Removal – allows for repair of the damage caused by the virus.<br>– Deny Access – prohibits the file from being accessed once infected.<br>– Delete – complete removal of the infected file from the system.<br><br>Anti-Virus Scan Engine Update Capabilities<br>• Anti-virus signatures need to be updated continuously, either through a manual |

| | | | |
|---|---|---|---|
| | or automated process.<br>• Shall provide a secure procedure for keeping the detection engine up-to-date with the latest detection signatures & scan engine techniques (new viruses are discovered daily)<br>• Shall provide for automated updates of both scan engine and signatures on a scheduled interval or as needed.<br>• Virus scan engine shall have the ability to stay up-to-date with the latest developments in malicious software detection.<br><br><u>Anti-Virus Installation Criteria</u><br>• Anti-Virus software shall be capable of automatic deployment and installation via the following:<br>– Installation via image – anti-virus software shall be able to be included in the standard E-mail or Groupware application image deployed within the enterprise.<br>– Remote installation – Anti-virus software shall support deployment to remote systems (dial-up, VPN, etc.) providing the same level of protection to these devices.<br>• Anti-virus software deployment (and updates) shall be transparent to end-users.<br>• Anti-virus software shall provide "Wizard-enabled" installation routines to automate and expedite installation.<br><br><u>Service and Support</u><br>• State virus protection products shall be backed by vendors who offer 24 x 7, 365 days a year phone support.<br>• Anti-virus vendors shall provide a comprehensive documentation and assistance package, including a facility for pro-active timely warnings of new malicious software and virus events.<br>• Anti-virus vendors shall provide "Virus Catalog Support" including:<br>– A lexicon of known viruses detailing descriptions, how they are spread, what they do, how they are recognized and how to remove them.<br>– Downloads or links to disinfection tools.<br>– A clear and concise description of the anti-virus tools functionality, including procedures for updating the product with new detection signatures.<br>– General advice to end-users on attacks and avoidance measures. | | |
| *Source Reference* | N/A | | |
| *Standards Organizations* | | | |
| *Name* | ISCA Labs | *Website* | www.iscalabs.com |
| *Contact Information* | ISCA Labs is a division of TruSecure Corporation and can be reached at 1-888-396-8348 (info@trusecure.com) | | |

| Government Body | | | |
|---|---|---|---|
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) | *Website* | http://csrc.nist.gov/ |
| *Contact Information* | inquiries@nist.gov | | |
| **KEYWORDS** | | | |
| *Keywords/Aliases* | Virus, virus detection, malicious code, virus products, virus reporting, anti-virus vendors, anti-virus engine, zoo, trojan horse, backdoor, worm, stealth, blended threat, boot sector infector, companion, denial of service, dropper, file infector, logic bomb, malware, multi-partite, overwriting, parasitic, polymorphic, tunneling, variant, terminate and stay resident (tsr), management, content filtering | | |
| **COMPONENT CLASSIFICATION** | | | |
| *Classification* | ☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset* | | |
| *Rationale for Component Classification* | | | |
| *Rationale for Component Classification* | | | |
| *Conditional Use Restrictions* | | | |
| *Restrictions* | | | |
| *Migration Strategy* | | | |
| *Migration Strategy* | | | |
| *Impact Position Statement* | | | |
| *Position Statement on Impact* | | | |
| **CURRENT STATUS** | | | |
| *Current Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | 02-06-2003 | *Date Accepted / Rejected* | 02-27-2003 |
| *Reason for Rejection* | | | |
| *Last Date Reviewed* | | *Last Date Updated* | |
| *Reason for Update* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

| DEFINITION | |
|---|---|
| *Name* | Compliance Component - Virus Detection and Elimination Criteria for Gateways |
| *Description* | To make available to the State Enterprise a set of minimum criteria for the selection of anti-virus software and products for security protection of Gateways. |
| *Rationale* | All Gateways within the State computer environment shall execute an anti-virus security product that conforms to a minimum set of compliance criteria. These criteria shall serve as a checklist to help administrators choose the appropriate anti-virus solution for their environment. |
| *Benefits* | To significantly improve Gateway trust and security through a set of criteria for the following security services:<br>4. Multi-tiered virus protection.<br>5. Offload virus scan processing to a dedicated system.<br>6. Protection to Gateways from computer virus intrusion.<br>7. Detection of computer viruses on an infected Gateway.<br>8. Gateway recovery from a computer virus infection. |

| ASSOCIATED ARCHITECTURE LEVELS | |
|---|---|
| *Domain Name* | Security |
| *Discipline Name* | Technical Controls |
| *Technology Area Name* | Virus Detection and Elimination |
| *Product Component Name* | |

| COMPLIANCE COMPONENT TYPE | |
|---|---|
| *Component Type* | Guideline |
| *Component Sub-type* | |

| COMPLIANCE DETAIL | |
|---|---|
| *Guideline, Standard or Legislation* | **Virus Detection and Elimination Criteria for Gateways**<br><br>State computer Gateways shall run anti-virus software and procedures that meet the checklist of criteria detailed in the following service areas.<br><br><u>General Gateway Anti-Virus Criteria</u><br>• Gateways shall be scanning for viruses continuously.<br>• Gateway anti-virus software shall provide integration capabilities with an enterprise anti-virus policy management suite.<br>• All State Gateways shall execute a virus scan product certified by the ICSA Labs (http://www.icsalabs.com). ICSA Labs certification requires anti-virus products to detect 100% of all viruses “in the wild” as captured by the WildList Organization International (http://www.wildlist.org).<br><br><u>Virus Detection/Scanning Capabilities</u><br>• Anti-virus software shall be capable of detecting malicious software before it is executed.<br>• Shall support continuous real-time scanning capabilities. |

| | |
|---|---|
| | • Shall provide detection for all “in the wild” virus types (boot viruses, file viruses, macro viruses, and script viruses).<br>• Shall provide detection for Zoo type viruses (file viruses, macro viruses, script viruses, polymorphic viruses, other malware, false positives).<br>• Shall provide detection for archived and compressed file types (.ZIP, TAR, LZH, recursive and self-extracting archives, runtime-compressed files).<br>• Shall provide scanning capabilities for all standard office file formats (including embedded OLE objects and password protected files).<br>• Shall provide for flexible configuration to include/exclude file types, drives and directories from scans.<br>• Shall support both Inbound and Outbound real-time scan protection.<br>• Shall provide Internet Download and Content scanning for protection from suspicious web content, including:<br>  - ActiveX filtering and scanning<br>  - JavaScript filtering and scanning<br>• Shall provide Heuristic-scanning capabilities (intelligent analysis of unknown or suspicious sections of code).<br>• Gateway anti-virus software shall have the capability to scan all major message protocols including:<br>  - SMTP<br>  - POP3<br>  - HTTP<br>  - FTP<br>• Gateway anti-virus software shall support SPAM detection and anti-relay (DNS based black hole lists and administrative defined anti-relay).<br><br><u>Internet Content Filtering</u><br>• Gateway anti-virus products shall support the filtering of web content (including POP3 email) for tailored anti-viral support including filtering on items such as:<br>  - File size<br>  - DNS extensions (dns.com)<br>  - Web page content<br>  - File extensions<br>  - Multiple criteria<br><br><u>Virus Reporting Capabilities</u><br>• Anti-virus software shall provide remote notification of administrative alerts via the following methods:<br>  - SMTP/E-Mail<br>  - SNMP Alerts<br>  - Log to a file<br>  - Log to an Enterprise Repository<br><br><u>Post-Detection Virus Action Capabilities</u><br>• It is highly desirable that anti-virus software be able to eradicate malicious software and viruses detected through the following means:<br>  - Quarantine – moving the infected file into an area where it cannot cause more harm.<br>  - Virus Removal – allows for repair of the damage caused by the virus.<br>  - Deny Access – prohibits the file from being accessed once infected.<br>  - Delete – complete removal of the infected file from the system.<br><br><u>Virus Scan Engine Update Capabilities</u><br>• Anti-virus signatures need to be updated continuously, either through a manual or automated process. |

| | | | |
|---|---|---|---|
| | • Shall provide a secure procedure for keeping the detection engine up-to-date with the latest detection signatures & scan engine techniques (new viruses are discovered daily)<br>• Shall provide for automated updates of both scan engine and signatures on a scheduled interval or as needed.<br>• Virus scan engine shall have the ability to stay up-to-date with the latest developments in malicious software detection.<br><br><u>Anti-Virus Installation Criteria for Sever-based Gateways</u><br>• Anti-virus software shall be capable of automatic deployment and installation via the following:<br>– Installation via image – anti-virus software shall be able to be included in the standard Gateway server image deployed within the enterprise.<br>– Remote installation – Anti-virus software shall support deployment to remote systems (not locally-connected) providing the same level of protection to these devices.<br>• Anti-virus software shall provide "Wizard-enabled" installation routines to automate and expedite installation.<br><br><u>Service and Support</u><br>• State virus protection products shall be backed by vendors who offer 24 x 7, 365 days a year phone support.<br>• Anti-virus vendors shall provide a comprehensive documentation and assistance package, including a facility for pro-active timely warnings of new malicious software and virus events.<br>• Anti-virus vendors shall provide "Virus Catalog Support" including:<br>– A lexicon of known viruses detailing descriptions, how they are spread, what they do, how they are recognized and how to remove them.<br>– Downloads or links to disinfection tools.<br>– A clear and concise description of the anti-virus tools functionality, including procedures for updating the product with new detection signatures.<br>– General advice to end-users on attacks and avoidance measures. | | |
| *Source Reference* | N/A | | |
| *Standards Organizations* | | | |
| *Name* | ISCA Labs | *Website* | www.iscalabs.com |
| *Contact Information* | ISCA Labs is a division of TruSecure Corporation and can be reached at 1-888-396-8348 (info@trusecure.com) | | |
| *Government Body* | | | |
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) | *Website* | http://csrc.nist.gov/ |
| *Contact Information* | inquiries@nist.gov | | |

