DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

APR 0 8 2015

The Department of Defense recognizes that efficient and effective management of information technology services is a critical component of the DoD Chief Information Officer Enterprise Strategy and Roadmap as well as the success of the Joint Information Environment (JIE). Central to that principle is the application of a standard IT service management (ITSM) approach across the Department for the quality delivery of IT services to the DoD customer.

This Defense Enterprise Services Management Framework (DESMF) Edition II is a Department-level ITSM framework that provides a set of standards for managing IT services and establishes clear service management requirements for the acquisition and contracting of IT services and capabilities across the Department based on industry best practices. The DESMF Edition II builds upon the Defense Information System Agency (DISA) Enterprise Service Management Framework Edition 1 and expands the scope from DISA-owned or adjudicated IT services to all IT services and capabilities provided by the DoD. The DESMF will serve as the basis for DoD CIO oversight of IT services as the Department matures its ITSM capabilities.

The long-term intent is to mature the DESMF based on input and lessons learned from DoD Component ITSM implementation experiences. Components are encouraged to participate in DoD CIO ITSM enterprise governance processes to share their experiences and to ensure their ITSM equities are addressed.

My point of contact is Barbara McCain, barbara.l.mccain.civ@mail.mil, 571-372-4660.

Terry A. Halvorsen

Department of Defense (DoD)

Enterprise Service Management Framework

Edition II

08 Nov 13

EXECUTIVE SUMMARY

Driving toward service excellence is a virtuous goal for organizations today; in part because it is proven that a proactive service environment is less expensive to run than a reactive service environment. This document is the embodiment of the integration of various best practices, frameworks and standards that defines a Department-wide service management approach. It is a 'Service Oriented' framework that focuses on creating and managing services throughout the service lifecycle. It aligns and integrates processes for service management and defines processes at a high level, describing the *what*, not the *how*. This approach enables cross-functional teams the ability to create and improve processes in the common pursuit of service excellence. More in-depth process specific guidance is provided in supplemental companion documents located on the ITSM Community of Practice CoP and APAN. Hyperlinks to both are located in the Reference section of this document.

How to use the DESMF

There is no DoD standard terminology for much of the content within the DESMF. Therefore, it is necessary to know the author's definitions of a few key terms used in the document.

- S**ervice** is a means of delivering value comprised of people, processes and technology perceived by Customers and Users as a self-contained, single, coherent entity that enables them to achieve mission objectives and functions. (Source: ISO 20000, COBIT 5, ITIL V.2 & 3)
- **Policies** are formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of processes, standards, roles, activities, IT Infrastructure etc.
- **Process** is a structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. A process may include any of the roles, responsibilities, tools and management controls required to reliably deliver the outputs.
- P**rocedure** is a document containing steps that specify how to achieve an activity. Procedures are defined as a part of processes. As such, a change to a procedure does not necessarily change a process, just as a change to a process does not necessitate a policy change.

The DESMF is the authoritative framework used to address services and processes that are owned and adjudicated by DoD. The DESMF includes:

- Processes – Department-wide processes defined at a high level and guidance to establish authoritative Process Owners and Process Managers
- Purpose and Scope – The purpose and scope of each process in the lifecycle
- Metrics – Recommendations on the use of metrics as actionable items
- Process Workflow Guidance - Mapped activities and supporting explanation

The DESMF is not:

- Concept of Operations (CONOPS) – CONOPS for processes are developed separately from this document, but use this framework to align the efforts

- Implementation plan – While this document contains steps for process design work at a high level, it is not meant as a detailed project plan or as an overall ITSM implementation plan

Do not let the number of pages within the DESMF overwhelm you. This document is specifically designed to provide as much content as possible, divided into usable and manageable sections. We recommend that anyone responsible for leading an ITSM effort or participating in ITSM activities read all of sections 1 – 5 at a minimum.

Sections 6 – 7 contain domain, process and supporting functions content. A reader may want to focus on his or her specific area of responsibility, knowing that additional content is always available for review in electronic format.

Sections 8 – 10 contain References, Acronyms and a Glossary. *Hyperlinks are in the reference section for easy access for those who view the DESMF electronically.*

The Appendices provide more detail on specific topics.

With each new edition of the DESMF, content will be added, removed, or modified based on DESMF Community of Practice reviews and feedback. As with any framework referenced within the DESMF, take the information that is required and aligned with your specific environment, along with anything that may prove helpful, and be aware of the additional information available to you.

Contents

This page intentionally left blank.

1. Background

In 2004, the Defense Information Services Agency (DISA) commissioned a study from the Open GIS (Geospatial Information Services) Consortium, Inc. (OGC to define the role of Enterprise Service Management for DISA. The study recommended the adoption of a recognized framework for guiding principles in Information Technology Service Management (ITSM) initiatives. Based on that recommendation, DISA established the ITSM Office as an organizational change agent to lead the Agency in process improvement for governance, processes, and technologies.

The ITSMO quickly realized that there are many frameworks available for guidance throughout DoD and private industry. However, the Department lacked an *integrated* framework that encompasses best practices from multiple frameworks, and provides guidance to establish the structure, documentation, and roles and responsibilities to plan, implement, monitor and improve ITSM. To this end, the ITSMO utilized internal DISA expertise, conducted Domain specific workshops and topic related focus groups to create the DISA Enterprise Service Management Framework, Edition I.

DESMF Edition I was so well received that in May 2013, the DoD CIO issued a memorandum providing authority to DISA to, "develop policy and framework to establish the responsibilities and standards for ITSM." With that authority, the ITSMO was directed by the DISA Director to represent DISA and coordinate with the DoD CIO and Combatant Commands/Services/Agencies (CC/S/A's) and industry to further develop and mature the framework that establishes DoD-wide guidance for ITSM.

As the subject matter expert for service management, the DISA ITSMO worked closely with and gathered ideas, intellectual artifacts and best practices from expertise in the Military Services, other Agencies and industry to architect this framework. The Department of Defense Enterprise Service Management Framework, (DESMF) Edition II is the result of that collaboration and the DESMF is now referenced as an integral part of the Joint Information Environment (JIE). The use of and compliance within this framework provides a strong foundational structure and approach that can be utilized by CC/S/A's to deliver excellent services and support to our mission partners and the warfighter in theater.

1.1 Purpose

The purpose of the DESMF is to provide guidance on the application of best practices to plan, implement, monitor, and improve service management initiatives. Process initiatives and service implementation efforts should align with the framework. Supporting this purpose, the document will:

- Define the best practices that drive the implementation of the framework
- Define the overall structure to the DESMF, to include Domains and processes covering the entire lifecycle of IT service management
- Provide a general overview of processes in terms of purpose, scope, benefits, lexicon, and roles and responsibilities
- Define the controls framework required to meet compliance with the agreed standards
- Define the recommended interfaces between the Domains and the processes
- Recommend a set of milestones for process implementations

To better understand the purpose of the DESMF, it is necessary to understand the difference between a standard and a framework.

ISO/IEC 20000 is a standard and consists of a set of minimum requirements to audit an organization against effective IT Service Management. The standard promotes the adoption of an integrated process approach to effectively manage numerous linked activities. The core components of the standard contained within two documents are Part1, which includes requirements specified in "shall" statements that *must* be adhered to when seeking certification and Part 2, which includes "should" statements that a service provider *should* consider. More information about ISO/IEC 20000 can be found in the appendix.

A framework is used by an organization as a structure in which to align efforts and establish a minimum level of competency, as well as continually mature and improve. It provides a structure from which an organization can plan, implement, and measure.

The DESMF is based on several frameworks and methodologies. The flexibility of the DESMF is the ability to adopt and use the best framework for specific processes and functions within the DoD. Best practices and norms may come from bodies of knowledge such as the Information Technology Infrastructure Library (ITIL), COBIT, the Capability Maturity Model (CMM), Six Sigma, the enhanced Telecom Operations Map (eTOM – Business Process Framework), ISO/IEC 20000, ISO/IEC 27001, Total Quality Management (TQM) etc. Each has a particular area of emphasis but also brings consistency and ability to measure and improve performance. A common mistake is to assume that the frameworks are exclusive of each other and that all the parts of each framework must be implemented. The DESMF combines aspects of these frameworks, provides a uniform and common language and is structured to provide guidance to improve effectiveness and efficiency.

1.2 Scope and Goals

The scope of the DESMF applies to all services and capabilities provided by the DoD, and the ITSM processes that support those services. Service implementations and process efforts should align to the DESMF as the authoritative reference framework.

The goal of the DESMF is to provide a framework to successfully align the delivery of IT services with the mission of the Department. Successful IT Service Management (ITSM) builds a bridge between people, processes, and technology that result in a combined effort to promote new ideas, effectiveness, and efficiencies by standard methods and practices that deliver value to mission partners.

As the DESMF matures and incorporates additional best practices executed throughout DoD and industry, the aim is to research, develop, incorporate, publish and promote an authoritative, up-to-date, DoD accepted process architecture and service management practice for day-to-day use by DoD.

1.3 Alignment with DoD Strategic Documents

As a means to ensure the DESMF contains the strategic elements necessary to provide a focused and purposeful service management framework, key DoD strategic plans and initiatives must be considered and referenced. The following DoD level strategic baseline documents provide the required strategic alignment and baseline of key strategic concepts considered throughout this framework.

As depicted in the figure below, DoD Strategy Alignment originates from the Executive Branch's National Security Strategy (NSS) from which the Chairman of the Joint Chiefs of Staff develops the National Military Strategy (NMS). Once received, the Secretary of Defense uses the NMS and the Quadrennial Defense Review (QDR) Report to develop the DoD Strategic Management Plan (SMP) which is then used to produce the more detailed DoD Information Enterprise Strategic Plan (basis for the JIE), the DoD CIO Campaign Plan, and the DoD IT Enterprise Strategy and Roadmap (ITESR). Short descriptions of the DoD IE Strategic Plan, the DoD Campaign Plan, the DoD ITESR, and the DISA Strategic Plan are provided in the paragraphs below.

Figure 1.3: DoD Strategic Alignment

1.3.1 DoD Strategic Management Plan

The DoD Strategic Management Plan (SMP) establishes specific business goals that directly support the Strategic Goals of the National Military Strategy (NMS). It articulates the goals and objectives of the DoD business domain, while ensuring unity of effort across the enterprise. Key concepts of the DoD Strategic Management Plan are: (1) total force readiness, (2) financial management, (3) information security, (4) agility, and (5) improved processes across the department.

1.3.2 DoD Information Enterprise Strategic Plan & DoD IT Enterprise Strategic Roadmap (ITESR)

The DoD IE Strategic Plan and the DoD ITESR together, form the basis for a broad approach to achieving the DoD Joint Information Environment (JIE). These plans articulate how the DoD will strengthen its IT enterprise through integrated and interoperable frameworks to sustain US military might and status as the preeminent war fighting organization in the world. Key concepts in these plans are**:** (1) information as a strategic asset, (2) interoperable infrastructure, (3) synchronized and responsive operations, (4) identity and information assurance, (5) optimized investments, (6) agility and interoperability of the IM/IT/IA workforce.

1.3.3 DoD CIO Campaign Plan

The DoD CIO Campaign Plan supports the Department's Strategic Management Plan and provides the requirements necessary for the DoD CIO, to "build agile and secure information technology capabilities to enhance combat power and decision making while optimizing value. It provides guidance to operate and defend the JIE, which enables DoD to employ warfighting and support capabilities. The JIE is a secure environment, comprised of shared IT infrastructure, enterprise services, and single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security, and realize IT efficiencies.

The key concept is to enable a unified IT infrastructure and supporting services which are fully integrated, interoperable, secure, and centralized approach across all organizations within the department.

1.3.4 Services/Agencies Strategic Plans

Alignment with the overall DoD strategy and direction is imperative for all DoD Agencies and Services. As an example, the DISA Strategic Plan target objective state provides for a Joint Information Environment (JIE) that optimizes the use of the DoD IT assets by converging communications, computing, and enterprise services into a single joint platform that can be leveraged for all Department missions.

Attainment of the JIE will reduce total cost of ownership, reduce the attack surface of networks, and enable mission partners to more efficiently access the IT resources for their missions. A collaborative JIE enables information sharing and interdependent enterprise services that are seamless, interoperable, efficient, and responsive to warfighter requirements.

In this manner, the DISA Strategic Plan supports and is aligned to the DoD Strategic Management Plan, the DoD IE Strategic Plan, the DoD ITESR and the DoD CIO Campaign Plan.

The DESMF in turn, provides a framework and common structure to enable the delivery of services to accomplish the mission of the Department.

1.4 Benefits of DESMF and Expected Outcomes

- Provides a single, definable, repeatable, and scalable documented framework for recommended best practices
- Clearly identifies roles and responsibilities for IT Service Management
- DoD will adopt characteristics of a high-performing organization; such as providing high service and availability levels, improved alignment between service provider and mission areas, and improved management of changes to ensure security and capability of the information enterprise
- Enables better decision making at all levels by identifying relationships and information items exchanged by all processes throughout the Service Management lifecycle.
- Services supporting the war fighter and/or mission partner will be implemented faster, more efficiently, and with higher quality
- Services will be measured transparently and traceable through the component and Agency level strategies to those of the DoD
- The costs associated with the entire service lifecycle are understood
- Compliance and subsequent auditing will be stabilized through repeatable processes
- Better understanding of the importance of IT services and the value derived from each service both from the provider as well as the mission partner perspective
- Supports ability of IT to measure and improve internal performance and service provisioning
- Improved mission partner satisfaction through a more professional, efficient approach to service delivery and support
- Secure information and data exchange

1.5 Critical Success Factors (CSF) for Framework Adoption

The successful adoption of the framework depends upon the following CSFs:

- **Form a guiding coalition** – Create a forum to provide guidance on enhancing and maintaining the DESMF
- **Create vision** – Clearly identify the gap that this initiative is trying to close between the use of current process frameworks and the future consolidated framework
- **Communicate the vision** – Create a directed training and communications plan for the adoption of the DESMF
- **Create short term wins** – Identify, mitigate, and report on pain points related to how services are currently provided
- **Create Key Performance Indicators (KPIs) –** KPIs are required to measure each CSF
- **Align KPIs/CSFs** – KPIs are required to align with customer, mission partner, and DoD goal and plans

1.6 Guidance and Implementation Principles

The basic lexicon for the DESMF is taken from ITIL®.

Rationale: ITIL® is the most widely utilized framework in the world as related to ITSM. A single ITSM lexicon is necessary to ensure proper communications related to the DESMF.

Implications: The various branches of the DoD should maintain a cooperative approach to defining, accepting, and socializing this terminology.

Each process should have a single Process Owner, accountable for process quality and integrity.

Rationale: Divided ownership creates a less optimized process and increases the likelihood of overlapping responsibilities and areas of the process being measured.

Implications: The various reporting structures within the agencies should allow for a matrix authority environment related to the process.

Processes and services should be designed with sufficient flexibility to ensure that not only the current needs of the warfighter are addressed, but that future needs in technology and capacity are anticipated and accounted for as part of the service lifecycle.

Rationale: Warfighter requirements change rapidly in a cyber environment and current processes must support agile service development and implementation.

Implications: Principles of agile development and understanding of concepts such as capacity on demand need be applied to all areas of support and development.

With the understanding that particular procedures and work instructions differ between and even within agencies, there should be consistent processes.

Rationale: In order to provide proper governance and measure the overall effect of implementing the DESMF, it is necessary to have consistent processes.

Implications: The various branches of the DoD should maintain a cooperative forum to continually improve the overall framework.

1.7 Utilizing the Framework for Process Improvement

As guidance, the steps below are a high level perspective (not intended to be all inclusive) of how to implement an ITSM or process improvement effort in an organization where this is a new or ongoing initiative. These steps correlate to the DESMF in the recommendation of creating Domains in order to aggregate and integrate tightly coupled processes so to more easily manage and communicate progress. As stated, the DESMF utilizes but also diverges from aspects of ITIL. The Domains are groupings of related processes that represent five stages of the service lifecycle; Service Strategy, Service Design, Service Transition, Service Operations, and Continual Service Improvement. The DESMF provides guidance,

however it is to the organizations discretion as to how to adopt best practices and adapt them to work in their specific environment.

- **Define Outcomes for Implementation**
    - Define Critical Success Factors (CSFs) and Key Performance Indicators (KPIs)
    - Create the process implementation roadmap – this is the overall plan to identify the order of the process implementations and how the implementation should occur.
- **Create Governance Structure and Align with Domains**
    - Define the Area of Responsibility (AOR) for each Domain
    - Define the Governance workflow
    - Develop the Governance Communications Plan
    - Develop the architectures for the Pilot, IOC, and FOC support organizations required and align with current and future-state organizations for ownership
- **Define Organizational Process Ownership**
    - Identify areas best suited for ownership of processes
    - Identify Process Owners
    - Create the implementation roadmap to ensure Process Owners are available to give guidance to other Process Owners at appropriate phases of implementation
- **Create a Training Plan**
    - Develop framework training requirements
    - Identify required training levels
        - Domain Owner
        - Process Owner
        - Process Manager
        - Service Owner
        - Service Manage
        - General Staff
- **Determine Risk Strategy**
    - Define criteria for decisions
    - Identify risk assessment processes
    - Identify risk mitigation activ

2 Organizational Considerations

2.1 Organizational Change Management (OCM)

Implementing new policies, processes, and procedures within any DoD organization affects the entire Department; employees, customers, and stakeholders. To ignore the human side of change increases risks of failure through fear and resistance. Those responsible for IT Service Management (ITSM) must be aware of the potential impact on the people within an organization when implementing changes to policies, procedures, and processes. In essence, those responsible for ITSM are organizational change agents who must build a bridge between people, processes, and technology.

Organizational Change Management (OCM) provides a framework to address the human side of change. There are many frameworks to choose from and the best frameworks are those that are flexible enough to address general, specific, similar, and unique qualities of an organization's culture. Once an organization chooses to adopt ITSM practices, changes to the ethos, values, and guiding principles may be required. Those changes, along with leadership vision and purpose for the ITSM effort, support the people who are impacted. Through *well planned* OCM, people develop trust and learn new behaviors that enable a smooth and efficient transition from the old state of doing business to the desired state of doing business.

As the DESMF provides guidance and advisement on applying the best practices to implement ITSM, these best practices will be more successful and facilitated more effectively, with focused attention in the following areas:

- Obtaining Executive and other Organizational Leadership/Stakeholder's sponsorship.
- Understanding the Organization's current culture.
- Leveraging existing procedures, policies, etc; don't try to fix what isn't broken.
- Communicating the need for the change, the desired results of the change, as well as highlight achievements towards the change.
- Creating a strong Change Champion network with representation from all levels of the organization, customer and other stakeholders.
- Ensuring new changes/requirements are aligned to the organization's strategic vision and objectives.
- Institutionalizing the change – through training and *consistent* implementation of performance criterion (recognition/awards, promotions, or consequences).
- Identifying and executing quick wins to show early measures of success.
- Identifying and documenting overall risks while specifying mitigation plans to address those risks

A new understanding of IT as a weapon system is required to achieve a Joint Information Environment (JIE) and improve a secure net-centric information enterprise. The most important asset of any defense system is the people who are responsible for managing and operating the system. As the DESMF matures, each OCM area mentioned above will be developed as a framework for managing the effects of implementing new ITSM processes within the Department of Defense.

2.2 Organizational Governance

Organizational Governance is the system—people, processes, and technologies--by which Agencies direct and control its equities. It involves regulatory rules and guidance, and defines roles and relationships between the Organizational Directors, high-level decision-making boards, and stakeholders (e.g., suppliers, mission partners, or communities) affected by the Organizations activities. With this system in place, Organizational Governance provides greater accountability for decision-making around the use of IT in the best interest of all stakeholders.

Internal stakeholders are the directors, executives, and other employees of the Organization. Much of the focus in Organizational Governance is concerned with mitigation of conflicts of interests between stakeholders. Ways of mitigating or preventing these conflicts of interests include the processes, policies, laws, and decision-making bodies which have impact on the way the Organizational is controlled. An important theme of Organizational Governance is the nature and extent of accountability and responsibility of different decision-making groups within the organization.

There is renewed interest in corporate governance practices, particularly in relation to accountability, since the high-profile collapses of a number of large corporations during 2001-2002. Their demise is associated with the passing of the Sarbanes-Oxley Act in 2002, intending to restore public confidence in corporate governance. Sarbanes-Oxley has greatly increased regulatory interest and is one of the reasons why the DESMF is needed. DoD Agencies have regulatory requirements, e.g., DoD 5000 Series Regulations, the Business Capability Lifecycle (BCL), and Clinger Cohen Act, that industry and ITIL do not address. The DESMF provides guidance for alignment on how to adapt industry best practices without violating regulatory requirements.

Organizational Governance differs from Information Technology (IT) Governance. IT Governance is a subset discipline of Organizational Governance, through performance and risk management. Organizational Governance systematically involves everyone: board members, executive management, staff and mission partners. It establishes the structure used by the organization to establish transparent accountability of individual decisions, and ensures the traceability of decisions to assigned responsibilities.

2.3 IT Governance

DESMF IT Governance is aligned with the International standard for IT Governance; ISO/IEC 38500, governance frameworks such as COBIT and guidance from renowned sources such as the IT Governance Institute. The realization of a need for Enterprise IT Governance has expanded within industry and government in the past ten years. Industry realized during the 1990s that the organization chart (chain of command) was sufficient to execute business processes. However, it soon realized that IT needed to be controlled to reduce risks and costs associated with developing IT capability and align IT initiatives that drive business strategic objectives. The establishment of an IT Governance structure, subordinate and integrated to the business organization chart addresses those purely IT problems and decisions that directly impact the strategic focus of the business.

DoD has adopted several different IT Governance structures to better direct and control IT initiatives. This was a direct result of the need to control risks, suppliers, costs, and alignment of IT initiatives to strategic and tactical mission objectives in support of the warfighter. IT Governance exists to resolve IT problems by communicating succinct decisions, allocating authority to make decisions, and controlling IT initiatives. Operating in the DoD IT environment poses special problems that can be addressed with a top down, integrated IT Governance model. IT Governance must be established at many levels to address the IT problems at those levels. IT Governance enhances the Situational Awareness and Command & Control of the chain of command by setting up policies and compliance measures that direct and control ITSM. If we correctly view the chain of command as the equivalent of the business organization chart, IT Governance is as vital to the DoD as it is in the private sector.

It is hard to find a high performing organization that doesn't have IT Governance established. Large and small businesses, non-profits, universities, health care, and many DoD and government civilian organizations have established IT Governance. In most cases, organizations that are not high performing can trace one of the major inhibitors to attainment of goals as lack of IT Governance. ITSM processes and services drive business processes and services delivered to the customer and other consumers. IT Governance bodies direct, control, and evaluates the operational IT community, provides conflict resolution, and sets policies to ensure all ITSM processes are effective and services are properly controlled.

2.3.1 Compliance

All IT Governance bodies must ensure compliance with all Federal Government and DoD policies and regulations. There are also directives and decisions from higher level governance bodies that each governance body must ensure compliance to including standardization. Governance bodies must clearly communicate and enforce compliance measures. Non-compliance can be reported to the next level structure as an exception.

2.3.2 Risk Management

It is a core responsibility of IT Governance bodies to address risks to the enterprise related to IT initiatives. Risk always exists whether or not it is detected or recognized. Risks include risk to the mission, operations, compliance, strategic direction, investments, service delivery, information assurance, manpower, and others. In other words, risks include anything that could impact the strategic objectives and operational readiness of

the organization the governance body directs and controls. Risk surveillance, detection, evaluation and response should be imbedded into the IT Governance system. A risk register should be maintained and appropriate personnel assigned by the governance body to manage IT risk issues within the organization.

2.3.3 Service Execution

An important focus of IT Governance should be on the success of service execution. The organization must determine any governance or control problems that introduce risks to service execution and then implement a governance structure to address and govern the problem areas. This could be a combination of a decision authority body and supporting councils. The goal is to not have an overly bureaucratic structure as this can obstruct progress, but instead enable agile decision making in order to provide effective and resilient services. Successful service execution drives mission alignment and customer satisfaction and the governance structure must allocate decision rights and accountability without becoming overly burdensome.

2.3.4 Performance Measurement

In any DoD IT organization, the use of measures is necessary to determine if the effort is on course, or if a course correction is needed. Key to any governance framework is measurement reporting because measurements determine whether IT is meeting the mission objectives through established performance levels and desired results. The actual metrics for performance measurements should be determined by stakeholders and customers of the services, based on their specific requirements. Governance ensures those measurements are transparent, timely and receive the management oversight necessary for successful evaluation of the promised value of ITSM. Performance measures help align the enterprise to a set of common ITSM goals and produce positive results. The measures should be in common understandable language and not tech-speak. Measurement reporting is the only method that allows the enterprise to control IT initiatives and set course corrections when necessary.

