NIH Enterprise Architecture

Enterprise Systems Management Architecture

Enterprise Systems Monitoring

21 April 2004

Table of Contents

Table of Contents

(Continued)

List of Figures

List of Tables

1.0 Introduction

Enterprise Systems Management (ESM) services are the processes and tools that monitor the hardware, software, applications, networks and operational elements in the IT environment. The primary objective of ESM is to improve the service levels provided by the IT environment. The ESM discipline is complicated by several factors:

- Number of components that need to be managed
- Variety of elements that need to be managed, including legacy components
- Ongoing maturation of ESM methodology and toolsets
- Types of problems those elements can experience
- The fact that ESM is also often implemented as an afterthought to the infrastructure and is rarely considered when the infrastructure is designed and implemented.

Because infrastructure is implemented independently by 27 Institutes and Centers (ICs), the decentralized structure and differing work environments also contribute to the complexity of the ESM challenge at NIH.

This document establishes the NIH ESM architecture that can be implemented enterprisewide. This content has been developed and agreed-upon by a cross-IC domain team to address the full scope of the ICs' requirements. The ESM Domain Team built on the work done by the previous year's Network Domain Team by further documenting the "as is" architecture and developing a future-state, "to be," direction. Additionally, the ESM Domain Team developed a "pattern" that shows how these products should work together.

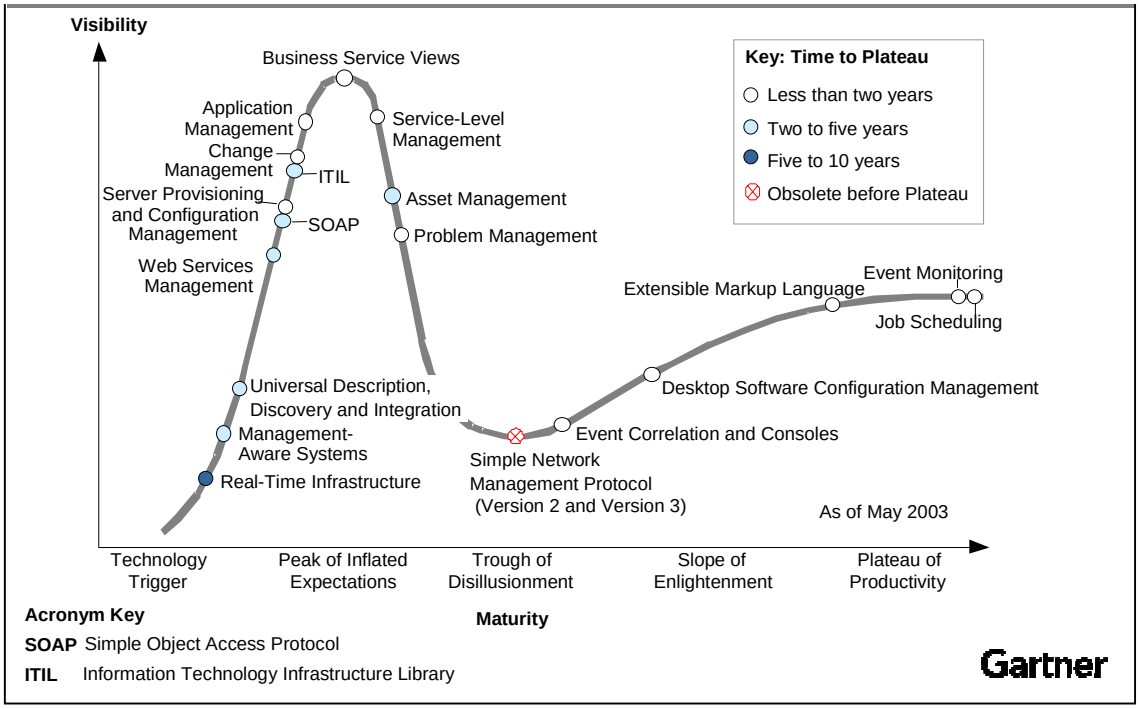
Throughout the domain team meetings, NIH technologists considered how to leverage current technologies and skills while planning how to expand NIH's ESM capabilities. Domain team members examined how current practices within some ICs can be leveraged across NIH as well as what new leading practices should be implemented. Improved ESM effectiveness will allow NIH to address the needs of the major enterprise applications more proactively and thereby deliver better value to the business.

Overview of ESM Market Maturity

In an effort to leverage industry best practices and to take advantage of leading research in this field, the ESM Domain Team reviewed the most current data on ESM implementation profiles from a Gartner survey dated May 2003 and ESM market adoption of emerging technologies. These snapshots of ESM market maturity provide context for how NIH has chosen to focus their ESM implementation efforts in the areas most likely to provide a cost-effective, positive impact for the business.

ESM capabilities to manage newer technologies typically lag the adoption of the technologies that need to be managed. This lag may be represented on a Hype Cycle. A Hype Cycle is a graphic representation of the maturity, adoption and business application of specific technologies. Hype Cycles also show how and when technologies move beyond the hype, offer practical benefits and become widely accepted. For example, Universal Description, Discovery and Integration (UDDI) and Simple Object Access Protocol (SOAP) are widely adopted as Web services technologies. However, vendors of enterprise management tools are just starting to look at the management implications of these technologies, as evidenced by their position in the ESM Hype Cycle (reference Figure 1).

Figure 1. Enterprise Systems Management Hype Cycle 2003



Source: Gartner, 2004

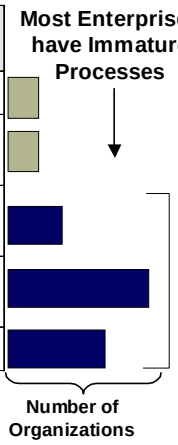
Successful implementation of ESM goes beyond installing the right technology. It requires re-engineering the IT management people, processes and technology around the business's required service levels. Even the best tools cannot improve systems availability, performance, reliability and recoverability without the right escalation procedures, job responsibilities and understanding of the environment being managed.

Additionally, ESM products require a lot of customization to coax reasonably useful technical data from the tools, while the goal of business service views remains elusive for most IS organizations. Currently, most tools can only integrate at the technical level, not at the business process view.

With the commercial toolsets lagging technology, coupled with the overall complexity in order to deploy them, it is no wonder that most enterprises are considered to be either "reactive" or "chaotic" when measured against the Effective Process Development Maturity Model, as shown in the following figure.