| KEYWORDS | | | |
|---|---|---|---|
| *Keywords/Aliases* | Virus, virus detection, malicious code, virus products, virus reporting, anti-virus vendors, anti-virus engine, zoo, trojan horse, backdoor, worm, stealth, blended threat, boot sector infector, companion, denial of service, dropper, file infector, logic bomb, malware, multi-partite, overwriting, parasitic, polymorphic, tunneling, variant, terminate and stay resident (tsr), management | | |
| **COMPONENT CLASSIFICATION** | | | |
| *Classification* | ☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset* | | |
| ***Rationale for Component Classification*** | | | |
| *Rationale for Component Classification* | | | |
| ***Conditional Use Restrictions*** | | | |
| *Restrictions* | | | |
| ***Migration Strategy*** | | | |
| *Migration Strategy* | | | |
| ***Impact Position Statement*** | | | |
| *Position Statement on Impact* | | | |
| **CURRENT STATUS** | | | |
| *Current Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | 02-06-2003 | *Date Accepted / Rejected* | 02-27-2003 |
| *Reason for Rejection* | | | |
| *Last Date Reviewed* | | *Last Date Updated* | |
| *Reason for Update* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

| DEFINITION | |
|---|---|
| *Name* | Compliance Component - Virus Detection and Elimination Criteria for Servers |
| *Description* | To make available to the State Enterprise a set of minimum criteria for the selection of anti-virus software and products for security protection of servers. |
| *Rationale* | All servers within the State computer environment shall execute an anti-virus security product that conforms to a minimum set of compliance criteria. These criteria shall serve as a checklist to help administrators choose the appropriate anti-virus solution for their environment. |
| *Benefits* | To significantly improve server trust and security through a set of criteria for the following security services:<br>9. Protection to servers and media from computer virus intrusion.<br>10. Detection of computer viruses on an infected server system or media.<br>11. Server recovery from a computer virus infection. |

| ASSOCIATED ARCHITECTURE LEVELS | |
|---|---|
| *Domain Name* | Security |
| *Discipline Name* | Technical Controls |
| *Technology Area Name* | Virus Detection and Elimination |
| *Product Component Name* | |

| COMPLIANCE COMPONENT TYPE | |
|---|---|
| *Component Type* | Guideline |
| *Component Sub-type* | |

| COMPLIANCE DETAIL | |
|---|---|
| *Guideline, Standard or Legislation* | **Virus Detection and Elimination Criteria for Servers**<br><br>State servers shall be protected with anti-virus software and procedures that meet the checklist of criteria detailed in the following service areas.<br><br><u>General Server Anti-Virus Criteria</u><br>• Anti-virus scanner software shall be run on all servers even if the networks perimeter devices are scanning for viruses.<br>• All servers shall be scanned for viruses at least once a day.<br>• Server anti-virus software shall provide integration capabilities with an enterprise anti-virus policy management suite.<br>• All State servers shall execute a virus scan product certified by the ICSA Labs (http://www.icsalabs.com). ICSA Labs certification requires anti-virus products to detect 100% of all viruses "in the wild" as captured by the WildList Organization International (http://www.wildlist.org).<br><br><u>Virus Detection/Scanning Capabilities</u><br>• Anti-virus software shall be capable of detecting malicious software before it is executed.<br>• Shall support both On-Access (real-time) and On-Demand (flexible) scanning capabilities.<br>• Shall provide detection for all "in the wild" virus types (boot viruses, file viruses, |

| | |
|---|---|
| | macro viruses, and script viruses).<br>• Shall provide detection for Zoo type viruses (file viruses, macro viruses, script viruses, polymorphic viruses, other malware, false positives).<br>• Shall provide detection for archived and compressed file types (.ZIP, TAR, LZH, recursive and self-extracting archives, runtime-compressed files).<br>• Shall provide scanning capabilities for all standard office file formats (including embedded OLE objects and password protected files).<br>• Shall provide for flexible configuration to include/exclude file types, drives and directories from scans.<br>• Shall support both Inbound and Outbound real-time scan protection.<br>• Shall provide Internet Download and Content scanning for protection from suspicious web content, including:<br>- ActiveX filtering and scanning<br>- JavaScript filtering and scanning<br>• Shall provide Heuristic-scanning capabilities (intelligent analysis of unknown or suspicious sections of code).<br><br><u>Virus Reporting Capabilities</u><br>• Anti-virus software shall provide the ability for detection notification via both audio and visual alerts.<br>• Anti-virus software shall provide remote notification of administrative alerts via the following methods:<br>- SMTP/E-Mail<br>- SNMP Alerts<br>- Log to a file<br>- Log to an Enterprise Repository<br><br><u>Post-Detection Virus Action Capabilities</u><br>• It is highly desirable that Anti-virus software be able to eradicate malicious software and viruses detected through the following means:<br>- Quarantine – moving the infected file into an area where it cannot cause more harm.<br>- Virus Removal – allows for repair of the damage caused by the virus.<br>- Deny Access – prohibits the file from being accessed once infected.<br>- Delete – complete removal of the infected file from the system.<br><br><u>Virus Scan Engine Update Capabilities</u><br>• Anti-virus signatures need to be updated continuously, either through a manual or automated process.<br>• Shall provide a secure procedure for keeping the detection engine up-to-date with the latest detection signatures & scan engine techniques (new viruses are discovered daily)<br>• Shall provide for automated updates of both scan engine and signatures on a scheduled interval or as needed.<br>• Virus scan engine shall have the ability to stay up-to-date with the latest developments in malicious software detection.<br><br><u>Anti-Virus Software Configuration Security</u><br>• Anti-virus product configurations and settings shall be able to be password protected to prevent misuse and disablement.<br>• Anti-virus software shall support multiple & customizable definitions of security rights to various levels of the software configuration settings.<br><br><u>Anti-Virus Installation Criteria</u><br>• Anti-virus software shall be capable of installation on clustered servers. |

| | | | |
|---|---|---|---|
| | • Anti-virus software shall be capable of automatic deployment and installation via the following:<br>  - Installation via image – anti-virus software shall be able to be included in the standard file server images deployed within the enterprise.<br>  - Remote installation – anti-virus software shall support deployment to remote systems (not locally-connected) providing the same level of protection to these devices.<br>• Anti-virus software shall provide "Wizard-enabled" installation routines to automate and expedite installation.<br><br><u>Service and Support</u><br>• Virus protection for servers shall support full virus protection in clustered server environments.<br>• State virus protection products shall be backed by vendors who offer 24 x 7, 365 days a year phone support.<br>• Anti-virus vendors shall provide a comprehensive documentation and assistance package, including a facility for pro-active timely warnings of new malicious software and virus events.<br>• Anti-virus vendors shall provide "Virus Catalog Support" including:<br>  - A lexicon of known viruses detailing descriptions, how they are spread, what they do, how they are recognized and how to remove them.<br>  - Downloads or links to disinfection tools.<br>  - A clear and concise description of the anti-virus tools functionality, including procedures for updating the product with new detection signatures.<br>  - General advice to end-users on attacks and avoidance measures. | | |
| *Source Reference* | N/A | | |
| *Standards Organizations* | | | |
| *Name* | ICSA Labs | *Website* | www.icsalabs.com |
| *Contact Information* | ICSA Labs is a division of TruSecure Corporation and can be reached at 1-888-396-8348 (info@trusecure.com) | | |
| *Government Body* | | | |
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) | *Website* | http://csrc.nist.gov/ |
| *Contact Information* | inquiries@nist.gov | | |
| KEYWORDS | | | |
| *Keywords/Aliases* | Virus, virus detection, malicious code, virus products, virus reporting, anti-virus vendors, anti-virus engine, zoo, trojan horse, backdoor, worm, stealth, blended threat, boot sector infector, companion, denial of service, dropper, file infector, logic bomb, malware, multi-partite, overwriting, parasitic, polymorphic, tunneling, variant, terminate and stay resident (tsr), management, server | | |
| COMPONENT CLASSIFICATION | | | |
| *Classification* | ☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset* | | |
| *Rationale for Component Classification* | | | |
| *Rationale for Component Classification* | | | |

| Conditional Use Restrictions | | | |
|---|---|---|---|
| Restrictions | | | |
| **Migration Strategy** | | | |
| Migration Strategy | | | |
| **Impact Position Statement** | | | |
| Position Statement on Impact | | | |
| **CURRENT STATUS** | | | |
| Current Status | ☐ In Development ☐ Under Review ☒ Approved ☐ Rejected | | |
| **AUDIT TRAIL** | | | |
| Creation Date | 02-06-2003 | Date Accepted / Rejected | 02-27-2003 |
| Reason for Rejection | | | |
| Last Date Reviewed | | Last Date Updated | |
| Reason for Update | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

# Compliance Component Blueprint

| DEFINITION | |
|---|---|
| *Name* | Compliance Component - Virus Detection and Elimination Criteria for Workstations |
| *Description* | To make available to the State Enterprise a set of minimum criteria for the selection of anti-virus software and products for security protection of workstations. |
| *Rationale* | All workstations within the State computer environment shall execute an anti-virus security product that conforms to a minimum set of compliance criteria. These criteria shall serve as a checklist to help administrators choose the appropriate anti-virus solution for their environment. |
| *Benefits* | To significantly improve workstation trust and security through a set of criteria for the following security services:<br>12. Protection to workstation computer systems and media from computer virus intrusion.<br>13. Detection of computer viruses on an infected workstation system or media.<br>14. Workstation recovery from a computer virus infection. |
| **ASSOCIATED ARCHITECTURE LEVELS** | |
| *Domain Name* | Security |
| *Discipline Name* | Technical Controls |
| *Technology Area Name* | Virus Detection and Elimination |
| *Product Component Name* | |
| **COMPLIANCE COMPONENT TYPE** | |
| *Component Type* | Guideline |
| *Component Sub-type* | |
| **COMPLIANCE DETAIL** | |
| *Guideline, Standard or Legislation* | **Virus Detection and Elimination Criteria for Workstations**<br><br>State computer workstations shall be protected with anti-virus software and procedures that meet the checklist of criteria detailed in the following service areas.<br><br><u>General Workstation Anti-Virus Criteria</u><br>• Virus scanner software shall be run on all workstations even if the networks perimeter devices are scanning for viruses.<br>• All workstations shall be scanned for viruses at least once a day.<br>• Workstation anti-virus software shall provide integration capabilities with an enterprise anti-virus policy management suite.<br>• All State workstations shall execute a virus scan product certified by the ICSA Labs (http://www.icsalabs.com). ICSA Labs certification requires anti-virus products to detect 100% of all viruses “in the wild” as captured by the WildList Organization International (http://www.wildlist.org).<br><br><u>Virus Detection/Scanning Capabilities</u><br>• Anti-virus software shall be capable of detecting malicious software before it is executed.<br>• Shall support both On-Access (real-time) and On-Demand (flexible) scanning |