2.3.5 Resource Management

One focus of IT Governance is concerned with the effective and efficient management of resources to achieve strategic goals and objectives – another risk management vector. Areas in scope include ensuring manpower availability, utilization and skill sets meet the requirements of the mission. Education and proficiency training of human resources are addressed and progress tracked. In commercial organizations, IT Governance is responsible for IT budgets, for software and equipment, making proposals to higher level governance bodies and tracking and reporting variance. IT budgets are solely the responsibility of the IT Governance system and aligned with the mission, strategy and objectives of the organization. This may or may not be the case in DoD organizations.

3 Common Process Control (CPC)

3.1 Common Process Control Activities

To enhance effectiveness and control of process policies, standards, process activities, performance measures and overall process improvement, every process includes common control activities. These common control

activities provide a standard approach to process monitoring, reporting and evaluating process performance and effectiveness. These common control activities provide the process owner with built-in process governance and continual service improvement for every process. There are three common control activities in each process:

- Establish Process Framework
- Monitor, Manage and Report
- Evaluate Process Performance

The Establish Process Framework activity is always the first activity. The Monitor, Manage and Report activity is always the next-to-last activity. The Evaluate Process Performance activity is always the last activity. These control activities ensure a continual service improvement loop in every DESMF process.

3.2 Establish Process Framework

This activity defines all direction, guidance, policies, and procedures for how to perform the process. All of this is collectively referred to as the "<*process name*> process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for changes and improvements to the process framework. The process framework is a collection of information, not necessarily a single document, which includes:

- Process purpose, scope, goals, capabilities and outcomes
- Process policies, standards, and conceptual models
- Process data requirements
- Role responsibilities
- Organizational responsibilities
- Detailed procedures and best practices, including, but not limited to:
- Interfaces with other processes and programs
- Measurements and controls
- Tool requirements
- The following tasks are performed in this activity:
- Review Process Evaluation Recommendations
- Specify Process Purpose, Scope, Goals, and Capabilities
- Define Process Policies, Standards, and Conceptual Models
- Determine Process Data Requirements
- Identify Process Roles and Responsibilities
- Assign Process Responsibilities to Organizations
- Determine Process Procedures
- Determine Process Relationships to Other Processes
- Define Measurements and Controls
- Determine Technology Needs
- Create Project Proposals
- Communicate and Deploy Framework

3.3 Monitor, Manage and Report

Activities are monitored to determine whether suitable progress is being made. Results are reported which point to any need for management intervention. The Process Manager is continually monitoring the normal work of the process. This is a government retained activity. The following tasks are performed in this activity:

- Review Progress of process
- Identify Items of Interest
- Record and Report Findings
- Perform/Assign Corrective Action(s)

3.4 Evaluate Process Performance

This activity describes tasks required to assess how well the process is executed and recommends improvements to the "<process name> process framework". It includes the capture of information on the relationship with other domains and/or process areas, and the suitability of procedures and training necessary to ensure continued success. This is a government retained activity and provides for a continuous improvement loop ensuring that the process remains fit for purpose and identifies where changes to the process might be required. The following tasks are performed in this activity:

- Collect Feedback from Stakeholders
- Produce Process Metrics
- Review Existing Documentation
- Assess Process Execution
- Audit Process
- Assess Process Framework
- Collect Evaluation Results
- Recommend Improvement Initiatives
- Complete Evaluation
- Communicate to Stakeholders

4 Roles and Responsibilities

Roles are a set of responsibilities, behaviors, activities and authority granted to a person or team. One person or team may have multiple roles. In this section, some potential key roles are defined.

4.1 Executive Sponsor

The Executive Sponsor is accountable for the framework implementation, and responsible for securing spending authority and resources. The Executive Sponsor is a vocal and visible champion who legitimizes goals and objectives, keeps apprised of major activities, is the ultimate decision-maker, and has final approval of all scope changes; signs off on approvals to proceed to each succeeding phase.

4.2 Domain Owner

The primary responsibility of the Domain Owner is to ensure that the processes within the Domain provide support to the Service Owners, who have accountability for the services that are provided. The Domain Owner is accountable for all of the processes in the Domain, the interfaces and process interdependencies and for process maturity levels. The Domain Owner ensures proper resourcing, the appointment of Process Owners, and the strategy for each Domain. The Domain Owners work reciprocally to ensure proper handoffs between the Domains. The Domain Owners represent their Domain on the upper governance boards, while establishing governance boards to handle Domain specific matters related to policy, standards, and overall command and control for the Domain.

4.3 Service Owner

The Service Owner is accountable for one or more services throughout the entire service lifecycle, regardless of where the technology components, processes or professional capabilities reside. This includes the synchronization of resources that support the service including resources that are located out of the Service Owner organizational control. The Service Owner is responsible for continual improvement and the management of change affecting the services under their care and is a primary stakeholder in all of the underlying IT processes which enable or support the service they own. This role has the authority and responsibilities that include ensuring that activities are performed to identify, document and fulfill service requirements. The Service Owner is also responsible for ensuring that the following controls are built into the service during the Service Design phase:

- Mission partner requirements
- Operational requirements related to Event Management, Continuity of Operations (COOP), and training
- Command and control requirements for both normal operations and when on heightened alert
- Situational Awareness requirements for required stakeholders
- Auditing requirements, both financial and for SLA compliance
- Any required information sharing interface points

4.4 Process Owner

The person fulfilling this role is accountable for ensuring that the process is being performed according to the agreed and documented process and is meeting the objectives of the process definition. There is one Process Owner per process. The Process Owner has the following responsibilities:

- Accountable for the process design
- Establish a team to design and define the enterprise process
- Ensure that the process is "Fit for Purpose"
- Document and publicize the process
- Define appropriate standards to be employed throughout the process
- Review integration issues between the various processes
- Ensure appropriate resourcing to implement the process
- Ensure that all relevant staff has the required technical and business understanding, knowledge and training in the process and understand their role in the process
- Define Key Performance Indicators (KPIs) to evaluate the effectiveness and efficiency of the process and design reporting specifications
- Periodically audit the process to ensure compliance to policy and standards
- Review opportunities for process enhancements and for improving the efficiency and effectiveness of the process
- Attend top-level management meetings to assess and represent the process requirements and provide management information

4.5 Process Manager

In matters that pertain to the process, the Process Manager is answerable to the Process Owner and performs the day-to-day operational and managerial tasks demanded by the process activities. The Process Manager does not necessarily fall within the Process Owner's chain of command. In addition, the Process Manager has the following responsibilities:

- Ensure that the process is used correctly
- Manage resources assigned to the process team
- Provide management and other processes with strategic decision making information related to the process
- Monitor the process, using qualitative and quantitative Key Performance Indicators (KPIs) and make recommendations for improvement
- Play a key role in developing requirements for the process tools
- Function as a point of escalation for questions related to the process
- Identify training requirements of support staff and ensure that proper training is provided to meet the requirements

- Provide metrics and reports to management and mission partners in accordance with outlined procedures and agreements

4.6 Service Manager

This role is responsible for managing the end-to-end lifecycle of one or more IT services. The Service Manager provides leadership on the development of the business case and architecture, service deployment and lifecycle management schedules, performs service cost management activities in close partnership with other organizations such as operations, engineering and finance. The Service Manager is also responsible for the controls built into the service.

4.7 Product Owner

This role is responsible for overseeing the end-to-end lifecycle of one or more IT products. The Product Owner ensures the product(s) are fit for purpose and meet requirements of all associated services

4.8 Subject Matter Expert (SME)

Subject Matter Experts provide guidance in the provisioning of services to mission partners by providing the solutions and delivery of process implementation throughout the lifecycle and various maturity levels. The SME further provides direction and support to integrate the process with other service supporting processes.

4.9 Other Roles as Required

An organization may create any role that is necessary to support its ITSM efforts. Other key participants/roles in the process implementation effort are:

- **Senior Leaders/Directors** – Depending on how an organization is structured, there may be senior leaders who are not Domain Owners but have demonstrable interest in the outcome of process implementation and are ultimately responsible for securing spending authority and/or providing resources.
- **Process Design Team or Core Team** – Process definition and development will require a cohesive team of process experts and SME's that come together until the process is implemented or objectives are met and then disband. This team may include roles such as Process Developer, Process Analyst, Process Architect etc.
- **Dedicated members** – Points of contact from the various stakeholder organizations and field offices who participate in the implementation. They act as the contact point for the implementation team from the affected groups and provide status information to the management of their respective organizations.
- **Stakeholders** – Individuals from the Agency who have a stake in the process implementation and mission partners whose support is needed during the implementation.
- **Financial support** – Someone who understands the funding required for resourcing the implementation project, and understands Return on Investment (ROI) and Total Cost of Ownership (TCO) concepts, both in general and in context to the Agency.

- **Education coordination** –As training programs are developed, it will be necessary to have a training expert to assist in ensuring that employees who take the training can be credited for their time and that management has a method for tracking.

4.10 Generic RACI Format

Below is guidance for RACI development which is referenced in 'Define Roles and Responsibilities' in the section 'General Steps for DESMF Service Management Process Design'. The RACI example correlates to a generic process and depicts roles for process activity.

Figure 4.10: Generic RACI Format

Responsible	Roles who execute one or more process activities. There may be multiple "R" roles for a process activity, however there must be at least one.
Accountable	Role ultimately accountable for the work. Individual with final decision authority. There is only one "A" per process activity.
Consulted	Roles that need to be consulted before a final decision can be rendered. Two-way communication is assumed.
Informed	Roles who must be informed when decision is made or action taken. One-way communication is assumed.

Activity Number	Activities	[Process] Management Process Owner	[Process] Management Process Manager	[Process] Management Process Developer	[Process] Management Process Analyst
[XXX1]	Establish [Process] Management Framework	A	R	I	C
[XXX2]	[Process Activity]	I	A	I	R
[XXX3]	[Process Activity]	I	A	I	R
[XXX4]	[Process Activity]	I	A	I	R

[XXX5]	Monitor, Manage and Report [Process] Management	I	A	I	R
[XXX6]	Evaluate [Process] Management Performance	A	R	R	R

Role	Description
[Process] Management Process Owner	The strategic role accountable for the Process. This role: • Is accountable to senior management for the proper design, execution, and improvement of the process • Ensures that the process is being carried out, but does not run the day-to-day operation of the process • Receives regular updates concerning the performance of the process and represents this process concerning all decisions being made by senior management
[Process] Management Process Manager	This is a tactical role and: • Runs the day-to-day operation of the process • Takes overall direction from the [Process] Management Process Owner • Oversees the direction and operation of the process • Provides appropriate reporting to interested parties
[Process] Management Process Developer	This role is responsible for coordinated process development: • Charter • CONOPs • Form Process Development Team • Communication Plan • Develop High-level Design • Develop Detailed Design • Develop Transition Plan for Implementation •
[Process] Management Process Analyst	This role: • Responsible for Process Execution • Complete required training • Support Process development, design and Implementation • Implement process • Provide continuous process improvement support

5 General Steps for DESMF Service Management Process Design

The following steps apply to all processes.

5.1 Define Scope and Objectives

- Determine and document business objectives and boundaries of project
- Gain necessary concurrence or authority to proceed
- Determine the relevance and impact of DoD, Agency and IT Strategic Plans and related policies
- Consider aligning the project schedule to Defense Acquisition Management System (DAMS) and/or Joint Capabilities Integration Development System (JCIDS) model
- Create implementation Road Map

5.2 Validate the Current Environment

- Collect existing process documentation
- Identify existing roles & responsibilities
- Document "As-Is" process environment
- Identify pain points for quick wins (see 5.11 Identify & Implement Quick Wins)
- Identify supporting tools
- Document tool gaps
- Consider using industry tools that show the mapping between ITIL, COBIT and ISO 20000 to help with gap analysis

5.3 Develop High-Level Process Definition

- Identify CSFs and high level KPIs
- Document high level process definitions
- Define high level process inputs and outputs
- Consider aligning process definitions and metrics with ISO 20000. Parts 4 and 5 are useful.

5.4 Define Roles and Responsibilities

- Identify skills and knowledge level
- Create RACI matrix mapping activities to process roles
- Develop cross-functional relationships

5.5 Document Detailed Work Flow for Each High Level Activity

- Document detailed procedures for each high level activity
- Create communications plan

5.6 Build the Process

- Document "To-Be" process environment
- Create workflow
- Incorporate Common Process Control activities
- Define inputs and outputs at a detailed level
- Incorporate control information
- Determine appropriate metrics
- Document tool requirements, including interfaces to other processes

5.7 Develop Appropriate Metrics and Supporting Measures

There is a difference between metrics and measurements. A measurement is an indication of the size, quantity, amount or dimension of a particular attribute of a product, service or process while a metric is a measurement of the degree that any attribute belongs to a system, service, product or process. For example, the number of errors in a system would be a measure, while the number of errors per person hours would be a metric. The fact that a measurement is not used as a metric does not mean resources should be expended to curtail its collection, only that the data should no longer be manipulated and reported upon.

Other guidelines for metrics:

- Review which metrics to collect on a regular schedule. There needs to be a reason and a decision for each metric collected. If there are no longer decisions being made, do not expend resources in collecting and analyzing the metric.
- Metrics should show a change in percentages, not simply a change in number. i.e., percent of incidents categorized incorrectly is more effective then number of incidents categorized incorrectly.

The DESMF integrates monitoring and reporting activities and tasks into each defined process. Guidance for metrics can be found in many of the major frameworks (ITIL ®, COBIT ®, eTOM ®, etc.). For instance:

- ISO 20000-4: Process Reference Model, Section 5.14 (Measurement) provides a very brief process definition that identifies context, purpose, outcomes, and traceability within ISO 20000.

5.8 Define and Document Knowledge Transfer and Training Requirements

- Develop Training Program
- Deliver Process and Tool Training

5.9 Identify & Implement Quick Wins

During a process improvement initiative, one must balance the need for a stronger process foundation with the need to demonstrate more immediate value from the process. The result of this analysis is known as Quick Wins. Quick wins have common characteristics:

- Lower level of effort than other initiatives while still adding value in a relatively short period of time
- Important to the overall process improvement effort
- Eases organizational pain points

An immediate focus on quick wins helps engage key members of the organization to improve the process. Their involvement is recognized by others and establishes momentum for additional improvements that may require more time and commitment. The key is to begin building sponsorship at all levels of the organization by demonstrating real benefits that add real value.

5.10 Finalize Process Guide

- Use appropriate Process Guide template to produce and publish Guide
- Content will have been created throughout the process design
- Post the Process Guide and communicate its existence and location
- Incorporate version control per organizations rules

6 DESMF Domain Structures

The Domain sections that follow are divided along the five areas identified within the ITIL® v3 framework. These are Service Strategy, Service Design, Service Transition, Service Operations, and Continual Service Improvement. Processes are positioned within the Domain sections. This was a logical way to organize this information; however, individual ITSM efforts may locate process efforts in different domains than what is depicted in this document. The interfaces between the processes within each Domain are identified and there is a section which is focused on Functions.

6.1 Service Strategy (SS) Domain

The achievement of DoD's mission is dependent upon the alignment of the Department strategies to the overall strategic vision. This includes the strategy to achieve overall Agency/Organization service capability and strategies for each service offered.

At the center of the service lifecycle is Service Strategy. This is where organizational objectives and mission partner needs are aligned. Service Strategy ensures that the organization is in a position to understand and handle costs and risks associated with the service portfolio, and have the foundation for operational effectiveness and quality performance.

The processes in Service Strategy provide guidance and direction to support mission partners and identify, select, and prioritize service opportunities. A prime goal of Service Strategy is to understand why a service is provided *before* deciding how to provide the service.

Domain Metrics

The metrics for the Service Strategy Domain are actionable measures for decisions related to improving the performance of the process and guiding resource allocation. Metrics must be viewed in an overall context of the DESMF. As an example, a common metric for Financial Management is "Return on Investment (ROI)". This calculation usually stems from a comparison of reduced costs against a monetary investment. For much of the process work, there may be no measurable cost reduction, but rather cost avoidance and a decrease in the amount spent on unplanned work. For this, ROI may not be suitable or actionable. Instead, actionable metrics must be applied to quantify and evaluate that which is critical to DoD and to support the mission.

6.1.1 Strategy Generation Management (SGM)

6.1.1.1 Purpose

The purpose of the Strategy Generation Management process is to set direction for the use of information technology (IT); develop and communicate strategic plans for services that support mission and business enterprise plans and requirements, and ensure those plans support the organization's strategy. This process exists to set goals and decide on areas of change for IT and Service Management capabilities in support of the organization's overall strategic vision. This process defines and maintains an organization's perspective and plans with regards to its services and the management of those services. It establishes the mechanisms to determine which services are best suited to meet mission outcomes and the criteria to effectively manage and measure those services. This process ensures the strategy is defined, maintained, and meets mission objectives.

IT Strategy – The IT Strategy is the overarching IT architecture executed in support of Department or Agency strategy and mission. It includes the strategy around application management, infrastructure management, and technological direction etc; all IT elements needed to support the mission.

IT Service Strategy – The strategy to define and execute 'services' that meet the objectives of the mission partners. It supports and is a subset of the IT Strategy.

IT Service Management (ITSM) Strategy – The plan for implementing and executing the 'processes' used to manage services.

Service Strategy - The strategy that a service provider will follow to define and execute services that meet a customer's business objectives.

6.1.1.2 Scope

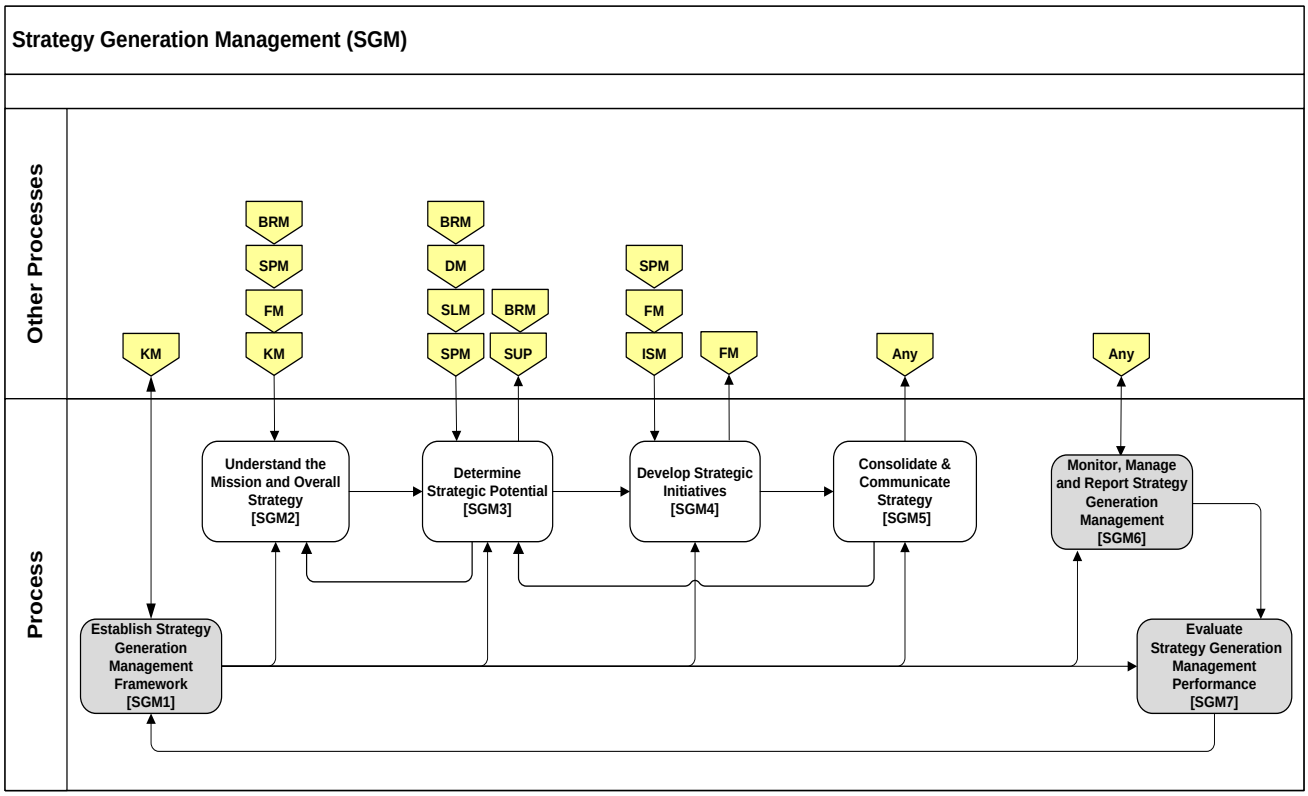
The overall strategy of an organization is determined by its mission, vision, goals, and short and long-term objectives. This includes the strategy of the IT Architecture, portfolio management (other than services), application management, infrastructure management, project management and technological direction. This includes a specification of the 'type' of services to be delivered and the mission partner(s) who will receive the services, as well as the services that meet the objectives of the IT Strategy. The strategy of an individual service is defined and realized in the Service Portfolio Management process and documented in the service portfolio.

6.1.1.3 Process Benefits and Expected Outcomes

- Clear and concrete short term goals are derived from and are traceable back to specific long term plans
- The Strategy is clearly communicated throughout the organization through proactive use of tailored communication plans/packages via available communication methods and channels
- The overarching strategy directly supports the organization's mission and strategic vision

- New or changed service management capabilities required by the strategy are well defined
- Initiatives (including dependencies) required to achieve the strategy are well defined
- A balanced scorecard and related measurement capability to measure strategic progress is established
- A strategy that ensures priorities and resources are aligned in development of appropriate services
- A documented understanding of the constraints, and mitigation of these constraints, with regards to meeting mission partner requirements
- Proactive instead of reactive response for demands placed by various stakeholders

6.1.1.4 Process Workflow Guidance



Strategy Generation Management Activity Level Workflow

6.1.1.5 Activities

[SGM1] Establish Strategy Generation Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for changes and improvements to the Strategy Generation Management process framework.

[SGM2] Understand the Mission and Overall Strategy This activity analyzes the mission strategy and plans, and develops a sound understanding. In this activity, the establishment of financial implications in terms that identify the benefits for IT and service related change occurs. The potential value of IT with organizational objectives is compared and incorporated into a specification of requirements that facilitate the direction in which the organization is driving to support the business or mission. Change priorities are established and identified as agreed to with the understanding and insight of key stakeholders.

[SGM3] Determine Strategic Potential

This activity creates and maintains a model of the organization's IT and service management capabilities to include associating this model with the architecture baseline, service portfolio, and associated cost metrics. A gap analysis is conducted between current capabilities and the strategic wants and needs of the organization. This activity documents new opportunities presented by emerging technologies in the marketplace and identifies the threat of declining technologies. It assesses the impact on IT and service management capabilities of architecture changes, IT research, IT portfolio performance and IT strategy effectiveness. Strategic implications of the organizational strategy is analyzed in terms of strengths, weaknesses, opportunities and threats (SWOT) and a plan for potential changes to the IT capabilities as a result of this analysis is documented. This activity documents IT and service management goals, required capabilities and potential IT value, and shows alignment of IT to overall direction and organizational goals.

[SGM4] Develop Strategic Initiatives

This activity evaluates the current architecture and innovation opportunities to identify new initiatives or improve existing initiatives. This activity obtains required approvals, and secures necessary changes to IT budgets.

[SGM5] Consolidate and Communicate Strategy

This activity creates and maintains a comprehensive network to champion the strategy. Using the content and value of the strategic IT initiatives, this activity creates a communications plan. Events for communicating the strategy and agreement from stakeholders to participate at those events are identified. Other means, such as Web lectures, portals, newsletters, etc. for communicating the strategy and preparing a tailored communications package for each delivery venue are identified. Finally, this activity obtains and summarizes feedback.

[SGM6] Monitor, Manage and Report Strategy Generation Management

In this activity, all Strategy Generation Management activities are monitored to determine whether suitable progress is being made. Results are reported, and unsatisfactory results may lead to review of actions. In addition, responses are provided to requests for information and status of the process.

[SGM7] Evaluate Strategy Generation Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the process. It includes documenting information, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the strategy process remains fit for purpose and identifies where changes to the process might be required.

