
Section 9. ETA Enterprise Systems Management Domain

The ETA Enterprise Systems Management (ESM) Domain defines the operational aspects of IT services delivery and identifies generally accepted industry policies, practices, standards, and processes for administering, monitoring, and controlling hardware and software components of the infrastructure.

ESM activities include but are not limited to, network monitoring, monitoring servers, applications monitoring, net-flow analyzer, troubleshooting tools, helpdesk, assets management, storage management, wireless LAN management, event management, and performance management.

ESM processes focus on methods, techniques and procedures relating to IT service management (configuration management, event and state management, fault detection and isolation, performance measurement, patch management, vendor relationship management including Service Level Agreements (SLA), release management, change control, problem reporting, and hardware and software retirement).

ESM addresses three major topics, Service Delivery, Service Support, and Operations Management. The Service Support topic is further sub-divided into Supporting and Changing sub-topics.

Domain-wide Requirements

The following domain-wide requirements pertain to all topics and components in the Enterprise Systems Management Domain.

- 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.
- 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.
- ESM-R-03** **Security, Confidentiality, Privacy, and Statutes**. IT systems shall adhere to all security, confidentiality and privacy policies, and applicable statutes.
- ESM-R-23** **Components of Services Provided**. *Providers of enterprise services shall adopt and publish operational standards that are required to manage, control, support, and monitor infrastructure components supporting the services that they provide. The published operational standards are considered mandatory components of the services provided to customers.*

ESM operational standards related to services received through VITA are published on the VITA website under VITA Services

Service Delivery

Service Delivery relates to managerial and procedural activities that 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.

- 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.
- 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.
- ESM-R-06 Financial Management for IT Service Management** - Agencies with ESM responsibilities shall implement accounting processes and procedures that 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.
- 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.

Service Support

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 customer-facing issues and problems.

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. The Service Desk is the single point of contact for all customer communications, tracking of customer contacts, and maintenance of a repository of customer data.

-
- 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 events¹. 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.
- ESM-R-09 Incident Management**² - 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.
- ESM-R-10 Problem Management**³ - Agencies with ESM responsibilities shall institute procedures for problem handling. These 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 standardized methods and procedures are used for efficient and prompt handling of all changes, releases, and configuration actions in order to minimize the impact on service quality commitments, and consequently improve the day-to-day operations of the IT organization.

- 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.
- 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.
- ESM-R-13 Configuration Management** - Agencies with ESM responsibilities shall establish a cost effective automated Configuration Management process and

¹ 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.

² 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.

³ 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 to control and identify all IT assets⁴ (Configuration Item [CI]) and their physical locations. CIs must be documented in a Configuration Management Database (CMDB)⁵. 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 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.

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

Service Monitoring and Control

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.

- 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

⁴ 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.

⁵ 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.

International Standards Organization (ISO) 20000⁶ and support performance metrics agreed to in SLAs. In the case where internally developed ESM tools⁷ 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.

- 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 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

The Commonwealth data is vital to providing citizen services. Exercising strict data management controls necessitates having operating processes and procedures that ensure that the data is protected, retrievable, and recovered in a timely manner to meet business continuity requirements. Storage Management is concerned with data custody and control of the environment. Storage Management operational process consists of two major focus areas: (1) Data Backup, Restore, and Recovery Operations and (2) Storage Resource Management.

- 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 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.
- ESM-R-21 Systems Administration** - Agencies with ESM responsibilities shall develop and maintain appropriate operations policies, procedures, and standards to

⁶ 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>

⁷ Internally developed tools shall be engineered using Systems Development Life cycle (SDLC) methodology that complies with the Commonwealth's software development policy and standards.

ensure day-to-day management of the IT infrastructure environment. Developed policies, procedures, and standards shall comply with applicable ETA policies and standards.

- 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.

Technology for Enterprise Systems Management

Specific enterprise systems management tools are not addressed in this release of the ETA Standard. Future updates to this standard may address specific tool sets that support the requirements in this standard.