Commonwealth of Virginia

Enterprise Technical Architecture (ETA)

Enterprise Systems Management

Version 1.1 July 1, 2016

Prepared by:

Virginia Information Technologies Agency
ETA Enterprise Systems Management Domain Team

(This Page Intentionally Left Blank)

Enterprise Systems Management Domain Team Members

Cindy Bryce ..... VITA, Computer Services
Peter Ritscheid ..... Virginia Department of Health
Susan Rudloff ..... VITA, CSS DEUS
Tony Shoot ..... Northrop Grumman Corporation
Chuck Tyger .....VITA, Technology Strategy and Architecture
Lynn Wasz ..... VITA, Finance
Steve Crabtree ……....VITA, VCCC
Easton Rhodd (Team Facilitator) .....VITA, Technology Strategy and Architecture

The Enterprise Systems Management Domain team began its work by delineating the team's goals, objectives, and scope of work. Discussions included how the domain interfaces with other architecture domains, present and future directions, and how often the information provided in this document is to be updated. The team also reviewed input from industry publications and subject matter experts. The results of the team's efforts, research, and deliberations are provided throughout this document

Enterprise Systems Management Domain Report: Version History		
Revision	**Date**	**Description**
1.0	07-10-2006	Initial
1.1	*07-01-2016*	*Update necessitated by changes in the Code of Virginia and organizational changes in VITA. The changes are administrative. There are no substantive changes to the principles, recommended practices or requirements.*

Review Process

Technology Strategy and Solutions Directorate Review

The domain report was reviewed and approved by ~~Jerry Simonoff, Director and Paul Lubic, the Associate Director of Policy, Practices, and~~ *the Manager of the Enterprise Architecture* Division.

Online Review

Participation of all Executive Branch agencies was encouraged through a review and comment period via VITA's Online Review and Comment Application (ORCA). Technology businesses and the general public were also actively encouraged to use ORCA to provide comments. All comments were considered and many resulted in modifications to the final document. Additionally, the Domain team provided the reviewers with responses to their comments.

(This Page Intentionally Left Blank)

Table of Contents

Executive Summary

The ETA defines the required Information Technology (IT) requirements that will support the Commonwealth's business strategies and specifies IT policies, principles, standards, and recommended practices for the Commonwealth.

This ESM is part of the ETA and defines vital architectural components related to the management and control of hardware, infrastructure related software, and operating processes.

The ESM domain team was commissioned to develop and define recommended practices, procedures, and standards to address:

1. Coordination of ESM services,
2. Operational processes and procedural aspects of ESM, and
3. Technical processes that monitor and control applications, databases, server platforms, network components, and user's interactions.

This effort produced several principles, recommended practices, and requirement statements that will allow the Commonwealth to deliver on IT service obligations. The goal of these principles, recommended practices, and requirements is to support the creation of an ETA that:

- Provides timely system performance information to manage the IT infrastructure.
- Provides cost and financial data to determine infrastructure Total Cost of Ownership (TCO).
- Ensures business partners' Quality of Service (QoS) requirements are consistently met.
- Ensures an open infrastructure environment by limiting the use of proprietary systems management tools and products.
- Encourages unfettered information access and availability.
- Assists with the selection of and deployment of systems management tools and products to support business performance requirements.
- Reduces cycle time required to respond and resolve customer's issues and problems.
- Establishes a monitoring management system to control all aspects of the infrastructure environment.

Agencies with ESM responsibilities will benefit greatly be integrating these requirements and recommended practices into their IT service organization.

(This Page Intentionally Left Blank)

Overview

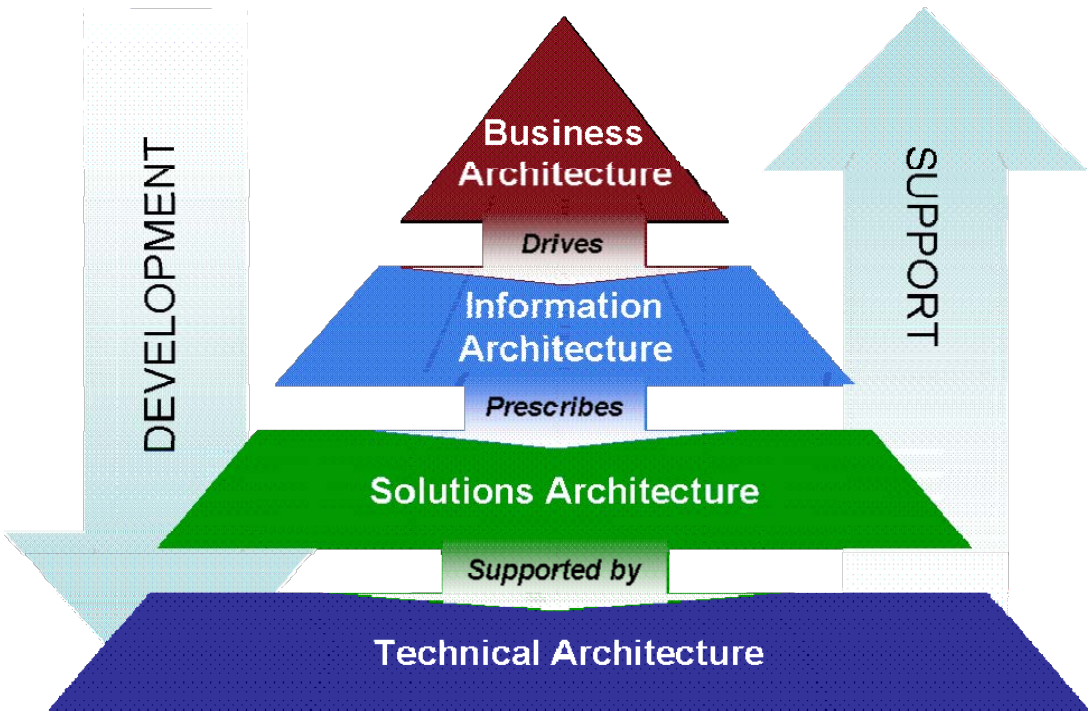
The Commonwealth's Enterprise Architecture is a strategic asset used to manage and align the Commonwealth's business processes and Information Technology (IT) infrastructure/solutions with the State's overall strategy.

The Enterprise Architecture is also a comprehensive framework and repository which defines:

- the models that specify the current ("as-is") and target ("to-be") architecture environments,
- the information necessary to perform the Commonwealth's mission,
- the technologies necessary to perform that mission, and
- the processes necessary for implementing new technologies in response to the Commonwealth's changing business needs.

The Enterprise Architecture contains four components as shown in the model in Figure 1.

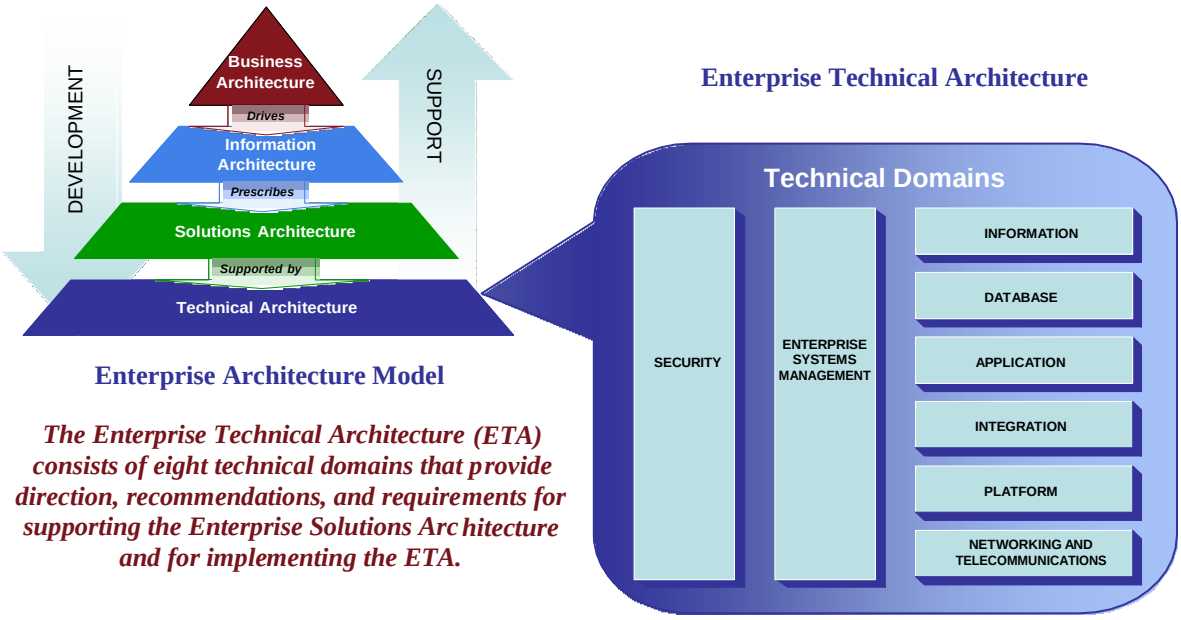
Figure 1
Commonwealth of Virginia Enterprise Architecture Model



The Business Architecture drives the Information Architecture which prescribes the Solutions Architecture that is supported by the Technical (technology) Architecture.