| | |
|---|---|
| | capabilities.<br>• Shall provide detection for all “in the wild” virus types (boot viruses, file viruses, macro viruses, and script viruses).<br>• Shall provide detection for Zoo type viruses (file viruses, macro viruses, script viruses, polymorphic viruses, other malware, false positives).<br>• Shall provide detection for archived and compressed file types (.ZIP, TAR, LZH, recursive and self-extracting archives, runtime-compressed files).<br>• Shall provide scanning capabilities for all standard office file formats (including embedded OLE objects and password protected files).<br>• Shall provide for flexible configuration to include/exclude file types, drives and directories from scans.<br>• Shall support both Inbound and Outbound real-time scan protection.<br>• Shall provide Internet Download and Content scanning for protection from suspicious web content, including:<br>- ActiveX filtering and scanning<br>- JavaScript filtering and scanning<br>• Shall provide Heuristic-scanning capabilities (intelligent analysis of unknown or suspicious sections of code).<br><br><u>Virus Reporting Capabilities</u><br>• Anti-virus software shall provide the ability for detection notification via both audio and visual alerts.<br>• Anti-virus software shall provide remote notification of administrative alerts via the following methods:<br>- SMTP/E-Mail<br>- SNMP Alerts<br>- Log to a file<br>- Log to an Enterprise Repository<br><br><u>Post-Detection Anti-Virus Action Capabilities</u><br>• It is highly desirable that anti-virus software be able to eradicate malicious software and viruses detected through the following means:<br>- Quarantine – moving the infected file into an area where it cannot cause more harm.<br>- Virus Removal – allows for repair of the damage caused by the virus.<br>- Deny Access – prohibits the file from being accessed once infected.<br>- Delete – complete removal of the infected file from the system.<br><br><u>Virus Scan Engine Update Capabilities</u><br>• Anti-virus signatures need to be updated continuously, either through a manual or automated process.<br>• Shall provide a secure procedure for keeping the detection engine up-to-date with the latest detection signatures & scan engine techniques.<br>• Shall provide for automated updates of both scan engine and signatures on a scheduled interval or as needed.<br>• Virus scan engine shall have the ability to stay up-to-date with the latest developments in malicious software detection.<br><br><u>Anti-Virus Software Configuration Security</u><br>• Anti-virus product configurations and settings shall be able to be password protected to prevent misuse and disablement.<br>• Anti-virus software shall support multiple & customizable definitions of security and rights to various levels of the software configuration settings.<br><br><u>Anti-Virus Installation Criteria</u> |

| | | | |
|---|---|---|---|
| | • Anti-virus software shall be capable of automatic deployment and installation via the following:<br>– Installation via image – anti-virus software shall be able to be included in the standard workstation image deployed within the enterprise.<br>– Remote installation – Anti-virus software shall support deployment to remote systems (not locally-connected) providing the same level of protection to these devices.<br>• Anti-virus software deployment (and updates) shall be transparent to end-users.<br>• Anti-virus software shall provide "Wizard-enabled" installation routines to automate and expedite installation.<br><br><u>Service and Support</u><br>• State anti-virus protection products shall be backed by vendors who offer 24 x 7, 365 days a year phone support.<br>• Anti-virus vendors shall provide a comprehensive documentation and assistance package, including a facility for pro-active timely warnings of new malicious software and virus events.<br>• Anti-virus vendors shall provide "Virus Catalog Support" including:<br>– A lexicon of known viruses detailing descriptions, how they are spread, what they do, how they are recognized and how to remove them.<br>– Downloads or links to disinfection tools.<br>– A clear and concise description of the anti-virus tools functionality, including procedures for updating the product with new detection signatures.<br>– General advice to end-users on attacks and avoidance measures. | | |
| *Source Reference* | N/A | | |
| *Standards Organizations* | | | |
| *Name* | ICSA Labs | *Website* | www.icsalabs.com |
| *Contact Information* | ICSA Labs is a division of TruSecure Corporation and can be reached at 1-888-396-8348 (info@trusecure.com) | | |
| *Government Body* | | | |
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) | *Website* | http://csrc.nist.gov/ |
| *Contact Information* | inquiries@nist.gov | | |
| KEYWORDS | | | |
| *Keywords/Aliases* | Virus, virus detection, malicious code, virus products, virus reporting, anti-virus vendors, anti-virus engine, zoo, trojan horse, backdoor, worm, stealth, blended threat, boot sector infector, companion, denial of service, dropper, file infector, logic bomb, malware, multi-partite, overwriting, parasitic, polymorphic, tunneling, variant, terminate and stay resident (tsr), management, PC | | |
| COMPONENT CLASSIFICATION | | | |
| *Classification* | ☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset* | | |
| *Rationale for Component Classification* | | | |
| *Rationale for Component Classification* | | | |

| Conditional Use Restrictions | | | |
|---|---|---|---|
| Restrictions | | | |
| **Migration Strategy** | | | |
| Migration Strategy | | | |
| **Impact Position Statement** | | | |
| Position Statement on Impact | | | |
| **CURRENT STATUS** | | | |
| Current Status | ☐ In Development ☐ Under Review ☒ Approved ☐ Rejected | | |
| **AUDIT TRAIL** | | | |
| Creation Date | 02-06-2003 | Date Accepted / Rejected | 02-27-2003 |
| Reason for Rejection | | | |
| Last Date Reviewed | | Last Date Updated | |
| Reason for Update | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

# Compliance Component Blueprint

| DEFINITION | |
|---|---|
| *Name* | Compliance Component - Virus Detection and Elimination Criteria for Wireless Devices |
| *Description* | To make available to the State Enterprise a set of minimum criteria for the selection of anti-virus software and products for security protection of Wireless Devices (e.g. PDAs) which connect directly (via a wireless adapter) or connect indirectly (via a cradle) to it's computer networks.<br><br>All Wireless Devices used within the State computer environments that are directly or indirectly connected to enterprise networks or computers shall execute an anti-virus security product that conforms to a minimum set of compliance criteria. These criteria shall serve as a checklist to help administrators choose the appropriate anti-virus solution for their environment. |
| *Rationale* | When using wireless devices there is a major security gap, as server and workstation anti-virus applications can't protect from a virus being introduced during a sync operation with the wireless device. |
| *Benefits* | To significantly improve wireless device trust and security through a set of criteria for the following security services:<br>15. Protection to workstation computer systems and servers from computer virus intrusion transmitted via wireless devices.<br>16. Detection and protection computer viruses on an wireless handheld system.<br>17. Wireless handheld device recovery from a computer virus infection. |

| ASSOCIATED ARCHITECTURE LEVELS | |
|---|---|
| *Domain Name* | Security |
| *Discipline Name* | Technical Controls |
| *Technology Area Name* | Virus Detection and Elimination |
| *Product Component Name* | |

| COMPLIANCE COMPONENT TYPE | |
|---|---|
| *Component Type* | Guideline |
| *Component Sub-type* | |

| COMPLIANCE DETAIL | |
|---|---|
| *Guideline, Standard or Legislation* | **Virus Detection and Elimination Criteria for Wireless Devices**<br><br>Wireless devices, which connect to State systems or networks, shall be protected with anti-virus software and procedures that meet the checklist of criteria detailed in the following service areas.<br><br><u>General Wireless Handheld Anti-Virus Criteria</u><br>• Wireless anti-virus software shall protect the sync operation and/or the wireless device, even if the workstation and network perimeter devices are scanning for viruses.<br>• Wireless handheld anti-virus software shall protect against malicious data as transferred via:<br>– Sync operations with a workstation or network<br>– Infrared transfer with another handheld device, laptop, or workstation<br>– Wireless network or Internet connections |

| | |
|---|---|
| | • Wireless virus protection shall cover all major palm top operating systems including:<br>  - Palm OS<br>  - Pocket PC<br>  - Windows CE<br>  - Symbian EPOC<br><br><u>Virus Detection/Scanning Capabilities</u><br>• Wireless device anti-virus software shall be capable of detecting malicious software before it is transferred to workstations or networks.<br>• Shall provide detection for all “in the wild” virus types (boot viruses, file viruses, macro viruses, and script viruses).<br>• Shall provide detection for Zoo type viruses (file viruses, macro viruses, script viruses, polymorphic viruses, other malware, false positives).<br>• Shall provide detection for archived and compressed file types (.ZIP, TAR, LZH, recursive and self-extracting archives, runtime-compressed files).<br>• Shall provide scanning capabilities for all standard office file formats (including embedded OLE objects and password protected files).<br>• Shall provide for flexible configuration to include/exclude file types, drives and directories from scans.<br>• Shall provide Internet Download and Content scanning for protection from suspicious web content, including:<br>  - ActiveX filtering and scanning<br>  - JavaScript filtering and scanning<br>• Shall provide Heuristic-scanning capabilities (intelligent analysis of unknown or suspicious sections of code).<br><br><u>Post-Detection Anti-Virus Action Capabilities</u><br>• If a virus is discovered, all synchronization between the wireless device and the workstation or network shall be disabled until the destructive code can be removed from the device.<br>• It is highly desirable that anti-virus software be able to eradicate malicious software and viruses detected through the following means:<br>  - Quarantine – moving the infected file into an area where it cannot cause more harm.<br>  - Virus Removal – allows for repair of the damage caused by the virus.<br>  - Deny Access – prohibits the file from being accessed once infected.<br>  - Delete – complete removal of the infected file from the system.<br><br><u>Virus Scan Engine Update Capabilities</u><br>• Anti-virus signatures need to be updated, either through a manual or automated process.<br>• Shall provide a secure procedure for keeping the detection engine up-to-date with the latest detection signatures & scan engine techniques (new viruses are discovered daily).<br>• Shall provide for automated updates of both scan engine and signatures during synchronization processes.<br>• Virus scan engine shall have the ability to stay up-to-date with the latest developments in malicious software detection.<br><br><u>Anti-Virus Installation Criteria</u><br>• Anti-virus software shall be capable of flexible deployment techniques.<br>• Anti-virus software deployment (and updates) shall be transparent to end-users.<br>• Anti-virus software shall provide “Wizard-enabled” installation routines to automate and expedite installation. |