Figure 2. Effective Process Development Maturity Model

Level	IT Management Process Maturity	Management Process to Deploy	Representative Vendors
4	Value	Business activity monitoring	Systar, Managed Objects
3	Service	Capacity planning, workload management, SLA management	BMC Software, TeamQuest Compuware, Resonate, SAP (CCMS), Concord Communications
2	Proactive	Performance management, change/configuration management, job scheduling, automation	Precise Software, Mercury Interactive, Serena, Computer Associates, Novadigm, SAP (CCMS)
1	Reactive	Console/event management, integrated trouble tracking, backup and recovery	Micromuse, BMC Software, Tivoli, HP, SAP (SSMS)
0	Chaotic	Helpdesk	Peregrine, Computer Associates, HP



Source: Gartner, 2004

Therefore, NIH has chosen to invest primarily in achieving proficiency in the second level of IT Management Process Maturity, labeled Proactive, in Figure 2. Although some process improvements in levels 0 and 1 are required as prerequisites, NIH will focus on extracting the benefits of proactive availability, problem and performance management of infrastructure and applications.

1.1 Enterprise Systems Monitoring Domain Team

This report comprises the compilation of findings and recommendations derived from the joint NIH-Gartner Enterprise Architecture project team. A team of nineteen subject matter experts from various ICs, including the Center for Information Technology (CIT), worked together for three weeks to develop the ESM architecture patterns and bricks in this report. Gartner provided subject matter expertise and facilitation for the decisions that were made by NIH. These IC representatives contributed to this effort:

- Leslie Anderson, CIT
- Gene Cartier, SRA
- Robert Cox, NIAID
- Ron Davis, NCRR
- Phil Day, CIT
- James Del Priore, CIT
- Saundra Emma, CIT/DNST
- Barrett Grieb, CC
- Andrew Hartman, NCI
- William (Bill) Jones, CIT
- Doug Meyer, CIT
- Alex Rosenthal, CIT
- Scot Ryder, NIDCD
- Chris Stenger, OD & NCMHD
- Quang Tran, NIMH
- Jack Vinner, CIT.

1.2 Scope

This report focuses on standardizing ESM tools at NIH within the geographic scope of the NIH and IC locations in the United States. These tools are needed to address the ESM requirements of four enterprise systems and their supporting infrastructure:

- MS-Exchange, the NIH consolidated e-mail solution
- Clinical Research Information System (CRIS), which is currently being developed and deployed
- eRA/IMPACII, a core grants management system
- NBS, the NIH Business System.

ESM also includes other disciplines that have not been addressed in this iteration of the architecture (see Table 1). These areas will be addressed in future iterations of the Enterprise Architecture. It is also expected that the ESM process implementation efforts in 2004 could refine the tactical and strategic directions contained in this report.

The business objectives of this team were to provide toolset recommendations for the ESM disciplines that would enable better end-user service levels of availability and performance for enterprise applications that serve NIH and a majority of the ICs. The ESM Domain Team focused on tool selection for four of the nine major disciplines of ESM, as identified in the following table.

Table 1. ESM Scope

System Management Discipline	In Current Scope?
Availability Management	Yes
Business Service Management	No
Capacity Planning	No
Change Management	No
Configuration Management	No, current state has been documented, but future work is required to refine and define this brick.
Event Management (Manager of Managers)	Yes
Performance Management	Yes, although next iteration of the architecture may do further refinement of this brick.
Problem Management	Yes
Security Management	No

The scope of managed elements includes:

- WAN and network elements
- Enterprise applications and their supporting application and database servers
- Storage systems and SANs that support enterprise applications.

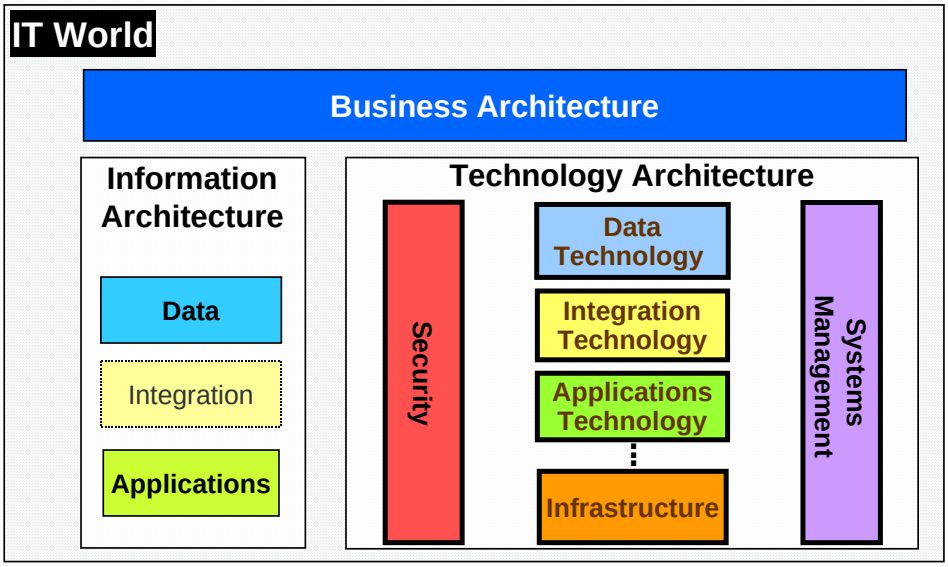
The ESM Domain Project did *not* address the processes required for each discipline. ESM process definition and implementation is a separate, yet coordinated effort at NIH.

1.3 Enterprise Systems Monitoring in the NIH Enterprise Architecture Framework

The *NIH Enterprise Architecture Framework* and *NIH Enterprise Architecture Matrix* are based on the Federal Enterprise Architecture Framework (FEAF) and the FEAF Matrix.[1]

The NIH EA Framework recognizes three distinct component architectures: the Business Architecture, Information Architecture and Technical Architecture. The NIH EA Framework is illustrated in Figure 3.

Figure 3. NIH Enterprise Architecture Framework



Source: Gartner, 2004

The ESM Domain is part of the technology architecture within the NIH EA Framework and is labeled “Systems Management” in the shaded vertical box in the lower right of Figure 3.

The NIH EA Matrix provides five potential *perspectives* or views of the architecture, at increasing levels of detail. The NIH EA Matrix is shown in Figure 4.

[1] Level IV of the FEAF, derived from the Zachman Framework

Table 2. NIH Enterprise Architecture Matrix

	Data Architecture	Application Architecture	Technology Architecture
Planner Perspective	List of Enterprise Business Objects	List of Business Processes, + multi-enterprise processes.	List of Business Locations and Business Partners
Owner Perspective	Semantic Model	Business Process Models (including multi-enterprise)	Business Logistics System + multi-enterprise logistics
Designer Perspective	Logical design patterns; Use enterprise business objects	Logical design patterns, by style	Integration technology for enterprise systems
Builder Perspective	Physical design patterns; Use shared database if applicable	Logical design patterns, by style	Physical design patterns; Use bricks from TRM or request a waiver. TRM includes security, NIH network, other infrastructure
Subcontractor Perspective	Project scope	Use common services or APIs, if defined	

Source: Gartner, 2004

This architecture report focuses on the Planner, Owner and Designer views, as shown in Table 2.