The Enterprise Technical Architecture (ETA) shown in Figure 2 consists of eight technical domains that provide direction, recommendations and requirements for supporting the Solutions Architecture and for implementing the ETA. The ETA guides the development and support of an organization's information systems and technology infrastructure.

Figure 2
ETA Relationship to the Enterprise Architecture



Each of the domains is a critical piece of the overall ETA. The Networking and Telecommunications and Platform Domains address the infrastructure base and provide the foundation for the distributed computing. The Enterprise Systems Management, Database, Applications, and Information Domains address the business functionality and management of the technical architecture. The Integration Domain addresses the interfacing of disparate platforms, systems, databases and applications in a distributed environment. The Security Domain addresses approaches for establishing, maintaining, and enhancing information security across the ETA.

This report addresses the Enterprise Technical Architecture Enterprise Systems Management Domain and includes requirements and recommended practices for Virginia's agencies[1, 2].

[1] This report provides hyperlinks to the domain report Glossary in the electronic version. In the electronic and printed versions, the hyperlinks will have the appearance established by the preferences set in the viewing/printing software (e.g., Word) and permitted by the printer. For example, the hyperlinks may be blue and underlined in the screen version and gray and underlined in the printed version.

[2] The Glossary entry for agency is critical to understanding ETA requirements and standards identified in this report and is repeated here. **State agency or agency -** Any agency, institution, board, bureau, commission, council, or instrumentality of state government in the executive branch listed in the appropriation act. ETA requirements/standards identified in this report are applicable to all agencies

This report was developed by the Enterprise Systems Management Domain team, which was commissioned to identify domain related requirements and recommendations. Identified requirements and technology product standards from this domain report will be combined with requirements and technology product standards from other technical domain reports into a single ETA Standard for review and acceptance by the Information Technology Investment Board (ITIB). *In 2010 the ITIB was replaced by the Information Technology Advisory Council (ITAC).*

Concerning local governments, courts, legislative agencies, and other public bodies, while they are not required to comply with a requirement unless the requirement is a prerequisite for using a VITA service or for participating in other state-provided connectivity and service programs, their consideration of relevant requirements is highly recommended. This architecture was designed with participation of local government and other public body representatives with the intent of encouraging its use in state and local interconnectivity efforts.

including the administrative functions (does not include instructional or research functions) of institutions of higher education, unless exempted by language contained in a specific requirement/standard.

Commonwealth of Virginia: To-Be ETA

The to-be Enterprise Technical Architecture envisioned for the Commonwealth will be one where the Commonwealth's citizens and other customers who wish to access Virginia services will do so by utilizing an Enterprise Portal via standard web browsers.

Where appropriate, these online government services will be developed, delivered and supported using a Service-Oriented Architecture (SOA) based on open and industry standard solutions. Selected legacy applications will be exposed to the SOA using web services.

The SOA will be supported by an Enterprise Service Bus that provides Orchestration and Choreography Services to the agencies.

Central integration and coordination will be managed by an Integration Competency Center (ICC) that supports agency needs such as: asynchronous message queuing and persistence.

Large complex *mission critical* applications that need to be reliable, scalable, secure and highly available will be n-tiered and will utilize business rule and workflow engines.

Enterprise application software for the core government administrative business functions will be consolidated and the underlying business processes modernized. An Application Management Center of Excellence will service and manage the new enterprise applications that replace existing legacy and silo-based applications.

Data will be exchanged among systems, agencies, institutions of higher learning, localities, the federal government, and partners using XML based standards such as the Global Justice XML Data Model and the National Information Exchange Model.

The number and types of software tools and products used by the Commonwealth will be decreased to reduce complexity. This will create the opportunity for agencies to refocus their current in-house IT resources to achieve higher levels of expertise on the fewer required products resulting in, among other benefits, a lower dependence on outside contractors.

Agency software applications and customer services will be delivered and supported by an IT infrastructure that will:

- Be responsive, agile, modular, scalable, reliable, secure, and highly available (24x7)
- Utilize ITIL (IT Infrastructure Library) best practices
- Have extensive and proactive technology refreshment
- Utilize a shared services model for technology delivery
- Have a single secure state-wide network and Intranet
- Have a state-of-the-art data center and back-up facility
- Consolidate agency servers in their most cost-effective locations

- Unify statewide electronic mail services
- Employ innovative procurements, supplier partnerships, and financing arrangements to fund, expedite, and ensure the performance of future initiatives
- Provide a statewide customer care center
- Improve the cost performance of IT utilized by the Commonwealth

Transition:

The Commonwealth will transition from silo-based, application centric and agency centric information technology investments to an enterprise approach where applications are designed to be flexible. This allows agencies to take advantage of shared and reusable components, facilitates the sharing and reuse of data where appropriate, and makes the best use of the technology infrastructure that is available.

The implementation of the to-be architecture will take some time. It is not the intent of the Commonwealth to force agencies to replace their existing systems. The migration to the to-be architecture will occur as Agencies consider new information technology investments or make major enhancements/replacements to their existing systems. It is important to note that the Commonwealth ETA is not static; it needs to continue to evolve to support changing business strategies and technology trends.

Rationale:

Agencies can achieve the following benefits resulting from the Commonwealth's implementation of the ETA:

- Better responsiveness to changing business needs and rapidly evolving information technologies.
- Greater ease of software application integration and application interfacing.
- Easier secure access to data and information to enable interagency collaboration and sharing.
- Increased levels of application interoperability within the Commonwealth, with other states and municipalities, and with the Federal government.
- Increased sharing and re-use of current information technology assets.
- Faster deployment of new applications.
- Reduction in costs required to develop, support and maintain agency applications.

Definition of Key Terms

All of the Enterprise Systems Management Domain ETA standards and requirements considered to be critical components for implementing the Commonwealth's ETA are included in this report.

The report presents three forms of technical architecture guidance for agencies to consider when planning or when making changes or additions to their information technology:

- Requirements – mandatory enterprise technical architecture directions. All requirements are included within the ETA Standard.
- Technology Component Standard Tables - indicate what technologies or products that agencies may acquire at a particular point in time. These are mandatory when acquiring new or replacing existing technology or products. All technology component standard tables are included within the ETA Standard.
- Recommended Practices - provided as guidance to agencies in improving cost efficiencies, business value, operations quality, reliability, availability, decision inputs, risk avoidance or other similar value factors. Recommended Practices are optional.

The following terminology and definitions are applicable to the technology component standard tables presented in this report:

Strategic:

This technology is considered a strategic component of the Commonwealth's Enterprise Technical Architecture. It is acceptable for current deployments and shall be used for all future deployments.

Emerging:

This technology requires additional evaluation in government and university settings. This technology may be used for evaluative or pilot testing deployments or in a higher education research environment. Any use, deployment or procurement of this technology beyond higher education research environments requires an approved *Commonwealth Enterprise Technical Architecture Exception*. The results of an evaluation or pilot test deployment should be submitted to the **VITA Technology Strategy and Solutions: Policy, Practice and Architecture Division** for consideration in the next review of the Enterprise Technical Architecture for that technology.

Transitional/Contained:

This technology is not consistent with the Commonwealth's Enterprise Technical Architecture strategic direction. Agencies may use this technology only as a transitional strategy for moving to a strategic technology. Agencies currently using this technology should migrate to a strategic technology as soon as practical. A migration or replacement plan should be included as part of the Agency's IT Strategic Plan. New deployments or procurements of this technology require an approved *Commonwealth Enterprise Technical Architecture Exception.*

Obsolescent/Rejected:

This technology may be waning in use and support, and/or has been evaluated and found not to meet current Commonwealth Technical Architecture needs. Agencies shall not make any procurements or additional deployments of this technology. Agencies currently using this technology should plan for its replacement with strategic technology to avoid substantial risk. The migration or replacement plan should be included as part of the Agency's IT Strategic Plan.

Agency Exception Requests

Agencies that desire to deviate from the requirements or the technology component standards specified in this report shall request an exception for each desired deviation and receive an approved *Enterprise Technical Architecture Change/Exception Request Form* prior to developing, procuring, or deploying such technology or not complying with a requirement specified in this report. The instructions for completing and submitting an exception request are contained within the *Commonwealth Enterprise Architecture Policy*.