6.1.2 Business Relationship Management (BRM)

6.1.2.1 Purpose

The purpose of Business Relationship Management is to identify, monitor and manage customer and stakeholder needs and expectations. Corrective actions are taken and implemented based on the Business Relationship data collected to meet and increase results of customer satisfaction goals.

6.1.2.2 Scope

BRM encompasses all business outcomes related to mission partner engagements. This relationship covers the entire lifecycle of the services offered, from the agreement to create a service, to the retirement or decommissioning of a service. BRM and Service Level Management (SLM) are similar in that each has a high degree of mission partner interaction. Many organizations combine the role of Business Relationship Manager and Service Level Manager. The specific difference is that BRM builds the relationships with mission partners and SLM defines mission partner requirements and negotiated service levels.

BRM understands the mission objectives, as well as the environment in which the services operate. This enables the service provider to identify and respond to the needs of the customer and manage mission partner and stakeholder expectations of the service provider. Customer relationships, as a subset of the business relationship, are fostered and aligned to maximize customer satisfaction, value perception and retention.

<u>BRM and CRM</u>
The ability to see both perspectives will help to understand that Business Relationship Management (BRM) and Customer Relationship Management (CRM) are different, yet must work hand-in-hand.
BRM aims to maintain a positive relationship with customers and identifies the needs of existing and potential customers and ensures that appropriate services are developed to meet those needs. There are conflicting views around the definition. Some see CRM as a sub-set of BRM because CRM only deals with customers, who are only one type of stakeholder. Others see BRM as being the IT Service Management equivalent of CRM.

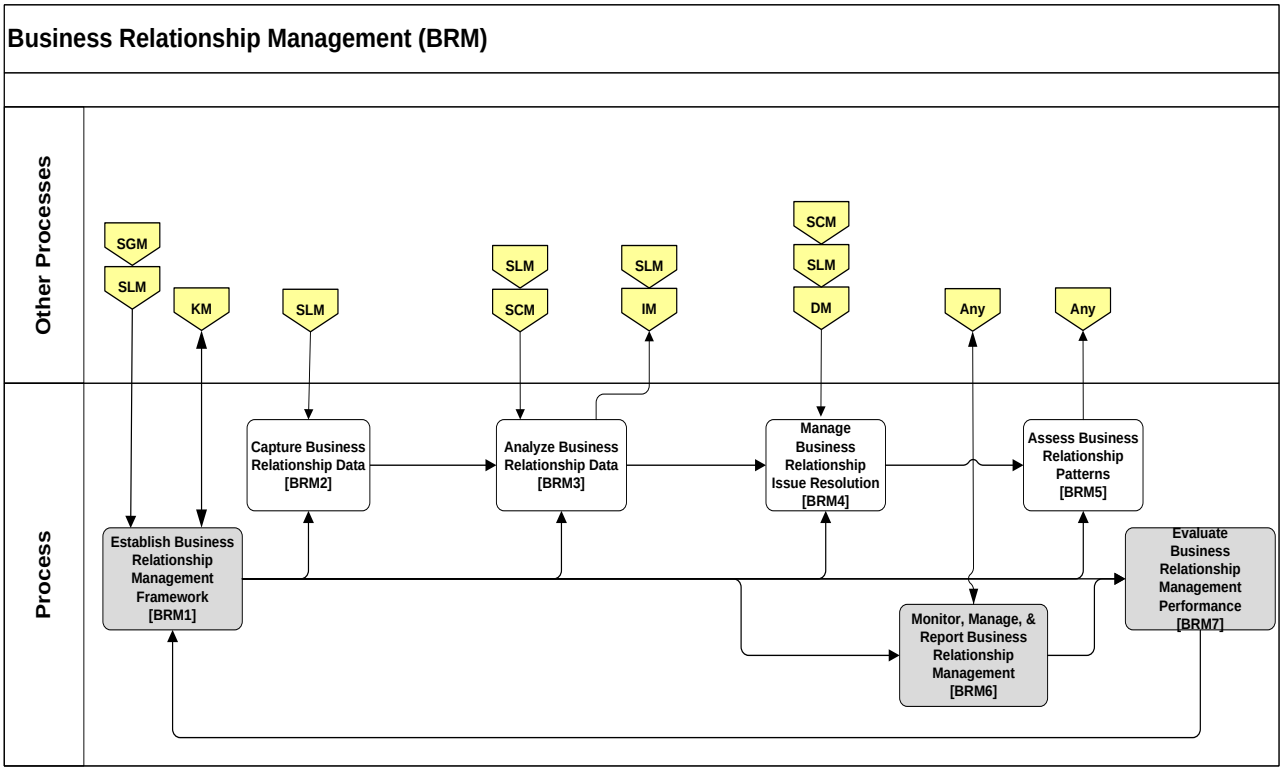
Like most distinctions in ITSM efforts, it's a matter of how these practices are adopted and the choice at how to best adapt best practices to suit specific circumstances and respond to the objectives of customer and business. Many organizations have a CRM process or similar already embedded in customer service, and it's good to be able to make a link between this and BRM.

The Service Desk is already involved in BRM, even if not recognized. Even if only viewed as a service encounter, a good or bad experience with the Service Desk can positively or negatively influence the relationship between the service provider and mission partner.

6.1.2.3 Process Benefits and Expected Outcomes

- A strategy for defining and maintaining business relations between the mission partner and the provider is defined and implemented
- Awareness of mission partners, their needs and major changes are maintained
- Service performance status and reports are monitored for potential business relationship or customer satisfaction impacts and improvements
- Mission partner satisfaction is monitored, measured and reported
- Approved actions to maintain or improve customer satisfaction are implemented
- Contractual disputes are resolved
- Service complaints (and compliments) are recorded, investigated, acted upon, reported, formally closed and when necessary, escalated
- Facilitates ongoing communication with mission partners
- Expedition of the cultural focus on mission partner satisfaction
- Reduced breaches in Service Level Agreements
- Ability to anticipate mission partner needs through the greater understanding of their goals and use of provided capabilities
- Increased trust because of the partnership established between the service provider and mission partner

6.1.2.4 Process Workflow Guidance



6.1.2.5 Activities

[BRM1] Establish Business Relationship Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "BRM process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for changes and improvements to the BRM process framework.

BRM2] Capture Business Relationship Data This activity involves gathering business relationship data. This includes the identification of mission partners and establishing points of contact. Data is also gathered on data points identified such as; Technology metrics (utilization, performance and availability), process metrics (Service Level Agreements (SLA), Key Performance Indicators (KPIs), and activity metrics for the Service Level Management process), customer satisfaction metrics and service execution metrics. This activity gathers only needed information for analysis. In collecting the data both passive and proactive methods are employed.

[BRM3] Analyze Business Relationship Data

Analysis of the data collected identifies:

- Results for the current reporting period regarding Business Relationships
- Business Relationship trending
- Root causes for underlying customer satisfaction issues

[BRM4] Manage Business Relationship Issue Resolution

Analysis results are used to create action plans that address issues and provide status of issue resolutions to stakeholders. The notification and communication plan is incorporated into this activity to apprise management and senior leadership.

[BRM5] Assess Business Relationship Patterns

This activity performs trending analysis of satisfaction data. Its purpose is to identify the underlying cause of trends; negative and positive. Once identified, the issue is communicated and assigned the appropriate resolution plan.

[BRM6] Monitor, Manage and Report Business Relationship Management

This activity supports continuous monitoring and analysis of operational results data and comparison with service achievement reporting to identify Business Relationship Management trends and issues. Business Relationship Management information is used to generate detailed service component reporting as well as provide perspective on overall service availability. All Business Relationship Management activity is monitored to determine whether suitable progress is being made. Unsatisfactory results are reported and may result in actions taken to address any issues.

[BRM7]Evaluate Business Relationship Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Business Relationship Management process. It includes the capture of information on records, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Business Relationship Management process remains fit for purpose and identifies where changes to the process might be required.

6.1.3 Demand Management (DM)

6.1.3.1 Purpose

The purpose of Demand Management is to provide an understanding of the mission partner demand for a particular service and to plan early for provisioning of capacity and other aspects of support for the service. This process may influence mission partner demand for services and seeks to proactively understand the mission partner workload (demand) with the available resources (supply) through analysis, trending and forecasting.

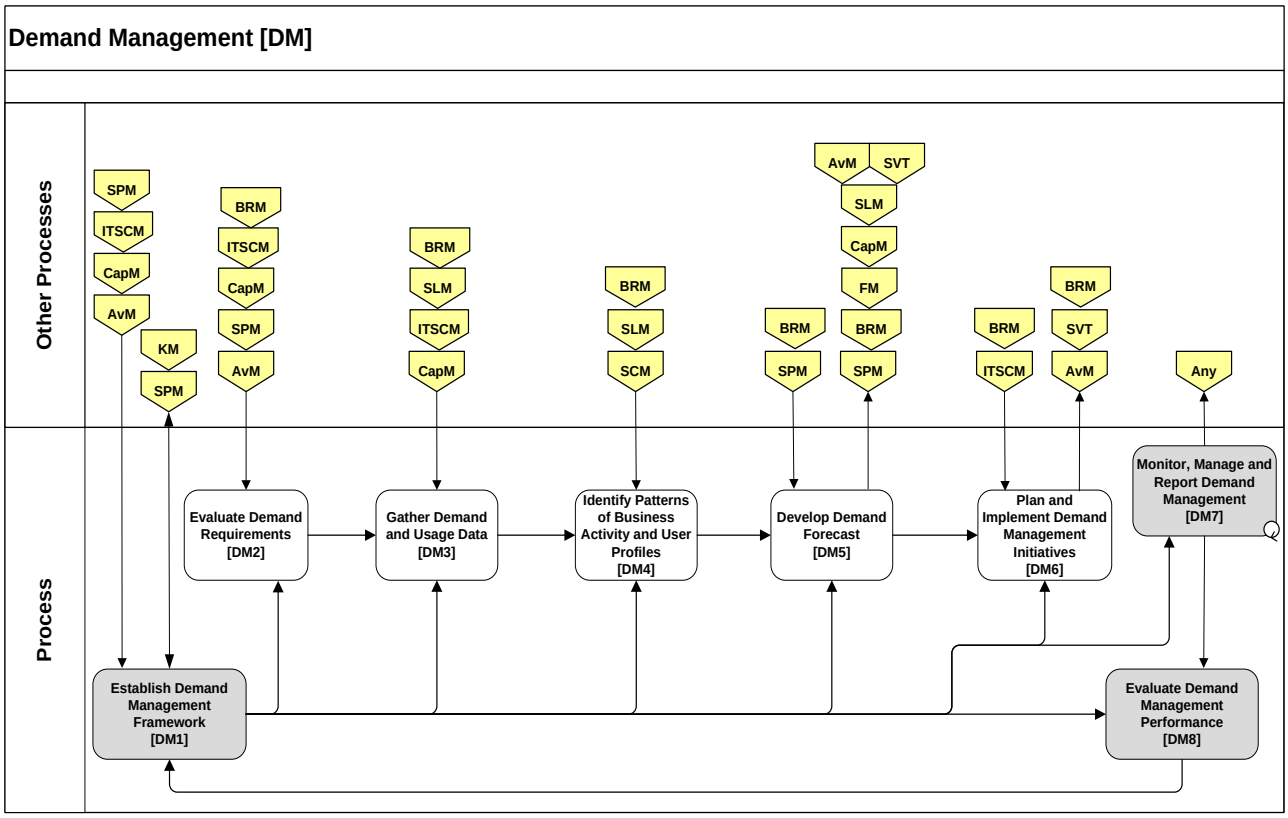
6.1.3.2 Scope

The Demand Management process seeks to understand the expected mission behavior of all demand resources across the enterprise at the individual user level and aggregated level, to represent the overall impact on IT. The Demand Management process translates demand from mission requirements in IT service terms (i.e. consumption units). It identifies gaps and misalignment between demand and supply, and proposes policies and incentives designed to minimize or close gaps. This is beneficial to planning IT capacity and other resources as required.

6.1.3.3 Process Benefits and Expected Outcomes

- Improved IT flexibility in response to dynamic business (mission partner, supplier, environmental etc) changes through a structured approach to evaluating strategic and financial impact of service demand
- Quicker reaction to changing needs
- Improved Capacity Planning efforts through improved forecasting of demand
- Accurate cost information to support IT investment decisions
- Accurate cost information to determine cost of ownership for ongoing services
- Enables planning a more efficient use of IT resources
- Service demand is a key factor in prioritization of resources
- Supports Service Level Management and SLA's and OLA's
- Proactive contingency plans are in place for demand variances

6.1.3.4 Process Workflow Guidance



Demand Management Activity Level Workflow

6.1.3.5 Activities

[DM1] Establish Demand Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "DM process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for changes and improvements to the DM process framework.

[DM2] Evaluate Demand Requirements

This activity determines the conduit for analyzing business demand. This is important because it establishes the data collection requirements from processes that provide raw data via Knowledge Management (e.g. Request Fulfillment and Capacity Management). The execution of this activity is advised to properly establish strategy prior to the collection, analysis, and subsequent decisions that occur in Demand Management.

[DM3] Gather Demand and Usage Data

This activity collects and consolidates demand data from multiple sources for further analysis. A comprehensive analysis of demand is used for demand forecasting and initiative evaluation.

[DM4] Identify Patterns of Business Activity and User Profiles

In this activity, patterns of end-user behaviors are evaluated and used to synchronize consumption (demand) with capacity (supply) of IT Resources. Incoming data and known upcoming initiatives from Service Portfolio Management are helpful to determine requirements for the Demand Management process.

[DM5] Develop Demand Forecast

This activity uses the service demand baseline and collected data along with aggregated historical data to generate a demand forecast. This forecast will provide insight to upcoming demand requirements, including expected high/low demand periods.

[DM6] Plan and Implement Demand Management Initiatives

This activity uses Demand Forecast information to predict misalignment between demand and supply of IT resources and services. It creates strategy to realign resources and services through policy, incentives and/or IT resource investment. When a decision to shape demand through incentives is made, analysis is performed to shape demand through methods such as Incentives/Penalties, Off-Peak Pricing, Volume Discounts, Tiered Service Levels, etc. This activity concludes with the formulation and communication of a prioritized set of recommendations (e.g. Plans of action, investment recommendations, etc.)

[DM7] Monitor, Manage and Report Demand Management

In this activity, all Demand Management activity is monitored to determine whether suitable progress is made. Unsatisfactory results are reported and may result in actions taken to address any issues.

[DM8] Evaluate Demand Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Demand Management process. It includes the capture of information, relationship with other process areas, and suitability of procedures and training. It is used as a basis to ensure the Demand Management process remains fit for purpose and identifies where changes to the process might be required.

6.1.4 Financial Management for IT Services (FM)

6.1.4.1 Purpose

The purpose of the Financial Management process is to control budgeting, accounting and chargeback for service provision. From the IT standpoint, Financial Management secures funding to create and maintain the enterprise architecture necessary to support services that the Department or Agency has strategically determined to provide. Finally, FM should provide transparency into the spending and cost recovery of the all services provided in the IT environment.

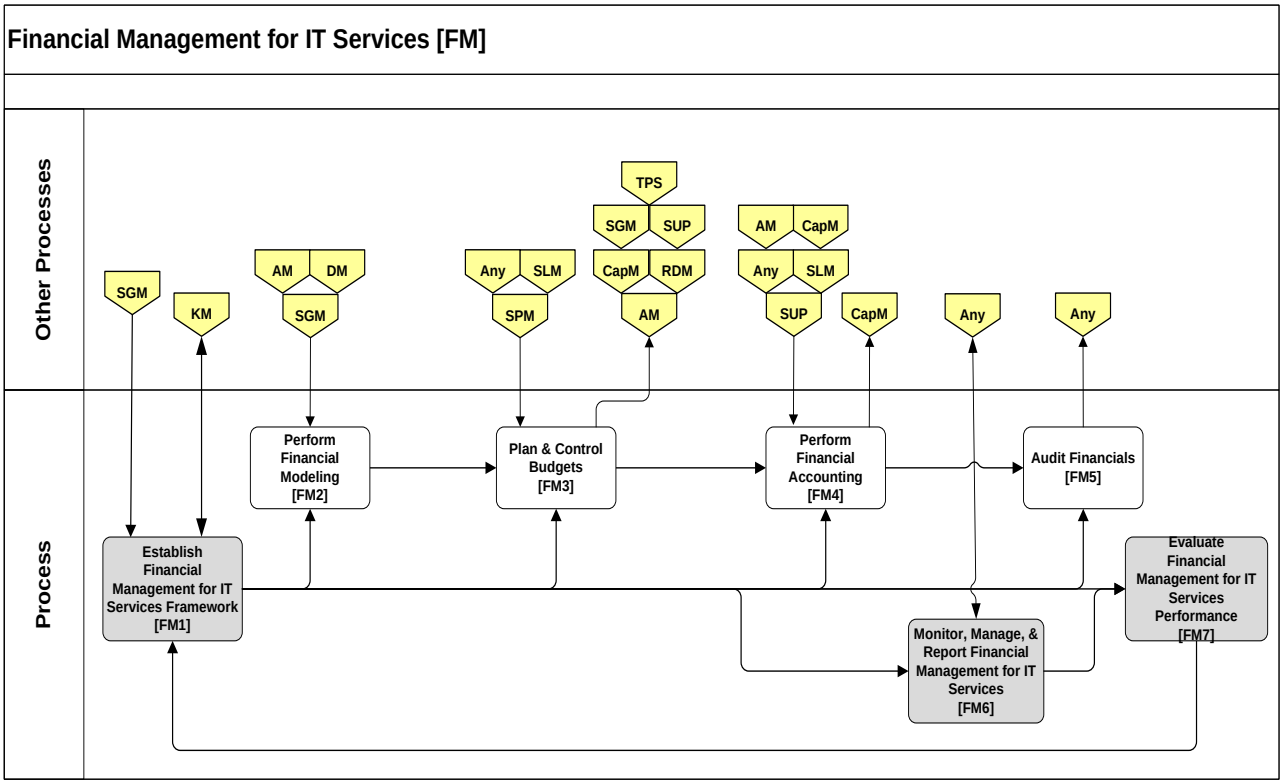
6.1.4.2 Scope

The scope of FM for IT Services covers aspects of three sub-processes associated with overall process; budgeting, accounting, and charging. Budgeting tasks include predicting, controlling expenditures and monitoring budgetary adjustments. Accounting identifies the costs of delivering IT Services, compares those costs with budgeted costs, and manages variance from the budget. All accounting practices must be aligned to the wider accountancy practices of the whole of the service provider's organization. . If applicable, a charging system is developed to recover the cost of IT provision.

6.1.4.3 Process Benefits and Expected Outcomes

- Increased confidence in setting and managing budgets
- Accurate cost information to support IT investment decisions
- Accurate cost information for determining cost of ownership for ongoing services
- More efficient use of IT resources throughout the organization
- IT is understood in concepts of "Return on Value" (ROV) and Return on Investment (ROI) as related to services provided
- Cost and spend are better understood by the IT staff
- Investment decisions are made as part of the overall strategy
- Deviations from the budget and costs are communicated to affected parties
- Controls demonstrating compliance to congressional mandates are recognized and built in during strategy

6.1.4.4 Process Workflow Guidance



Financial Management for IT Services Activity Level Workflow

6.1.4.5 Activities

[FM1] Establish Financial Management for IT Services Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "FM process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity which generates recommendations for changes and improvements to the FM process framework.

[FM2] Perform Financial Modeling

Financial *modeling* determines likely financial outcomes for a wide range of propositions, whether limited to management of IT finances or to proposals relating to the business, infrastructure, service variations or any other consideration requiring cost benefit analysis. Requests will differ in some ways and require innovative modeling approaches. For example: Service valuation, Demand modeling, Service investment analysis and Variable cost dynamics.

[FM3] Plan and Control Budgets

Plan and controlling budgets, ensures that predicted costs are in alignment with the actual budget; if budget is exceeded *early warnings* are given.

[FM4] Perform Financial Accounting

Financial Accounting determines costs incurred to provide IT Services and provides high-level analysis of those costs and the value provided by the expenditure. The goal of financial accounting is to understand *what drives* IT costs and whether IT delivers *good value* for the money invested. As a result, Financial Accounting aids investment and renewal decisions, identifies poor value for money and costs of changes, and performs Return on Investment (ROI) and cost-benefit analysis.

[FM5] Audit Financials

The purpose of the Audit Financials activity is to confirm conformance to financial standards and best practices. Financial data and the inter-workings of the Financial Management Process are examined using defined criteria and guidelines.

[FM6] Monitor, Manage and Report Financial Management for IT Services

In this activity, all process activities are monitored on an ongoing basis to ensure that suitable progress is made. Gaps are reported and may result in corrective modifications to the processes. This process also manages requests for information and status.

[FM7] Evaluate Financial Management for IT Services Performance

The purpose of this activity is to evaluate the performance of the Financial Management for IT Services process and identify improvement areas to the overall process. Continuous Improvement considerations include reviews of foundations and interfaces, all activities within the process, and adaptability of the process and the roles and responsibilities assigned. FM is also evaluated against goals and measures, to quantify its influence on overall IT improvements. Improvements include insights and lessons learned from observation and analysis of activity accomplishments and results.

6.1.5 Service Portfolio Management (SPM)

6.1.5.1 Purpose

The purpose of the Service Portfolio Management Process is to evaluate and prioritize service investments proposals to ensure value to mission. It is involved with the entire lifecycle of the service, from the time service is requested, until it is decided that the service will be discontinued and decommissioned. Service Portfolio Management ensures that the right set of services is offered to meet the mission at the appropriate cost level. It is the decision framework that facilitates the decision making process regarding what services are offered to meet mission partner needs. A Service Portfolio is different than an IT Portfolio. It may be implemented as a part of an IT Portfolio, Project Portfolio or Enterprise Portfolio. The focus of the Service Portfolio Management process is on service offerings.

6.1.5.2 Scope

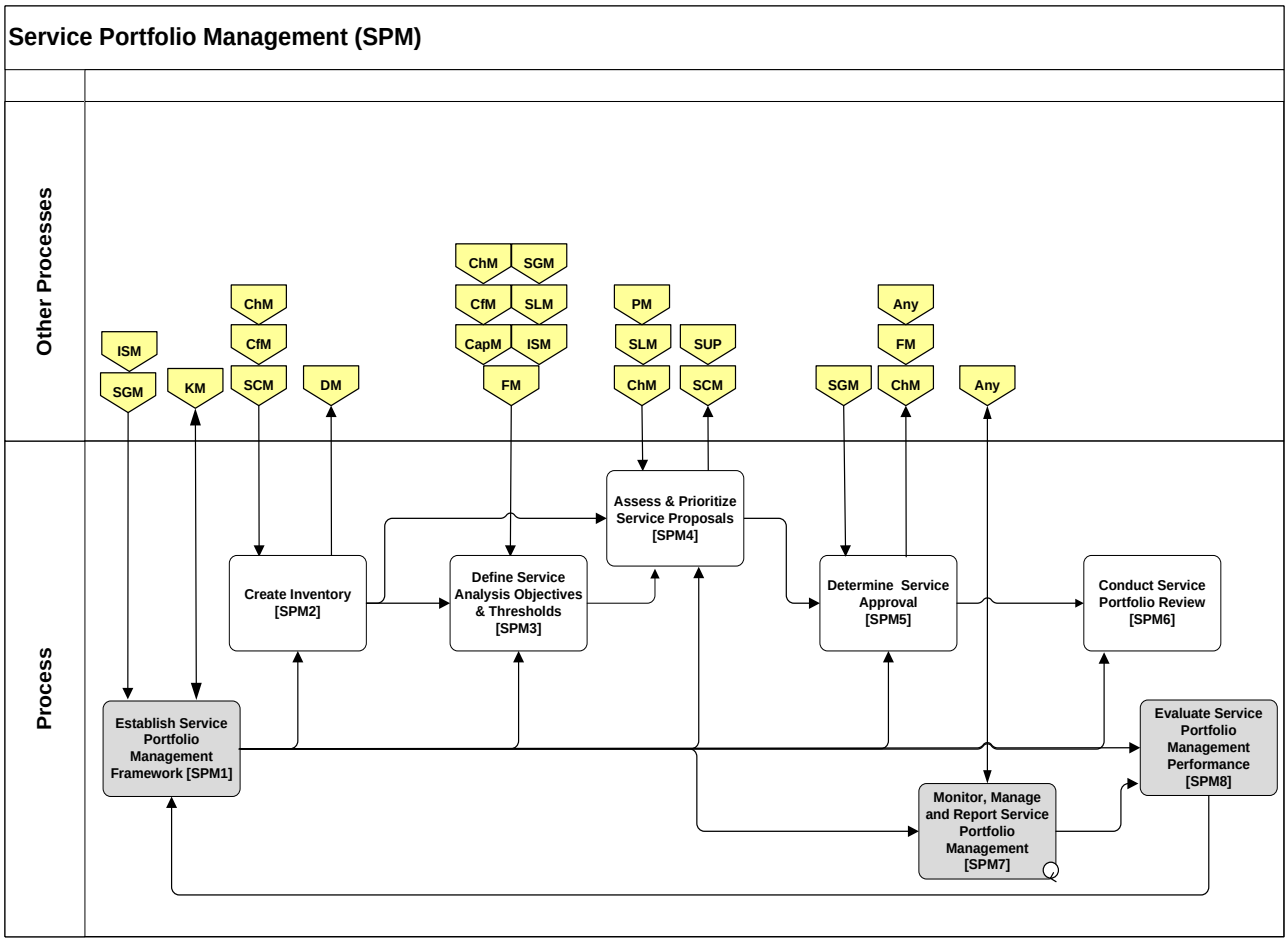
The scope of Service Portfolio Management encompasses all IT related services offered, and may reside in one of three service lifecycle phases:

- **Service Pipeline** – Services under consideration for investment ,or residing in the Service Design Domain or Service Transition Domain
- **Service Catalog** – Services that are currently available and can be browsed by the mission partner base, normally considered operational and candidates for Continual Service Improvement
- **Retired** – Services that are no longer deployed and are unavailable to the mission partner

6.1.5.3 Process Benefits and Expected Outcomes

- Aligned service investment decisions with business (mission) and mission partner needs
- Created/analyzed business cases
- Aligned and prioritized services
- Decisions are communicated and resources are properly allocated
- Investments are prioritized and selected based on stakeholder goals and return on investment
- Focus on managed services increases efficiency in bringing new services to realization
- Allocation of resources for changes and additions to the service portfolio are mission based
- The Service Portfolio reflects mission partner expected outcomes
- Risk assessment for creating services are handled in a consistent, measured process
- Services are continually and consistently evaluated for their value to mission partners

6.1.5.4 Process Workflow Guidance



Service Portfolio Management Activity Level Workflow

6.1.5.5 Activities

[SPM1] Establish Service Portfolio Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "Service Portfolio Management process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for changes and improvements to the SPM process framework.