Table 3. Enterprise Systems Monitoring Alignment With the NIH Enterprise Architecture Matrix

	Data	Applications	Technology
Planner View	N/A	N/A	■ **Scope** in Section 1.2 of this document
Owner View	N/A	N/A	N/A
Designer	N/A	N/A	■ **Patterns** in Section 2.0 of this document identify the various ESM disciplines that monitor the hardware, software and operational elements of the computing systems and the networking components that inter-connect them.
Builder	N/A	N/A	■ **Bricks** in Section 3.0 of this document that specify the tools to monitor the hardware, software and operational elements of the computing systems and the networking components that inter-connect them.

Source: Gartner, 2004

1.4 Principles

The ESM Domain Team identified principles and supporting rationales as shown in Table 3. Each identified principle should be universally accepted and should be stable so as to withstand changes in ESM technologies and products. They should maintain a clear relevancy with policy changes in NIH programs and management approaches as well as reflect the general policy directions and framework of the Federal Government.

The principles are accompanied by rationales that explain their importance and business implications. While the statement of each principle should remain constant, the rationales and implications will evolve over time, as they respond to factors such as the current information management environment within NIH, internal initiatives, external forces and changes in the NIH mission, vision and strategic plan.

Table 4. ESM Architecture Principles

Principle	Rationale
Preferred Source for ESM Tools: Tools will be selected by preferring: first commercially available packages, then Government-off-the-shelf (GOTS) solutions and then shareware solutions, with custom-built solutions as a last resort.	The objective for ordering these preferences is to minimize maintenance efforts through selecting tools that are well supported by a stable, reliable source. Cost, functionality, speed-to-implementation and other considerations will also be evaluated, ranked and included in the decision.
ESM Coverage: ESM tools will integrate across all NIH organizations.	NIH needs a complete systems view of all components that support enterprise applications, including within the ICs. This is compatible with the Principal principle.
Self-Service: ESM tools will provide a self-service interface for checking system, network or problem status.	ICs should have access to system, network or problem status without calling the Help Desk or NOC. This capability would assist them in their own troubleshooting and service level processes. Leading practices also recommend allowing users to check the status of their own problems.
Support EA Standards: ESM solution will address EA products and standards as specified in other domain bricks.	The ESM architecture will support the target enterprise infrastructure, databases and applications at NIH.

Source: Gartner, 2004

1.5 Summary of Key Decisions

- A single Event Management (Manager of Managers [MoM]) platform will be selected.
  - This will allow for consolidated management of infrastructure elements across architecture layers and organizational boundaries.
  - The MoM will be either CA Unicenter or HP OpenView.
- Mercury Interactive Topaz is considered the strategic tool for Application Management.
- Oracle Enterprise Monitoring is considered the strategic tool for database monitoring.

- The selected MoM will be used in conjunction with CiscoWorks and the Fluke suite to manage network elements.
- Remedy is considered the strategic solution for Problem Management.
- While tactical solutions for Performance Management have been identified in the interim, there is a need to define a longer-term strategic approach.
- A strategic toolset for Server Management will be selected once there is greater clarity on the direction for the overall server infrastructure.
- A strategic toolset for Storage Management will be selected once the overall direction for enterprise storage solutions has been determined.
  - A tactical toolset supporting the existing infrastructure of storage technologies has been identified.
- The ESM Enterprise Architecture will evolve in breadth and detail to support the process and organizational implementation of ESM at NIH.

1.6 Benefits of Enterprise Systems Monitoring

Like many large organizations, NIH is a complex environment with a great deal of diversity in both technologies and applications that support some common processes and many unique functions. Enabling those common processes to be supported in a consistent and reliable way requires that the enterprise applications that support automation of those common processes be managed from end to end. This necessitates understanding the topology of IT elements that make up those enterprise applications and having strong ESM capabilities to manage those elements.

The objective of the ESM domain is to improve service levels for critical enterprise applications. Ideally, NIH ESM processes and tools should enable proactive problem avoidance and faster problem remediation through better availability management, which would drive benefits in three areas:

- Proactive problem identification and resolution can avoid interruptions to user service and result in:
  - Better productivity for users due to less downtime
  - Reduced risk of outages that could impact NIH mission activities
  - Fewer help desk calls, leading to reduced cost of service.
- Providing a better understanding of systems availability issues will improve IT's ability to enhance current capabilities.
  - IT organizations can provide better cost estimates for delivering a given level of availability for existing or new applications.
  - Provide a basis for implementing other ESM services.

- Leveraging fewer ESM solutions across NIH can improve the productivity and effectiveness of IT staffs.
  - By focusing on a smaller set of products, NIH technologists can develop deeper skills and greater proficiency.
  - Potential cost savings can also accrue if volume purchase agreements are deemed to be advantageous.

This ESM architecture effort was undertaken to achieve these benefits by positioning NIH with the proactive operational capabilities to address end-to-end management of NIH's enterprise applications. Troubleshooting and problem avoidance across these applications components will be significantly enhanced as end-to-end visibility is achieved.

2.0 ESM Design Patterns

Design patterns may be *logical* or *physical.* Logical design patterns do not specify technology platforms, products or brand names. A logical design pattern may be implemented by one or more related physical design patterns. Patterns provide design guidance to implementation teams and can occur in one domain or span multiple domains. Patterns provide a reference model ("blueprint") for the technology elements that can be combined to solve a specific problem.[1]

The following section details the High-Level ESM Pattern. Additional patterns will be added to this section as they are architected.

2.1 Pattern 1: High-Level ESM Pattern

2.1.1 Description

The High-Level ESM Pattern is a logical pattern that shows how the different ESM disciplines and operational elements are related. Understanding the connections and dependencies amongst the disciplines is key to prioritizing and sequencing the establishment of ESM within the NIH enterprise. This will require a selection of tools, development of processes and procedures and commitment of people. This pattern provides context for any additional ESM patterns that will be developed as the ESM architecture evolves through the people, process and technology evolution.

2.1.2 High-Level ESM Pattern Solution

This High-Level ESM Pattern in Figure 5 represents a work in progress and will continue to change as the ESM market matures and its component technologies evolve. Several of the components in the diagram are represented with a dashed line, which indicates a potential future development for NIH.

Business Service Management is depicted as future functionality at the top of the diagram and represents how NIH would align IT infrastructure and applications with the business processes they enable. Business Service Management, when properly implemented, will provide NIH with level 4 capabilities in the Effective Process Development Maturity Model shown in Figure 2 in section 1.0.