(This Page Intentionally Left Blank)

Enterprise Systems Management Scope

Domain Processes and Components

The ESM domain team's mission was to develop Commonwealth policies, requirements, and recommended practices for administering, monitoring, and controlling IT infrastructure components and processes. The Information Technology Infrastructure Library (ITIL) was adopted as the baseline for implementing ESM processes and the starting point to define the domain scope. The team's research identified domain components illustrated in figure 3 below for inclusion in the Commonwealth's ESM framework.

Figure 3 - ESM Processes and Components

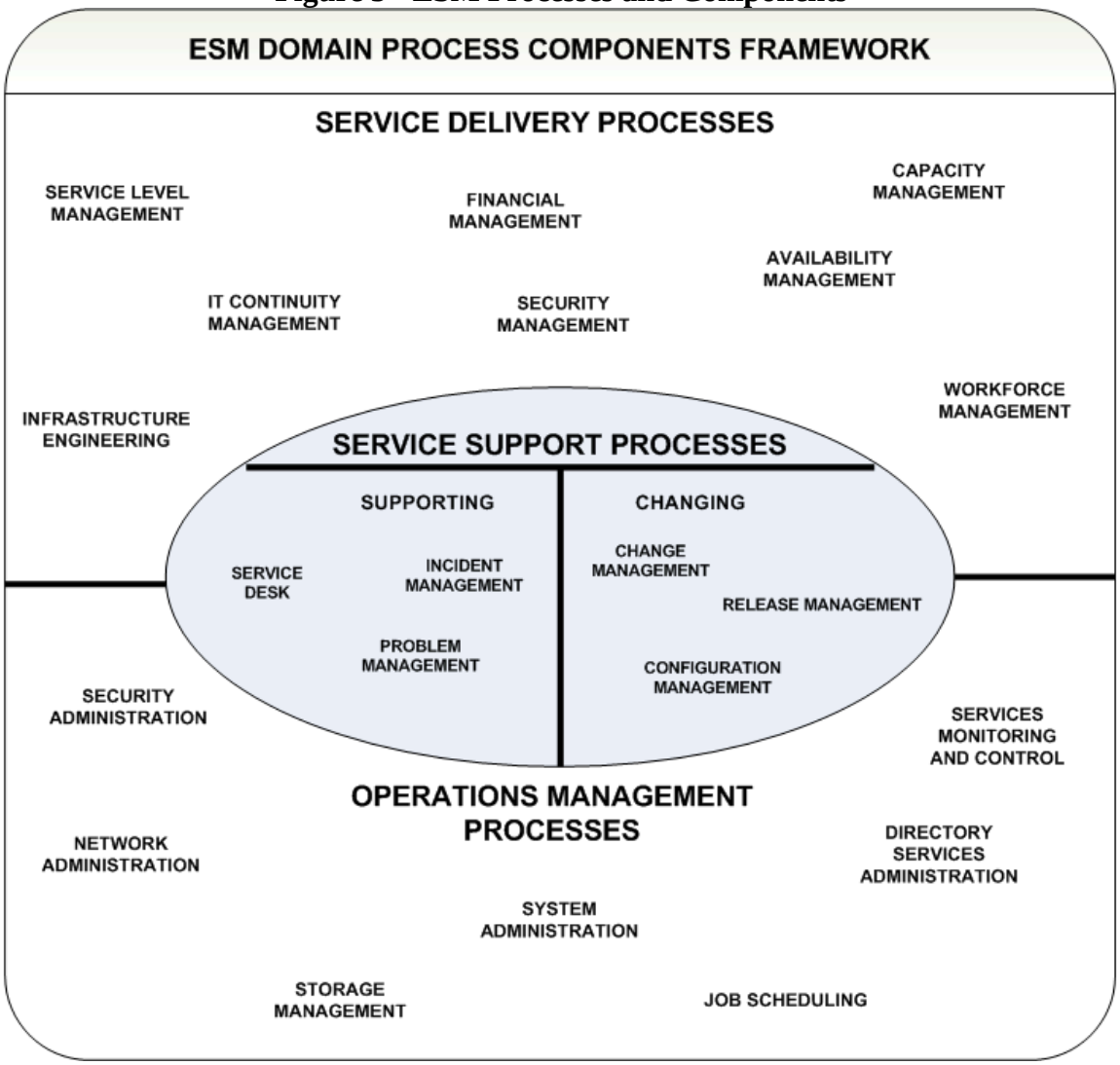


Figure 3 represents the Commonwealth's vision for ESM. This framework was derived from subject matter expert's knowledge of ITIL and infrastructure operations. To

complement this knowledge, other industry sources were consulted in order to gain an understanding of best practices and emerging trends.

There are three core processes or technology topics within the framework: Service Delivery, Service Support, and Operations Management. Each core process or technology topic defines critical components necessary to meet or exceed customers' expectations.

- *Service Delivery* relates to managerial and procedural activities operations management must support to meet customers' business requirements. The management actions and activities associated with this core process are planning, administration, cost control, service options catalog, and customers' service management.

- *Operations Management* is responsible for the day-to-day administration of all infrastructure components. Key tasks associated with this core process are highly technical in nature. They include installation; repairs; maintenance; jobs management; performance monitoring and data capture for reporting; and fault management to name a few. Operations Management therefore complements the Service Delivery process.

- *Service Support* is the connection between the other core processes. The primary role for Service Support is to be the communication channel between the customer and the IT service organization. There are two sub-processes, supporting and changing, by which customer's interactions take place. It is through these sub-processes that IT service personnel handle all customers facing issues and problems.

Scope of this Report

This report addresses the following ESM domain processes and related components:

- *Service Delivery*
  - Service Level Management
  - Capacity Management
  - Financial Management
  - IT Continuity Management
  - Availability Management
  - Infrastructure Engineering
  - Security Management
  - Workforce Management

- *Service Support*
  - Supporting
    - Service Desk
    - Incident Management
    - Problem Management

  - Changing
    - Change Management
    - Release Management
    - Configuration Management

- *Operations Management*
  - Services Monitoring and Control
  - Network Administration
  - Storage Management
  - Systems Administration
  - Directory Services Administration
  - Job Scheduling
  - Security Administration

Future Enterprise Systems Management Domain Initiatives

A key feature of any ESM function is the ability to utilize an integrated automated tool to manage and control infrastructure components. There are many vendors' solutions with varying degree of features that may meet some or all ITIL framework recommendations.

This report does not address ESM tools at this time due to the depth of research required to propose a set of generic tools that will meet most of the Commonwealth's EMS requirements.

The "tools" question may be revisited in the future using criteria developed from the practical experiences of the domain team members and validated using external independent industry data. When this research is completed, results will be included within a future release of the technology standards and/or an update to this report.

In the interim however, the requirements and recommended practices discussed in this report can provide direction to ESM responsible agencies should the need arise to acquire ESM tools.

(This Page Intentionally Left Blank)

Domain-wide Principles, Recommended Practices and Requirements

The following principles, recommended practices, and requirements pertain to all components, in all situations and activities related to the ESM Domain. Component specific principles, recommended practices, and requirements are discussed below in the "Enterprise Systems Management Domain Technical Topics" section.

Domain-wide Principles

In addition to the principles identified in the "*Commonwealth of Virginia Enterprise Architecture – Conceptual Architecture*", the ESM domain team identified the following ESM Domain-specific principle:

ESM-P-01: **Enterprise Systems Management Best Practices -** Information Technology Infrastructure Library (ITIL) disciplines provide the foundation on which to implement ESM processes.

Rationale:
ESM is a complex undertaking. Complexity increases the Commonwealth's infrastructure risk and largely affects how well agencies deliver quality citizen services. To mitigate complexity risks, IT service entities must have a consistent way of managing the IT infrastructure. ITIL provides a proven management framework and methodology developed from industry best practices.

Implication:
By adopting ITIL as the basis for ESM, agencies will have the benefit of a "turnkey" solution that is consistent and repeatable in all infrastructure situations. When implemented as designed, ITIL eliminates guesswork and trial and error actions on the part of IT infrastructure personnel.

Domain-wide Recommended Practices

ESM-RP-01: **Environmental and Physical Controls –** Data center environmental and physical controls should limit exposures and risks that might affect the delivery of consistent services. These controls should be reviewed on a regular basis.

Rationale:
Environmental and physical controls support the business requirement of providing appropriate physical facilities that protect the IT equipment and people against man-made and natural hazards.

Domain-wide Requirements

ESM-R-01: **Authorized Access –** Agencies shall restrict access to any IT infrastructure resources including ESM tools in

conformance with the Commonwealth's security policies and procedures.