[SPM2] Create Initial Services Inventory

Collect data about all services. This includes services that are operational as well as services currently in development. This activity should be done only once to create the Service Portfolio and the parameters around how services are made visible to the customers, or retired as no longer offered or supported. If the

service is currently offered, it belongs in the Service Catalog where it is visible to customers and under control of the Service Catalog Management Process. If it is a service that is currently in the design phase, it is a 'pipeline' service and under control of the SPM process to determine when the service can be visible to customers via the Service Catalog. If the service is retiring, SPM ensures appropriate activities and customer visibility to the service is removed from Service Catalog.

[SPM3] Define Service Analysis Objectives and Thresholds

Define service analysis objectives and thresholds to develop a roadmap to identify how services are assessed and moved through different stages of the service lifecycle. These objectives are used to assess candidate services and include references to availability and capacity plans, financial constraints, customer satisfaction objectives, and other artifacts. Thresholds for moving a service from 'pipeline' to the service catalog are also determined.

[SPM4] Assess and Prioritize Service Proposals

Review service proposals and determine which should be accepted for consideration. Develop or update the business case for each service proposed; which may include the identification of the key performance indicators, anticipated user base and frequency, alternative solutions, technical scope, financial metrics (ROI, TCO), benefit cost analysis, intangibles, major assumptions and constraints, opportunity cost analysis, gap analysis, analysis of alternatives, sensitivity analysis, risk assessment, impact analysis and contingencies. Categorize and prioritize each service or change to service proposed.

[SPM5] Determine Service Approval

Review service proposals and make a decision on approval to proceed. Request additional information for clarification as needed. Update the Service Portfolio accordingly.

[SPM6] Conduct Service Portfolio Review

Perform a comprehensive review of the service portfolio and evaluate service balance and alignment. The review determines corrections to the mix of services to better maximize services offered. Monitor and evaluate to ensure service is within agreed cost, schedule, and scope constraints. Evaluate actual results against planned results.

[SPM7] Monitor, Manage and Report Service Portfolio Management

In this activity, all Service Portfolio Management activity is monitored to determine progress. Unsatisfactory results are reported and may result in actions taken to address any issues.

[SPM8] Evaluate Service Portfolio Management Performance

This activity describes tasks required to assess the efficiency and effectiveness of the Service Portfolio Management process. It includes the capture of information on records, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Portfolio Management process remains fit for purpose and identifies where changes to the process might be required.

6.1.6 Service Catalog Management (SCM)

6.1.6.1 Purpose

The purpose of the Service Catalog Management process is to provide an authoritative source of consistent information on all approved services and to ensure that the information is accessible to those who are authorized to view it. Service Catalog Management defines, collates and publishes approved descriptions, under change control, of all services using terms aligned to the customer's view of services and understandable by those without a detailed technical understanding.

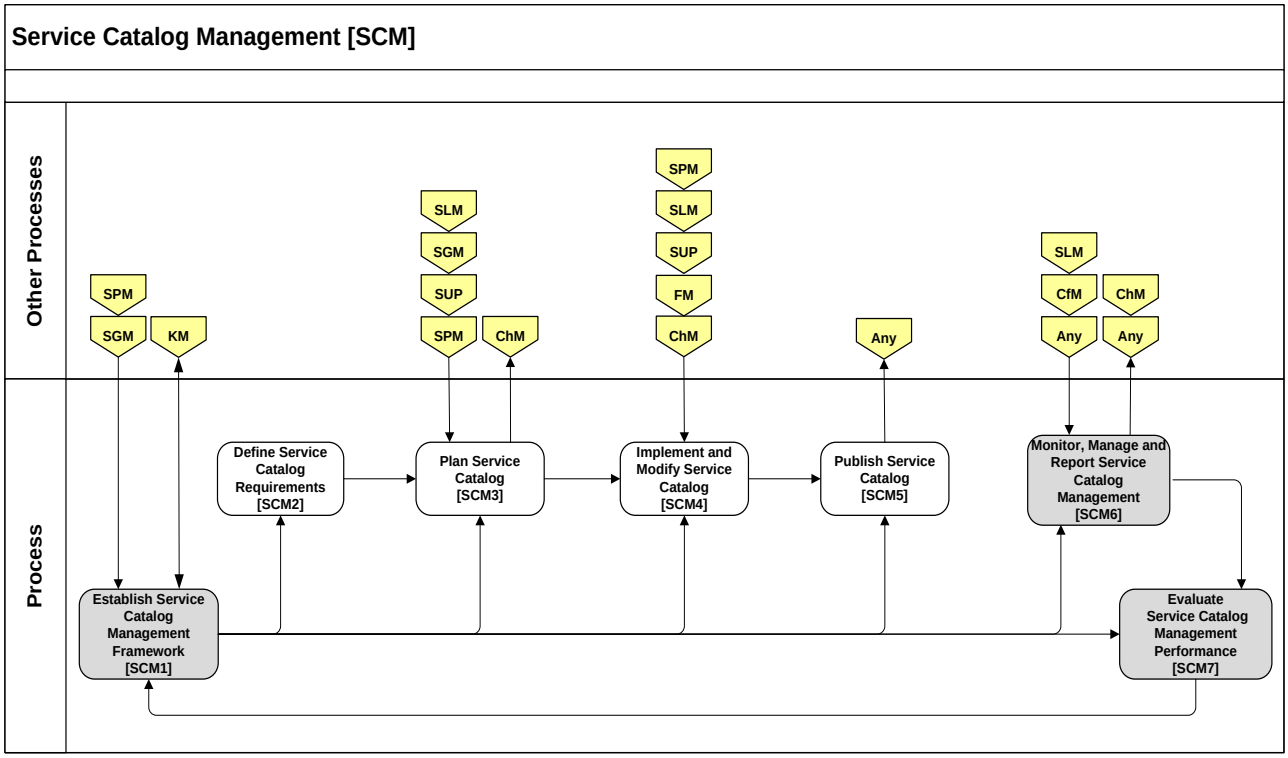
6.1.6.2 Scope

The scope of Service Catalog Management is to provide and maintain accurate information on all active services and all services in transition to production. These services may be represented individually, or as packages. Information about the services includes service definition, service levels, points of contact, ordering and service request information. SCM correlates closely with SPM with regards to service offering timelines, service interfaces and dependencies.

6.1.6.3 Process Benefits and Expected Outcomes

- A single authoritative source of information on services offered
- Provides mission partners an automated interface to the "menu" of services
- A process for maintaining the information for the services provided in a controlled fashion
- Services offered match mission partner requirements
- Demand for services are measured quantitatively, allowing for improved resource alignment
- Better prioritization of resources resulting in lowered costs and quicker delivery of services

6.1.6.4 Process Workflow Guidance



Service Catalog Management Activity Level Workflow

6.1.6.5 Activities

[SCM1] Establish Service Catalog Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "SCM process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for changes and improvements to the SCM process framework. **[SCM2] Define Service Catalog Requirements**

This activity identifies all of the requirements for a service catalog, including overall structure, content requirements, navigation, views for different user groups, etc. Requirements come from a variety of sources, including Service Portfolio Management, Service Level Management, user representatives and stakeholders.

[SCM3] Plan Service Catalog

After requirements are defined for the service catalog, this activity plans and designs the service catalog. This involves designing catalog appearance, structure, navigation, relationships and ensuring the catalog is actionable.

[SCM4] Implement and Modify Service Catalog

The implementation and modification of the service catalog is carried out by this activity. This activity executes all tasks associated with catalog structure, appearance, navigation, and content. All modifications are approved before the catalog is published.

[SCM5] Publish Service Catalog

In this activity, a newly implemented or updated service catalog is published to authorized user groups.

[SCM6] Monitor, Manage and Report Service Catalog Management

This activity supports continuous monitoring and analysis of operational results data and comparison with service achievement reporting to identify Service Catalog Management trends and issues. Service Catalog Management information is used to generate detailed service component reporting as well as a perspective on overall service availability.

[SCM7] Evaluate Service Catalog Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Service Catalog Management process. It includes the capture of information, relationship with other process areas, and suitability of procedures and training. It is used as a basis to ensure the Service Catalog Management process remains fit for purpose and identifies where changes to the process might be required.

6.2 Service Design (SD) Domain

Service Design ensures that services are designed to align and match current and future requirements. Service Design as a Domain controls planning and organizing of resources, infrastructure, communications, and physical and logical components of services to improve service quality and the interaction and understanding between the service provider and its mission partners. This is culminated in a comprehensive Service Design Package (SDP).

The Domain ensures that goals and objectives of Service Strategy are built and managed in line with the vision and mission of the Department. Service Design relies heavily on Service Owners to understand requirements, needs, and service *behavior* of mission partners. Service Design is accountable for changes to existing services, creation of new services, and management of the removal of existing services. Service Design coordinates with Service Operations to ensure the data necessary for monitoring and responding to service variances is built into every service.

Note on Multi-Vendor/Multi-Provider Projects

Part of Service Design should include a definition of the intended structure of the support organizations. In addition to the ISO/IEC 20000-1 as guidance for comprehensive process definition, ISO/IEC 20000-3 is useful for multi-provider endeavors. While it describes certification accountability and ownership for multi-provider environments, the principles contained in the standard are directly transferrable and applicable. When dealing with multiple providers, or when a tiered service organization is in place (Government supported by contractors), it is critical to have the relationships and interfaces between operational entities clearly defined, and a plan in place for managing them. Additional ISO/IEC 20000 information can be found in the Appendix.

Note on Defining Contract Language

With regards to contractually defining a requirement for "process compliance", the Federal Acquisition Regulation (FAR) mandates how the government can and cannot dictate the manner in which contractor-internal processes and procedures are followed. If the requirement is that the contractor shall use the Change Management Process described in DESMF Edition II, there are relatively straight-forward methods of assuring the desired outcome. One method is simply to mandate in the Contract Deliverable Requirements List (CDRL) that reports about the process or service performance follow what is described in the DESMF or ITSM related materials. For example, "The contractor shall use the provided reports for Change Management," or "the contractor shall report the following information for Change Management." As ensuring outcomes is the purpose of Service Management, ensure that your contract language speaks to the process outcome, and uses metrics described in this document.

Domain Metrics

The metrics for this domain are actionable measures for decisions related to improving the performance of the process and guiding resource allocation. Metrics must be viewed in an overall context of the DESMF. As an example, a common metric for Availability Management is "% of time network is available". This metric means nothing unless it is broken down and applied to service availability, and thus provides no

useful information for decision making. More correctly, actionable metrics must be applied to measure that which is critical to design management.

6.2.1 Design Coordination (DC)

6.2.1.1 Purpose

The purpose of Design Coordination is to ensure the consistent and effective design of new, changed or the retirement of IT services. Design Coordination facilitates all service design objectives are met by providing a single point of contact for the efforts in this lifecycle stage.

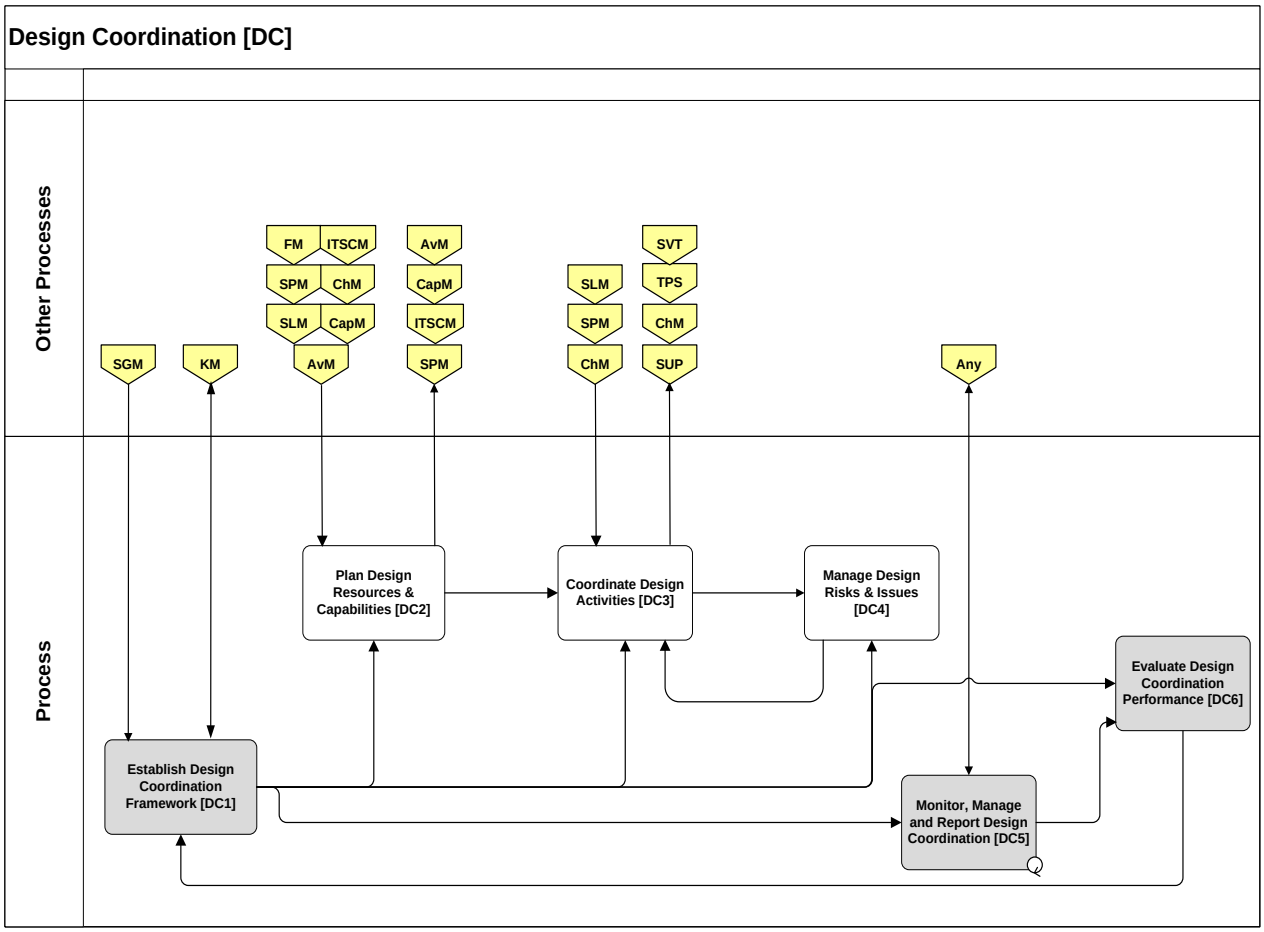
6.2.1.2 Scope

Design Coordination includes all new or changed services that enter the design phase. This is primarily as part of a project, and requires coordination with the Transition Planning and Support counterpart. Design Coordination will work with the Service Owner to ensure all requirements are integrated into the new or updated Service Design Package (SDP) for each IT Service. If appropriate, this will include DOTMLPF-P requirements (reference Appendix). Additionally, Design Coordination will work with the Service Owner to ensure all security requirements (as provided by Service Strategy) are integrated in to the new or updated SDP for each IT Service.

6.2.1.3 Process Benefits and Expected Outcomes

- Reduced costs associated with reworking design issues
- Accountability for the Service Design Package (SDP)
- Ensured architectural consistency
- Consistent design approach and coordination of all design activities
- Ensures all service models and service solution designs conform to security policies
- Reusable design practice
- Overall improvement in the quality of IT service within the imposed design constraints by reduction in rework once they have been transitioned into the live production environment
- Service models and service solution designs adhere to strategic, architectural, governance and DoD and JIE requirements

6.2.1.4 Process Workflow Guidance



Design Coordination Activity Level Workflow

6.2.1.5 Activities

[DC1] Establish Design Coordination Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "Design Coordination process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for changes and improvements to the DC process framework.

[DC2] Plan Design Resources and Capabilities

The purpose of this activity is to coordinate and plan the resources, capabilities, standards, methods, techniques, technologies, and environments related to a specific SDP.

[DC3] Coordinate Design Activities

In this activity, the focus is on the coordination of all design activities across projects/changes and the management of schedules, resources, conflicts, suppliers and support teams as required.

[DC4] Manage Design Risks and Issues

In this activity, formal risk assessment and management techniques are used to manage risks associated with design activities and reduce the number of issues that can be attributed to poor design.

[DC5] Monitor, Manage and Report Design Coordination

This activity supports continuous monitoring and analysis of operational results data and comparison with service achievement reporting to identify Design Coordination trends and issues. Design Coordination information is used to generate detailed service component reporting as well as perspective on overall service availability.

[DC6] Evaluate Design Coordination Performance

This activity describes tasks required to assess the efficiency and effectiveness of Design Coordination. It includes the capture of information on records, relationships with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Design Coordination process remains fit for purpose and identifies where changes to the process might be required.

6.2.2 Availability Management (AvM)

6.2.2.1 Purpose

The purpose of the Availability Management process is to ensure that availability of approved IT resources for business or mission requirements are consistently met or exceeded. Availability Management is concerned with meeting future availability needs of a new or expanding service base and ensures that services remain cost effective.

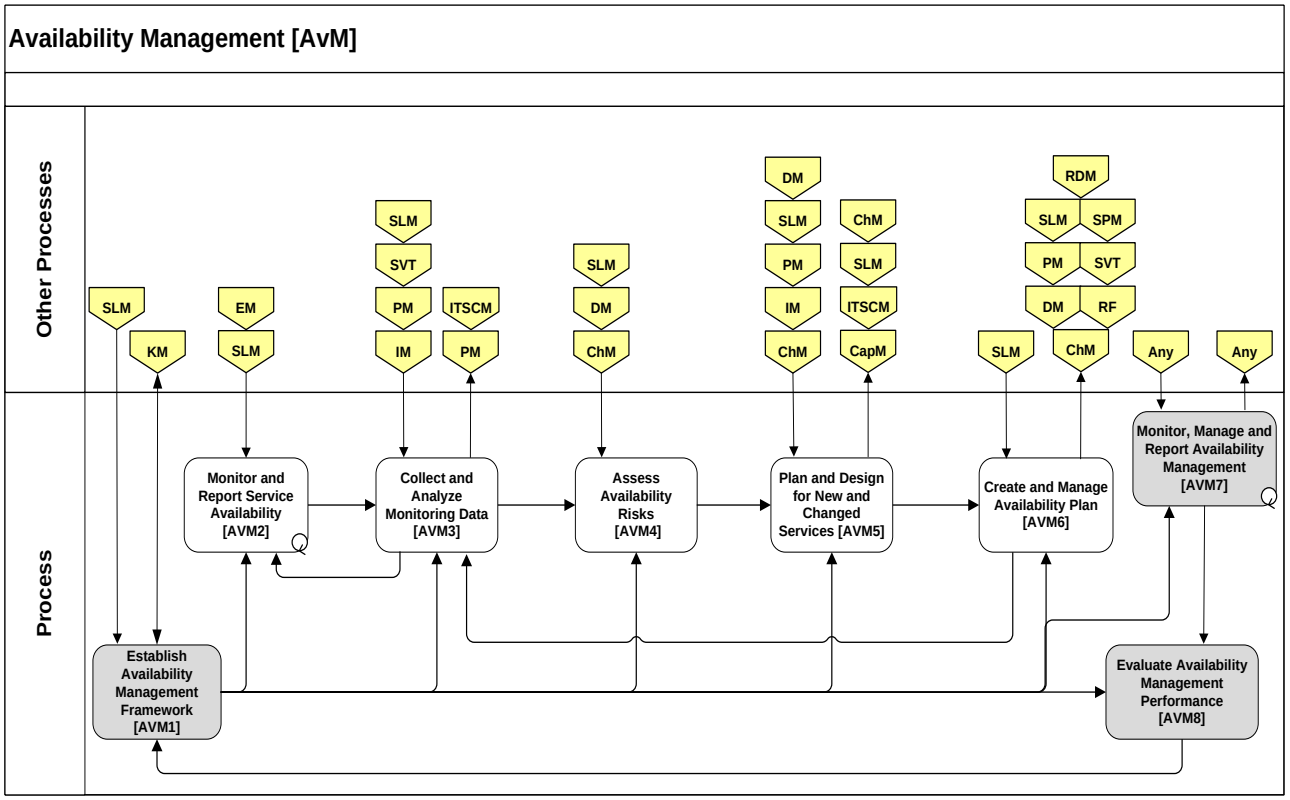
6.2.2.2 Scope

Availability Management is responsible for safeguarding the interests of the stakeholders and interested parties by ensuring that approved service levels are met as defined in Service Level Agreements (SLAs). It includes defining, analyzing, planning, measuring and continually improving all aspects of IT resource availability. This process produces and maintains an up-to-date Availability Plan that reflects current and future needs.

6.2.2.3 Process Benefits and Expected Outcomes

- Ensures an Availability Plan is developed and is in alignment with business goals and agreements
- Resources are better utilized as services are placed on infrastructure that is based on availability requirements
- The Availability Plan helps identify service availability issues prior to outages
- Mission partner satisfaction rises as availability increases and incidents decrease
- SLAs are met, with regard to uptime and availability
- There is a quantitative approach and plan to addressing availability
- Services are designed and engineered to meet availability requirements
- Issues with availability are viewed holistically, not service by service
- Frequency and duration of service interruptions are reduced over time
- SLAs are written with achievable availability goals
- An up-to-date Availability Plan mitigates risk when new services are considered or a service is deploying to an expanded user base
- Underlying causes of unanticipated service non-availability are identified and analyzed
- Corrective actions are taken to address identified underlying causes for non-availability

6.2.2.4 Process Workflow Guidance



Availability Management Activity Level Workflow

6.2.2.5 Activities

[AvM1] Establish Availability Management Framework

This activity defines all direction, guidance, policies, and procedures for how this process will be performed. All of this is collectively referred to as the "Availability Management process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity which generates recommendations for changes and improvements to the Availability Management process framework.

[AvM2] Monitor and Report Service Availability

As appropriate for the infrastructure environment, this activity monitors and reports on service and network availability using defined toolsets. Service availability measures the end-to-end availability of critical and noncritical services provided. Network availability is defined as the percent of time the network is capable of transmitting data as designed among users and to/from gateways to external networks and sites.