Event Management, or MoM, and **Problem Management** are two critical components of ESM. Information from other ESM disciplines like Availability, Performance, Security, Configuration Management and Change Management are correlated in the MoM. The MoM then interacts closely with the **Problem Management** system by triggering trouble tickets or incident reports.

[1] Technology represented by "bricks" or specific technologies inside a brick.

The **Availability Management** disciplines are represented in the lightly shaded rectangle on the left of the pattern. Five services monitor, collect and correlate the data from the managed elements. Availability Management tools provide proactive and predictive capabilities. They typically provide data on the health of the managed elements to support a dashboard view of systems availability.

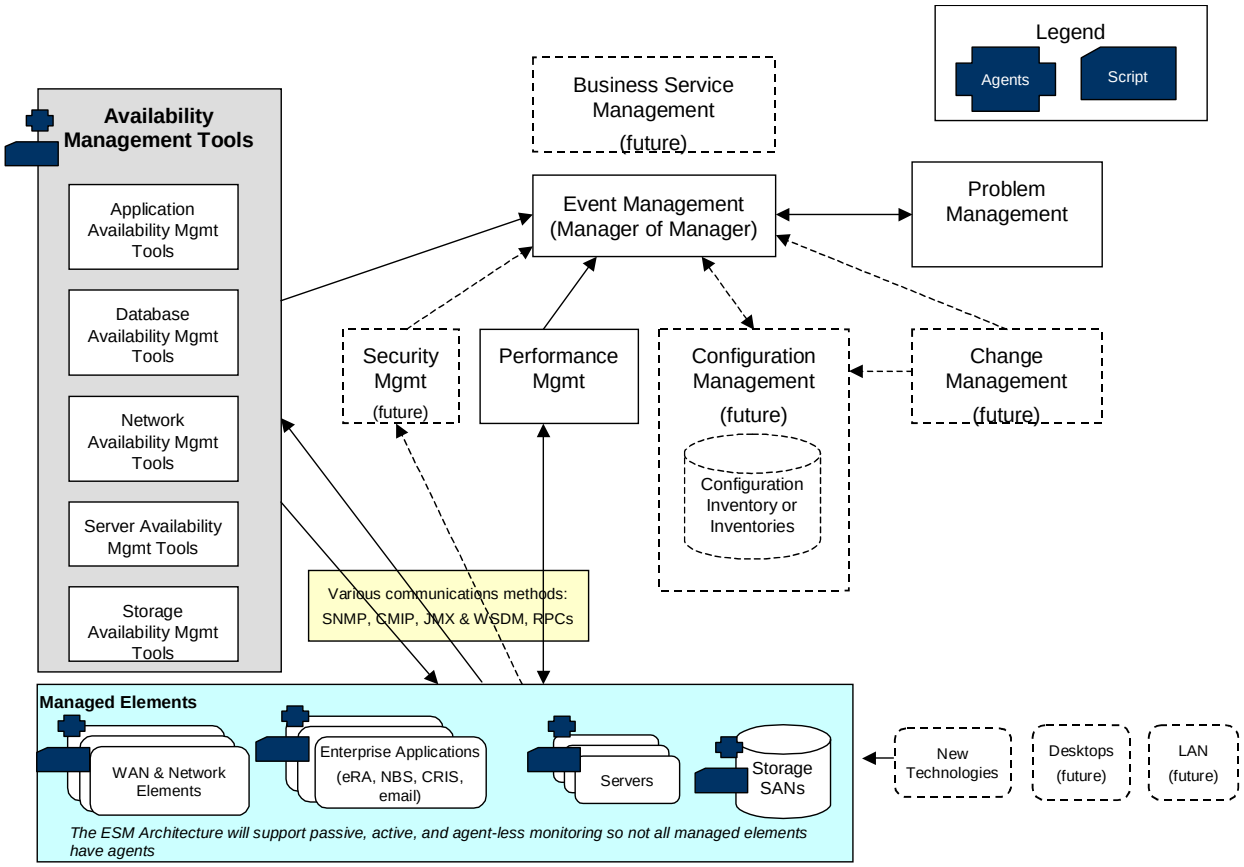
Performance Management represents the trending of end-to-end response time and network, system and application component performance parameters to predict short-term future performance degradation and has direct interfaces to the Managed Elements and the Event MoM.

Security Management, Configuration Management and Change Management are each displayed as future elements to the diagram; however, the basic interaction with the in-scope elements is depicted.

Managed Elements at the bottom of the diagram show which technical components are in scope for this iteration of the ESM Architecture. Future architecture efforts could extend the elements that are managed by ESM to include new technologies, workstations and additional applications.

The **Scripts** and/or **Agents** are software that reside on the managed elements and interact with the management tools through various communication protocols: Simple Network Management Protocol (SNMP), Common Management Information Protocol (CMIP), Java Management Extensions (JMX) and Web Site Design Method (WSDM), or remote procedure calls (RPC). The actual mechanism used for each interaction between the ESM tools and the managed elements is determined by the chosen tool.

Figure 4. High-Level ESM Pattern



Source: Gartner, 2004

2.1.3 Benefits

This pattern:

- Establishes the framework and roadmap for NIH
- Provides foundation from which NIH can achieve higher levels in the Effective Process Development Maturity Model shown in Figure 2
- Identifies the initial relationship between the disciplines, managed elements and the MoM for the NIH ESM framework
- Enables proactive monitoring to be established for critical applications.

2.1.4 Limitations

This pattern shows some areas where further refinement and definition is needed within the ESM architecture. Configuration management is needed to provide a consistent end-to-end view of the components and connections required to deliver service to the

users. Although not shown in this pattern, many of the other ESM tools would eventually need to access the configuration inventory.

As NIH builds greater capabilities in the ESM area, additional elements could also be added to the scope of managed elements. If analysis of the problem management records suggests that service interruptions could be prevented at the desktop or laptop level, then those systems could also be monitored. And the continuous introduction of new technologies into the NIH environment should include some consideration of ESM requirements and scope to ensure acceptable service levels of availability, performance and capacity.

This pattern also does not address the relationships between people, processes and technology, which are key to the success of ESM implementations. This solution is also limited by the functionality available in packaged applications, which have not yet implemented the latest technologies and leading practices.