Rationale:

Ensuring that appropriate information system security procedures are implemented and monitored improves IT service delivery performance. Business units expect information to be safeguarded against unauthorized use, disclosure, modification, damage, or loss.

ESM-R-02: **Adhere to Information Technology Infrastructure Library Framework (ITIL).** IT operational and services processes shall adhere to the ITIL framework best practices methodology.

Rationale:

- ITIL provides "industrial strength" processes for IT operation and service delivery.
- ITIL is repeatable and consistent in all IT service delivery situations.
- ITIL is vendor neutral.
- ITIL provides methods and techniques that will ensure increased customer satisfaction.

ESM-R-03: **Security, Confidentiality, Privacy, and Statutes.** IT systems shall adhere to all security, confidentiality and privacy policies, and applicable statutes.

Rationale:

- Agencies must protect sensitive data (SSN, Credit card numbers, etc.)
- Safeguards sensitive and proprietary information.
- Enhances public trust.
- Enhances the proper stewardship over public information.
- Ensures the integrity of the information.

Enterprise Systems Management Domain Technical Topics

The ESM domain framework (see Figure 3) shows the Commonwealth's IT infrastructure management approach within the ETA. The following sections discuss each ESM domain topic and detail associated principles, recommended practices, and requirements.

These principles, recommended practices, and requirements apply to all agencies. Throughout this document, the term "*agencies*" by itself is defined as any agency, institution, board, bureau, commission, council, or instrumentality of state government in the executive branch listed in the appropriation act. ETA requirements/standards identified in this report are applicable to all agencies including the administrative functions (does not include instructional or research functions) of institutions of higher education, unless exempted by language contained in a specific requirement/standard. In addition, the term "a*gencies with ESM responsibilities*" refers to only those agencies that **install, support, and maintain** infrastructure components on a routine basis.

Service Delivery

The Service Delivery topic defines what IT services the business requires to meet business commitments. This topic consists of eight (8) components.

- Service Level Management
- Capacity Management
- Financial Management
- IT Continuity Management
- Availability Management
- Infrastructure Engineering
- Security Management
- Workforce Management

Service Level Management

The goals for Service Level Management are to successfully deliver, maintain, and improve IT services. It is the means by which the business owners and the IT department orchestrate core IT services required to meet normal business operations.

A key objective for Service Level Management is to seek alignment with business priorities and manage IT service delivery at acceptable costs. To achieve the goals and objectives noted previously, IT organizations and business partners must gain a full understanding of IT services offered. Steps generally employed for implementing Service Level Management include the following high-level activities:

- Create a service catalog: This non-technical document describes services available to the business. All significant elements within each service area are enumerated. Service Level Agreements (SLAs) are constructed from this source.
- Develop relevant SLAs: SLAs document agreed service levels and priorities. Methods for measuring performance are also defined in these documents.
- Monitor and report: Performance measures defined in the SLAs must be monitored. Measurement data are continually collected and compared with stated SLA thresholds. Monitoring is meaningless if there are no feedback mechanisms to report variances; non-reporting would render the SLA inoperable.
- Perform reviews: Both business and IT management review data to assess and evaluate IT services delivery performance in relationship to SLA terms. The report data provides both business and IT decision makers with information on how well service level choices reflect the business needs.

Recommended Practice:

ESM-RP-02: **Service Level Management Process –** Agencies with ESM responsibilities should establish a Service Level Management Process in order to effectively and efficiently deliver on customers' service expectations.

Rationale:

Sturm et al characterized Service Level Management as "… the disciplined, proactive methodology and procedures used to ensure that adequate levels of service are delivered to all IT uses in accordance with business priorities and at acceptable costs" [3] It is incumbent on the IT organization to understand the range of service offerings including levels of priorities and business importance of each. Service Level Management is the precursor to the Service Level Agreement.

Requirement:

ESM-R-04: **Service Level Agreement -** Agencies shall ensure that service delivery expectations are defined and documented in a Service Level Agreement (SLA). The SLA must include performance requirements and methods for measuring IT service delivery against performance targets.

Capacity Management

Capacity Management is the process of planning, analyzing, sizing, and optimizing infrastructure capacity requirements to satisfy business demand in a timely manner and at

[3] Sturm, R., Morris, W., and Jender, M. (2000). *Foundations of Service Level Management.* Sams, Macmillan USA Indianapolis, p 13.

a reasonable cost. This process should be proactive and responsive to business needs because resources cannot be added after a capacity problem has been detected without affecting business performance[4].

Capacity requirements evolve from qualitative and quantitative values agreed to in the SLA. The Capacity Management process relies on a set of iterative tasks (monitoring, analysis, modeling, optimizing, and change initiation) to achieve its goals[5]. Managing performance and capacity ensures that adequate resources are available and optimal use is made of resources. Key areas to be considered are business requirements regarding availability and performance, use of automated monitoring tools, use of modeling tools to evaluate workload forecasts, capacity utilization and forecasting, and resource availability and scheduling.

Requirement:

ESM-R-05: Capacity Planning and Performance Monitoring Management - Agencies with ESM responsibilities shall perform capacity planning and performance monitoring to ensure infrastructure resources are appropriately sized to meet current and planned workload demands.

Rationale:

Managing performance and capacity ensures that adequate capacity is available and best optimal use is made of IT resources to meet performance expectations. Key areas to be considered are business needs regarding availability and performance, use of automated monitoring tools, use of modeling tools to evaluate workload forecast, capacity utilization and forecasting, and resource availability and scheduling.

Financial Management

The purpose of financial management within the ESM domain is to ensure sound fiscal management of IT resources. This is accomplished by instituting processes and procedures to collect expense or cost data for consumed resources. Financial management helps IT managers make informed decisions when planning for IT investment.

Financial management consists of the following activities:

- Cost Accounting: This activity involves the identification of assets and activities (cost elements) to which costs are assigned. It also involves the development of cost allocation models whereby the costs related to each cost element are

[4] Menasce, D., Almeida, V., and Dowdy, L. (1994). *Capacity Planning and Performance Modeling*. Prentice Hall, Englewood Cliffs.

[5] "Microsoft Operations Framework". Retrieved 12/15/2005 from http://www.microsoft.com/mof

distributed fairly and equitably to customers. Cost Accounting is responsible for developing operational financial reports for management.

- Budgeting: Budgeting requires a great amount of communication and coordination, which has the benefit of aligning the IT department's objectives to business objectives.
- Project Investment Appraisal: IT infrastructure is always in a constant change. It is necessary for IT decision makers to assess the financial impact of short and long-term changes in the environment. Project Investment Appraisal[6] as an analytical tool highlights advantages or disadvantages for any proposed environmental change.
- Cost Recovery: Costs associated with provisioning of IT service costs are recovered using a "cost allocation" formula. In essence, costs are allocated based on the SLA.

Requirement:

ESM-R-06: Financial Management for IT Service Management - Agencies with ESM responsibilities shall implement accounting processes and procedures that will identify and attribute costs for IT resources used to support the business processes. The process shall provide data in a timely manner for Total Cost of Ownership (TCO) analysis and reporting.

IT Continuity Management

The main goal for IT Continuity Management is to ensure that the IT organization is capable of providing service to the customer in the event that the primary operating site becomes inoperable. With the advent of government services access by citizens almost on a 24x7 basis, organizations must have sound procedures to recover from any disaster in a timely manner to meet customers' expectations.

There are several events that need to be addressed when implementing IT Continuity Management. These events include but are not limited to hardware failures, environmental issues, and human errors. If not handled correctly and in a timely manner, these events could have a severe impact on systems availability (availability risks). Organizations must therefore "design in" countermeasures to mitigate identified business risks.

IT Continuity Management is a risk base planning exercise to mitigate identified business risks that have significant impact on service delivery. IT organizations must decompose IT layers into manageable tasks and assign relevant costs to risks associated with each particular layer. Within the IT organization, there are the following information technology layers:

[6] Sometime referred to as Feasibility Study.

- Service: This is the function IT operations management is helping the business perform. Business units use various business applications hosted by the IT organization to support the business. Knowledge of business services utilized by the business unit will determine the risk levels and cost impact to the business should there be service interruption.
- Application: The business application is what the customer sees. It is through the business application that the business unit accesses services.
- Middleware (Integration)[7]: Middleware is not visible to the customer but is a vital part of service delivery. Business applications in many instances would not operate without the middleware. Middleware includes databases, web services, and messaging systems.
- Operating System: Operating Systems control the allocation and usage of hardware resources.
- Hardware: Hardware is comprised of all components found in the data center and in the customers' workspace. Hardware is also extended to internal components whose failure will result in the customer's inability to access service.
- LAN/WAN: LAN/WAN is the organization's network that provides communication between computing equipment and the customers interactions with the systems.
- Facilities: Facilities consist of the building that houses the data center and any associated components. Examples of facilities components are buildings, environmental controls instruments, physical security appliances, and fire suppression equipments.