| | | | |
|---|---|---|---|
| | Service and Support<br>• State virus protection products shall be backed by vendors who offer 24 x 7, 365 days a year phone support.<br>• Anti-virus vendors shall provide a comprehensive documentation and assistance package, including a facility for pro-active timely warnings of new malicious software and virus events.<br>• Anti-virus vendors shall provide "Virus Catalog Support" including:<br>– A lexicon of known viruses detailing descriptions, how they are spread, what they do, how they are recognized and how to remove them.<br>– Downloads or links to disinfection tools.<br>– A clear and concise description of the anti-virus tools functionality, including procedures for updating the product with new detection signatures.<br>– General advice to end-users on attacks and avoidance measures. | | |
| *Source Reference* | N/A | | |
| *Standards Organizations* | | | |
| *Name* | ICSA Labs | *Website* | www.icsalabs.com |
| *Contact Information* | ICSA Labs is a division of TruSecure Corporation and can be reached at 1-888-396-8348 (info@trusecure.com) | | |
| *Government Body* | | | |
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) | *Website* | http://csrc.nist.gov/ |
| *Contact Information* | inquiries@nist.gov | | |
| KEYWORDS | | | |
| *Keywords/Aliases* | Virus, virus detection, malicious code, virus products, virus reporting, anti-virus vendors, anti-virus engine, zoo, trojan horse, backdoor, worm, stealth, blended threat, boot sector infector, companion, denial of service, dropper, file infector, logic bomb, malware, multi-partite, overwriting, parasitic, polymorphic, tunneling, variant, terminate and stay resident (tsr), management, palm top, palm pilot, handheld, PDA | | |
| COMPONENT CLASSIFICATION | | | |
| *Classification* | ☒ *Emerging* ☐ *Current* ☐ *Twilight* ☐ *Sunset* | | |
| *Rationale for Component Classification* | | | |
| *Rationale for Component Classification* | | | |
| *Conditional Use Restrictions* | | | |
| *Restrictions* | | | |
| *Migration Strategy* | | | |
| *Migration Strategy* | | | |
| *Impact Position Statement* | | | |
| *Position Statement on Impact* | | | |

| CURRENT STATUS | | | |
|---|---|---|---|
| *Current Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | 02-06-2003 | *Date Accepted / Rejected* | 02-27-2003 |
| *Reason for Rejection* | | | |
| *Last Date Reviewed* | | *Last Date Updated* | |
| *Reason for Update* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

| Definition | |
|---|---|
| *Name* | Technology Area - Intrusion Detection Systems (IDS) |
| *Description* | Intrusion Detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network. Intrusion Detection Systems (IDS) are software or hardware products that automate this monitoring and analysis process. |
| *Rationale* | Intrusion detection allows State organizations to protect their systems from the threats that come with increasing network connectivity and reliance on information systems. Given the level and nature of modern network security threats, the question for security professionals should not be *whether* to use IDS, but which IDS features and capabilities to use. |
| *Benefits* | • IDS prevents problem behaviors by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse a system.<br>• IDS detects attacks and other security violations that are not prevented by other security measures.<br>• An IDS can act as a quality control for security design and administration.<br>• IDS provides useful information about intrusions that do take place, allowing improved diagnosis, recovery, correction of causative factors, and data for potential prosecution. |
| **Associated Discipline** | |
| *Discipline Name* | Technical Controls |
| **Keywords** | |
| *Keywords/Aliases* | Honey Pot, intrusion, cracker, buffer overflows, passwords, sniffing, exploit, denial-of-service, Java, ActiveX, SMURF, DNS, probes, logging, auditing, monitoring, anomaly, patterns, exploits, misuse |
| **Associated Compliance Components** | |
| *Compliance Component Names* | • Host-Based IDS<br>• Network-Based IDS<br>• Application-Based IDS |
| **Associated Product Components** | |
| *Product Component Names* | |
| **Technology Area Detail** | |
| *Supporting Documentation* | NIST SP 800-31 Intrusion Detection Systems (IDS) |
| *Source Reference* | www.csrc.nist.gov/publications/nistpubs |

| Standards Organizations / Government Body | | | |
|---|---|---|---|
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) | *Website* | http://csrc.nist.gov/ |
| *Contact Information* | inquiries@nist.gov | | |
| **CURRENT STATUS** | | | |
| *Technology Area Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | 3/27/2003 | *Date Accepted / Rejected* | 05/14/2003 |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | |
| *Updated By* | | | |
| *Reason for Update* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

# Compliance Component Blueprint

| Definition | |
|---|---|
| *Name* | Compliance Component - Network-Based Intrusion Detection Systems (NIDS) |
| *Description* | Network-Based Intrusion Detection Systems (NIDS) detect attacks by capturing and analyzing network traffic. NIDS are dedicated software or hardware systems that "sit" on a network and analyze network packets.<br><br>NIDS often consist of a set of single-purpose sensors placed at various points in a network. These sensors monitor network traffic, performing local analysis of that traffic and reporting attacks to a centralized console. |
| *Rationale* | The first step in delivering an efficient and secure network intrusion protection strategy is accurately detecting all possible threats. To achieve this goal, multiple detection methods should be employed to ensure comprehensive coverage.<br><br>The failure to secure State networks with NIDS puts agencies at a much greater risk of loss. A single attack can cost millions of dollars in time spent recovering from the attack and liability for compromised data and hardware. The damage from an attack to State services can also include inconvenience to citizens and the loss of public confidence. |
| *Benefits* | • NIDS identify and prevent security threats from compromising secure networks.<br>• The deployment of NIDS has little impact on network performance. NIDS are usually passive devices that listen on a network without interfering with the normal operation of a network.<br>• NIDS can be made very secure against attack and even made invisible to many attackers. |
| **Associated Architecture Levels** | |
| *Domain Name* | Security |
| *Discipline Name* | Technical Controls |
| *Technology Area Name* | Intrusion Detection Systems |
| *Product Component Name* | |
| **Compliance Component Type** | |
| *Component Type* | Guideline |
| *Component Sub-type* | |
| **Compliance Detail** | |
| *Guideline, Standard or Legislation* | **General NIDS Requirements**<br><br>• Administrators shall be trained on the IDS before implementation. Despite vendor claims of ease of use, training and/or experience are necessary to manage any IDS.<br>• It is preferred to have the NIDS controlled directly from a central location(s). However, the NIDS may be agent-based where response decisions are made at the agent.<br>• IDS administrators shall be able to create or change policies easily.<br><br>**NIDS Deployment Requirements**<br><br>• NIDS shall be deployed in conjunction with Host-Based IDS to fully protect the system. |

- It is recommended that organizations install the NIDS first on critical networks. Once administrators are familiar with the NIDS, it may be installed on the remainder of the organization's networks.
- NIDS shall be installed on any Network where sensitive or critical information is transmitted.
- It is preferred to install IDS Management software on a dedicated system in the target networks being monitored.
- It is preferred to have the NIDS use an agent-manager (server) architecture, where policy is created and modified on the manager and automatically distributed to all agents.
- It is preferred that Server agents poll the manager at periodic intervals for policy changes or new software updates.

**NIDS Analysis Requirements**

- NIDS shall utilize information from operating system audit trails and system logs.
- NIDS shall have easy-to-use tools to analyze the logs.
- NIDS shall detect, and preferably prevent, the following:
- System scanning (probing the target with different kinds of packets to garner information about the system, such as topology, active systems, operating systems and software in use),
- Denial of Service (DoS) (slow or shut down targeted systems or hosts), and
- Penetration (unauthorized acquisition and/or alteration of system privileges, resources, or data).
- NIDS shall use Misuse Detection methods (matching a predefined pattern of events describing an attack) and may include Anomaly Detection (abnormal, unusual behavior) components.
- Administrators shall follow a schedule for checking the results of the NIDS to ensure attackers have not modified the system.

**NIDS Response Requirements**

- NIDS shall respond in real-time.
- It is preferred that IDS provide active responses to intrusions by:
  - Collecting additional information:
- Turning up the number of events logged, or
- Capturing all packets, not just those targeting a particular port or system.
  - Changing the environment:
- Terminating the connection, or
- Reconfiguring routers and firewalls to:
  - Block packets from the intruder's IP address,
  - Block network ports, protocols or services, or
  - Sever all connections that use certain network interfaces.
- NIDS administrators shall work closely with router and firewall administrators when creating rules for routers and firewalls to ensure intruders cannot abuse the feature to deny access to legitimate users.
- NIDS may provide passive responses requiring subsequent human action to intrusions by:
  - Generating alarms and notifications with popup windows, cellular phones, pagers and email, or
  - Reporting alarms and alerts using SNMP traps and plug-ins to central network management consoles.
  - All NIDS communications shall be secure and use encrypted tunnels or other cryptographic measures.

| | |
|---|---|
| | - NIDS shall create output with the following information for each intrusion detected:<br>- Time/date<br>- Sensor IP address<br>- Specific attack name<br>- Source and destination IP addresses<br>- Source and destination port numbers<br>- Network protocol used<br>- Description of the attack type<br>- Attack severity level<br>- Type of loss expected<br>- Type of vulnerability exploited<br>- Input validation (buffer overflow or boundary condition)<br>- Access validation (faulty access control mechanism)<br>- Exceptional condition<br>• Environmental (unexpected interaction with an application and the operating system or between two applications)<br>• Server Configuration<br>• Race (delay between the time a system checks to see if an operation is allowed and the time it performs the operation)<br>• Design<br>• Software types and versions vulnerable<br>• Patch information to counter the attack<br>• References to advisories about the attack or vulnerability<br>- It is preferred that NIDS reports combine redundant attack entries and make attacks of highest importance stand out. |
| *Source Reference* | NIST SP 800-31 (www.csrc.nist.gov/publications/nistpubs)<br>Intrusion Detection Systems (IDS),<br><br>NIST SP 800-18 (www.csrc.nist.gov/publications/nistpubs)<br>CERT Guide to System and Network Security Practices (www.cert.org/security-improvement/) |

| *Standards Organizations* | | | |
|---|---|---|---|
| *Name* | | *Website* | |
| *Contact Information* | | | |

| *Government Body* | | | |
|---|---|---|---|
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) | *Website* | http://csrc.nist.gov/ |
| *Contact Information* | inquiries@nist.gov | | |

| KEYWORDS | |
|---|---|
| *Keywords/Aliases* | Honey Pot, intrusion, cracker, buffer overflows, passwords, sniffing, exploit, denial-of-service, Java, ActiveX, SMURF, DNS, probes |

| COMPONENT CLASSIFICATION | | | | |
|---|---|---|---|---|
| *Classification* | ☐ *Emerging* | ☒ *Current* | ☐ *Twilight* | ☐ *Sunset* |
| *Rationale for Component Classification* | | | | |

| | | | |
|---|---|---|---|
| *Rationale for Component Classification* | | | |
| *Conditional Use Restrictions* | | | |
| *Restrictions* | | | |
| *Migration Strategy* | | | |
| *Migration Strategy* | | | |
| *Impact Position Statement* | | | |
| *Position Statement on Impact* | | | |
| CURRENT STATUS | | | |
| *Current Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |
| AUDIT TRAIL | | | |
| *Creation Date* | 04/03/2003 | *Date Accepted / Rejected* | 5/14/2003 |
| *Reason for Rejection* | | | |
| *Last Date Reviewed* | | *Last Date Updated* | |
| *Reason for Update* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