3.0 ESM Bricks

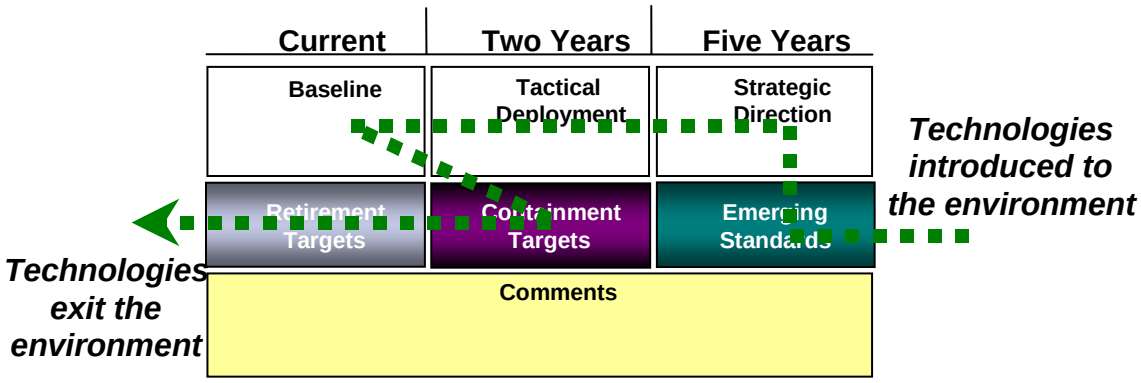
In the Technical Reference Model (TRM), baseline and planned technology choices for elements meet in a chart called a "brick." Bricks represent the physical building blocks of the enterprise IT systems — they identify specific technologies used to implement solutions. Bricks document both NIH's current ("as is") environment and future ("to be" or target) states. The planning horizon is five years.

Each brick captures:

- A description of the technology and its role
- Specific implications, dependencies, deployment and management strategies
- Technology elements, categorized.

A brick template is shown below:

Figure 5. The Technical Brick



Source: Gartner, 2004

The technology choices for architectural elements are categorized as follows:

- **Baseline** technologies include current technology and/or process element(s) in use.
- **Tactical** technologies are recommended for use in the near or tactical time frames (next two years). Currently available products needed to meet existing needs are identified here.
- **Strategic** technologies provide strategic advantage and might be used in the future. Usually, marketplace leaders are identified here, as they are likely to provide better benefits and meet the anticipated needs of the business.
- **Retirement** technology and/or process elements targeted for de-investment during the architecture planning horizon (five years).
- **Containment** includes technology and/or process elements targeted for limited (maintenance or current commitment) investment.

- **Emerging** technology and/or process elements are to be evaluated for future use based on technology availability and business need. These technologies may not be new to the marketplace, but are simply not yet in use at NIH. In this case, the products may be a fit for emerging needs at NIH.

NIH's ESM architecture includes the following bricks:

- Availability — Application Management
- Availability — Database Management
- Availability — Network Management
- Availability — Server Management
- Availability — Storage Management
- Configuration Management
- Event Management — MoM
- Performance Management
- Problem Management.

3.1 Brick 1: Availability — Application Management

Availability — Application Management is the monitoring, collecting and correlating performance, event and availability statistics to predict and, thus, avoid potential downtime for application servers and application services. This discipline involves using automated tools to avoid problems (e.g., automatically increasing file space when it reaches a threshold) and job scheduling to reduce operator error and improve the availability of batch applications and data.

Table 5. Availability — Application Management Brick

Baseline Environment (Today)	Tactical Deployment (zero to two years)	Strategic (two to five years)
■ Alert Site ■ Big Brother ■ Exchange's Link Monitor ■ HP OpenView ■ IPSentry ■ LMonk ■ MailCheck ■ Micromuse SMS ■ Nagios ■ NetIQ ■ PageSentry ■ Pelican ■ SiteScope ■ WhatsUp Gold	■ Alert Site ■ HP OpenView ■ Nagios ■ SiteScope ■ Mercury Interactive Topaz Web Monitoring Suite For E-mail: ■ CA Unicenter (Exchange Agent) ■ ipMONITOR ■ Exchange Link Monitor ■ Other tools TBD	■ Mercury Interactive Topaz Web Monitoring Suite
Retirement (Technology to eliminate)	**Containment (No new deployments)**	**Emerging (Technology to track)**
■ Big Brother ■ LMonk	■ IPSentry ■ *MailCheck* ■ Micromuse SMS ■ PageSentry ■ *Pelican* ■ WhatsUp Gold	■ Technologies that manage J2EE applications, such as Wily Technologies ■ Technologies customized for managing Oracle Financials, such as Veritas/Precise and Oracle Enterprise Monitor ■ Technologies that manage .NET (Microsoft) applications ■ IT mapping tools, such as ❑ Relicore ❑ Cendura ❑ Collation ❑ Appilog

Comments
■ Additional strategic tools will be determined after elements to be monitored are defined in the ESM process design and implementation efforts. ■ Tools in *italics* font were designated as Containment because there was no evidence from current deployments to consider those products as superior alternatives to the products that were designated Tactical and Strategic. ■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.

3.2 Brick 2: Availability — Database Management

Availability — Database Management is collecting and correlating performance, event and availability statistics to predict and, thus, avoid potential downtime for database management systems.

Table 6. Availability — Database Management Brick

Baseline Environment (Today)	Tactical Deployment (zero to two years)	Strategic (two to five years)
■ Auto DBA (NBS) ■ Custom Shell Scripts ■ Nagios ■ Oracle Enterprise Monitoring ■ PerfMon ■ Quest Monitoring Tool	■ Auto DBA (NBS) ■ CA Unicenter ■ Custom Shell Scripts ■ Oracle Enterprise Monitoring ■ PerfMon ■ Quest Monitoring Tool	■ Oracle Enterprise Monitoring
Retirement (Technology to eliminate)	**Containment (No new deployments)**	**Emerging (Technology to track)**
	■ Nagios	■ Other leading or innovative database management products such as: ❑ LeccoTech ❑ NetIQ
Comments		
■ Nagios is designated as Strategic for other ESM bricks, but not for database monitoring. ■ Additional strategic tools will be determined after elements to be monitored are defined in the ESM process design and implementation efforts. ■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.		

3.3 Brick 3: Availability — Network Management

Availability — Network Management is collecting and correlating performance, event and availability statistics to predict and, thus, avoid potential downtime for network elements and end-to-end connections.