Requirement:

ESM-R-07: **IT Continuity Management -** Agencies with ESM responsibilities shall establish an IT disaster recovery plan that reflects SLA service delivery requirements. This risk-based plan shall incorporate the operating constraints of the business continuity plan. The plan shall address all critical applications, middleware, operating systems, hardware, and network connectivity elements. In addition, there shall be procedures to test the IT disaster recovery plan periodically and update the plan based on the test outcome or environment changes.

Availability Management

Availability Management ensures that IT Services Management is consistently and cost effectively delivering the level of service the customer expects. Use of monitoring tools and controlling techniques and or methods ensure system components or services perform required functions as engineered. Service availability is expressed as the

[7] Please see "Integration Domain Report" for expanded discussion on this technology.

proportion of time that the service is actually available for use within the agreed service timeline (the availability ratio).

The prime focus of Availability Management is handling the routine availability risks that occur on a day-to-day basis. IT Service Continuity Management focuses on extreme and relatively rare availability risks, such as fire and flood, and acts as a catchall for any unanticipated availability risks. Availability Management draws on work prioritization schedules and identifies the key IT infrastructure components that support these critical services and determine whether they contain any single point of failure or other risks to service delivery that can be cost-effectively mitigated using appropriate countermeasures.

Current IT services can have their availability levels significantly improved or stabilized through the adoption of a formal Availability Management process. On the other hand, new IT services offers the best opportunity for achieving availability targets in a cost-effective manner since availability considerations can be built in at the earliest stages of technology selection. Availability Management should be applied to:

- All new IT services and existing services where service level requirements (SLRs) or service level agreements (SLAs) are established.
- IT services that are defined as critical business functions, even when no SLA exists.
- The suppliers (internal and external), that form the IT support organization as a precursor to the creation of a formal SLA.
- All aspects of IT infrastructure and supporting organization that delivers services to the customer.

Recommended Practice:

ESM-RP-03: Availability Management - Agencies with ESM responsibilities should perform an IT operations risk assessment to determine the impact of service delivery degradation and/or loss of service on the business unit.

Infrastructure Engineering

Infrastructure Engineering (IE) promotes the development and use of consistent IT standards and policies pertaining to infrastructure components and processes. Implementing IE will improve the operability of installed infrastructure updates or releases by ensuring they are compatible with the existing infrastructure and services, as well as the changes planned for them.

IE enhances IT management’s ability to deliver technology services and functionality to meet business objectives while reducing the likelihood of failed infrastructure project deployments.

IE coordinates management activities relating to the creation and application of consistent IT operational policies and standards to control development, deployment, and

utilization of tools and services within the infrastructure environment. By using IE, IT management will be in a better position to:

- Develop standards, policies, benchmarks, and guidelines for managing routine infrastructure tasks, maximize systems availability, ensure supportability of critical infrastructure components, and installation of infrastructure components that are interoperable.
- Provide management controls ensuring ESM solutions are operable at the right level and select the timing for new solutions design and changes.
- Ensure infrastructure alignment with business objectives.
- Improve manageability of the infrastructure layers.
- Perform periodic quality assurance reviews of ESM activities.

Requirement:

There are no Infrastructure Engineering requirements at this time.

Security Management

Securing information systems used to manage and transmit data is important to the Commonwealth. Threats to the Commonwealth's infrastructure resources come in many forms such as hacking, virus, and human error that are ever changing.

IT Service Management must adopt information security standards issued by the Commonwealth and implement procedures that will mitigate operational risks and exposures associated with threats identified previously. Creating a secure environment entails achieving fundamental security objectives such as confidentiality, integrity, and availability.

These security objectives are achieved through the enforcement of procedures. Controls fall into three distinct categories:

- *Administrative controls* consist of policies, standards, processes, and procedures that define the principles and directives for a secure environment.
- *Physical controls* that ensure access to information processing resource facilities are restricted to authorized individuals.
- *Technical controls* consist of hardware devices and software programs that protect the systems and data.

Security management affects ESM functions such as Release, Change, Configuration, Availability, and Continuity Management.

Requirement:

Please see Domain-wide Requirements Section for Security Management Requirements[8].

Workforce Management

Workforce Management is vital function of IT Service Management. From an ESM perspective, it is important to have in place a plan that maps service delivery commitments to required skills and competencies.

The IT architecture and SLA terms and conditions are the determining factors for assessing the level of skills and competencies required across all ESM processes. Lack of the right skills may expose the IT Operations Management organization to unacceptable risks and foster customer's dissatisfaction.

IT Operations Management after understanding the business needs and unique complexity of the infrastructure should develop a human resource plan that is shared with the Human Resources Organization. IT Operations Management utilizes this plan to ensure that IT services are delivered in a manner that supports the business objectives.

Some key features of this plan include employee orientation, job descriptions, continuous workforce skills assessment, workforce retention strategies, monitoring of personnel absence (ensuring continuous coverage), employee performance management, and rewards.

Recommended Practice:

ESM-RP-04: Educate and Train Personnel: In order to ensure proper use of resources, agencies with ESM responsibilities should educate and train IT service personnel in the use of infrastructure resources to limit the chance of human errors.

Rationale:

To achieve the business requirement of ensuring that acceptable Quality of Service (QoS) goals are met in a consistent manner, identification of training needs ensures that service delivery problems are handled in a manner that will improve customer satisfaction, encourage proactive management style, and consistently utilize industry best practices.

Requirement:

There are no requirements for Workforce Management at this time.

[8] The security domain discusses fully the overarching information systems security principles, policies, requirements, and practices relating the ETA.

Service Support

Service Support includes the activities that support Service Delivery and Operations Management. This topic includes the following two sub-topics and six (6) components:

- Supporting
    - Service desk
    - Incident Management
    - Problem Management
- Changing
    - Change Management
    - Release Management
    - Configuration Management

Supporting

The *Supporting* sub-topic is a set of process capabilities that are directly related to customer interactions with the IT service organization. Customer interactions can include reporting of problems and incidents, requests for service; and obtaining information about service events, actions, and opportunities that could improve individual productivity. This is accomplished through a Service Desk that is the single point of contact for all customer communications along with tracking customer contacts, and maintaining a customer data repository.

Service Desk

The Service Desk provides communication, information, and resolution to customers who are experiencing service issues and problems with any IT infrastructure component (layer). IT service personnel also utilize this facility to receive and provide information relating to service issues and/or problems. Service Desk models include:

- **Centralized:** A centralized Service Desk supports all users within the organization, regardless of their geographical location.
- **Decentralized:** A decentralized Service Desk has a number of service desks located at various geographical locations.
- **Virtual Service Desk:** The virtual Service Desk is based upon advances in network performance and telecommunications— the physical or geographical location of the Service Desk is immaterial.

  A virtual Service Desk combines elements of both the centralized and decentralized Service Desks in that users utilize a consistent route to access the Service Desk, but their call may be routed to any one of a number of locations, depending on a number of factors (time of day, local public holidays, call volumes, and so on).

Requirement:

ESM-R-08: **Service Desk -** Agencies shall utilize a Service Desk facility that is staffed with properly trained personnel who can

minimally respond to level 1- type problems, incidents, and events[9]. The Service Desk shall utilize an automated contact management tool and is the single point of contact for all IT service requests and services communications.

Incident Management

Incident Management is the process of restoring normal service operation as quickly as possible in order to minimize the adverse impact on business operations.

By definition, an incident is any deviation from the expected standard operation of a system or service. Incident Management involves restoration of services utilizing standard processes of investigation, diagnosis, resolution, and recovery.

Requirement:

ESM-R-09: **Incident Management[10] -** Agencies with ESM responsibilities shall establish an Incident Management process and procedures. The process and procedures shall enable restoration of normal service operation as quickly as possible and minimize the impact on business operations. Procedures shall include steps to address actions such as incident detection, recording, classification, initial support, investigation, diagnosis, resolution, recovery, closure, ownership, monitoring, tracking, and communication.

Problem Management

Problem Management is the process of minimizing the adverse impact of incidents and problems caused by errors in the IT infrastructure. It should also prevent recurrence of incidents related to those errors.

Problems are abnormal conditions caused by one or more incidents, for which the cause is undetermined at the time of onset. Problem Management techniques pinpoint and remove the root cause of these incidents, and to the extent possible determine what infrastructure component contributed to the error condition.