# Compliance Component Blueprint

| Definition | |
|---|---|
| *Name* | Compliance Component - Host-Based Intrusion Detection Systems (HIDS) |
| *Description* | Host-Based Intrusion Detection Systems (HIDS) operate on information collected from within an individual computer system. This vantage point allows HIDS to analyze activities to determine exactly which processes and users are involved in an attack on a particular system or host. HIDS can see the outcome of an attempted attack, as they can directly access and monitor the data files and operating system processes targeted by the attack. |
| *Rationale* | The first step in delivering an efficient and secure intrusion protection strategy is accurately detecting all possible threats. To achieve this goal, multiple detection methods including HIDS should be employed to ensure comprehensive coverage.<br><br>The failure to secure any State host system with HIDS puts agencies at a much greater risk of loss. A single attack can cost millions of dollars in time spent recovering from the attack and liability for compromised data and hardware. The damage from an attack to State services can also include inconvenience to citizens and the loss of public confidence. |
| *Benefits* | • HIDS can detect attacks that cannot be seen by a Network-Based IDS since they monitor events local to a host.<br>• HIDS can often operate in an environment where network traffic is encrypted.<br>• HIDS are unaffected by switched networks.<br>• HIDS can detect, and in some cases prevent, attacks that involve software integrity breaches, such as Trojan Horses.<br>• HIDS have the ability to monitor local files for any changes or modifications.<br>• HIDS can see the outcome of an attempted attack since they can directly access and monitor the data files and operating system processes targeted by the attack. |
| **Associated Architecture Levels** | |
| *Domain Name* | Security |
| *Discipline Name* | Technical Controls |
| *Technology Area Name* | Intrusion Detection Systems |
| *Product Component Name* | |
| **Compliance Component Type** | |
| *Component Type* | Guideline |
| *Component Sub-type* | |
| **Compliance Detail** | |
| *Guideline, Standard or Legislation* | **General HIDS Requirements**<br><br>• Administrators shall be trained on the IDS before implementation. Despite vendor claims of ease of use, training and/or experience are absolutely necessary to manage any IDS.<br>• It is preferred to have the HIDS controlled directly from a central location(s). However, the HIDS may be agent-based where response decisions are made at the host.<br>• IDS administrators shall be able to create or change policies easily.<br><br>**HIDS Deployment Requirements**<br><br>• HIDS shall be deployed in conjunction with Network-Based IDS to fully protect |

the system.
- It is recommended that organizations install the Network-Based IDS first, followed by the HIDS installation on critical servers. Once administrators are familiar with the HIDS, it may be installed on the remainder of the organization's hosts.
- HIDS shall be installed on any host where sensitive or critical information is stored.
- It is preferred to install IDS Management software on a separate system from the target host being monitored.
- It is preferred to have the HIDS use an agent-manager (server) architecture, where policy is created and modified on the manager and automatically distributed to all agents.
- It is preferred that host agents poll the manager at periodic intervals for policy changes or new software updates.

**HIDS Analysis Requirements**

- HIDS shall utilize information from operating system audit trails and system logs.
- HIDS shall have easy-to-use tools to analyze the logs.
- HIDS shall detect, and preferably prevent, the following:
  - System scanning (probing the target with different kinds of packets to garner information about the system, such as topology, active hosts, operating systems and software in use),
  - Denial of Service (DoS) (slow or shut down targeted systems or hosts), and
  - Penetration (unauthorized acquisition and/or alteration of system privileges, resources, or data).
- HIDS shall use Misuse Detection methods (matching a predefined pattern of events describing an attack) and may also include Anomaly Detection (abnormal, unusual behavior) components.
- Administrators shall follow a schedule for checking the results of the HIDS to ensure attackers have not modified the system.

**HIDS Response Requirements**

- HIDS shall respond in real-time.
  - It is preferred that HIDS provide active responses to intrusions by:
    - Collecting additional information:
      - Turning up the number of events logged, or
      - Capturing all packets, not just those targeting a particular port or system.
      - Changing the environment:
      - Terminating the connection, or
      - Reconfiguring routers and firewalls to:
      - Block packets from the intruder's IP address,
      - Block network ports, protocols or services, or
      - Sever all connections that use certain network interfaces.
      - HIDS administrators shall work closely with router and firewall administrators when creating rules for routers and firewalls to ensure intruders cannot abuse the feature to deny access to legitimate users.
      - HIDS may provide passive responses requiring subsequent human action to intrusions by:
      - Generating alarms and notifications with popup windows, cellular phones, pagers and email, or
      - Reporting alarms and alerts using SNMP traps and plug-ins to

| | |
|---|---|
| | central network management consoles.<br>- All HIDS communications shall be secure and use encrypted tunnels or other cryptographic measures<br>- HIDS shall create output with the following information for each intrusion detected:<br>- Time/date<br>- Sensor IP address<br>- Specific attack name<br>- Source and destination IP addresses<br>- Source and destination port numbers<br>- Network protocol used<br>- Description of the attack type<br>- Attack severity level<br>- Type of loss expected<br>- Type of vulnerability exploited<br>- Input validation (buffer overflow or boundary condition)<br>- Access validation (faulty access control mechanism)<br>- Exceptional condition<br>- Environmental (unexpected interaction with an application and the operating system or between two applications)<br>- Host Configuration<br>- Race (delay between the time a system checks to see if an operation is allowed and the time it performs the operation)<br>- Design<br>- Software types and versions vulnerable<br>- Patch information to counter the attack<br>- References to advisories about the attack or vulnerability<br>- It is preferred that HIDS reports combine redundant attack entries and make attacks of highest importance stand out. |
| *Source Reference* | NIST SP 800-31 (www.csrc.nist.gov/publications/nistpubs) Intrusion Detection Systems (IDS),<br><br>NIST SP 800-18 (www.csrc.nist.gov/publications/nistpubs)<br>CERT Guide to System and Network Security Practices (www.cert.org/security-improvement/) |

| *Standards Organizations* | | | |
|---|---|---|---|
| *Name* | | *Website* | |
| *Contact Information* | | | |

| *Government Body* | | | |
|---|---|---|---|
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)<br><br>CVE Vulnerability Search on ICAT Metabase | *Website* | http://csrc.nist.gov/<br><br>http://icat.nist.gov/ |
| *Contact Information* | inquiries@nist.gov | | |

| KEYWORDS | |
|---|---|
| *Keywords/Aliases* | Honey Pot, intrusion, cracker, buffer overflows, passwords, sniffing, exploit, denial-of-service, Java, ActiveX, SMURF, DNS, probes |

| COMPONENT CLASSIFICATION | | | |
|---|---|---|---|
| *Classification* | ☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset* | | |
| *Rationale for Component Classification* | | | |
| *Rationale for Component Classification* | | | |
| *Conditional Use Restrictions* | | | |
| *Restrictions* | | | |
| *Migration Strategy* | | | |
| *Migration Strategy* | | | |
| *Impact Position Statement* | | | |
| *Position Statement on Impact* | | | |
| CURRENT STATUS | | | |
| *Current Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |
| AUDIT TRAIL | | | |
| *Creation Date* | 04/03/2003 | *Date Accepted / Rejected* | 05/14/2003 |
| *Reason for Rejection* | | | |
| *Last Date Reviewed* | | *Last Date Updated* | |
| *Reason for Update* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

| DEFINITION | |
|---|---|
| *Name* | Compliance Component - Application-Based Intrusion Detection Systems (IDS) |
| *Description* | Application-Based IDS is a special subset of Host-Based IDS (HIDS) that analyzes the events transpiring within a software application. The most common information source for Application-Based IDS is the application's transaction log file. |
| *Rationale* | The ability to interface with applications directly allows Application-Based IDS to detect suspicious behavior such as users exceeding their security authorization. |
| *Benefits* | • Application-Based IDS monitors the interaction between user and application, which traces activity to individual users.<br>• Application-Based IDS works with applications that access encrypted data since it interfaces with the application at transaction endpoints where information is presented to users in unencrypted form. |
| **ASSOCIATED ARCHITECTURE LEVELS** | |
| *Domain Name* | Security |
| *Discipline Name* | Technical Controls |
| *Technology Area Name* | Intrusion Detection Systems |
| *Product Component Name* | |
| **COMPLIANCE COMPONENT TYPE** | |
| *Component Type* | Guideline |
| *Component Sub-type* | |
| **COMPLIANCE DETAIL** | |
| *Guideline, Standard or Legislation* | **General Application-Based IDS Requirements**<br>• Administrators shall be trained on the Application-Based IDS before implementation. Despite vendor claims of ease of use, training and/or experience are absolutely necessary to manage any IDS.<br>• It is preferred to have the Application-Based IDS controlled directly from a central location(s). However, the Application-Based IDS may be agent-based where response decisions are made at the agent.<br>• Application-Based IDS administrators shall be able to create or change policies easily.<br><br>**Application-Based IDS Deployment Requirements**<br>• Application-Based IDS shall be deployed in conjunction with Network-Based IDS (NIDS) and/or HIDS to fully protect the system.<br>• It is recommended that organizations install the NIDS first, followed by the HIDS, and then the Application-Based IDS installation on critical servers.<br>• Application-Based IDS shall be enabled on hosts that have critical applications.<br>• Application transaction logs shall be enabled.<br>• It is preferred to install Application-Based IDS Management software on a separate system from the application being monitored.<br>• It is preferred to have the Application–Based IDS use an agent-Manager (server) architecture, where policy is created and modified on the manager and automatically distributed to all agents. |

- It is preferred that application agents poll the manager at periodic intervals for policy changes or new software updates.