[AvM3] Collect and Analyze Monitoring Data

In this activity, service availability monitoring data is obtained and analyzed. The data comes from a variety of sources, including: service level monitoring data, Incident information and trends, Problems and Known Errors and service testing data.

[AvM4] Assess Availability Risks

SLAs, OLAs, and UCs are reviewed for availability terms, conditions and targets, and availability-specific requirements. Availability requirements contribute key data to the Availability Plan. This activity assesses the impact of changes to services, versus monitoring to mitigate risks of non-compliance to or negatively impacting SLAs.

[AvM5] Plan Availability for New and Changed Services

The Availability Manager receives approved (Request for Change) RFCs, workarounds and fixes for availability incidents and problems. When new and changed services are proposed, the Availability Management process will proactively adjust the Service Availability Plan, to allow for new SLAs and monitoring through the SLM process.

[AvM6] Create and Manage Availability Plan

This activity generates the Availability Plan that summarizes resource availability optimization decisions and commitments for the planning period. It includes availability profiles, targets, issues descriptions, and historical analyses of achievements with regard to target summaries, and documents lessons learned. The Availability Plan is a comprehensive record of the approach and success in meeting the organization's expectations for IT resource availability.

[AvM7] Monitor, Manage and Report Availability Management

In this activity, Availability Management activities are monitored to determine whether suitable progress is being made. Results are reported and unsatisfactory results may lead to review of Availability Management actions. In addition, responses are provided to requests for information and status of the Availability Management process.

[AvM8] Evaluate Availability Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Availability Management process. It includes the capture of information on records, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Availability Management process remains fit for purpose and identifies where changes to the process might be required.

6.2.3 Capacity Management (CapM)

6.2.3.1 Purpose

The purpose of the Capacity Management process is to ensure that service capacity meets current and future agreed requirements and performance levels. This information is maintained and updated in a Capacity Plan.

6.2.3.2 Scope

This process ensures there are sufficient resources and capacity to meet current and future negotiated and approved requirements in a cost effective and timely manner. Capacity Management ensures proactive measures to improve service performance are implemented wherever it is cost justified. It maintains a balance between costs and capacity, supply and demand, and ensures that agreed performance levels are met. The scope includes almost all configuration items (CIs) and the following resources are taken into consideration:

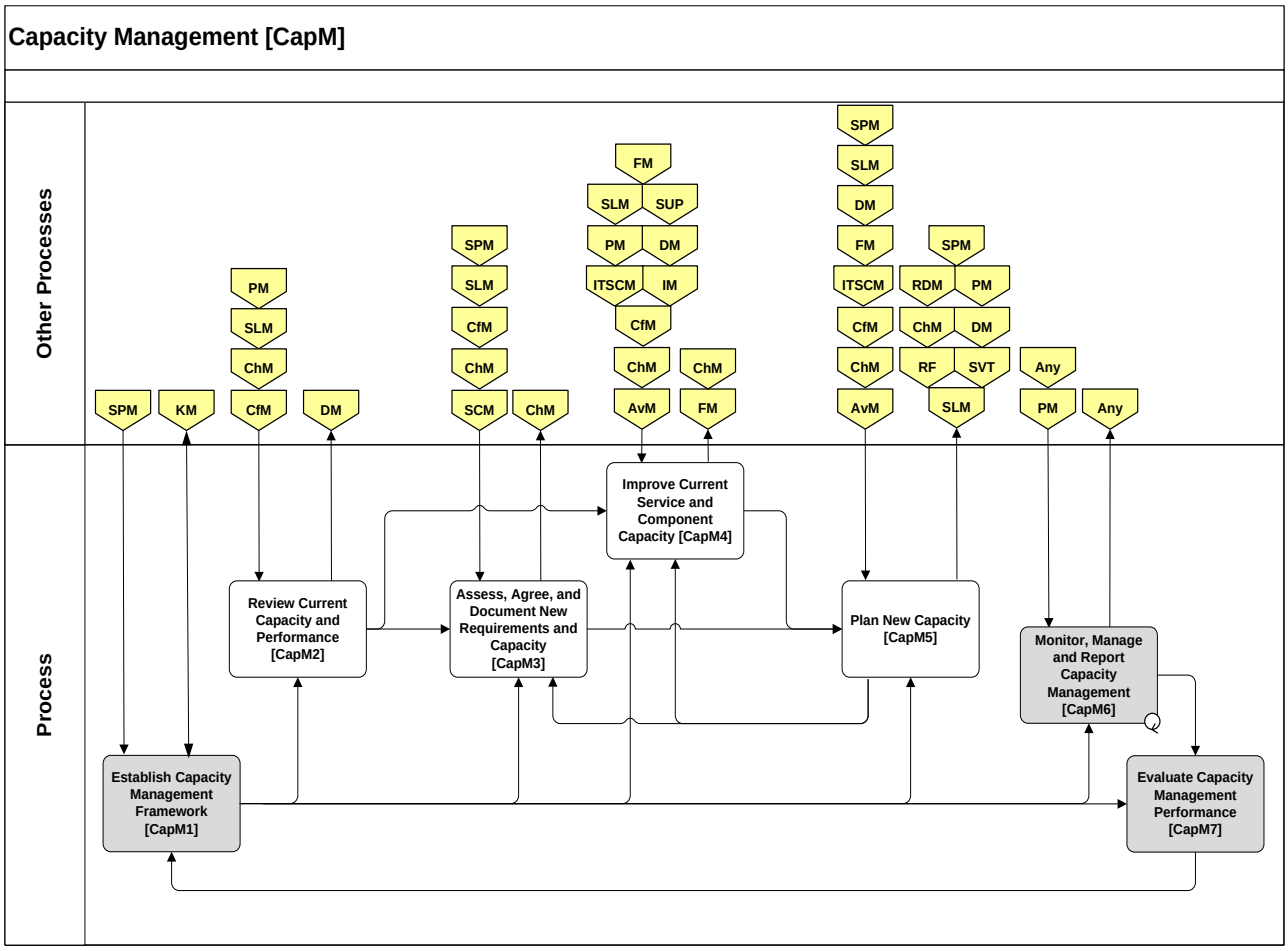
- Computer hardware, network resources
- Software
- People
- Other environment resources like warming/cooling equipment, furniture for staff

(Basically, anything that is a contributing factor to the performance of the services)

6.2.3.3 Process Benefits and Expected Outcomes

- A Capacity Plan is developed based on capacity and performance requirements and adjusted for future capacity and performance needs
- Uninterrupted availability and performance levels during peak periods
- Unnecessary expenses caused by "last minute" purchases or re-allocation of resources are avoided
- Proactive management of capacity reduces performance and capacity related incidents
- Mature Capacity Management is essential to cloud computing
- Business and IT alignment, focusing greater attention and resources in business-critical services
- Infrastructure growth is planned to meet business needs
- Reduction to risks in running the production environment
- Fewer over-capacity issues to address
- Overall infrastructure budget is spent more effectively
- Capacity usage is monitored, analyzed and performance is tuned

6.2.3.4 Process Workflow Guidance



Capacity Management Activity Level Workflow

6.2.3.5 Activities

[CapM1] Establish Capacity Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "Capacity Management process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for making changes and improvements to the Capacity Management process framework.

[CapM2] Review Current Capacity and Performance

This activity invokes a regular review of reports on service and component capacity and performance to ensure that service performance meets or exceeds all agreed performance targets.

[CapM3] Assess, Agree, and Document New Requirements and Capacity

This activity monitors patterns of business and service activity and service level plans through performance, utilization and throughput of IT services and the supporting infrastructure, environmental, data, and application components. This activity involves the use of trending, forecasting, modeling techniques, and thresholds to plan upgrades, enhancements and estimated future requirements.

[CapM4] Improve Current Service and Component Capacity

This activity manages the performance and capacity of services, components, and resources by monitoring, analyzing and tuning to make the most efficient use of existing IT resources. Analysis of the monitored data *may* identify areas of configuration that can be tuned for improved service, system, and component resource utilization or the performance of a particular service.

[CapM5] Plan New Capacity

This activity is a continuous, iterative process that produces a Capacity Plan to document current levels or resource utilization and service performance. It becomes a tool that reflects Capacity Management goals by incorporating the current mission operation and its requirements. The plan should be updated to forecast future requirements for resources that support all services (existing and new) that are based on mission requirements.

[CapM6] Monitor, Manage and Report Capacity Management

This activity supports continuous monitoring and analysis of operational results data and comparison with service achievement reporting to identify Capacity Management trends and issues. Capacity Management information is used to generate detailed service component reporting and provide perspective on overall service availability.

[CapM7] Evaluate Capacity Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Capacity Management process. It includes the capture of information on records, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Capacity Management process remains fit for purpose and identifies where changes to the process might be required.

6.2.4 Information Security Management (ISM)

6.2.4.1 Purpose

The purpose of the Information Security Management (ISM) process is to manage information security at an approved level of security within all service management activities. This includes compliance with the DoD and Services specific information security requirements. ISM ensures that security controls required to perform service management activities effectively protect information assets. This includes preserving the confidentiality, integrity, and accessibility of all data transported.

- **Confidentiality**: data/information must only be accessible to its predefined recipients
- **Integrity**: the data/information must be correct and complete
- **Availability**: data/information must be accessible when needed

6.2.4.2 Scope

The scope of ISM includes all use and misuse of all IT systems that support the DoD mission and services. This is done from four aspects:

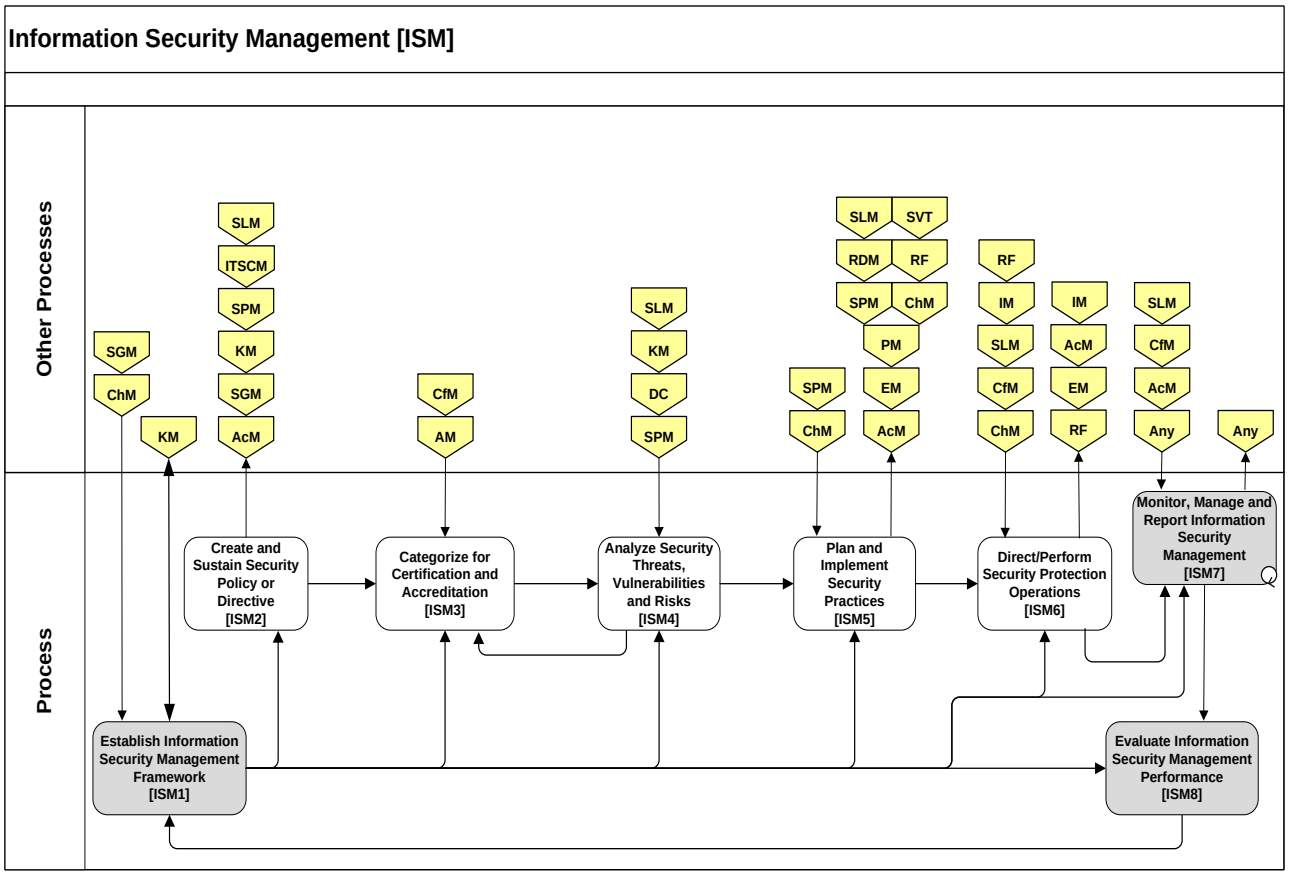
- **Personal** – Defines security policies as related to human resources and staff awareness and responsibilities
- **Procedural** – Procedures to control security that flow from the security policy and process
- **Facilities** – Controls used to protect any physical sites against security incidents
- **Technical** – Controls used to protect the IT infrastructure against security incidents

Some organizations use this process to include only data in electronic or digital form and others use this process to include all information, electronic, paper, phone calls, building access etc. Regardless of scope implemented, this process is congruous to the IT Service Continuity Management process.

6.2.4.3 Process Benefits and Expected Outcomes

- Information security requirements are identified and established
- Security awareness is heightened
- Information security risks are identified and assessed
- Information security incidents are enumerated and recorded
- Assets and processes are more productive
- Data provided is protected, accurate, and available when needed
- Effective access to information by authorized personnel
- Proactive management identifying potential security vulnerabilities before they cause a security-related incident
- All information exchanges can be trusted
- In conjunction with Incident Management, incidents are detected and managed in a controlled fashion

6.2.4.4 Process Workflow Guidance



Information Security Management Activity Level Workflow

6.2.4.5 Activities

[ISM1] Establish Information Security Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "ISM process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for changing and improving the ISM process framework.

[ISM2] Create and Sustain Security Policy or Directive

This activity incorporates the aims and objectives for the security that is to be established. It maintains relevancy as circumstances change for the service provider and its customer set.

[ISM3] Categorize for Certification and Accreditation

This activity assigns or verifies the security classification level of information assets to support Certification and Accreditation (C&A).

[ISM4] Analyze Security Threats, Vulnerabilities and Risks

This activity identifies security threats, vulnerabilities and risks. It includes mitigation recommendations based on analysis and policy guidance from applicable security instructions.

[ISM5] Plan and Implement Security Practices

This activity establishes the Security plan in compliance with applicable security instructions. It defines and creates an appropriate security infrastructure and procedures, translates actions in the plan to security directives, and communicates them to the appropriate audiences.

[ISM6] Direct/Perform Security Protection Operations

This activity executes prescribed information security controls and procedures by operating and activating protections within IT solutions and services. It monitors the full range of information security measures and capabilities, responds to service or authorization requests, and monitors real-time intrusion prevention/detection with established response criteria. Additionally, this activity notes information security violations and initiates incidents when required.

[ISM7] Monitor, Manage and Report Information Security Management

This activity addresses review of security controls and mechanisms and determines whether they effectively implement security policies and procedures as described in applicable security instructions. This activity works hand-and-hand with [ISM 6], as it manages the documented information security violations. Security assessments, inspections and audits occur in this activity.

[ISM8] Evaluate Information Security Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the ISM process. It includes the capture of information on records, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the process remains fit for purpose and identifies where changes to the process might be required.

Special Note on the boundaries of Information Security Management process

Implementation of this process varies widely. Some organizations keep the process solely related to 'information assets' and even go further to more narrowly scope what constitutes the information that this process addresses. Process scopes can include/exclude aspects of Cyber Security as well or define a specific Cyber Security process. Other organizations expand this process to not only address information assurance aspects but also to include a broader scope of security including personnel security, physical security, operations security (OPSEC), industrial security etc.

6.2.4.6 The Information Security Management System (ISMS)

Each of the following requirements should be addressed within the Information Security Management System (ISMS):

- ISMS Established
  - Shall have defined the scope and boundaries of their specific ISMS in terms of the characteristics of the business, location, assets and technology, and a method for address exceptions.
  - The ISMS policy is defined in terms of the characteristics of the business, its organization, location, assets and terminology which includes a framework for setting objectives, takes into account business and legal or regulatory requirements, and contractual security obligations.
- Risk Assessment Approach Defined:
  - The risk assessment approach for the DoD, interagency and provider shall include risk assessment methodology specific to the ISMS, business information security, legal and regulatory requirements, as well as acceptance criteria for accepting risk and acceptable levels of risk. The risk assessment methodology selected shall ensure that risk assessments produce comparable and reproducible results.
- Risk Identification:
  - The assets and asset owners are identified within the scope of the ISMS.
  - The threats, vulnerabilities and the impact that losses of confidentiality, integrity and availability may have on the assets have been defined.
- Analyze and evaluate the risks:
  - The business impacts upon the organization that may result from security failures have been assessed. The business impact takes into account the consequences of a loss of confidentiality, integrity or availability of the assets.
  - The levels of risk have been estimated.
  - There is a determination whether the risks are acceptable or require treatment using the criteria established.
- Identify and evaluate options for the treatment of risks:
  - Actions include:
    - Applying appropriate controls
    - Accepting risks, providing that they clearly satisfy the organization's policies and criteria for accepting risks
    - Avoiding Risks
    - Transferring the associated business risks to other parties, e.g. insurers, suppliers.
- Control objectives and controls for the treatment of risks are selected
  - Control objectives and controls shall be selected and implemented to meet the requirements identified by the risk assessment and risk treatment process.
- Management approval has been obtained for the proposed residual risks.
- Management authorization to implement and operate the ISMS is obtained.
- A Statement of Applicability shall be prepared that includes the following:
  - The control objectives and controls currently implemented
  - The exclusion of any control objectives and controls and the justification for their exclusion.

Additional guidance can be found in ISO/IEC 27001:2005, Information Technology-Security Techniques-Information Security Management Systems Requirements.
** Refer to Appendices for detailed information on NIST 800-53*

6.2.5 IT Service Continuity Management (ITSCM)

6.2.5.1 Purpose

The purpose of the IT Service Continuity Management process is to manage the risks that could affect critical services and ensure there is a plan to recover minimum agreed business continuity-related service levels in support of an overall Continuity of Operations Plan (COOP).

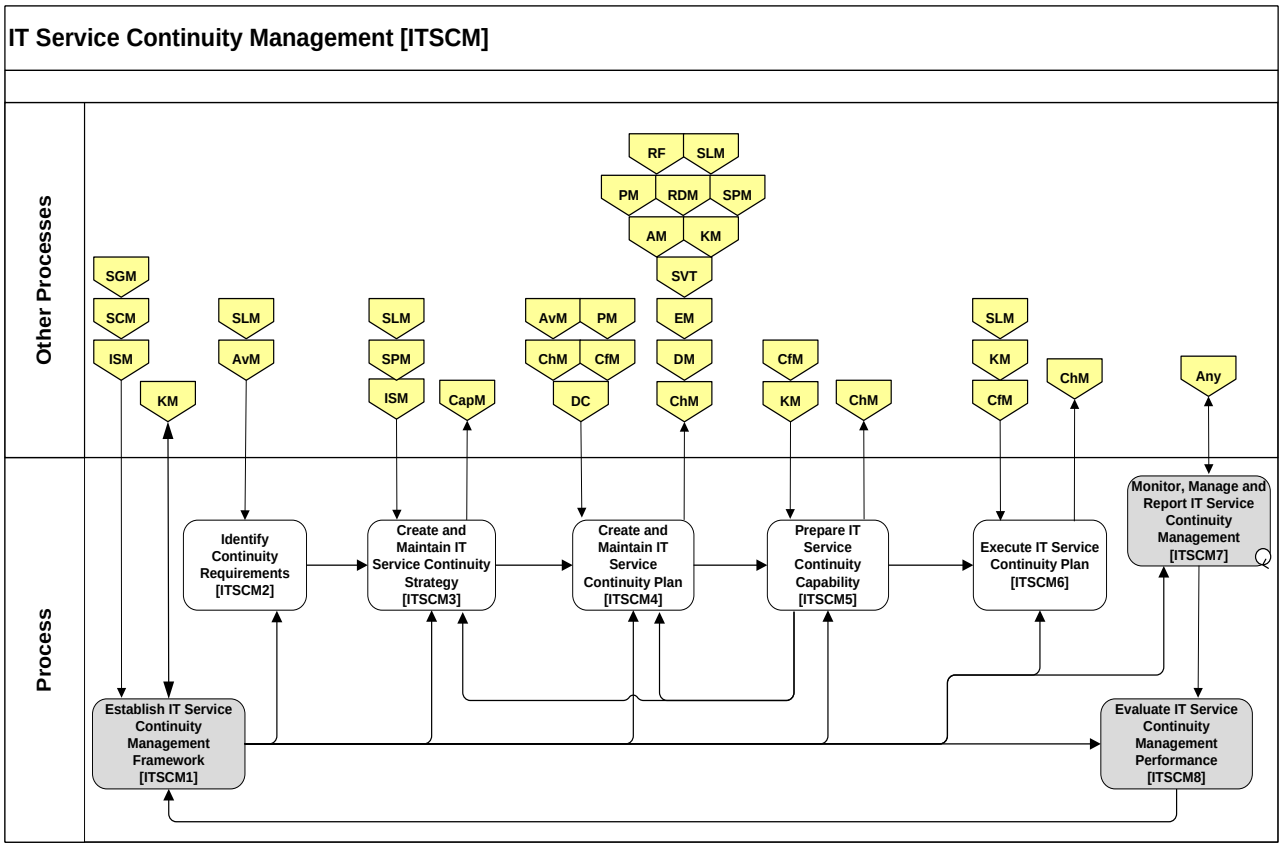
6.2.5.2 Scope

ITSCM is responsible for safeguarding the interests of all stakeholders served. It identifies risks, minimizes the impact of service disruptions and ensures the required technical and service facilities can be recovered within required and agreed timeframes. It includes plans to provide agreed upon levels of service in exceptional circumstances. ITSCM is the technical component of the overall COOP and should include planning for appropriate redundancy to reduce the impact of potential component outages. ITSCM is proactive in supporting the plan to avoid disaster situations and reactive to execute the plan after major events. Periodic testing of the COOP should be conducted.

6.2.5.3 Process Benefits and Expected Outcomes

- Controlled recovery of systems
- Better understand and address weaknesses that may affect the mission before a disaster occurs
- Identification of critical services and functions
- Prioritization of services allow for better utilization of resources during recovery
- Tested plans reduce downtime in the event of a disaster
- Confidence that the mission can be fulfilled under less than ideal conditions
- The ITSCM Plan sets procedures that are regularly tested and updated to prevent, address, and recover from major disruptions and loss of critical services for extended periods
- Reduction to overall risk of failures in the production environment
- Mission partner confidence in ability to provide support in a crisis

6.2.5.4 Process Workflow Guidance



IT Service Continuity Management Activity Level Workflow

6.2.5.5 Activities

[ITSCM1] Establish IT Service Continuity Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "ITSCM framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for making changes and improvements to the ITSCM framework.

[ITSCM2] Identify Continuity Requirements

This activity identifies those requirements that are critical to continuing operations at the level required for mission essential functions. The activity continues with a risk assessment that identifies what might occur in the event of a disruption or degradation.

[ITSCM3] Create and Maintain IT Service Continuity Strategy

This activity is responsible for identifying risk reduction measures for the identified continuity requirements, and establishing what countermeasures and recovery options exist to support these requirements. It takes into account the types of risk that might be encountered and the potential costs involved for each recovery option. The outcome of this activity is an agreed to IT Service Continuity Strategy and a set of IT Service Continuity requirements.

[ITSCM4] Create and Maintain IT Service Continuity Plan

This process is responsible for identifying the resources (e.g. people, processes, technology, facilities, and communications) necessary to support the required services in the event that the COOP is invoked. This activity also identifies the actions necessary for successful invocation of the plan. It is responsible for the ongoing maintenance of the plan and takes into account changes to mission essential functions and changes to the infrastructure.

[ITSCM5] Prepare IT Service Continuity Capability

This process ensures that an invocation of the COOP results in the ability to recover and restore required services to a predetermined level, and in a predetermined timeframe. It has the responsibility for ensuring that all plans are tested regularly, both on a planned and unplanned basis; that the process passes audit requirements, and that the results from tests are captured and fed back to other processes to ensure that the COOP remains fit for purpose.