Requirement:

ESM-R-10: **Problem Management[11] -** Agencies with ESM responsibilities shall institute procedures for problem handling. These

[9] Level 1-type problems, incidents, and events are user calls to the service desk that the service desk analyst can resolve directly with the user using prior experience and/or information accessed from a knowledge base.

[10] An incident is any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service.

[11] A problem is a condition resulting from multiple incidents or a significant incident for which the cause is unknown but the impact is significant. Problem Management's purpose is the detection, resolution, and prevention of future incidents.

procedures shall include steps for performing root cause analysis of incidents and correction of the error to the satisfaction of the customer.

Changing

The *Changing* sub-topic is a set of process capabilities that ensure the use of standardized methods and procedures for efficient and prompt handling of changes, releases, and configuration actions in order to minimize the impact on service commitments, and consequently improve the day-to-day operations of the IT organization.

Change Management

Change Management consists of administrative actions and process activities for handling all changes in a standardized and efficient manner to minimize the risk of change-related incidents. By definition Change Management is any action that alters the form, fit or function of one or more infrastructure components. Changes are initiated by using a request for change (RFC) form that details the proposed change, justification for the change and authorization to make the change.

Requirement:

ESM-R-11: **Change Management -** Agencies with ESM responsibilities shall establish a Change Management process and institute procedures that provide for the analysis, implementation, and follow up of all environmental changes requested including those made due to problem resolution. The process shall support change initiation and control actions, support the ability to conduct impact assessments, handle changes in an automated manner including emergencies, document all changes in the configuration management database, demonstrate chain of custody for the change, and comply with release policies.

Release Management

Release Management is the process of ensuring that all technical and non-technical aspects of the release are considered in order to optimally handle the release and bridge the gap between application development and infrastructure operations.

Release Management involves actions necessary to successfully plan and deploy authorized releases into production. The Release Management process starts with a Change Management approval of the RFC form.

Release planning is then initiated to identify activities and resources required to successfully deploy a release into the production environment. This include documenting the processes, tools, all components necessary, and technologies required to deploy the release into production.

Requirement:

ESM-R-12: **Release Management –** Agencies shall establish a release management process. Process activities shall include procedures for hardware, license/version control across the infrastructure, rollout planning, communication protocols, and quality control of the process.

Configuration Management

Configuration Management is the process of identifying, recording, and reporting on all IT infrastructure components. A key element for successful Configuration Management is the ability to discover, identify, verify, and record all configuration items in a central or federated configuration database.

Requirement:

ESM-R-13: **Configuration Management -** Agencies with ESM responsibilities shall establish a cost effective automated Configuration Management process and procedures to control and identify all IT assets[12] (Configuration Item [CI]) and their physical locations. CIs must be documented in a Configuration Management Database (CMDB)[13]. The CMDB shall have the ability to create a parts list of every CI in the system, define the relationship of CIs in the system, track the current and historical status of each CI, track all Requests for Change (RFC) to the system, and verify that the CI parts list is correct and complete.

Operations Management

Operations Management is responsible for the systems and sub-systems (infrastructure) utilized to deliver IT services. The infrastructure consists of all hardware and operating systems software. In addition, business applications and integration (middleware) software are also within the purview of this process.

Operations Management is responsible for the installation and execution of all software that processes data and effects customer interactions with systems. Each infrastructure

[12] ITIL framework use the "lowest common denominator" principle for IT asset management. Configuration item is the term used to describe all components necessary for IT operations. Configuration Management activities include: (1) planning, (2) identification, (3) control, (4) status accounting, and (5) verification and audit. Any configuration item therefore is considered as an IT asset thus IT asset management is not treated as a separate function but instead handled as an integral part of the Configuration Management process.

[13] Many vendors' product offerings view CMDB as the most important repository within ESM. While non-automated methods are an option, it is not a recommended practice. ESM tools that have the ability to perform "auto discovery" to capture, record, track, define relationships, and handle changes etc are the preferred option. Use of manual procedures will over time lose its usefulness and could become cost prohibitive.

component that is capable of providing operating performance and status data, is configurable, and requires daily monitoring and maintenance.

Operations Management includes Security Administration, Network Administration, Storage Management, Systems Administration, Services Monitoring and Control, Directory Services Administration, and Job Scheduling.

Services Monitoring and Control

Service Monitoring and Control (SMC) is responsible for the real-time observation and alerting of health conditions (performance thresholds including sources of failures) for IT infrastructure components and, where appropriate, automatically correcting any service exceptions. SMC also gathers data that can be used by other ESM processes to improve IT service delivery.

By adopting SMC processes, IT Operations Management is better able to predict service disruptions and to respond to actual service incidents as they arise, thus minimizing negative business impacts. Factors that may affect Service Monitoring and Control effectiveness include:

- *Business dependency*: Reliance on IT infrastructure and IT services, and it's role in business delivery continues to expand. With this dependency, IT customers have greater exposure to infrastructure failures, which often have a severe impact to critical business functions.
- *Business investment*: Many organizations have realized the competitive advantage (or costs avoidance) that IT provides and are poised to make substantial investments in developing the IT infrastructure. This forces a greater demand for demonstrable availability and continuation of services along with long-term benefits.
- *Technology complexity*: As the IT infrastructure continues to become larger and more distributed, it becomes more difficult to understand all the intricate requirements necessary to keep the IT infrastructure in suitable condition.
- *Business change*: With business-side imperatives changing direction at a much faster pace, there is an increased demand to shorten IT technology delivery life cycles, increase architecture agility, and make better use of tools.

The key benefits of effective Service Monitoring and Control are:

- *Early identification* of actual and potential service failures.
- *Timely resolution* of actual and potential service breaches with automated corrective actions.
- *Minimized* business impact of incidents and potential incidents.
- *Reduction* in actual service breaches.
- *Availability* of up-to-date infrastructure performance data.
- *Availability* of up-to-date service level and operating level performance data.
- *Continuous* alignment between business requirements and performance monitoring.
- *Linking* technology changes to evolution of monitoring tools.

- *Maximized* usage of management tools through effectively planned and integrated processes.

The Service Monitoring and Control process interacts with the Incident Management process to ensure that data on automatically resolved faults is available to Incident Management and that any situations that cannot be immediately addressed using the automated control mechanism are directly forwarded to Incident Management for proper handling. Infrastructure components that are deemed critical to the delivery of the end-to-end service should be monitored to the component level if possible.

Service Monitoring and Control consists of procedures and tools for proactive notification of events that may have severe consequences on the business. In addition, to the extent performance metrics are defined, monitoring of these metrics is important for SLA management and reporting.

Requirements:

ESM-R-14: **Metrics -** Agencies with ESM responsibilities shall implement operational performance metrics, data collection processes, and conduct regular reviews to ensure performance targets are on track and variations are addressed in a timely manner.

ESM-R-15: **Monitoring Capability -** Agencies with ESM responsibilities shall establish a system event monitoring console and institute systems performance alert thresholds to ensure systems faults are averted and corrective measures are taken to limit the chance of total systems failure.

ESM-R-16: **Monitoring and Control Tools -** Agencies with ESM responsibilities shall use Commercial–off– the Shelf (COTS) ESM tools that meet the goals of the International Standards Organization (ISO) 20000[14] and support performance metrics agreed to in SLAs. In the case where internally developed ESM tools[15] provide the best course of action, the tool shall comply with the ITIL process and appropriate dedicated staff resources(s) shall be assigned on a continuous basis to provide ongoing maintenance and updates.

[14] International Standard Organization (ISO) 20000 (which replaces BS15000) defines the requirements for an IT Service Management System. It sets out the main processes to deliver IT services effectively. The standard supports all aspects of ITIL. Details for ISO 20000 can be accessed at http://20000.fwtk.org/iso-20000.htm

[15] Internally developed tools shall be engineered using Systems Development Life cycle (SDLC) methodology that complies with the Commonwealth's software development policy and standards.

Network Administration

Network Administration is concerned with provisioning and operation of network services, including Dynamic Host Configuration Protocol (DHCP), Windows Internet Name Service (WINS), and Domain Name System (DNS), on a day-to-day basis. This component provides fundamental guidance for operating these services and maintaining the hardware layer on which they reside.

Network Administration also presents a unified approach to the operation and maintenance of network infrastructures, including Remote Access Service (RAS), local area networks (LANs), and wide area networks (WANs). The goal of Network Administration is to provide and reference a solid foundation of processes for administering a network environment on a day-to-day basis.

This entails managing and providing operational support for various elements within the production environment. The objectives include providing planning and deployment services to expand existing network facilities, as well as support services to troubleshoot and repair faults in the network environment.