**Application-Based IDS Analysis Requirements**

- Application-Based IDS shall utilize, at a minimum, information from an application's transaction log files.
- Application-Based IDS shall have easy-to-use tools to analyze the logs.
- Application-Based IDS shall use Misuse Detection methods (matching a predefined pattern of events describing an attack) and may also include Anomaly Detection (abnormal, unusual behavior) components.
- Application-Based IDS may be configured to intercept the following types of requests and use them in combinations and sequences to constitute an application's normal behavior:
- File System (file read or write)
- Network (packet events at the driver (NDIS) or transport (TDI) level)
- Configuration (read or write to the registry on Windows)
- Execution Space (write to memory not owned by the requesting application. For example, attempts to inject a shared library DLL into another process)
- Operators shall follow a schedule for checking the results of the Application-Based IDS to ensure attackers have not modified the system.

**Application-Based IDS Response Requirements**

- Application-Based IDS shall respond in real-time.
- It is preferred that Application-Based IDS provide active responses to intrusions by:
- Collecting additional information by turning up the number of events logged, or
- Terminating the user's access.
- Operators shall be extremely careful when creating rules to ensure intruders cannot abuse the feature to deny access to legitimate users.
- Application-Based IDS may provide passive responses requiring subsequent human action to intrusions by:
- Generating alarms and notifications with popup windows, cellular phones, pagers and email, or
- Reporting alarms and alerts using SNMP traps and plug-ins to central network management consoles.
  - All Application-Based IDS communications shall be secure and use encrypted tunnels or other cryptographic measures.
  - Application-Based IDS shall create output with the following information for each intrusion detected:
  - Time/date
  - Sensor IP address
  - Specific attack name
  - Source and destination IP addresses
  - Network protocol used
  - Description of the attack type
  - Attack severity level
  - Type of loss expected
  - Type of vulnerability exploited
  - Access validation
  - Exceptional condition
  - Environmental (unexpected interaction with the operating system or between two applications)
  - Host Configuration
  - Race (delay between the time a system checks to see if an operation is

| | | | |
|---|---|---|---|
| | allowed and the time it performs the operation)<br>- Design<br>- Software types and versions vulnerable<br>- Patch information to counter the attack<br>- References to advisories about the attack or vulnerability<br>- It is preferred that Application-Based IDS reports combine redundant attack entries and make attacks of highest importance stand out. | | |
| *Source Reference* | NIST SP 800-18 (www.csrc.nist.gov/publications/nistpubs)<br>CERT Guide to System and Network Security Practices (www.cert.org/security-improvement/) | | |
| *Standards Organizations* | | | |
| *Name* | | *Website* | |
| *Contact Information* | | | |
| *Government Body* | | | |
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)<br><br>CVE Vulnerability Search on ICAT Metabase | *Website* | http://csrc.nist.gov/<br><br>http://icat.nist.gov/ |
| *Contact Information* | inquiries@nist.gov | | |
| KEYWORDS | | | |
| *Keywords/Aliases* | Honey Pot, intrusion, cracker, buffer overflows, passwords, sniffing, exploit, denial-of-service, Java, ActiveX, SMURF, DNS, probes, logging, auditing, monitoring, anomaly, patterns, exploits, misuse | | |
| COMPONENT CLASSIFICATION | | | |
| *Classification* | ☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset* | | |
| *Rationale for Component Classification* | | | |
| *Rationale for Component Classification* | | | |
| *Conditional Use Restrictions* | | | |
| *Restrictions* | | | |
| *Migration Strategy* | | | |
| *Migration Strategy* | | | |
| *Impact Position Statement* | | | |
| *Position Statement on Impact* | | | |
| CURRENT STATUS | | | |
| *Current Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |
| AUDIT TRAIL | | | |
| *Creation Date* | 04/03/2003 | *Date Accepted / Rejected* | 05/14/2003 |

| | | | |
|---|---|---|---|
| *Reason for Rejection* | | | |
| *Last Date Reviewed* | | *Last Date Updated* | |
| *Reason for Update* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

# Technology Area Blueprint

| Definition | | | |
|---|---|---|---|
| *Name* | Technology Area - Logical Access Controls | | |
| *Description* | Logical access controls are protection mechanisms that limit users' access to information and restrict their forms of access on the system to only what is appropriate for them. Logical access controls are typically a system of measures and procedures, both within an organization and in the software products used, aimed at protecting computer resources (data, programs and terminals) against unauthorized access attempts. | | |
| *Rationale* | Logical Access Control policies and procedures provide assurance that access to operating systems, programs, and data is limited to properly authorized individuals. | | |
| *Benefits* | • Preventing intruders from entering state systems<br>• Constraining the authorized users to their legitimate purposes | | |
| **Associated Discipline** | | | |
| *Discipline Name* | Technical Controls | | |
| **Keywords** | | | |
| *Keywords/Aliases* | Misuse, entry, least privilege, create, read, write, update, delete | | |
| **Associated Compliance Components** | | | |
| *Compliance Component Names* | • Logon Banners<br>• Date/Time Controls<br>• Inactivity Controls | | |
| **Associated Product Components** | | | |
| *Product Component Names* | | | |
| **Technology Area Detail** | | | |
| *Supporting Documentation* | NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems | | |
| *Source Reference* | www.csrc.nist.gov/publications/nistpubs | | |
| *Standards Organizations / Government Body* | | | |
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) | *Website* | http://csrc.nist.gov/ |
| *Contact Information* | inquiries@nist.gov | | |
| *Name* | National Security Agency (NSA), Security Recommendation Guides | *Website* | http://nsa2.www.conxion.com/index.html |
| *Contact Information* | W2KGuides@nsa.gov | | |
| **Current Status** | | | |
| *Technology Area Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |

| AUDIT TRAIL | | | |
|---|---|---|---|
| *Creation Date* | 3/6/2003 | *Date Accepted / Rejected* | 03/24/2003 |
| *Created By* | | | |
| *Reason for Rejection* | | | |
| *Last Date Updated* | | *Last Date Reviewed* | |
| *Reason for Update* | | | |
| *Updated By* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

# Compliance Component Blueprint

| Definition | |
|---|---|
| *Name* | Compliance Component - Date/Time Controls |
| *Description* | Restrictions based on time and day bolsters the control environment. The intent is to require more than simple access controls, normally based on user-IDs and passwords. |
| *Rationale* | Hackers are most active at night, just when systems are sparsely staffed, if staffed at all. If users stay logged on, hackers can attack their network assets and use them to attack other systems. |
| *Benefits* | Reduces the amount of time the account is open to unauthorized access. |

| Associated Architecture Levels | |
|---|---|
| *Domain Name* | Security |
| *Discipline Name* | Technical Controls |
| *Technology Area Name* | Logical Access Controls |
| *Product Component Name* | |

| Compliance Component Type | |
|---|---|
| *Component Type* | Guideline |
| *Component Sub-type* | |

| Compliance Detail | |
|---|---|
| *Guideline, Standard or Legislation* | • Whenever possible access control should constrain the user to use of the system within a limited working day and only on normal working days of the week (some systems even make allowances for denying access on public holidays). Such a restriction helps prevent misuse of the system out of hours by an employee (a cleaner, perhaps) or by a hacker (who often rely on out-of-hours access to avoid detection by legitimate users).<br>• Similarly, restrictions should be placed on the workstations the user can employ and on the applications that can be run on a particular workstation. This measure is particularly useful in limiting very privileged activities (system support, security administration, for example) to certain workstations and thus putting a physical barrier in the way of a would-be attacker. |
| *Source Reference* | NIST SP 800-18 (www.csrc.nist.gov/publications/nistpubs)<br>CERT Guide to System and Network Security Practices (www.cert.org/security-improvement/) |

| *Standards Organizations* | | | |
|---|---|---|---|
| *Name* | Carnegie Mellon University, CERT/Coordination Center (CERT/CC) | *Website* | www.cert.org |
| *Contact Information* | cert@cert.org | | |

| *Government Body* | | | |
|---|---|---|---|
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) | *Website* | http://csrc.nist.gov/ |
| *Contact Information* | inquiries@nist.gov | | |

| KEYWORDS | | | |
|---|---|---|---|
| *Keywords/Aliases* | Access, times, work schedule, hours, system availability, after hours | | |
| **COMPONENT CLASSIFICATION** | | | |
| *Classification* | ☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset* | | |
| *Rationale for Component Classification* | | | |
| *Rationale for Component Classification* | | | |
| *Conditional Use Restrictions* | | | |
| *Restrictions* | | | |
| *Migration Strategy* | | | |
| *Migration Strategy* | | | |
| *Impact Position Statement* | | | |
| *Position Statement on Impact* | | | |
| **CURRENT STATUS** | | | |
| *Current Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |
| **AUDIT TRAIL** | | | |
| *Creation Date* | 3/6/2003 | *Date Accepted / Rejected* | 03/24/2003 |
| *Reason for Rejection* | | | |
| *Last Date Reviewed* | | *Last Date Updated* | |
| *Reason for Update* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

| Definition | |
|---|---|
| *Name* | Compliance Component - Inactivity Controls |
| *Description* | Inactivity controls prevent unauthorized disclosure of information and unauthorized system usage by terminating an electronic session after a pre-determined time of inactivity. |
| *Rationale* | Appropriate inactivity safeguards must be used to prevent unauthorized access to or use of information, data, and software resident on computers, peripheral devices, and storage media, or transmitted over communication lines or networks. Inactivity controls are particularly necessary in open offices where there are no walls and many people leave their computers on and available for anyone who happens to walk by. |
| *Benefits* | • Prevent unauthorized disclosure<br>• Prevent unauthorized system usage |
| **Associated Architecture Levels** | |
| *Domain Name* | Security |
| *Discipline Name* | Technical Controls |
| *Technology Area Name* | Logical Access Controls |
| *Product Component Name* | |
| **Compliance Component Type** | |
| *Component Type* | Guideline |
| *Component Sub-type* | |
| **Compliance Detail** | |
| *Guideline, Standard or Legislation* | • If the computer system contains sensitive information, users shall log-out or invoke a password-protected screen saver before leaving their computer unattended.<br>• If there has been no activity on a computer terminal, workstation, or microcomputer (PC) for a maximum of thirty (30) minutes, the system shall be electronically locked. Re-establishment of the session shall take place only after the user has renewed access via the proper authentication, such as a password.<br>• During computing sessions, user ids are locked out or disabled after specified period of inactivity.<br>– For normal users, screen lockout will occur after a maximum of 30 minutes of inactivity.<br>– For users with administrative or system-level privileges, screen lockout will occur after a maximum of 15 minutes of inactivity.<br>– Users will be required to re-enter their password to continue their sessions after screen lockout due to inactivity.<br>– Prior to screen lockout, the user may receive a display on the screen warning the user of a pending screen lockout.<br>• User IDs that are inactive on the system for a specific period of time (e.g., three months) should be disabled.<br>• User id inactivity results in suspension of access authorization and requires renewal of privileges.<br>– 4 consecutive days of inactivity following notification of new user id setup.<br>– 120 consecutive days of inactivity of existing user ids. |