[ITSCM6] Execute IT Service Continuity Plan

This process is responsible for implementing the COOP according to predetermined criteria. It is responsible for maintaining mission operational requirements for an unspecified amount of time, and for ensuring a controlled restoration to normal service.

[ITSCM7] Monitor, Manage and Report IT Service Continuity Management

In this activity, ITSCM activities are monitored to determine whether suitable progress is being made. Results are reported, and unsatisfactory results may lead to review of ITSCM actions. In addition, responses are provided to requests for information and status of the ITSCM process.

[ITSCM8] Evaluate IT Service Continuity Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of ITSCM. It includes the capture of information on records, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the ITSCM process remains fit for purpose and identifies where changes to the process might be required.

6.2.6 Service Level Management (SLM)

6.2.6.1 Purpose

The purpose of Service Level Management (SLM) is to provide a framework of regular contact between the consumer and the provider of a service to negotiate and document service level targets and responsibilities. Service Level Agreements (SLAs) and Operational Level Agreements (OLAs) are developed to understand specific and measurable targets with regard to the level of service quality.

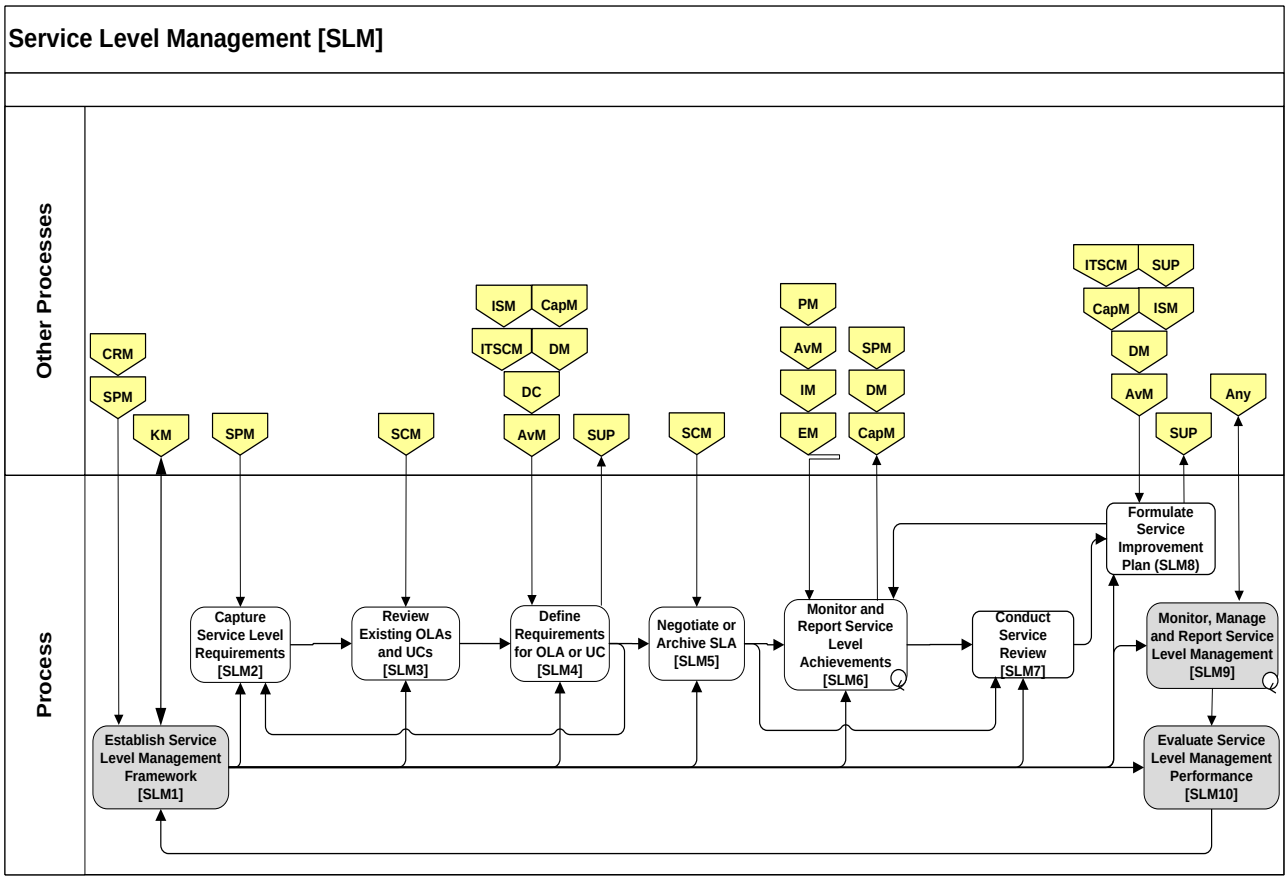
6.2.6.2 Scope

The scope of SLM is a reciprocal relationship and representation of the Agency to the mission partner and the mission partner to the Agency with regards to service quality. A clear and unambiguous expectation to the level of service being delivered is paramount to ensure mission partner satisfaction. The process coordinates the amount and availability of service components for an entire service to enable delivery of the service requirements and agreed service level objectives to the stakeholder. It monitors and reports on the service levels attained.

6.2.6.3 Process Benefits and Expected Outcomes

- The culture will establish a business-value, service-oriented viewpoint
- Financial savings through improved service quality and better resource usage in resolving outages
- Provider and mission partner will better understand each other's responsibilities related to services
- Providers and mission partners develop mutually beneficial relationships and deliver relevant services that improve mission partner satisfaction
- Improved planning based on user agreements
- Improved management through a focus on service delivery and business goals
- Services are continually and consistently monitored and measured quantitatively and qualitatively
- Services and dependencies are identified
- Service level objectives and workload characteristics for services are defined in SLAs

6.2.6.4 Process Workflow Guidance



Service Level Management Activity Level Workflow

6.2.6.5 Activities

[SLM1] Establish Service Level Management Framework

This activity defines all direction, guidance, policies, and procedures for how this process will be performed. All of this is collectively referred to as the "SLM process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate SLM Performance activity, which generates recommendations for changes and improvements to the SLM process framework.

[SLM2] Capture Service Level Requirements

This activity facilitates the discussions with mission partner stakeholders to capture desired service level requirements and service level targets. These requirements are reflected in the various agreements utilized to support the service, such as Service Level Agreements (SLAs), Operation Level Agreements (OLAs) and/or Underpinning Contracts (UCs).

[SLM3] Review Existing OLAs and UCs

This activity reviews the outlines of the required OLAs and UCs required to support a new service to determine if OLAs or UCs already exist that will meet the technical requirements.

[SLM4] Define Requirements for OLA or UC

This activity defines the complete requirements for new OLAs and/or UCs or modifications to existing OLAs and/or UCs. Technical requirements must have clearly defined boundaries and handoffs.

[SLM5] Negotiate or Archive SLA

Formalized requirements are negotiated between the provider and consumer of the service requirements into new or modified SLAs. In addition, SLAs that are no longer needed are archived. New and modified SLAs and UCs are published to the appropriate repositories and associated with corresponding services.

[SLM6] Monitor and Report Service Level Achievements

This activity is the continuous monitoring of service level achievements. The data is collected from various systems and tools. SLA data information (from service providers, monitoring applications, and stakeholder feedback) is run though reporting mechanisms to determine if SLA targets were met or missed.

[SLM7] Conduct Service Review

Using Service Level Achievement Reports, an analysis of the SLAs/OLAs/UCs is conducted to reveal and assess existing and potential gaps between target and actual service delivery or service level achievements. Any penalties are identified during these reviews.

[SLM8] Formulate Service Improvement Plan

A service improvement plan (SIP) is created from results of the service level achievement review, stakeholder feedback, and service delivery units, with regard to improvement suggestions. The SIP focuses on recommendations for SLA compliance improvements and specific target modifications.

[SLM9] Monitor, Manage and Report Service Level Management

This activity supports continuous monitoring and analysis of operational results data and comparison with service achievement reporting to identify Service Level Management trends and issues. Service Level Management information is used to generate detailed service component reporting as well as a perspective on overall service availability.

[SLM10] Evaluate Service Level Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Service Level Management process. It includes the capture of information on records, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Service Level Management process remains fit for purpose and identifies where changes to the process might be required.

6.2.7 Supplier Management (SUP)

6.2.7.1 Purpose

The purpose of the Supplier Management process is to ensure supplier services are integrated into service delivery to meet the approved requirements. It ensures that suppliers are managed to support the mission and service targets. Objectives include:

- Obtain maximum value for the money spent on suppliers
- Ensure contracts are aligned with Agency strategy and support the various aspects of Service Level Management

6.2.7.2 Scope

Suppliers are horizontally or vertically integrated participants in the supply chain of a service. Therefore, the process ensures that the service provider establishes commitments with suppliers who support the integration and alignment of services and agreements between the service provider and stakeholders. It verifies that suppliers are able to demonstrate management of subcontracted partners to meet obligations and contractual requirements. In all situations, the Federal Acquisition Regulation/Department of Defense Federal Acquisition Regulation Supplement (FAR/DFARS) takes precedence. The scope includes:

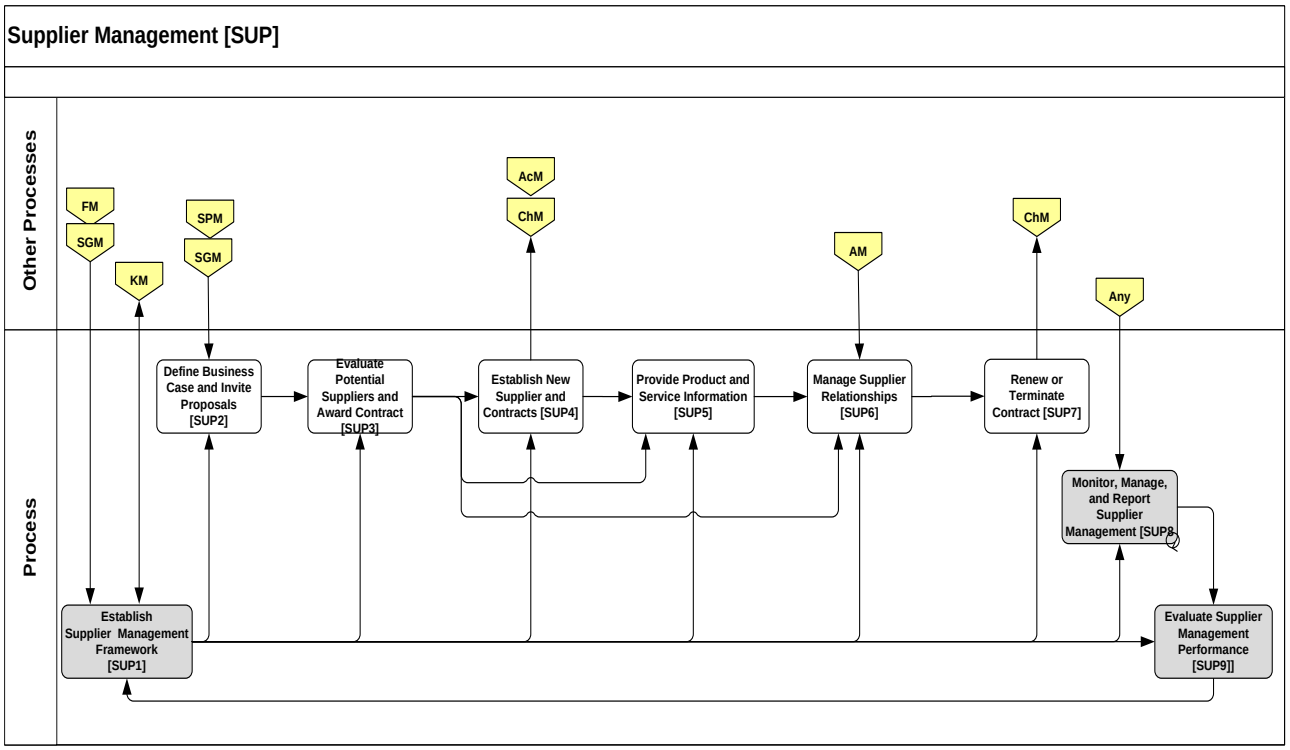
- Implementation and enforcement of a supplier policy
- Maintenance of a Supplier and Contract Database (SCD)
- Supplier and contract categorization and risk assessment
- Supplier and contract evaluation and selection
- Development, negotiation, and agreement of contracts
- Contract review, renewal, and termination
- Management of suppliers, supplier performance and contractual dispute resolution
- Agreement and implementation of service and supplier improvement plans
- Maintenance of standard contracts, terms and conditions

6.2.7.3 Process Benefits and Expected Outcomes

- Ensures that underpinning contracts and agreements with suppliers support and align with mission needs, Service Level Requirements (SLRs), and Service Level Agreements (SLAs)
- Obtain maximum value for supplier services
- Managed relationships with suppliers

- Roles and relationships between suppliers is determined
- Supplier obligations to meet service requirements are monitored
- Measured supplier performance
- Creation and management of supplier and contract information
- The capability of subcontracted suppliers to meet obligations is confirmed

6.2.7.4 Process Workflow Guidance



Supplier Management Activity Level Workflow

6.2.7.5 Activities

[SUP1] Establish Supplier Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "SUP process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for making changes and improvements to the SUP process framework.

[SUP2] Define Business Case and Invite Proposals

Define initial business case; includes costs, timelines, targets, value, and risks. Invite suppliers to provide proposals and/or bids for meeting defined business needs. Ensure draft proposals conform to strategy/policy.

[SUP3] Evaluate Potential Suppliers and Award Contract

Evaluate potential suppliers, identify alternatives, and select suppliers. Negotiate terms and conditions, responsibilities, resolution of disputes, renewals and extensions, and other contract content. Award selected supplier.

[SUP4] Establish New Supplier and Contract

Integrate new suppliers by providing supplier-appropriate access to necessary systems and data. Initiate supplier contracts and relationships.

[SUP5] Provide Supplier and Service Information

This activity provides information about supply items, such as a supply item catalog (hardware, software, services, and external resources that contains information about supply items,) potential suppliers for those items (including supplier priorities and options) and supply item availability.

[SUP6] Manage Supplier Delivery

This activity manages supplier delivery and evaluates supplier performance. During which, the review of supplier delivery against business, technical and financial criteria is performed. Relationships during delivery periods, including communication, risks, changes, failures, improvements, contracts, and interfaces are maintained. During this activity, supplier performance is periodically reviewed and assessed against business needs, targets, and agreements. The recommendation of possible delivery closure, renewal, or extension is given, as applicable.

[SUP7] Renew or Terminate Contract

In this activity, negotiations of the renewal, termination, or transfer of contracts with supplier is conducted. If contract is terminated or transferred, this activity manages the completion of the supplier relationship.

[SUP8] Monitor, Manage and Report Supplier Management

In this activity, all process activities are monitored to determine whether suitable progress is being made. Unsatisfactory results are reported and may result in intervention into process work. In addition, responses to requests for information and status about the process are provided.

[SUP9] Evaluate Supplier Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Supplier Management process. It includes the capture of information on records, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Supplier Management process remains fit for purpose and identifies where changes to the process might be required.

6.3 Service Transition (ST) Domain

The Service Transition Domain is responsible for assisting in the navigation of the design of services as they move from concept to production, the implementation of services, and making modifications to services as a result of required corrective actions or to improve an existing service. As such, it is the responsibility in this Domain to ensure the strategic vision of DoD is carried out and includes ensuring the creation of services in Service Design is carried out during the implementation phases.

The Information Security Management (ISM) framework identified through the Service Design domain, and the ISM policies, controls, and procedures are carried out in the Service Transition domain. The Domain Owner serves as guardian of the production environment, ensuring policies and processes designed and executed in the Domain mitigate the risks of changes to the production environment through analysis and testing, proper scheduling of modifications, recording of all aspects of the assets that support the services, and ensuring knowledge of services provided is properly available Department wide.

Domain Metrics

The metrics for this domain are actionable measures for decisions related to improving performance of the process and guiding resource allocation. Metrics must be viewed in an overall context of the DESMF. As an example, a common metric for change management is "# of incidents caused by changes". This number often goes up if testing is done poorly, if release documentation is not well publicized or if there are failures in the design package. More correctly, actionable metrics must be applied to measure that which is critical to Service Transition.

6.3.1 Transition Planning and Support (TPS)

6.3.1.1 Purpose

The purpose of Transition Planning and Support is to plan and coordinate the resources to take a new or changed service, or a service to be decommissioned (decided in Service Portfolio Management process) through Release and Deployment into the production environment, ensuring that the effort is accomplished within predicted cost, quality, time estimates, and acceptable levels of risk and with meeting all requirements in the Service Design Package.

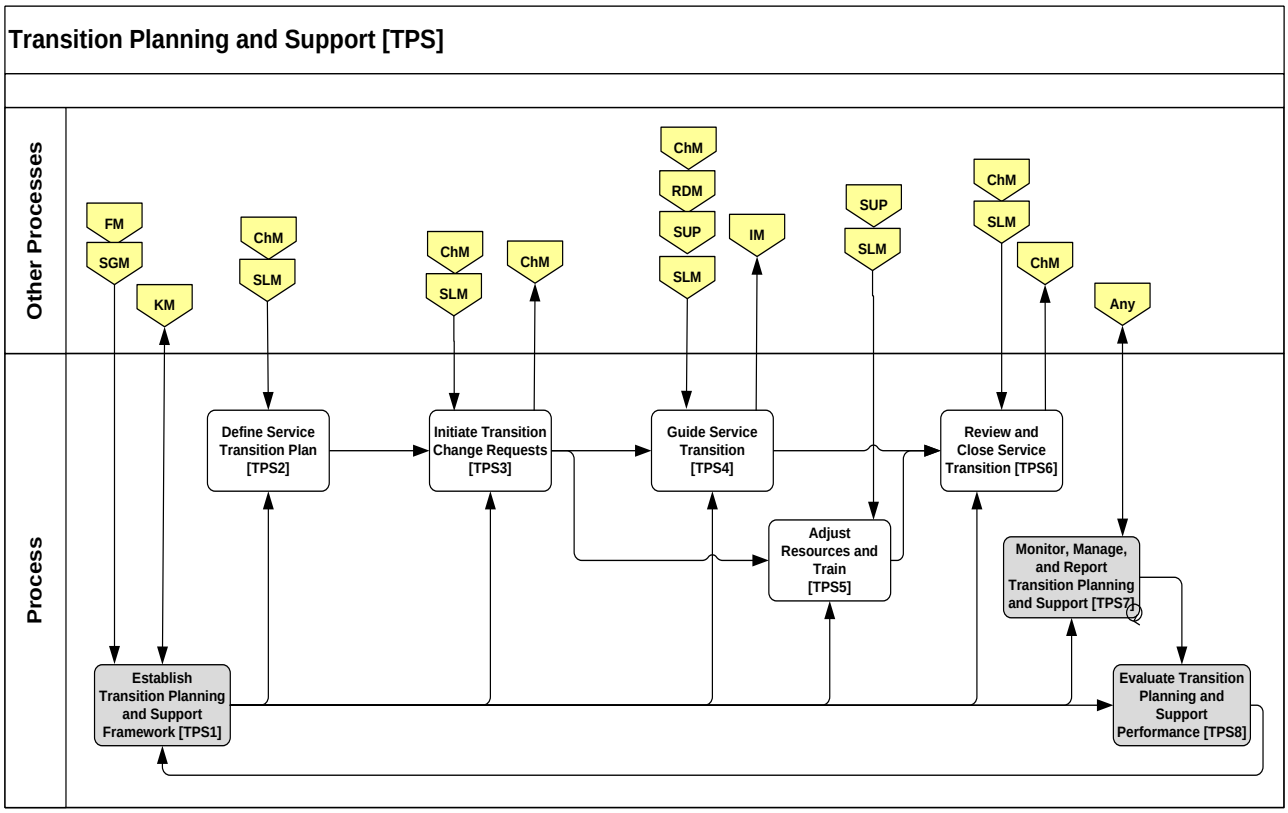
6.3.1.2 Scope

TPS ensures the service components are effectively integrated into a new or changed service and the service provider and mission partner are prepared to operate the solution to deliver the desired outcomes.

6.3.1.3 Process Benefits and Expected Outcomes

- Ensures integrity of all mission partner and service assets
- New or changed methods, procedures and measures for the new and changed service(s) are identified
- New or changed knowledge, skills and abilities are identified, approved, acquired and assigned
- Coordinated activities across projects, suppliers and service teams
- New or changed plans for Availability, IT Service Continuity, Capacity and Information Security are identified, communicated and employed (these are also identified with Service Design Coordination)
- Single point of communication related to service activities in scope
- Reduction in variation from requirements to production
- Ability to deliver more volumes of change at higher success rates
- Reduced variation in release schedule adherence due to standardized, holistic planning
- Improved integration of services with the mission partner's needs
- Consolidated deployment process
- Better planning and resource allocation
- Information regarding the outcome of the transitioned service is communicated to interested parties
- Improved risk management, and thus reduced adverse impact due to increased predictability of quality of service
- Better integration of supporting processes

6.3.1.4 Process Workflow Guidance



Transition Planning and Support Activity Level Workflow

6.3.1.5 Activities

[TPS1] Establish Transition Planning and Support Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "TPS process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for changes and improvements to the TPS process framework.

[TPS2] Define Service Transition Plan

As a blueprint for how the transition is carried out, the transition plan describes the activities needed to carry out the transition, as well as resource modifications, schedules, organizational changes, training, risks, communications, and other important considerations. The transition plan is used throughout the new or changed service transition.

[TPS3] Initiate Transition Change Requests

In this activity, all Requests for Change (RFC) needed for the service transition are created and submitted to the Change Management process. The RFCs are created with the appropriate sequencing and timing to properly choreograph the transition.

[TPS4] Guide Service Transition

As the transition-related Request for Change is executed, this activity provides support for deployments and other implementations related to the service transition. This includes ensuring that acquisitions related to the transition are completed on-time, release deployments are sequenced and coordinated properly, communications related to the transition are performed, pilots (if required) are carried out, post-installation testing occur, and other transition-related tasks are performed.

[TPS5] Adjust Resources and Train

Resources are added or removed as needed for the transition of the service. These resources include operations and support personnel. Early life support may be considered in resource adjustment. Users and other service-related personnel are provided job-appropriate training.

[TPS6] Review and Close Service Transition

The results of the service transition are reviewed to determine if the transition was carried out as intended. Deviations and deficiencies in the transition are addressed, possibly resulting in additional RFCs. When transition issues have been adequately addressed, the service transition is closed.

[TPS7] Monitor, Manage and Report Transition Planning and Support

This activity supports continuous monitoring and analysis of operational results data and comparison with service achievement reporting to identify Transition Planning and Support trends and issues. Transition Planning and Support information is used to generate detailed service component reporting as well as a perspective on overall service availability.

[TPS8] Evaluate Transition Planning and Support Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Transition Planning and Support process. It includes the capture of information, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Transition Planning and Support process remains fit for purpose and identifies where changes to the process might be required.

6.3.2 Asset Management (AM)

6.3.2.1 Purpose

The purpose of Asset Management is to manage the finances, contracts and usage of IT assets throughout their lifecycles to balance service requirements, total costs, budgeting, and compliance. The lifecycle ranges from procurement through deployment to use (and upgrades) to decommissioning (or reuse) to disposal. The difference between Configuration Management and Asset Management is that Configuration Management is concerned with the relationships between configuration items in support of the services, where as Asset Management manages the attributes of the asset such as costs, compliance etc.

Asset Management may also manage the assets of organizations not directly related to IT support of a service. In some instances the Asset and Configuration Management processes are one process, not two separate processes. And in some cases the Asset Management database becomes part of the Configuration Management System. The need of the organization drives the decision with regards to having one or two processes. The relationship of assets to services is covered under Configuration Management.