Through effective implementation of the Network Administration, IT Operations Management can expect to:

- Improve their deployment of network infrastructure components.
- Improve troubleshooting processes and associated incident-management processes.
- Increase network reliability.
- Enhance availability of IT solutions and services.

Network Administration is involved with the first three layers (physical, data link, and network) of the Open Systems Interconnection (OSI) model stack, which mostly consist of hardware. There is some overlap between network and system administration at the transport level, which includes the linking and networking protocols that enable the transfer of data from one point to another.

Requirement:

ESM-R-17: **Network Administration -** Agencies with ESM responsibilities shall ensure that critical networking infrastructure devices such as routers, switches, hubs, PBX/call manager, voice mail server, and other direct attached data communications devices are Simple Network Monitoring Protocol (SNMP) capable. Devices shall be configured to permit capture of all events required by the SLA and the captured data shall be stored in a Management Information Base (MIB) repository.

Procedures shall be integrated with the Service Monitoring and Control process.

Storage Management

Storage Management is concerned with the operation and maintenance aspects of data management. This process defines, tracks, and maintains data and data resources in the production IT environment.

Defining data and data resources involves the following tasks:

- Developing the necessary plans for classifying, storing, restoring, and recovering data.
- Developing the appropriate policies and procedures for storing, restoring, and recovering data.

Tracking data and data resources involves the following tasks:

- Developing the appropriate procedures for monitoring storage resources (availability, capacity, and performance).
- Monitoring storage resources usability to ensure business requirements are met.
- Predicting future storage needs based on current trends.

Maintaining data and data resources involves the following tasks:

- Submitting RFCs according to the Change Management process for any required changes to data and/or storage resources.
- Changing and tuning storage resources to improve availability, capacity, or performance (subject to the dictates of the Change Management process).
- Ensuring that data is stored in accordance with established data security policies.
- Taking appropriate action to meet changes to storage needs.

Storage Management operational process consists of the following two major focus areas (1) Data Backup, Restore, and Recovery Operations and (2) Storage Resource Management. Each area contains various activities and associated tasks, which are described below:

Data Backup, Restore, and Recovery Operations
Storing, restoring, and recovering data are key Storage Management operational activities. These activities ensure that the Commonwealth's data is stored properly and is available for restoration and recovery, according to IT disaster recovery plans.

Storage Resource Management
Storage Resource Management ensures that storage media is formatted according to specification and is installed with the appropriate file systems and that removable storage media is organized, used, recycled, and eventually retired according to technical specifications and business objectives.

In addition, Storage Resource Management involves using automated tools to monitor storage resources for availability, capacity, and performance thresholds. Exercising strict management controls over the data requires operating processes and procedures that will ensure that the data is protected, retrievable, and can be reconstructed in a timely manner to meet service delivery commitments.

Requirements:

ESM-R-18: **Policies and Procedures –** Agencies with ESM responsibilities shall establish data storage and archival retention policies and procedures that meet operating business requirements, statute, and regulatory mandates. To the extent, there are conflicting requirements, agencies shall take steps to address all conflicts with the appropriate mandating entity and document the resolution.

ESM-R-19: **Back-up and Recovery –** Agencies with ESM responsibilities shall ensure policies and procedures address back-up and recovery for all critical Commonwealth data and conduct testing of these procedures on a regular basis. Procedures shall address timing, frequency, and restore time objectives (RTO) that support the business continuity plan.

ESM-R-20: **Off-Site Retention –** Agencies with ESM responsibilities shall ensure critical back-up data files are rotated to an Off-Site location on a scheduled basis as defined in the back-up and recovery procedures. In addition, Off-Site locations shall comply with data security requirements as defined in the ETA security domain.

Systems Administration

The Systems Administration component is responsible for providing day-to-day administrative services in support of the production environment. This entails managing and providing operational support for various elements within the environment, such as network accounts (users, groups, distribution lists, and so on) and network resources (servers, printers, storage devices, and so on).

This function may also lend assistance to, or work in concert with, other ESM processes by providing basic monitoring services such as first level performance and capacity monitoring for the SMC [Services Monitoring and Control] activity.

There are several administration models available; each is influenced by the nature of the enterprise technical architecture (centralized, distributed, hybrid) adopted by the enterprise. Design of any systems administration model is contingent on size, capacity,

and technical capability of the architecture and competencies of the IT staff. Common industry models can be categorized into five operating modes (level of sophistication) and associated administrative structure (cost to deploy/support)[16].

Centralized Administration of Centralized Hardware

Centralized Administration typically assumes that all or most of the computing systems and resources being administered are centrally located.

While this is generally the case, there are situations where specific solutions (that is, custom applications, specialized databases, and so on) are not centralized in the corporate data center but instead are distributed to the remote site.

This distribution of some applications and databases does not prevent taking a centralized approach to the administrative model. The centralized/remote administration model, described below, accommodates both centralized administration and the distribution of some solutions.

This model offers the advantage of greater control over all resources, achieved through physically locating everything (systems and people) at a central site. Compared to the distributed, remote, and hybrid models, there is a reduction in operating costs because the model does not require maintaining remote data centers to support distributed systems and administrative resources.

The Centralized Administration model assumes that the enterprise is managing mission-critical, high-availability systems that require a full data center infrastructure, including highly available power, environmental conditioning, fault-tolerance in all data center components, and all the security systems appropriate to the deployment.

The disadvantage of the centralized administration model is that it requires maintaining high-speed bandwidth to all remote sites, along with the appropriate levels of redundancy and fault tolerance in the network links.

Centralized/Remote Administration of Distributed Hardware

The Centralized/Remote Administration model achieves most of the benefits of the completely centralized model. Most administration continues to be performed at the central location (central data center) thereby retaining the greatest control and consolidation of resources necessary to execute the administrative function.

Some control and resource consolidation is given up, however, due to the requirement of maintaining a remote data center environment with at least a minimal localized administrative presence.

[16] "Microsoft Operations Framework". Retrieved 12/15/2005 from http://www.microsoft.com/mof

Remedial system maintenance requirements on the distributed system may include system updates that require a reboot of the computer, as well as tape-backup and storage duties. There may be additional local-site administrative requirements depending on the application or specific system being managed.

This approach requires the build out of a data center facility in the remote or regional location to house servers or storage units. The implication of this approach is increased infrastructure costs since physical plant, power, wiring, HVAC, and security must be provided.

If the business applications evolve to the point where this model is no longer viable, a Distributed Administrative model may prove to be a better solution. In a Distributed Administrative model, the computing resources as well as the people resources are physically located at the remote location.

Centralized/Delegated Administration of Distributed Hardware

This model attempts to embrace the best of the Centralized and Remote Administration models with all of their inherent features and benefits, yet also realizes some of the benefits of the distributed administration model.

These benefits are achieved by pushing a relatively small and specialized subset of administrative tasks and responsibilities to the remote sites. As with the centralized model, the primary administrative function and administrative workforce reside at the central data center.

Certain circumstances dictate the need to distribute specific services, servers, and resources; in these cases, it may also be prudent and/or more efficient to allow some of the administrative tasks to be performed at the remote locations.

This is done by delegating very specific authority to the remote location resources. Very specific authority refers to a small subset of administrative rights and access that allow the remote administrators to perform specific, discrete tasks.

Distributed Administration of Distributed Hardware

Resources at remotely located sites perform the fundamental and critical support functions necessary to maintain the health, availability, and reliability of systems distributed to those sites.

There may continue to be business reasons for maintaining systems that are distributed to remote locations. Some of these reasons may be related to performance, scalability, a specific type of application, or the cost or availability of network bandwidth that would support a centralized solution.

Requirement:

ESM-R-21: **Systems Administration -** Agencies with ESM responsibilities shall develop and maintain appropriate operations policies, procedures, and standards to ensure day-to-day management of the IT infrastructure environment. Developed policies, procedures, and standards shall comply with all applicable ETA policies and standards.

Directory Services Administration

A Directory Service is both a management tool and an end-user tool. As the number of objects in a network grows, a directory service becomes essential. The directory service is the hub around which a large distributed environment operates.

Directory Services Administration ensures that information is accessible through the network by any authorized requester (users and applications) to find network resources (other users, servers, applications, tools, services), and other information over the network and to deal with the day-to-day operations, maintenance, and support of the Directory Service.

Recommended Practice:

ESM-RP-05: Directory Services Administration - Agencies where practical should leverage a common integrated directory service and institute procedures for ongoing maintenance of the directory.

Job Scheduling

Job Scheduling is concerned with ensuring the efficient batch processing of data at a pre-determined time and in a prescribed sequence to maximize the use of system resources and minimize negative business impacts. Execution of batch processes can be initiated in an automated manner or by manual means depending on the situation facing IT Operations Management.