| | | | |
|---|---|---|---|
| *Source Reference* | NIST SP 800-18 (www.csrc.nist.gov/publications/nistpubs)<br>CERT Guide to System and Network Security Practices (www.cert.org/security-improvement/) | | |
| *Standards Organizations* | | | |
| *Name* | Carnegie Mellon University, CERT/Coordination Center (CERT/CC) | *Website* | www.cert.org |
| *Contact Information* | cert@cert.org | | |
| *Government Body* | | | |
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) | *Website* | http://csrc.nist.gov/ |
| *Contact Information* | inquiries@nist.gov | | |
| KEYWORDS | | | |
| *Keywords/Aliases* | Idle, time out, login, screen saver, lockout | | |
| COMPONENT CLASSIFICATION | | | |
| *Classification* | ☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset* | | |
| *Rationale for Component Classification* | | | |
| *Rationale for Component Classification* | | | |
| *Conditional Use Restrictions* | | | |
| *Restrictions* | | | |
| *Migration Strategy* | | | |
| *Migration Strategy* | | | |
| *Impact Position Statement* | | | |
| *Position Statement on Impact* | | | |
| CURRENT STATUS | | | |
| *Current Status* | ☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected* | | |
| AUDIT TRAIL | | | |
| *Creation Date* | 3/6/2003 | *Date Accepted / Rejected* | 03/24/2003 |
| *Reason for Rejection* | | | |
| *Last Date Reviewed* | | *Last Date Updated* | |
| *Reason for Update* | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

# Compliance Component Blueprint

| Definition | |
|---|---|
| *Name* | Compliance Component - Logon Banners |
| *Description* | A Logon Banner is verbiage that an end-user sees at the point of access to a system which sets the right expectations for users regarding authorized and acceptable use of a computer system and its resources, data, and network access capabilities. These expectations include notice of authorized monitoring of users' activities while they are using the system, and warnings of legal sanctions should the authorized monitoring reveal evidence of illegal activities or a violation of security policy. |
| *Rationale* | Failure to include a logon banner regarding authorized and acceptable use of a computer system can make it difficult to prosecute violations when they occur. Legal cases exist in which defendants have been acquitted of charges for tampering with computer systems because no explicit notice was given prohibiting unauthorized use of the computer systems involved. In other cases, organizations have been taken to court for alleged violations of individual privacy because no notice was given and acknowledged regarding authorized monitoring of users' activities on computer systems. |
| *Benefits* | • Logon Banners are particularly important in cases that consider whether government employees enjoy a reasonable expectation of privacy in government computers.<br>• Pre-logon warning messages can deter unauthorized use, increase IT security awareness, and provide a legal basis for prosecuting unauthorized access.<br>• A key to establishing that a user has no right to privacy when using State networks and/or computer systems is the implementation of a logon banner. |
| **Associated Architecture Levels** | |
| *Domain Name* | Security |
| *Discipline Name* | Technical Controls |
| *Technology Area Name* | Logical Access Controls |
| *Product Component Name* | |
| **Compliance Component Type** | |
| *Component Type* | Guideline |
| *Component Sub-type* | |
| **Compliance Detail** | |
| *Guideline, Standard or Legislation* | Logon banners are required on all State Information Technology access points. Such a banner shall warn authorized and unauthorized users:<br>• What is considered the proper use of the system.<br>• Only authorized users are to proceed beyond the banner.<br>• Users who login represent that they are authorized to do so.<br>• Unauthorized system usage or abuse is subject to disciplinary action and/or civil and criminal action.<br>• Use of the system constitutes consent to monitoring.<br>• Use of the system constitutes consent to the retrieval and disclosure of information stored on the network.<br>• Users of the system shall have no reasonable expectation of privacy in the network.<br>• Contains express or implied limitations or authorizations relating to the purpose of any monitoring, who may conduct the monitoring, and what will be done with the fruits of any monitoring. |

| | | | |
|---|---|---|---|
| | • Require users to "click through" or otherwise acknowledge the banner before using the system.<br><br>Logon banners should not identify sensitive information about the organization, the data systems, network, hardware, operating system, system configuration, or other internal matters.<br>• The following is an example logon banner that could be used for users connecting to internal computer systems:<br><br>NOTICE TO USERS<br>This is a State computer system and is the property of the same. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.<br><br>Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized State and law enforcement personnel, as well as authorized officials of other agencies. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized personnel.<br><br>Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. Do not continue to use this system if you do not agree to the conditions stated in this warning.<br><br>• Each Agency should tailor its logon banners to their precise needs.<br>• Any questions should be directed to your organization's legal counsel. | | |
| *Source Reference* | NIST SP 800-18 (www.csrc.nist.gov/publications/nistpubs)<br>CERT Guide to System and Network Security Practices (www.cert.org/security-improvement/) | | |
| *Standards Organizations* | | | |
| *Name* | Carnegie Mellon University, CERT/Coordination Center (CERT/CC) | *Website* | www.cert.org |
| *Contact Information* | cert@cert.org | | |
| *Government Body* | | | |
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) | *Website* | http://csrc.nist.gov/ |
| *Contact Information* | inquiries@nist.gov | | |
| KEYWORDS | | | |
| *Keywords/Aliases* | Logon, username, welcome screen | | |
| COMPONENT CLASSIFICATION | | | |
| *Classification* | ☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset* | | |

| Rationale for Component Classification | | | |
|---|---|---|---|
| Rationale for Component Classification | | | |
| **Conditional Use Restrictions** | | | |
| Restrictions | | | |
| **Migration Strategy** | | | |
| Migration Strategy | | | |
| **Impact Position Statement** | | | |
| Position Statement on Impact | | | |
| **CURRENT STATUS** | | | |
| Current Status | ☐ In Development ☐ Under Review ☒ Approved ☐ Rejected | | |
| **AUDIT TRAIL** | | | |
| Creation Date | 3/6/2003 | Date Accepted / Rejected | 3/24/2003 |
| Reason for Rejection | | | |
| Last Date Reviewed | | Last Date Updated | |
| Reason for Update | | | |

Click on this link to return to the Security Blueprint Samples – Set Two.

## TECHNOLOGY ARCHITECTURE COMMUNICATIONS DOCUMENT SAMPLES

### *APPLICATION DEVELOPMENT CLASSIFICATION REPORT*

The following is an example of a communications document that Team Leaders or Managers might request. Once the Architecture Blueprints are documented, the range of communications documents is limited only by the requirements of the Audience and the criteria set forth by the architecture governance groups.

The Architecture Blueprint Vitality Process ensures the up-to-date data that is essential to the communication of useful information.

*Domain:* Application Architecture *Discipline:* Application Development Management

| *Technology Area* | *Emerging Technologies* | *Current Technologies* | *Twilight Technologies* | *Sunset Technologies* |
|---|---|---|---|---|
| Analysis/Design Environment | • Object Oriented Analysis and Design<br>• UML<br>• CDIF | • Information Engineering | • Structured Analysis and Design | |
| Programming Language / Environment | • Java | • Visual Basic<br>• COBOL II (MF, AS)<br>• C<br>• C++ | • COBOL (MF, AS)<br>• RPG (AS)<br>• Pascal | |
| Code / Screen Generation | • Advantage Joe | • Advantage Plex | • Power Builder<br>• Knowledgeware ADW | |
| Documentation | • 9 Standard Products | • JCIT reporting requirements | | |
| Commercial Products | • CRM | • ERP<br>• MRP | • General Ledger Software | |

## *ELECTRONIC COLLABORATION CLASSIFICATION REPORT*

*Domain:* Application Architecture | *Discipline:* Electronic Collaboration

| *Technology Area* | *Emerging Technologies* | *Current Technologies* | *Twilight Technologies* | *Sunset Technologies* |
|---|---|---|---|---|
| E-mail | | • SMTP<br>• MIME<br>• IMAP4<br>• POP3 | • OV/VM<br>• IMAP3<br>• POP2 | |
| Document Format | • XML | • .rtf<br>• .txt<br>• .pdf | | |
| Spreadsheet | | • MS Excel | • SYLK | |
| Images | • JPEG 2000<br>• SVG | • .bmp<br>• TIFF<br>• GIF<br>• JPEG<br>• MPEG | • Proprietary | |
| Document Digitizing | | • TWAIN<br>• ISIS | | |
| Character Recognition | | | | |
| Document Endorsement and Authentication | • Digitized signature<br>• Digitized signature with biometric data<br>• PKI digital signature (X.509v3)<br>• Biometric imprint | • Physical signature | | |
| Calendaring | • ICAP<br>• iCalendar | • MS Outlook | | |
| Electronic Forms | • XHTML Extended Forms<br>• XFA | • XFDL | • OFDL<br>• 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<br>• Biometrics | • Cypher lock<br>• Key card<br>• Bar code | • Property stickers<br>• Key locks | |
| User Security | | | | |
| *- Authentication* | • Smart cards<br>• Kerberos<br>• Biometrics | • Token-based-2-factor<br>• Certificates (x.509)<br>• Passwords<br>• RADIUS/TACACS | • Address-based | |
| *- Authorization* | | • Directory-based services<br>• LDAP | • Access-control-lists<br>• X.500<br>• Password protected directories<br>• OS-based systems | |
| *- Audit* | | • Vendor specific<br>• OS Specific | • SYSLOG | |
| Application Security | • Transport Layer Security (TSL) | • S/MIME<br>• PGP<br>• SSL<br>• Middle-ware<br>• Signed JAVA | • Privilege mode (root user)<br>• Embedded Application specific security | |
| Hardware / System Security | | • NT Domains<br>• TOPSECRET/ RACF/TACACS<br>• Virus control<br>• Intrusion detection | • ACF2 | |
| Data Security | • Advanced Encryption Standard (AES) | • CORBA<br>• Virus control<br>• PGP | • Embedded passwords | |
| Network Security | • AES (encryption) | • Firewalls/router ACL<br>• IPSEC<br>• Encryption (3 DES/RSA)<br>• Encrypted VPN<br>• Intrusion Detection<br>• Vulnerability Scanners | • Dedicated lines | |

*Domain:* Application Architecture | *Discipline:* Electronic Collaboration

| *Technology Area* | *Emerging Technologies* | *Current Technologies* | *Twilight Technologies* | *Sunset Technologies* |
|---|---|---|---|---|
| Security Administration | • Directory-based services | • Product specific | • Product specific | |

## DOMAIN/DISCIPLINE – COMBINATIONS

The nine Domains used as the example for the Tool-Kit are compiled from information gathered from states and counties that are already working with their enterprise architecture. As the architecture sample models evolve, the domains may change.