6.3.2.2 Scope

The scope is unique to the organization based on the established purpose of the process and needs of the organization. It can be confined to assets which directly affect services provided or can be as broad as to include physical assets as well. Thus, Asset Management is responsible for or could be responsible for managing:

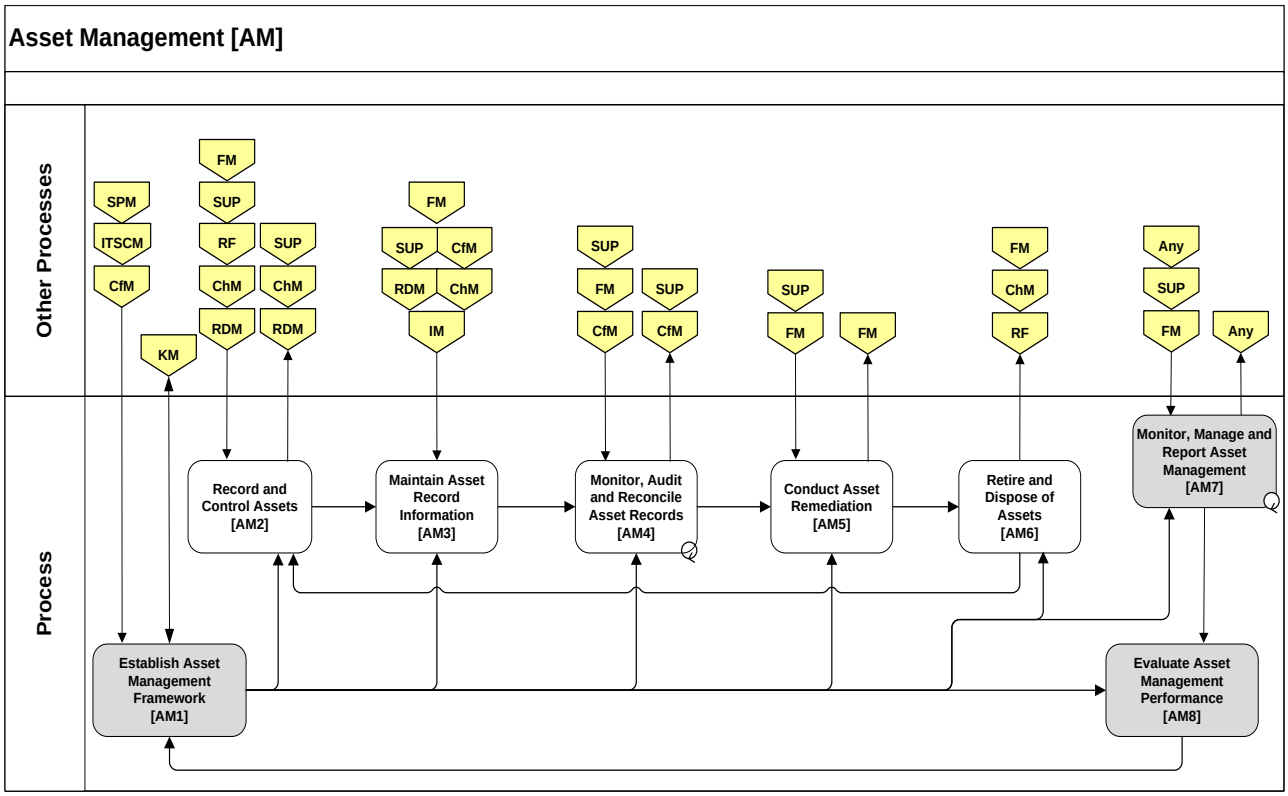
- Hardware (including maintenance)
- Software (including maintenance)
- Facilities (and related, such as desks, etc.)

6.3.2.3 Process Benefits and Expected Outcomes

- Creates improved procurement processes through centralization of all asset data and asset related financial information
- Simplifies inventory and auditing processes through centralization of asset data and asset related financial information
- More accurate risk assessments due to better asset tracking
- Improved understanding of the real cost of assets
- Increased insight into the Total Cost of Ownership of IT services through complete and detailed asset information
- Ensured compliance with statutes, regulations, directives and enterprise architecture
- Audit and governance compliance is assured

- Reduction in unnecessary or duplicate expenditures

6.3.2.4 Process Workflow Guidance



Asset Management Process Activity Level Workflow

6.3.2.5 Activities

[AM1] Establish Asset Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "AM process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for making changes and improvements to the AM process framework.

[AM2] Record and Control Assets

This activity prepares assets for use and includes receipt of assets from the supplier or when repurposing or redeploying existing assets. The activity also provides status of assets and pre-deployment actions, such as imaging and asset identification tags, assignment of assets and when applicable, transportation coordination of assets to new locations. This activity also executes the retirement and disposal of assets.

[AM3] Maintain Asset Record Information

The purpose of this activity is to maintain asset records: change, update, or delete asset data as required. Incident Management, Problem Management and Configuration Management can trigger modifications to asset data. This activity also administers the asset database, and performs asset reconciliation. The asset database includes all assets with a status designation such as ordered, in storage, assigned, retired, or disposed of, etc.

[AM4] Monitor, Audit and Reconcile Asset Records

In this activity, the status of IT assets is monitored. Compliance status for licensing and information security requirements is also monitored. Formal inventory audits of all physical assets occur in this activity. Additionally, audits of the Asset Management System and audit reconciliation are performed. Audits of logical assets include installed software on workstations and IT configurations or as required by the organization.

[AM5] Conduct Asset Remediation

This activity performs reporting and oversight for all assets requiring remediation, including remediation activities for missing and deployed assets. The goal of this activity is to ensure that assets which cannot be physically verified are accurately reflected in the Asset Management System. Assets may be marked as active, retired, missing, or deployed.

[AM6] Retire and Dispose of Assets

This activity ensures that all assets meet criteria for retirement and are returned to storage in preparation for disposal. Assets that have reached end-of-life are disposed of as required. Asset records and databases are updated with new status information.

[AM7] Monitor, Manage and Report Asset Management

In this activity, Asset Management activities are monitored to determine whether suitable progress is being made. Results are reported and unsatisfactory results may lead to review of Asset Management actions. In addition, responses are provided to requests for information and status of the Asset Management process.

[AM8] Evaluate Asset Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Asset Management process. It includes the capture of information, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Asset Management process remains fit for purpose and identifies where changes to the process might be required.

6.3.3 Change Management (ChM)

6.3.3.1 Purpose

The purpose of the Change Management (ChM) process is to ensure all changes are assessed, approved, implemented and reviewed in a controlled manner. To this end, Change Management ensures that any modification to the IT environment, whether it involves an addition, maintenance, or deletion of a service or service component, is in line with the overall mission strategy. This process provides standardized methods and procedures for efficient and prompt handling of technical changes, to minimize the impact of change-related incidents to service quality, and improves day-to-day operations of the organization.

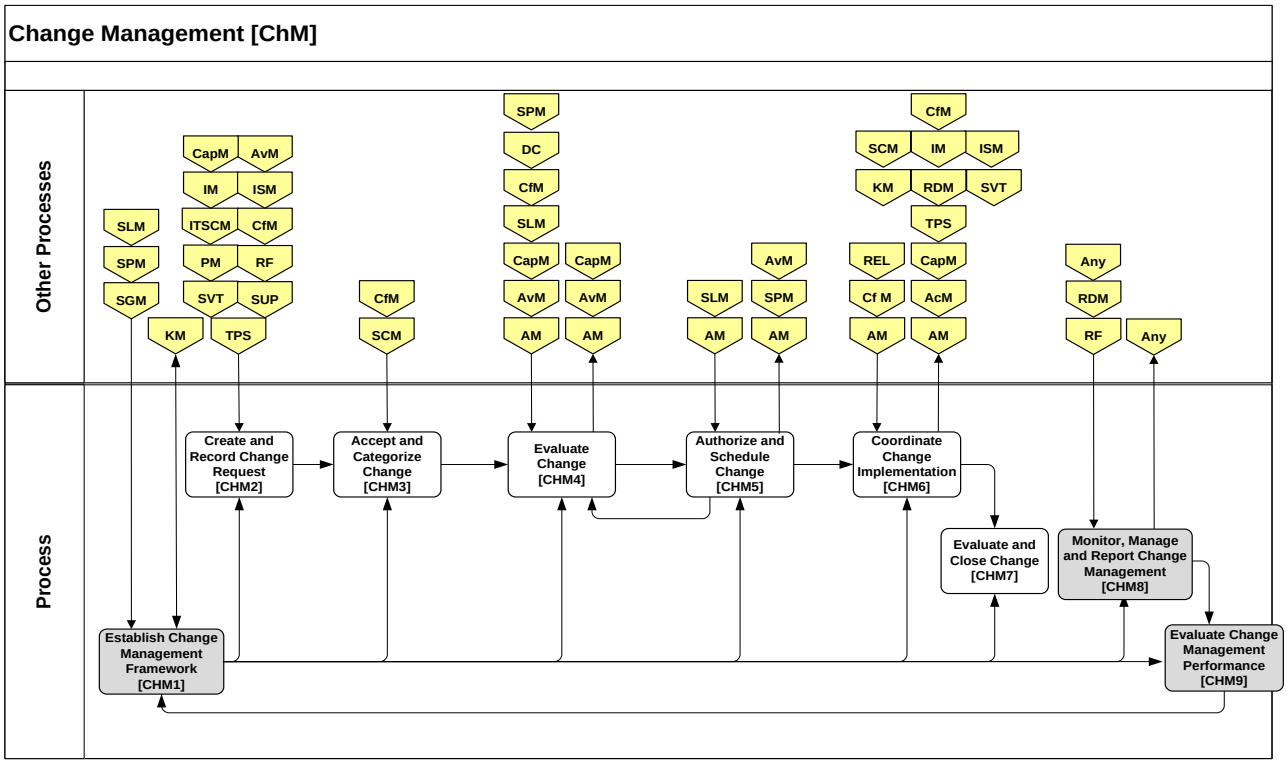
6.3.3.2 Scope

The scope of ChM encompasses any asset or configuration item (CI) that supports a service. Thus, ChM is responsible for managing the change process involving hardware (infrastructure), software and all documentation associated with running, supporting and maintaining production systems. All changes are planned and controlled to ensure timely updates with no unnecessary disruption or unintended consequences.

6.3.3.3 Process Benefits and Expected Outcomes

- Consistent tracking, scheduling and documentation of modifications to CIs
- As the change moves through its lifecycle, it's status is transparent
- Early identification of risk: The process includes submission of a risk analysis with every major change. This proactive approach mitigates risks in a manner that causes the least impact to mission partner service.
- Improved prioritizing and response to business and mission partner change proposals
- Implemented changes that meet mission partner agreed service requirements with optimized costs
- Contributes to governance, legal, contractual and regulatory requirements
- Reduced failed changes and therefore reduces service disruption, defects and re-work
- Provides change history throughout the service lifecycle
- Aids productivity of staff through minimizing disruptions due to high levels of unplanned or 'emergency' changes and hence maximizes service availability
- Reduces the Mean Time to Restore Service (MTRS), via quicker and more successful implementations of corrective changes
- Reduces risks associated with introducing change to the environment
- Reduces unplanned work due to reduction in incidents caused by change
- Increased number of standard changes, allowing for more efficient and timely implementations

6.3.3.4 Process Workflow Guidance



Change Management Process Activity Level Workflow Diagram

6.3.3.5 Activities

[ChM1] Establish Change Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "Change Management process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for changes and improvements to the Change Management process framework.

[ChM2] Create and Record Change Request

This activity involves formulating and storing the information about any change. The request will contain a defined outline of information established for assessment and other Change Management activities. Information can vary depending upon the context, scale, and potential impact of the requested change.

[ChM3] Accept and Categorize Change

This activity examines the Request for Change (RFC) to determine if it should be accepted for consideration. RFC acceptance requires all information to be logged. Incomplete information can cause a RFC to be returned for additional or amplifying information. After initial acceptance, the RFC is categorized.

ChM4] Evaluate Change

Each change is analyzed to determine impact on existing and planned CIs and the impact on resources required to build and deploy the change. This involves identifying the appropriate change model for handling the change, verifying appropriate change authority when necessary, scheduling a Change Advisory Board (CAB) meeting if specified by the change model, and obtaining a complete set of analysis results and issues. Assessment often assigns impact categorization classes such as minor, significant, or major.

[ChM5] Authorize and Schedule Change

This activity represents a decision checkpoint against the change based on impact. It examines the analysis results from the Evaluate Change activity and determines whether the change should be approved. If approved, the change deployment approach and targeted change deployment schedule are determined for the change. The manner in which the change is approved will depend on the organization structure, but formal approval will be obtained for each change from the change authority (CA). The activity for scheduling a change takes into account the Change Schedule, eliminating conflict between differing changes, and assigning appropriate resources accordingly.

[ChM6] Coordinate Change Implementation

This activity coordinates implementation of the change. If the approved change created or updated a solution, the solution components must first be built and tested. Approved changes are made available primarily through Release and Deployment Management (RDM); however, some changes are implemented through assignment by the Change Manager (within Change Management). This determination is made by Change Management policies and the appropriate change model. Change Management monitors the deployment of the change, as carried out by RDM.

[ChM7] Evaluate and Close Change

This activity contains the tasks involved in reviewing all implemented changes, after a predefined period has elapsed or another review trigger has been activated. It ensures that the change exhibits the desired effect and meets objectives, and that users and customers are satisfied with the results, or identifies any deficiencies. The review activity determines whether the implementation plan and the back-out plan, as appropriate, performed correctly, and whether the change was implemented on time and to cost. It determines whether any follow up action (such as the creation of a new Request for Change) is required. Subsequently, a formal close of the change is performed. The closure of a change includes updating other processes with the change status.

[ChM8] Monitor, Manage and Report Change Management

Continuous monitoring and analysis of operational results and comparison with service achievement reporting identifies Change Management trends and issues. Change Management data is used to generate detailed service component reporting as well as a perspective on service availability.

[ChM9] Evaluate Change Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Change Management process. It includes the capture of information, the relationship with other process areas, and the suitability of procedures and training. It is used to ensure the Change Management process remains fit for purpose and identifies where changes to the process might be required.

6.3.4 Change Evaluation (Eval)

6.3.4.1 Purpose

Change Evaluation is a formal evaluation process that is conducted prior to the execution of any significant change. The organization determines the definition (threshold) of significant changes that invoke this process. The goal of Change Evaluation is to provide accurate information to the Change Management process as to the impact and effect the change may have on service capability prior to acceptance of the change.

6.3.4.2 Scope

The scope of the changes to be formally evaluated is determined by the organization. As a guideline, this can include any change that introduces a new service, causes a substantial change to an existing service, or retires a service. It may also be determined by impact, or a project that impacts support, such as a reorganization or Service Desk consolidation. Resources, in time, equipment or money, may also be a consideration in determining if this process should be invoked from the Change Management process. When the Change Evaluation process ends, the Change Management process takes responsibility for further change activities.

6.3.4.3 Process Benefits and Expected Outcomes

- Additional focus and governance of significant changes
- Proper command and control of major changes
- Multiple risk analysis with each significant change
- Better allocation of resources
- Significant changes may undergo multiple risk analysis as they move through the change lifecycle
- All factors are considered prior to making a major change, including capability, tolerance for risk, organizational structure, resources, modeling, people, and all other projects and changes
- Major changes are viewed through service filters, not simply as IT projects
- Transparency into the status of the change

This process is invoked as a part of the Change Management process at the discretion of the organization. Thresholds are determined by the organization as to when this process is needed and executed. Activity flows for this process are not provided.

6.3.4.4 Process Workflow Guidance

(Not provided)

6.3.5 Configuration Management (CfM)

6.3.5.1 Purpose

The purpose of Configuration Management (CfM) is to control, identify, record, and report IT components, including versions (where appropriate), constituent components, states and most importantly, relationships to other IT components and services.

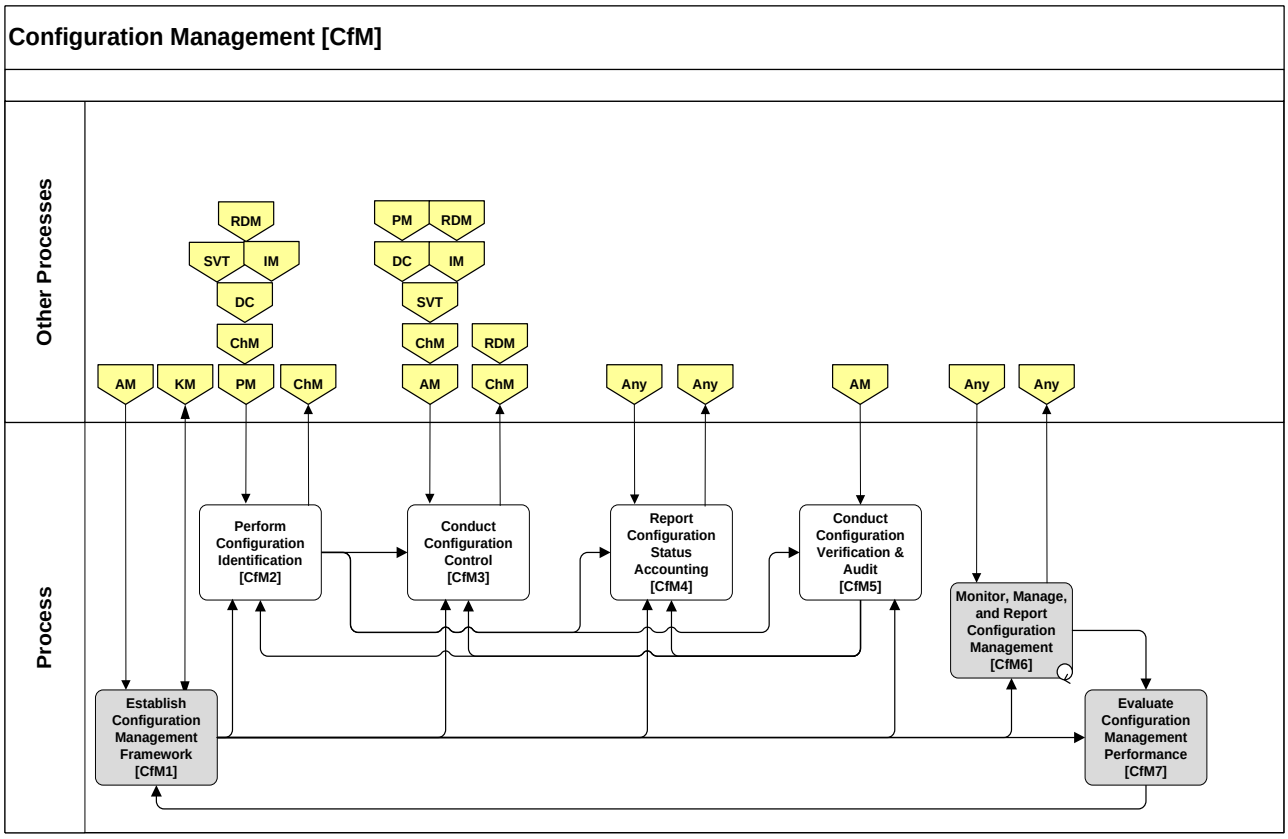
6.3.5.2 Scope

Configuration Items (CIs) are any components that need to be managed in order to deliver a service. CIs that should be under the control of Configuration Management include hardware, software, systems, services, applications, their relationships, and associated or related documentation, (e.g., Service Level Agreements). Configuration Management establishes and maintains the integrity of services and their configuration information to enable effective control of the services and to reduce the risk of unintended consequences during change execution.

6.3.5.3 Process Benefits and Expected Outcomes

- Accurate information on CIs and their documentation**:** This information supports all other Service Management processes, such as Release Management, Change Management, Incident Management, Problem Management, Capacity Management, and any necessary contingency planning. Configuration Management can provide information for upgrade planning and replacements.
- Facilitates adherence to legal obligations: Configuration Management maintains an inventory of all software and hardware within an IT infrastructure.
- Improves security by controlling versions of CIs in use**:** This makes it more difficult for those CIs to be changed accidentally, maliciously, or for erroneous versions to be added.
- Allows the organization to perform impact analysis and schedule changes safely, efficiently, and effectively: This reduces the risk of changes that may negatively impact the live environment.
- Unified view into Asset, Configuration, Change, Event, Problem, and Incident Management
- Better risk assessment for approving changes
- Better Incident Management, since failing components are traceable to services
- The status of and changes to CIs are effectively tracked and controlled

6.3.5.4 Process Workflow Guidance



Configuration Management Activity Level Workflow

6.3.5.5 Activities

[CfM1] Establish Configuration Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "CfM process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for changes and improvements to the CfM process framework.

[CfM2] Perform Configuration Identification

This activity identifies, defines and records the types of CIs under the control of Configuration Management, the CI naming conventions, attributes, relationships to other CI types, data integrity rules, and requirements and design documentation.

[CfM3] Conduct Configuration Control

This activity ensures that CIs and relationships and status are recorded accurately throughout each CI lifecycle. It generates configuration baselines and manages drift within acceptable limits. A baseline must be created to help restore a set of CIs to a known stable state if a change fails and its back-out plan is implemented.

[CfM4] Report Configuration Status

This activity makes CI information available to authorized requestors. The information ranges from detailed CI attributes and relationships to summarized information. It may cover an individual CI or a collection of CIs. CI information is provided in line with a planned schedule or in response to an individual request.

[CfM5] Conduct Configuration Verification & Audit

This activity ensures that CI information matches the physical reconciliation data, that naming conventions are adhered to and that the Definitive Media Library (DML) and/or secure repositories agree with the CI information. The audit is performed regularly, as stipulated by the Configuration Management Plan, or as requested by the Configuration Manager or other authorized personnel.

[CfM6] Monitor, Manage and Report Configuration Management

In this activity, all Configuration Management activity is monitored to determine whether suitable progress is being made. Unsatisfactory results are reported and may result in actions taken to address any issues.

[CfM7] Evaluate Configuration Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Configuration Management process. It includes the capture of information, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Configuration Management process remains fit for purpose and identifies where changes to the process might be required.

6.3.6 Knowledge Management (KM)

6.3.6.1 Purpose

The purpose of the Knowledge Management is to ensure that the right information is delivered to the appropriate place or person at the right time to enable informed decisions that improve performance, make the enterprise more efficient and to better serve the department workforce and mission partner. Knowledge Management provides the mechanism to help create, capture, share and act upon information in ways that will measurably improve the delivery and support of services as defined by DoD CIO mission. KM is the conduit to improve the Departments ability to execute core competencies in support of the mission.

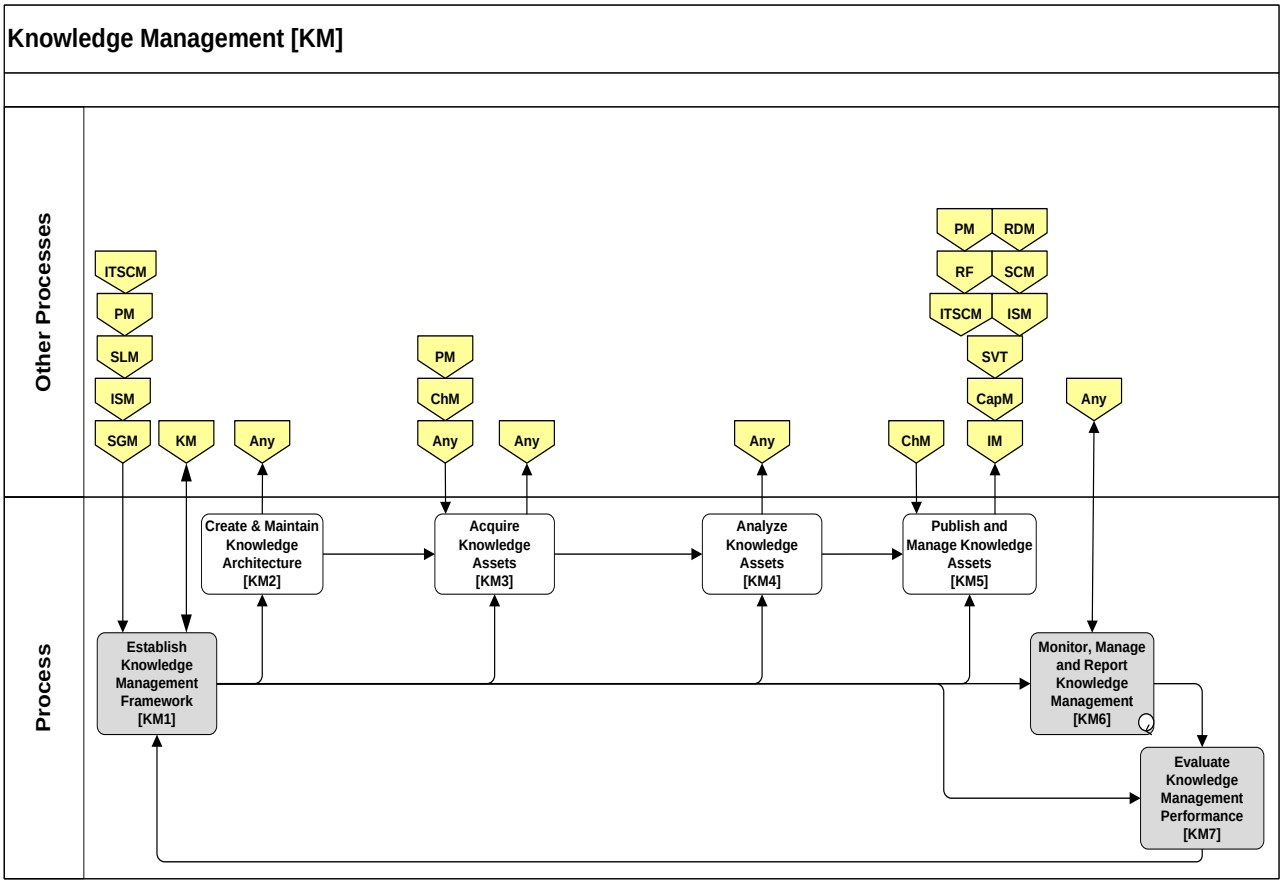
6.3.6.2 Scope

Although the scope of KM in every Command, Service and Agency (C/S/A) is much broader than the scope of this document, it's important to understand that the C/S/A Knowledge Management program in each C/S/A directly impacts the success of the mission. KM focuses on exploiting and realizing knowledge from the DoD workforce, fostering a culture where knowledge sharing can thrive, and increase overall value of intellectual capital required for making decisions. KM is a fundamental part of how the Department conducts it daily business.