Job Scheduling involves the continuous organization of jobs and processes into the most efficient sequence, maximizing system throughput and utilization to meet SLA requirements. Job scheduling entails defining[17]:

- *Job schedules*: Workloads are broken down into time periods (daily, weekly, monthly, annually) and jobs are scheduled for execution according to business needs, length of job, storage requirements, and associated dependencies.

[17] "Microsoft Operations Framework". Retrieved 12/15/2005 from http://www.microsoft.com/mof

- *Scheduling procedures*: Schedules are set up and maintained, conflicts and problems pertaining to scheduling are managed, and special needs (such as as-needed jobs) are accommodated.
- *Batch processing*: Jobs are executed according to the work schedule, run priority, and job dependencies.
- *Batch-processing procedures*: Procedures include but are not limited to the following:
    - Job documentation
    - Hardware instructions (for example, tape units, data cartridge units, and printers)
    - Console operations
    - Control checks
    - Problem management

Requirement:

ESM-R-22: **Job Scheduling -** Agencies with ESM responsibilities shall utilize an automated job scheduling system to control and organize workloads. Features should include, but are not limited to parameters, for execution time periods (daily, weekly, monthly, annually), execution length (start/finish), storage requirements, dependencies, and the ability to limit job execution bypass.

Security Administration

An information system with weak infrastructure security controls will eventually experience data loss, data disclosure, loss of system availability, corruption of data, and other security violations. Security can be broken up into the following six elements:

- *Identification:* Identification is concerned with user names and how users identify themselves to a computer system.
- *Authentication*: Authentication is concerned with passwords, smart cards, biometrics, and so forth. Authentication is how users demonstrate to the system that they are who they claim to be.
- *Access control (also called authorization):* Access control is concerned with access and privileges granted to users so that they may perform certain functions on a computer system.
- *Confidentiality*: Confidentiality is concerned with encryption. Confidentiality mechanisms help ensure that only authorized people can see data stored on or traveling across the network.
- *Integrity:* Integrity is concerned with checksums and digital signatures. Integrity mechanisms help ensure that data is not garbled, lost, or changed when traveling across the network.
- *Non-repudiation*: Non-repudiation is providing proof of data transmission or receipt so that the occurrence of a transaction cannot later be denied.

Requirement:

Please see Domain-wide Section for Security Administration Requirements.

Glossary

Following are Glossary entries pertaining to the ESM and required to support this document. Additional glossary definitions can be found in the ITRM Technology Management Glossary located on the VITA website here: http://www.vita.virginia.gov/projects/cpm/glossary.cfm.

Agency	Any agency, institution, board, bureau, commission, council, or instrumentality of state government in the executive branch listed in the appropriation act. ETA requirements/standards identified in this report are applicable to all agencies including the administrative functions (does not include instructional or research functions) of institutions of higher education, unless exempted by language contained in a specific requirement/standard.
Domain	The Enterprise Technical Architecture (ETA) is typically divided into logical groups of related technologies and components, referred to as "domains". The purpose of a Domain Architecture is to provide a combination of domain principles, best practices, reusable methods, products, and configurations that represent "reusable building blocks". Thus, the Domain Architecture provides the technical components within the Enterprise Architecture that enable the business strategies and functions. Note, the Conceptual Architecture serves as the foundation for the Domain Architectures, and ensures that they are aligned and compatible with one another.[18]
Enterprise	As used in this document and generally when discussing Enterprise Architecture topics, the *enterprise* consist of all Commonwealth of Virginia agencies as defined above.
ORCA	Online Review and Comment Application is a web based application managed by VITA to allow public comment and review of proposed policies, standards, and guidelines. ORCA may be accessed through the Commonwealth Project Management Web page or by pointing your Web browser to the URL http://apps.vita.virginia.gov/publicORCA.
Principles	High-level fundamental truths, ideas or concepts that frame and contribute to the understanding of the Enterprise Architecture. They are derived from best practices that have been assessed for appropriateness to the Commonwealth Enterprise Architecture.[19]

[18] COTS ETA Workgroup, *"Commonwealth of Virginia Enterprise Architecture – Common Requirements Vision"*, v1.1, December 5, 2000, p 26.
[19] COTS ETA Workgroup, *"Commonwealth of Virginia Enterprise Architecture – Conceptual Architecture"*, v1.0, February 15, 2001, p 5.

Product Standards	Are specifications for the use of specific hardware and software relative to the particular component.
Recommended Practices	Are activities which are normally considered leading edge or exceptional models for others to follow. They have been proven to be successful and sustainable and can be readily adopted by agencies. They may or may not be considered the ultimate "best practice" by all readers but for this place and time they are recommended practices and should be used and implemented wherever possible.
Requirements	Are activities that are considered strategic components of the Commonwealth's Enterprise Technical Architecture. They are acceptable activities for current deployments and must be implemented and used for all future deployments.
Topic	A topic is simply a logical subdivision of the domain. All components relevant to the Commonwealth's Technical Architecture are included within one if the identified topics.

Appendices

Acknowledgement

The domain team would like to thank their counterparts in the many states and federal government agencies whose excellent work preceded this. We couldn't have completed this report as quickly as it was done without the tireless energies obviously expended to complete their ETA documents. We also hope that other states will find this document useful in the design and updating of their own Enterprise Architecture. Significant contributions, references, and insights were derived from the following documents and web sites.

References and Links

Search terms used to access information resources used to develop this domain report were Enterprise Systems Management; Systems Management; ITIL; Systems Administration; Configuration Management; Enterprise Technical Architecture; CoBIT; IT Service Delivery; SLA; Storage Management; Network Administration; IT Performance Management. Information retrieved also provided other information sources relating to this domain research.

State and Federal Sites:

Federal CIO Council
http://www.cio.gov/index.cfm

Department of Energy
http://www.cio.doe.gov/Publications/csia/csia_final.pdf

Department of the Interior
http://www.doi.gov/ocio/architecture/index.html

State of New Mexico
http://www.cio.state.nm.us/architecture/index.html

State of Connecticut
http://www.ct.gov/doit/lib/doit/downloads/entpsys.pdf

State of North Carolina
http://www.ncsta.gov/docs/whitepaper/domain/enterprisetecnologyoverview.pdf

Industry IT Research Organizations and Consortia:

Gartner, Inc.:
http://www.gartner.com

The Open Group*:*

The Open Group Architectural Framework Enterprise Edition Version 8.1 (2003) http://www.opengroup.org/architecture/togaf/#download

ZIFA*:*

J.A. Zachman, Enterprise Architecture – A Framework, http://www.ziaf.com

Industry Vendors Whitepapers, Research Reports, and Publications.

Sturm, R., Morris, W., and Jender, M. (2000). *Foundations of Service Level Management*. Sams, Macmillan USA Indianapolis.

Menasce, D., Almeida, V., and Dowdy, L. (1994). *Capacity Planning and Performance Modeling*. Prentice Hall, Englewood Cliffs.

Kliem, R., and Ludin, I. (1992). *Data Processing Manager's Model Reports and Formants.* Prentice Hall, Englewood Cliffs.

Chiu, D., and Tsui, D. (2004). Modeling the Enterprise Infrastructure – An IT Service Management Approach. Retrieved 1/10/2006 from http://www.bmo.com

"Effortless Systems Management – How IT Performance Management Can Deliver More Business Value with Lower Operating Costs and Less Effort". Retrieved 1/7/2006 from http://www.bmc.com

"IT Discovery – Enables IT Service Management". Retrieved 11/20/05 from http://enterprisemanagement.com

"ITIL Best Practices: Maximizing the Business Value of IT – Part II". Retrieved 2/2/2006 from Http://www.mercury.com

"Best Practices for True Service-Delivery Implementation". Retrieved 2/2/2006 from http://www.mro.com

"NASCIO Enterprise Architecture Development Tool-kit". Retrieved 1/10/2006 from http://www.nascio.org/publications/index.cfm

"Aligning CoBIT, ITIL and ISO 17799 for Business Benefit". Retrieved 1/20/2006 from The IT Governance Institute http://www.itgi.org

"Key Criteria for Evaluating Application and Server Configuration Management Solutions". Retrieved 1/23/2006 from http://www.ptaknoelassociates.com

"Microsoft Operations Framework". Retrieved 12/15/2005 from http://www.microsoft.com/mof

"Operations Process Management – Automating IT Operations for Enhanced Efficiency and Effectiveness". Retrieved 12/12/2005 from http://www.optinuity.com

"ITIL and HP OpenView – Challenges in ITIL Compliance in Technology Products". Retrieved 1/20/2005 from http://www.dream-catcher-inc.com

"Event Correlation and Root Cause Analysis". Retrieved 3/2/2006 from http://www.ca.com