Table 7. Availability — Network Management Brick

Baseline Environment (Today)		Tactical Deployment (zero to two years)	Strategic (two to five years)
■ ActiveWATCH ■ Big Brother ■ CA Unicenter ■ CiscoWorks ■ Custom scripts ■ Dell OpenManage ■ Enterasys ■ Ethereal ■ EtherPeek ■ HP OpenView NNM ■ InfraTools ■ IP Check ■ Locally developed tools	■ Nagios ■ Navisphere ■ Netcool/Webtop Client ■ Nmap ■ PageManager ■ RRD ■ SiteScope ■ SolarWinds ■ thcrut ■ WhatsUp Gold ■ winFingerprint	■ CA Unicenter ■ CiscoWorks ■ EtherPeek ■ Fluke ■ HP OpenView NNM ■ Nagios ■ Netcool/Webtop Client ■ RRD	■ CiscoWorks ■ Either HP Openview or CA Unicenter ■ Fluke (Suite)
Retirement (Technology to eliminate)	**Containment (No new deployments)**		**Emerging (Technology to track)**
■ Big Brother ■ InfraTools ■ IP Check	■ *ActiveWATCH* ■ *Custom scripts* ■ *Dell OpenManage* ■ *Enterasys* ■ *Ethereal* ■ *IP Check* ■ *Locally developed tools* ■ *Navisphere* ■ *Nmap* ■ *PageManager* ■ *SiteScope* ■ *thcrut* ■ *WhatsUp Gold* ■ *winFingerprint*		■ Other leading or innovative network management products such as: ❑ Adlex ❑ Net QoS ❑ Voyence

Comments

- NIH needs to choose either the HP Openview or CA Unicenter framework as the enterprise strength network management tool.
- Tools in *italics font* were designated as Containment because there was no evidence from current deployments to consider those products as superior alternatives to the products that were designated Tactical and Strategic.
- Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products.
- Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.

3.4 Brick 4: Availability — Server Management

Availability — Server Management is collecting and correlating performance, event and availability statistics to predict and, thus, avoid potential downtime for servers and end-to-end connections.

Based on information from Gartner research and NIH experiences, the ESM Domain team decided to determine strategic vendors for NIH's Server Management needs at a future time. However, tactical deployments of vendors for Server management have been identified in Table 7.

Table 8. Availability — Server Management Brick

Baseline Environment (Today)	Tactical Deployment (zero to two years)	Strategic (two to five years)
■ CA Unicenter ■ CA-7 & CA-11 ■ Compaq Insight Manager ■ HP Openview ■ ipMONITOR ■ Nagios ■ NetIQ ■ Site Scope ■ Spong (Several Instances) ■ System Edge from Concord	■ CA Unicenter ■ Compaq Insight Manager ■ HP Openview ■ ipMONITOR ■ Nagios ■ NetIQ ■ Site Scope ■ Spong (Several Instances) ■ System Edge from Concord	■ TBD
Retirement (Technology to eliminate)	**Containment (No new deployments)**	**Emerging (Technology to track)**
	■ CA-7 & CA-11	
Comments		
■ Additional strategic tools will be determined after elements to be monitored are defined in the ESM process design and implementation efforts. ■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.		

3.5 Brick 5: Availability — Storage Management

Availability — Storage Management is collecting and correlating performance, event and availability statistics to predict and, thus, avoid potential downtime for storage subsystems.

Based on information from Gartner research and NIH experiences, the ESM Domain team decided to determine strategic vendors for NIH at a future time. However, tactical deployments of vendors for SAN management, storage resource management, provisioning, hierarchical storage management and storage policy management have been identified in Table 8.

Table 9. Availability — Storage Management Brick

Baseline Environment (Today)	Tactical Deployment (zero to two years)	Strategic (two to five years)
■ Custom Shell Scripts ■ EMC Control Center ■ Sun Enterprise Backup System ■ SysEdge Concord ■ Tivoli Storage Manager	■ Custom Shell Scripts ■ EMC Control Center ■ Sun Enterprise Backup System ■ SysEdge Concord ■ Tivoli Storage Manager	■ TBD
Retirement (Technology to eliminate)	**Containment (No new deployments)**	**Emerging (Technology to track)**
		■ Other leading or innovative network management products such as Veritas
Comments		
■ Additional strategic tools will be determined after elements to be monitored are defined in the ESM process design and implementation efforts. ■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.		

3.6 Brick 6: Configuration Management

Configuration Management is the documentation and management of the technical elements and relationships in the IT infrastructure, application and business process components. This discipline is an underpinning of problem, change and availability management. Configuration Management provides an understanding of how applications, business processes and IT elements relate, so that the impact or resolution priority of a change or problem (e.g., outage) can be determined. Which component relationships are tracked and how the information is used depend on the task required:

- Client configuration management tools focus on configuring and deploying operating system, patches and applications to client devices.
- Server configuration management tools focus on configuring and deploying operating system, patches, applications and content to servers.
- Network configuration management tools focus on documenting configuration files, auditing changes and deploying updates to network devices.
- IT service configuration management tools focus on discovering and documenting the relationships among the components that comprise an IT service — from end-user devices to servers, networks, storage, applications and data. These tools are prerequisites for achieving success with service-level, change, problem, availability and performance management.

This brick has captured many types of configuration management tools in the baseline environment. In the next iteration of the architecture, the following sub-categories of this brick will be created: client, server, network, business intelligence and IT service configuration management. Once the ESM implementation efforts refine the list of technology elements that must be managed, the strategic and tactical directions for each type of configuration management tool will be revisited.

Table 10. Configuration Management Brick

Baseline Environment (Today)		Tactical Deployment (zero to two years)	Strategic (two to five years)
■ Angry IP Scan ■ Applimation Change Manager for Oracle ■ Applimation Setup Reporter ■ CiscoWorks ■ Ecora Enterprise Auditor SMS ■ ePolicy Orchestrator ■ HP OpenView Operations ■ iTRACS	■ NetSight Element Manager ■ PatchLink ■ Rational Tools ■ Ringmaster ■ SMS ■ Spectrum Element Manager ■ System Update Services (SUS) ■ Update Expert ■ Visio professional ■ ZenWorks	■ Applimation Change Manager for Oracle ■ CA Unicenter ■ CiscoWorks ■ PatchLink ■ SMS ■ System Update Services (SUS) ■ Update Expert ■ ZenWorks	■ TBD
Retirement (Technology to eliminate)	**Containment (No new deployments)**		**Emerging (Technology to track)**
	■ *Angry IP Scan* ■ *Applimation Setup Reporter* ■ *Ecora Enterprise Auditor SMS* ■ *ePolicy Orchestrator* ■ *iTRACS*	■ *NetSight Element Manager* ■ *Rational Tools* ■ *Ringmaster* ■ *Spectrum Element Manager* ■ *Visio professional*	■ IT Mappings Tools such as: ❑ Relicore ❑ Cendura ❑ Collation ❑ Appilog ■ Other leading or innovative vendors of Configuration Management software, such as: ❑ Novadigm (HP) ❑ Blade Logic ❑ Opsware ❑ Altiris
Comments			
■ Additional strategic tools will be determined after elements to be monitored are defined in the ESM process design and implementation efforts. ■ Tools in *italics font* were designated as Containment because there was no evidence from current deployments to consider those products as superior alternatives to the products that were designated Tactical and Strategic. ■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.			