The Domains are further broken out into 26 technical functional areas, described in this document as Disciplines. Table 1depicts the 26 disciplines and the domains as used in this document.

Descriptions of the type of information contained in the disciplines used in this document are located in Appendix 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<br>• Knowledge Management<br>• GIS<br>• Data Storage |
| Application | • Application Development Management<br>• Electronic Collaboration |
| Integration | • Functional Integration<br>• Middleware |
| Access | • Access<br>• Branding<br>• Accessibility |
| Network | • Physical Network<br>• Network Management |
| Platform | • Platform<br>• Configuration Management |
| Systems Management | • Asset Management<br>• Change Management<br>• Console/Event Management<br>• Help Desk/Problem Management<br>• Business Continuity |
| Privacy | • Profiling<br>• Personalization<br>• Privacy |
| *Security* | • Enterprise Security<br>• Network Security<br>• Host Security |

*Table 1. Domains & Disciplines*

On the other hand, minimizing the number of domains may present the risk of once again dealing with a piece that becomes too huge to manage. It is best to keep the number of domains to a minimum of five and a maximum of 10.

The disciplines within each domain have been grouped logically, based on the close relationship between the discipline and the domain, as well as the relationships to other disciplines within the domain. Table 1 shows the disciplines and how they are grouped within the nine domains.
Figure 7 provides a pictorial view of the sample Domains that make up the Technology Architecture in this Tool-Kit.

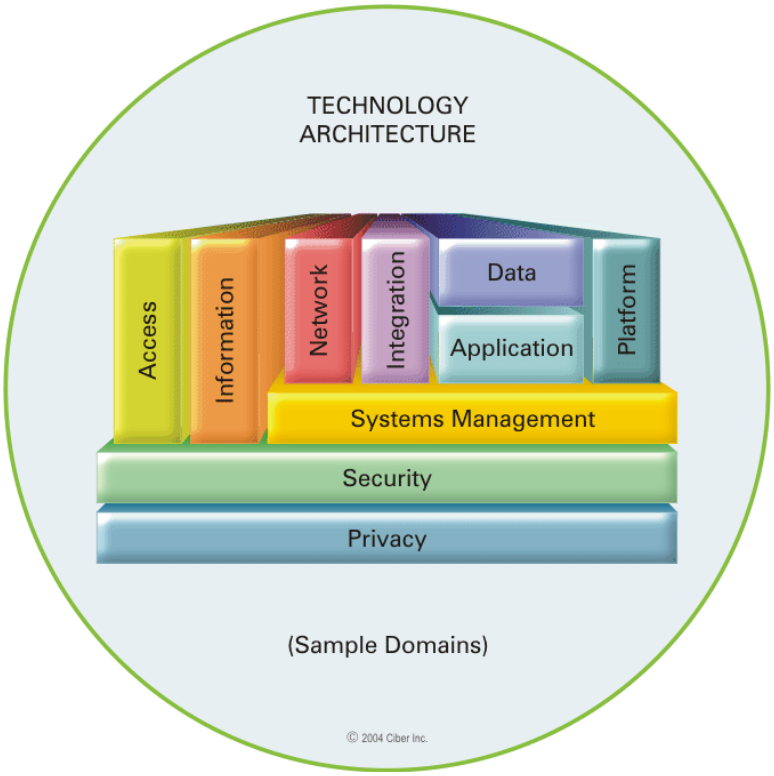



*Figure 7. Sample Technology Architecture Domains*

## DOMAIN/DISCIPLINE – INTERSECTIONS

Be aware that disciplines can also intersect with disciplines in other domains. Note all intersections so that changes made in one discipline will not be overlooked in another related discipline.

The matrix in Table 2 portrays an example of the relationships between disciplines. As with the choice of domains and disciplines, your ideas of how the relationships match up may differ from the example here. This is merely the example of the tool that was used to assist in determining the organization of the disciplines and domains for this project.

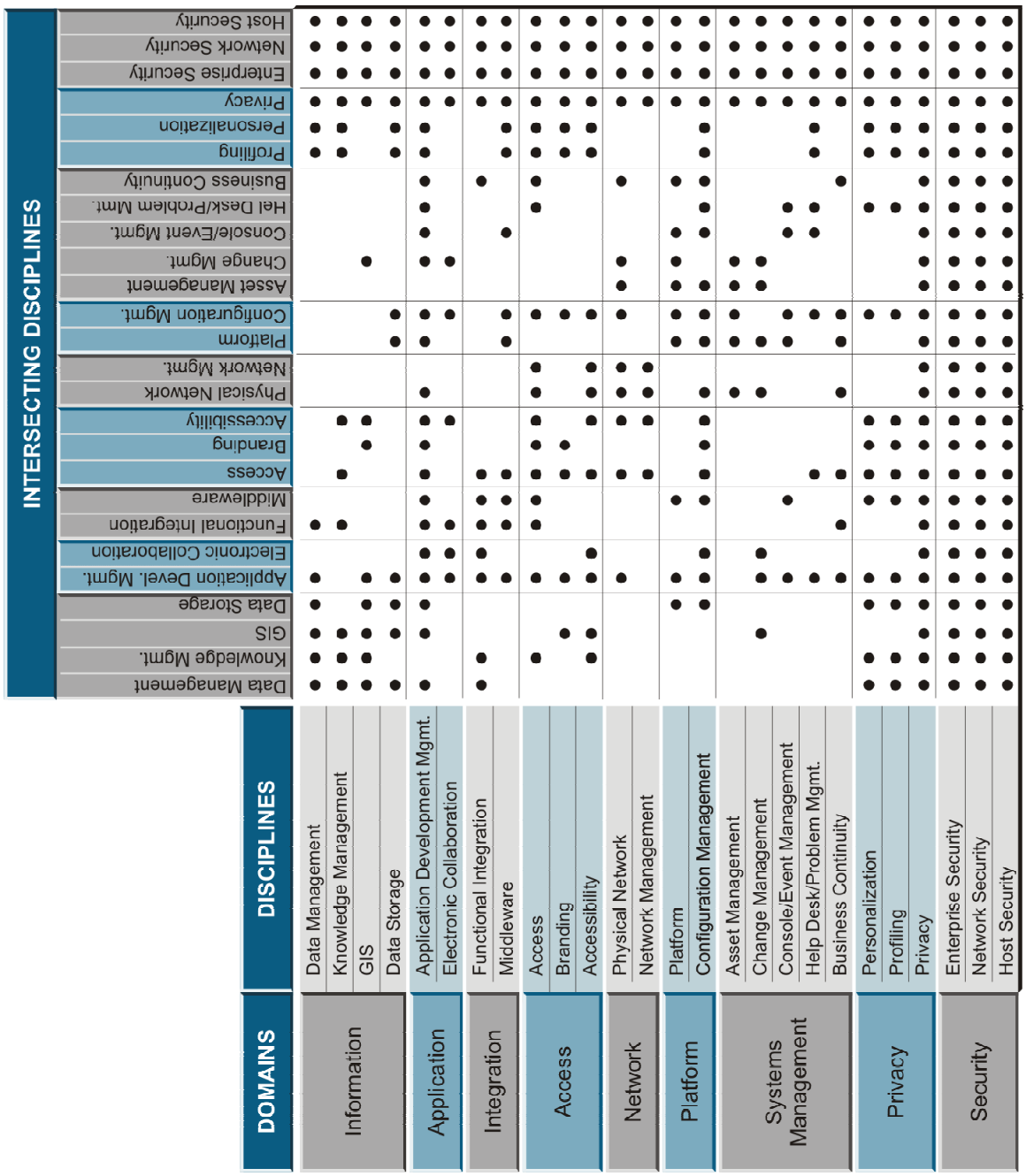
A tool such as this may be used within the organization to identify relationships and coordination efforts that must occur when decisions are made or changes are mandated. It is used for quickly identifying the points of coordination that are essential between the disciplines.

As mentioned earlier, when building a home we can rely on the experience of those who have previously built homes to provide plans and logical groupings of functions, such as plumbing, electrical, etc. By separating disciplines into logical categories, we can also utilize IT Subject Matter Experts in the various fields to perform the work or advise concerning items of importance.

Though the basic elements of every home built may follow a similar pattern, it is not necessary that every home be the same. In most cases, each home will have individual characteristics particular to the requirements of the owner, based on the environment, available funding, or personal preferences.

Likewise, while developing the enterprise architecture within the organization, be aware of required items and components particular to the organization and address them accordingly.

*Table 2. Domain-Discipline Intersection Matrix*



# SUMMARY/CONCLUSION

The Technology Architecture provides a framework, based on business needs that are aligned with technology, for developing technology solutions that operate across agencies and align with the business needs of state and local governments.

It is through the pursuit of a formal Technology Architecture that the following are provided:

- A demonstrable, repeatable approach to assuring critical technology standards are documented and shared throughout the enterprise
- A clear understanding of the enterprise's emerging, current, twilight and sunset technology products and/or compliance standards.
- Identification of opportunities to leverage linkage across government-wide entities and increase collaboration and sharing of technology and information
- A means to increase re-use of technology, systems, application or configurations and reduce redundancy throughout the enterprise.

The Technology Architecture identifies and inter-relates the technology assets of the enterprise to enable sharing and exchange of critical information. Though enterprise typically refers to the organization as a whole, the development of Technology Architecture can also be accomplished at an agency level. For example, in North Carolina, compliance standards are determined at the enterprise (statewide) level, and the products are determined at the agency level, based on the enterprise standards.

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

www.nascio.org