3.7 Brick 7: Event Management — MoM

Enterprise event management systems support the acceptance of events from elements in the IT infrastructure; consolidate, filter and correlate those events; notify the appropriate IT operations personnel of critical events; and automate corrective action where possible. Event management helps IT operations personnel contend with the deluge of events that come in from the IT infrastructure by narrowing the events to the likely cause of the problem and associating them with the potential business impact. The goals are to improve the mean time to isolate and repair problems and to prioritize problem resolution support efforts according to business process value. Event Management — Managers of Managers, or “MoM” products generally run on Unix or Windows and provide functionality in the following three key areas:

1. Event Collection/Consolidation: the ability to accept events from one or more of the following types of IT elements:
   - System (hardware and operating system)
   - Network
   - Storage
   - Database
   - Application (packaged, off-the-shelf and/or custom applications).
2. Event Processing/Correlation: the automated, out-of-the-box ability to process/correlate events through one or more of the following techniques:
   - De-duplication/filtering (for example, when multiple, repetitive events are received for the same problem on the same element, store the event once and increase a counter indicating the number of times it has been received, rather than flooding the user's screen with redundant events)
   - Event suppression (for example, suppress the sympathetic events that occur when elements downstream from a known problem are unreachable)
   - State-based correlation at the object level (for example, if a "link down" event is received for a router interface that then corrects itself and generates a subsequent "link up" event, the event management system correlates the two and clears the original link down event).
3. Event Presentation: the ability to present event data to the IT operations staff in one or more of the following ways:
   - On the console screen using color and sound (visual and audible alarms)
   - Through a Web interface
   - By pager and e-mail
   - By logical groupings (presenting groups of events that relate to business processes, IT services, departments, geographic regions or any other arbitrary, user-defined grouping).

Table 11. Event Management — MoM Brick

Baseline Environment (Today)	Tactical Deployment (zero to two years)	Strategic (two to five years)
■ CA Unicenter ■ HP Openview ■ MicroMuse ■ Nagios	■ CA Unicenter ■ HP Openview ■ Micromuse ■ Nagios	■ Either HP Openview **or** CA Unicenter
Retirement (Technology to eliminate)	**Containment (No new deployments)**	**Emerging (Technology to track)**
		■ Other leading or innovative vendors of Event Management tools, such as: ❑ Mercury Interactive Topaz Auto RCA ❑ Managed Objects ❑ HP Event correlation ❑ CA Neugent Technology
Comments		
■ NIH needs to choose either the HP Openview or CA Unicenter framework as the MoM. ■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.		

3.8 Brick 8: Performance Management

Performance Management is the trending of end-to-end response time and performance parameters from network, system and application components to predict short-term future performance degradation. This discipline assists in quicker problem diagnosis, thus reducing downtime, and can even provide advance warning of imminent problems so that they can be prevented proactively.

In the future, this brick will be further sub-categorized into: Database, Application, Server types, Storage, Network and Middleware.

Table 12. Performance Management Brick

Baseline Environment (Today)		Tactical Deployment (zero to two years)	Strategic (two to five years)
■ Applimation DB Downsizer ■ BMC/Mainview ■ CA Unicenter ■ CA/OPS/MVS ■ SysEdge ■ Envision ■ HP Insight Manager ■ HP OpenView ■ IP Monitor ■ ipscan	■ KeyNote/ (outsourced) ■ RRD ■ Nagios ■ NetScout nGenius ■ On Centennial ■ Open NMS ■ PerfMon ■ SiteScope ■ Visual Basic Console App (Homegrown)	■ CA Unicenter ■ HP Openview ■ Nagios ■ Perfmon ■ RRD ■ SiteScope ■ SysEdge	■ TBD
Retirement (Technology to eliminate)	**Containment (No new deployments)**		**Emerging (Technology to track)**
■ Visual Basic Console App (Homegrown)	■ *Applimation DB Downsizer* ■ *BMC/Mainview* ■ *CA/OPS/MVS* ■ *Envision* ■ *HP Insight Manager*	■ *IP Monitor* ■ *Ipscan* ■ KeyNote/ (outsourced) ■ NetScout nGenius ■ *On Centennial* ■ Open NMS	■ Performance management tools that leverage instrumentation in J2EE applications ■ Other leading or innovative vendors of Event Management tools, such as: ❑ Mercury Interactive Topaz ❑ IPM (Cisco) ❑ ProactiveNet ❑ Gomez

Comments

- Strategic tools will be determined after elements to be monitored are defined in the ESM process design and implementation efforts.
- Tools in *italics font* were designated as Containment because there was no evidence from current deployments to consider those products as superior alternatives to the products that were designated Tactical and Strategic.
- Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products.
- Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.

3.9 Brick 9: Problem Management

Problem Management is identifying, quickly resolving and preventing problems through root cause analysis and tracking. Problem management involves identifying and classifying problems, determining escalation procedures and documenting all the information surrounding the characteristics and resolution of the problem. All problems should be assigned a severity level according to the business risk and the potential impact of the problem. To ensure that problems have a minimal impact on the enterprise, problems must be prioritized, monitored and assessed for potential frequency of re-occurrences. Problem management includes fault, event and incident (or trouble ticket) management.

NIH will need to refine the problem management process workflow and prioritize which portions of that workflow can and should be automated and integrated into the MoM. The ESM domain team recognized that there is process work to be completed to fully leverage the capabilities of the existing Remedy Problem Management system, include establishing a Blackberry interface.

Table 13. Problem Management Brick

Baseline Environment (Today)	Tactical Deployment (zero to two years)	Strategic (two to five years)
■ Remedy Problem Management ■ E-mail Notifications ■ List Servers	■ Remedy Problem Management	■ Remedy Problem Management
Retirement (Technology to eliminate)	**Containment (No new deployments)**	**Emerging (Technology to track)**
■ List Servers	■ E-mail Notifications	
Comments		
■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.		

4.0 Gap Analysis

- NIH has not implemented an enterprisewide NOC.
- NIH has not yet standardized on ESM processes, tools and roles.
- The strategic product choice for the Event Management — MoM has not yet been identified or implemented.
- There is process work to be completed to fully leverage the capabilities of the existing Remedy Problem Management system, include establishing a Blackberry interface and standard operating procedures for event tracking.
- In a future iteration of the ESM Domain, Configuration Management will be broken out into sub-categories: Patch Management, Software Distribution, Provisioning, IT Mapping, Network Configuration Management.
- In a future iteration of the ESM Domain, Performance Management will be sub-categorized into: Database, Application, Server types, Storage, Network, Middleware
- NIH needs to document the end-to-end topology and the specific elements that must be monitored for each of the four enterprise applications: MS-Outlook, CRIS, eRA/IMPACII and NBS. These elements need to be described in a way that allows an end-to-end view of their components to be used for improved problem prevention, isolation and diagnosis.

5.0 Next Actions

At the conclusion of the domain team meetings, the team identified the following next steps:

- Define level of integration for what we want to share:
  - What types of alerts and adverse events should be propagated across IC boundaries?
  - How much configuration information needs to be accessible across IC boundaries for problem determination?
- Initiate a project to integrate ESM requirements into application development and package selection efforts.
  - Work with application developers to incorporate guidance for appropriate instrumentation into SDLC and project QA activities.
  - Work with application developers to develop an instrumentation toolkit that can be leveraged on development projects to build in instrumentation.
  - Ensure SDLC and project QA activities involve Operations, Maintenance and Support personnel on each project to ensure smooth turnover into production.
  - Consider using a virtual team to accomplish this integration.
- Establish an NIH-wide recommended set of commands and scripts to provide consistent data for ESM, including standard TCP command line tools (ping, traceroute, etc.) and network configuration, network node and protocol analyzer tools, such as SolarWinds.
- Document the end-to-end topology of the enterprise applications to define what technology elements need to be managed. This includes prioritizing which subnets need synthetic logins to accommodate support needs of VIPs.
- Develop approach for supporting and monitoring Section 508 accessibility tools and technology.
- Develop a security architecture (groups, roles, access privileges) for ESM implementation that allows an integrated window into the “Big Picture.”

Appendices

Appendix A—Glossary of Terms

Term	Definition
Asset Management	Managing and tracking the asset inventory, including the financial aspects of the configuration elements, primarily warranty, purchase, maintenance and operational costs. Can include analysis and tracking of availability and reliability history to help evaluate future purchases.
Availability Management — Application	Monitoring, collecting and correlating performance, event and availability statistics to predict and, thus, avoid potential downtime for application servers and application services. This discipline involves using automated tools to avoid problems (e.g., automatically increasing file space when it reaches a threshold) and job scheduling to reduce operator error and improve the availability of batch applications, online applications and data. This should also cover application support services, such as Web services, middleware and infrastructure applications like Active Directory.
Availability Management — Database	Monitoring, collecting and correlating performance, event and availability statistics to predict and, thus, avoid potential downtime for database services.
Availability Management — Network	Collecting and correlating performance, event and availability statistics to predict and, thus, avoid potential downtime for network elements and end-to-end connections. This discipline involves using automated tools to avoid problems and job scheduling to reduce operator error and improve the availability of the network.
Availability Management — Storage	Collecting and correlating performance, event and availability statistics to predict and, thus, avoid potential downtime for database servers, file servers and storage devices (SANs, NAS, DASD, RAID, etc.). This discipline involves using automated tools to avoid problems (e.g., automatically increasing file space when it reaches a threshold), backup and recovery of data, and job scheduling to reduce operator error and improve the availability of applications and data.
CMIP	Common Management Information Protocol provides more extensive data than SNMP and runs under the Open Systems Interconnection (OSI) communications suite.
Capacity Management	Extends performance management into predicting future IT resource needs. Capacity planning uses historical trends and information on new or changing workloads to help the IS organization avoid shortages and meet its service-level objectives.
Change Management	Process and governance around managing and authorizing changes to the production environment to improve quality of service (e.g., experience less downtime) through better planning, testing, coordinating and scheduling of application and IT infrastructure changes. The most common cause of people and process failures is change. Enterprises that have established strong change management practices typically have the highest levels of availability. When a change causes a problem, enterprises must have rollback procedures to minimize the overall outage. Furthermore, changes that cause extended outages may require an enterprise to invoke its business continuity plan.

Term	Definition
Configuration Management	Tracking and managing the technical elements and relationships in the IT infrastructure, application and business process components. This discipline is an underpinning of problem, change and availability management. Configuration Management provides an understanding of how applications, business processes and IT elements relate, so that the impact or resolution priority of a change or problem (e.g., outage) can be determined. Related to Asset Management (see above) Also related to software distribution (which is out of scope for this effort)
COTS	Commercial off-the-shelf software, i.e. commercial packages.
Event Management (MoM)	Event Management (MoM) has three key event management disciplines: 1. Event Collection/Consolidation — System must have the ability to accept events from one or more of the following types of IT elements: network devices, storage subsystems or devices, database systems, and applications (packaged, off-the-shelf and/or custom applications) 2. Event Processing/Correlation De-duplication/filtering, event suppression and state-based correlation at the object level 3. Event Presentation — On the console screen, through the Web, by pager and e-mail, by logical groupings.
GOTS	Government off-the-shelf software, i.e. government shareware.
J2EE	Java 2 Platform, Enterprise Edition is a standard for developing multi-tiered, component-based applications.
JMX	Java Management Extensions is an open technology toolset for building distributed, Web-based solutions for managing devices, applications and networks.
Performance Management	The trending of end-to-end response time and network, system and application component performance parameters to predict short-term future performance degradation (e.g., where performance parameters are outside of the baseline). This discipline assists in quicker problem diagnosis, thus reducing downtime.
Problem Management	Identifying, quickly resolving and preventing problems through root cause analysis. Problem management involves identifying and classifying problems, determining escalation procedures and documenting all the information surrounding the characteristics and resolution of the problem. All problems should be assigned a severity level according to the business risk and the potential impact of the problem. To ensure that problems have a minimal impact on the enterprise, problems must be prioritized, monitored and assessed for potential frequency of reoccurrences. Also includes incident (or trouble ticket) management and related escalation procedures.
SNMP	Simple Network Management Protocol provides system status and is based on TCP/IP.
Security Management	Ensuring the environment is secure from unauthorized access to data or systems and protected against malicious intrusion that could compromise the performance, capabilities or integrity of the systems. Identifying and

Term	Definition
	reacting to security incidents in real-time requires comprehensive system and network monitoring, Furthermore the ability to aggregate alarms and other information from disparate systems is necessary to correlate events and identify an incident. Includes ID/password management, intrusion detection, virus control and vulnerability analysis.
Service Level Management	Tracking and monitoring the services delivered and comparing actual delivery metrics on availability, recoverability and service times to the targets specified within Service Level Agreements.
WSDM	Web Site Design Method is a model for Web services management developed by a committee of the same name formed by the OASIS e-Business standards body.

Change History / Document Revisions

Date	Change Author	Change Authority	Change Event	Resulting Version
21 April 2004	C. Blanton	Jack Jones	Original Production	1.0

Client Contact Information

John F. Jones, Jr.
Chief IT Architect
Telephone: +1-301-402-6759
E-mail: jonesjf@mail.nih.gov

Gartner (Contractor Support) Contact Information

Terry McKittrick
Gartner Consulting
Telephone: +1-703-226 4779
Facsimile: +1-703-226 4702
E-mail: Terry.McKittrick@gartner.com