6.3.6.3 Process Benefits and Expected Outcomes

- Improved efficiency through reducing the need to rediscover knowledge
- Knowledge is acquired, structured, published and maintained
- Reduced incident and problem solving time through sharing of workarounds and previous resolutions
- Reduced design time through sharing of information related to current and past design projects
- Better strategic decisions based on captured and categorized knowledge, rather than institutional memory
- Improved decision making across the board, based on common knowledge
- Improved project management
- Gain overall efficiency through reuse of previous plans, documents, etc.
- Better sharing of internal best practices
- Increase innovation through knowledge sharing and collaboration
- Serve as a process enabler allowing for DoD's knowledge workers to share ideas and collaborate in ways that would not have been possible previously
- Improved project management through knowledge transfer and data availability in existing systems (i.e. allowing data transparency across PM systems).
- Proactively facilitates and rewards knowledge creation, transfer and use

6.3.6.4 Process Workflow Guidance



Knowledge Management Activity Level Workflow

6.3.6.5 Activities

[KM1] Establish Knowledge Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "KM process framework" and is used as reference information for all other activities. Knowledge Management responsibilities are integrated in career paths, job descriptions and skill requirements. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for making changes and improvements to the KM process framework.

[KM2] Create and Maintain Knowledge Architecture

The Knowledge Architecture is a framework of policies, standards and conventions for collection, formatting and organizing process and service information assets in a consistent manner. This architecture provides a reference model for use in designing and building processes and services. It also provides a way to define the various segments of KM as the organization matures this process through addressing priorities or weaknesses in KM.

[KM3] Acquire Knowledge Assets

This activity involves all tasks and operations required to harvest targeted information packages which require processing and manufacturing into knowledge assets. These assets are made available through the Service Knowledge Management System (SKMS). Knowledge asset acquisition activities use common processes based on standard data and information models.

[KM4] Analyze Knowledge Assets

Conduct a Subject Matter Expert (SME) analysis of captured raw knowledge assets, consequential information and data that has been extracted in the Acquire Knowledge Assets activity. It is envisioned that most knowledge assets will be harvested from authoritative data sources in a consistent format. These knowledge packages will require SME reviews for technical, legal and publication compliance. Once submitted, a rigorous material review process against prescribed submission criteria is performed.

[KM5] Publish and Manage Knowledge Assets

This activity covers all tasks required to make available and deliver knowledge assets to users. It can include both proactively and reactively supplying knowledge.

[KM6] Monitor, Manage and Report Knowledge Management

In this activity, all Knowledge Management activity is monitored to determine whether suitable progress is being made. This also includes monitoring and reporting knowledge performance including resolution enablement rate (i.e. first call resolution enablement rate) by each tier and responsible knowledge owner within each Tier. Unsatisfactory results are reported and may result in actions taken to address any issues.

[KM7] Evaluate Knowledge Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Knowledge Management process. It includes the capture of information, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Knowledge Management process remains fit for purpose and identifies where changes to the process might be required.

6.3.7 Release and Deployment Management [RDM]

6.3.7.1 Purpose

The purpose of this process is to deploy releases into the live environment in a controlled manner. Release and Deployment Management ensures the integrity of the live environment is protected and correct components are released. This must be in a time frame that meets the mission partner's service needs and does not cause a SLA breach.

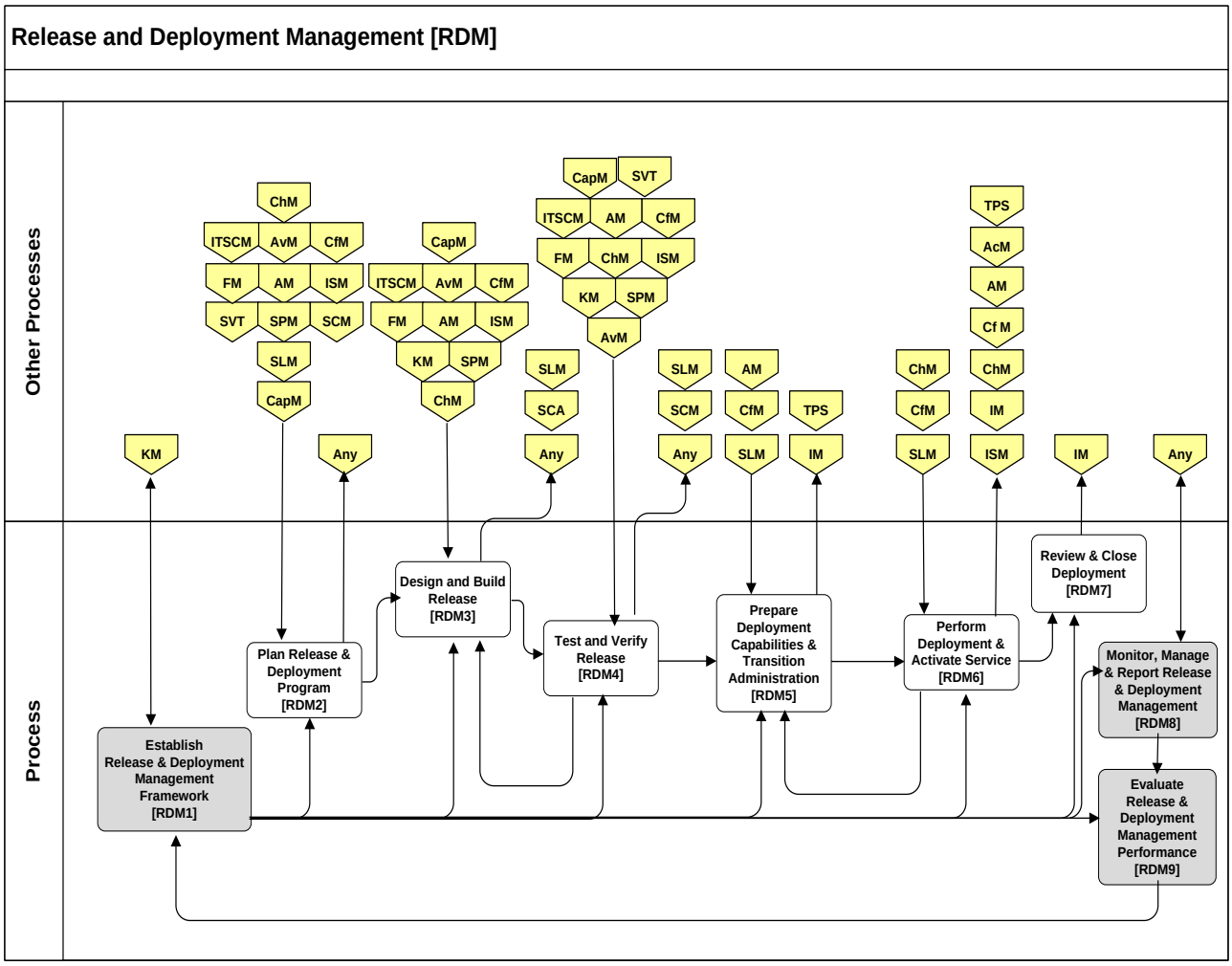
6.3.7.2 Scope

This scope includes the processes, systems and functions to package, build, test and deploy into the production or live environment for use. RDM establishes the service as specified in the Service Design Package (SDP) and formally hands the service over to Service Operations. The package includes all configuration items (CIs) required to implement the release.

6.3.7.3 Process Benefits and Expected Outcomes

- Minimized disruption of service to the mission partner, due to synchronization of Releases involving hardware and software components from different platforms and environments
- Releases are planned and performed with a business/service purpose
- Early life support becomes part of the process
- Effectively communicates and manages expectations of the mission partner during the planning and rollout of new releases
- Reduction in errors through the controlled release of hardware and software to the live environment
- Unsuccessful deployed releases are reversed and environment is recovered
- Enhanced use of resources due to combined efforts when testing new releases
- Overall reduction in configuration variance
- Reduction in unplanned work due to better control of service components and releases

6.3.7.4 Process Workflow Guidance



Release and Deployment Management Activity Level Workflow

6.3.7.5 Activities

[RDM1] Establish Release and Deployment Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "RDM process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for changes and improvements to the RDM process framework.

[RDM2] Plan Release and Deployment Program

This activity determines the approach for how each release is prepared and the type of deployment that is necessary. The release planning covers building, testing and verifying the release, as well as establishing a model for how the finalized release should be deployed.

[RDM3] Design and Build Release

This activity determines what needs to be built for the release and how it will be assembled and deployed. As a result, the release build, installation, and rollback scripts are designed at a high level. Software and hardware components are obtained for the build activity and the test environment is created.

[RDM4] Test and Verify Release

This activity tests the built Release Package and determines if installation, configuration, and rollback work properly. Once successful, the release is ready for deployment. If testing fails, the Release must go through another round of either design or build, and a subsequent re-testing.

[RDM5] Prepare Deployment Capabilities and Perform Transition Administration

This activity administers the transition of assets, resources, knowledge, and anything else that is transferred to or from the IT infrastructure. This ensures that appropriate asset data is provided to the Asset Management process to reflect the transition status. Items impacted include location, financial status (support contracts), and ownership.

[RDM6] Perform Deployment and Activate Service

This activity executes all tasks necessary to complete the actual deployment. In this activity, the capability status moves from “Not Deployed” to “Deployed. This activity verifies the integrity of the solution under deployment and transitions the new changed service to Operations.

[RDM7] Review and Close Deployment

This activity reviews tasks completed during deployments and determines if all objectives of the deployment plan were met. A management plan is established for outstanding risks, issues, incidents and known errors before the deployment is closed. Deployment is completed with a handover of the support to Service Operations.

[RDM8] Monitor, Manage and Report Release and Deployment Management

In this activity, all Release and Deployment Management activity is monitored to determine whether suitable progress is being made. Unsatisfactory results are reported and may result in actions taken to address any issues.

[RDM9] Evaluate Release and Deployment Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Release and Deployment Management process. It includes the capture of information on records, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Release and Deployment Management process remains fit for purpose and identifies where changes to the process might be required.

6.3.8 Service Validation and Testing (SVT)

6.3.8.1 Purpose

Service Validation and Testing provides evidence that the new/changed service meets the mission partner and mission requirements, including any documented SLAs, thus limiting risk as changes are introduced into the production environment. The service is tested explicitly against all parameters in the Service Design Package, including functionality, availability, continuity, security requirements, usability and regression testing.

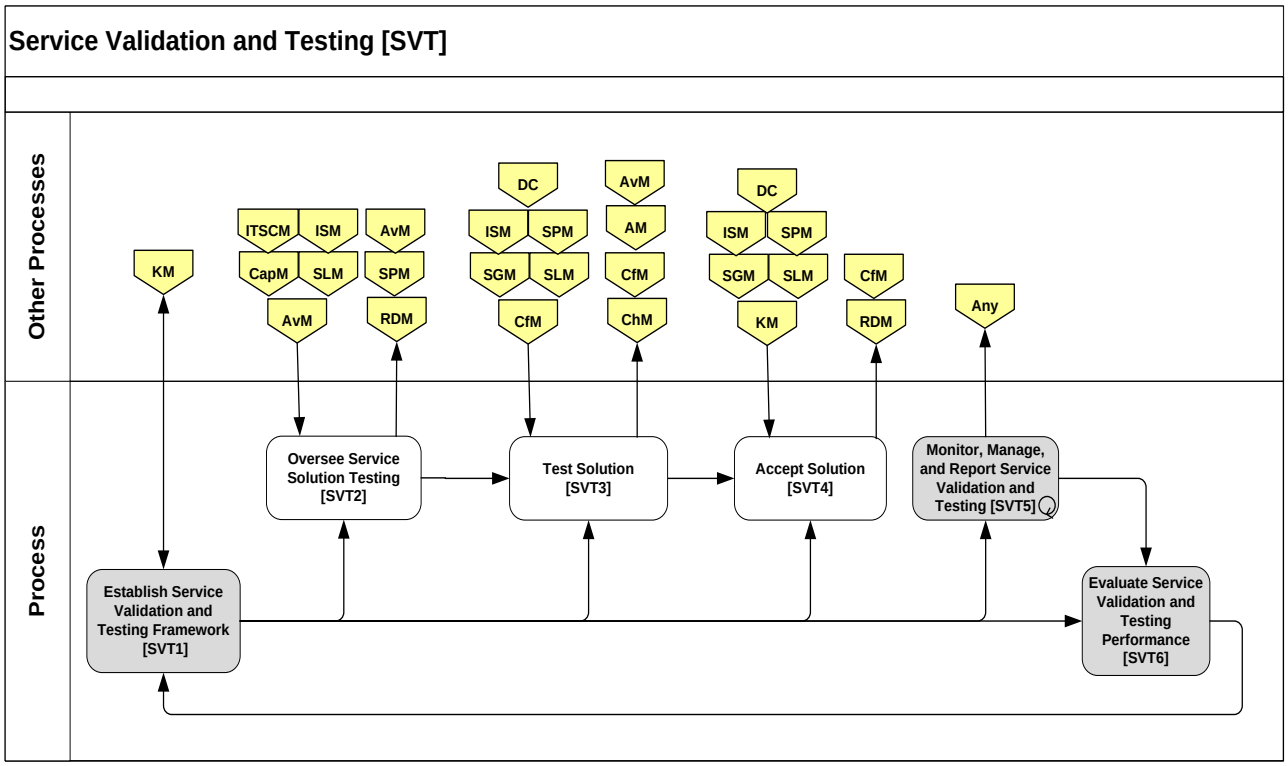
6.3.8.2 Scope

This process focuses on the testing and validation of a fully functional solution that is designed to meet stakeholder requirements and the stakeholder acceptance of that solution prior to roll-out. The scope of Service Validation and Testing is all approved releases, and those components as defined in Release and Deployment Management. It includes all configuration items required to implement a release, and the congruent and tangent systems that make up the production environment.

6.3.8.3 Process Benefits and Expected Outcomes

- Ensures releases meet the criteria for utility and warranty
- Mission partner confidence on the success of releases resulting in elevated satisfaction
- Testing is done from an overall service perspective, not just component or system
- Reduction in mission partner resources to test releases
- A structured validation and test process that provides evidence that the new or changed service supports the mission requirements as set in service strategy
- Ensures mission partner requirements are met as set forth in the Service Design Package
- Overall reduction in incidents

6.3.8.4 Process Workflow Guidance



Service Validation and Testing Activity Level Workflow

6.3.8.5 Activities

[SVT1] Establish Service Validation and Testing Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "SVT process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for changes and improvements to the SVT process framework.

[SVT2] Oversee Service Solution Testing

This activity is responsible for the testing the service prior to the introduction of changes to the environment that affects the service. SVT is more commonly an iterative process.

[SVT3] Test Solution

Solution testing validates the solution and its features conform to design specifications and requirements prior to deployment. It also verifies that interim work products exist and conform to standards.

[SVT4] Accept Solution

This activity validates that the proposed solution, either as individual artifacts or in its complete form, meets end-user acceptance criteria.

[SVT5] Monitor, Manage and Report Service Validation and Testing

This activity supports continuous monitoring and analysis of operational results data and comparison with service achievement reporting to identify Service Validation and Testing trends and issues. Service Validation and Testing information is used to generate detailed service component reporting as well as a perspective on overall service availability.

[SVT6] Evaluate Service Validation and Testing Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Service Validation and Testing process. It includes the capture of information on records, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Service Validation and Testing process remains fit for purpose and identifies where changes to the process might be required.

6.4 Service Operations (SO) Domain

The Service Operations Domain controls the full range of matters pertaining to sustaining assured information delivery, system and network availability, and information protection for information technology (IT) capabilities that support the provided services. The Domain Owner serves as the approval authority to introduce new initiatives, ensures standards-based configuration and operation of all infrastructure, controls the runtime aspects of services to ensure services behave correctly and within SLAs, administers and controls security policies, identifies incidents and infrastructure issues, performs problem resolution, and implements metrics that track the overall progress of the operations Domain. The Domain Owner must ensure that processes that support services are executed in a cost-effective manner and measure the effectiveness of controls to determine how well the controls achieved the planned control objectives. As such, processes must have an internal and external (mission partner) focus. It is within this Domain that the mission partner determines the ongoing value extended by the service provider. There are two key definitions whose difference is more prominent in the operations Domain than the other Domains:

Function: A team or group of people with like skill sets and the tools they use to carry out one or more processes or activities.

Process: A structured set of activities designed to accomplish a specific objective.

This difference is notable, since in addition to processes, the Service Operations Domain has several functions (Service Desk, Applications Management, Technical Management, and IT Operations Management). These functions are described in the Functions section of this document.

Domain Metrics

The metrics for this Domain are actionable measures for decisions related to improving the performance of the process and guiding resource allocation. Metrics must be viewed in an overall context of the DESMF. As an example, a common metric for Incident Management is "% of first call resolution". This number often goes up if incidents are repeated and the same workaround is applied a number of times. If Problem management supplies a permanent fix for the root cause of the incidents, and change management chooses to apply it, these incidents no longer occur, reducing the % of first call resolution. More correctly, metrics must be applied to measure that which is critical to Incident Management as well as other metrics associated with the processes in this Domain.

6.4. Access Management (AcM)

6.4.6.1 Purpose

Access Management is the process of granting authorized users the right to use a service while preventing access to non-authorized users. The process provides the ability to control and track who has access to data and services. ("Who" may be another system, service, or process, as well as an individual.) It contributes to achieving the appropriate confidentiality, availability, and integrity of the command's data and includes levels of access to the service catalog for requesting services, access to data, and access to facilities.

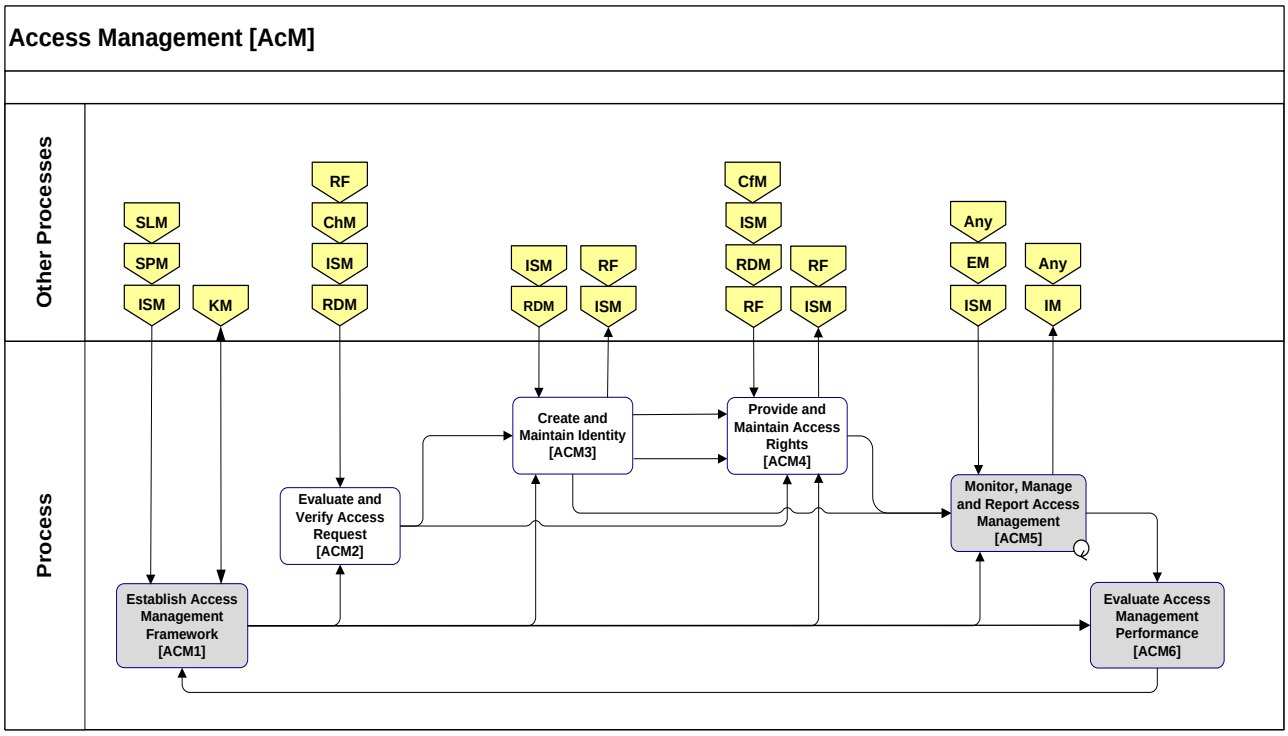
6.4.1.2 Scope

Access Management enables the management of the confidentiality, availability, and integrity of data and intellectual property. This process operates within and enforces controls described by IT security policies and organization directives; control of identities and their associated access rights will vary depending upon the level of access required and the adjudicated risk tolerance of malicious access.

6.4.1.3 Process Benefits and Expected Outcomes

- A definitive source permits users access to information and services while unauthorized access attempts receive denial of access
- An accurate identity and rights registry exists that undergoes periodic maintenance and review
- Access to services is aligned with strategy
- Data is protected from accidental and intentional attempts
- Better controlled environment when access needs to be revoked, such as job changes, retirements, and discontinuation of services
- Employees have the right access to perform their jobs
- Access to data and services is controlled
- Access-related security incidents are defined and access controls are regularly tested
- Consistent enforcement of service, data, and facilities access
- Processes in place to demonstrate compliance with DoD and other policies

6.4.1.4 Process Workflow Guidance



Access Management Activity Level Workflow

6.4.1.5 Activities

[AcM1] Establish Access Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "AcM process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for changes and improvements to the AcM process framework.

[AcM2] Evaluate and Verify Access Request

This activity evaluates and verifies the identity of the person listed in each request and verifies that a reasonable substantiation exists for the access to a system or application. This activity also verifies that the request has been approved by competent authority.

[AcM3] Create and Maintain Identity

This activity creates new identity records in the identity database and performs appropriate edits and deletions to existing identity records.

[AcM4] Provide and Maintain Access Rights

This activity provides access rights based on predefined policies, directives, and regulations. It updates the identity records to reflect updated access rights and confirms that access rights have been implemented or revoked. Access rights can be removed as well as granted. Accordingly, this activity will restrict or revoke rights to execute policies and decisions made by appropriate authority.

[AcM5] Monitor, Manage and Report Access Management

In this activity, Access Management activities are monitored to determine whether suitable progress is being made. Results are reported, and unsatisfactory results may lead to review of Access Management actions. In addition, responses are provided to requests for information and status of the Access Management process.

[AcM6] Evaluate Access Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Access Management process. It includes the capture of information, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Access Management process remains fit for purpose and identifies where changes to the process might be required.

6.4.2 Event Management (EM)

6.4.2.1 Purpose

The purpose of the Event Management process is to identify and prioritize all events that occur throughout the IT infrastructure and establish the appropriate response to those events. Event Management monitors, filters, and notifies of actions and occurrences that have an effect on the services provided. This process is proactive and reactive. Proactively, Operations is notified of events that may cause service degradation and outages enabling operations to take steps necessary to avert any SLA breach. Reactively, Event Management interfaces with Operations and Incident Management to provide information and corrective actions for those events.

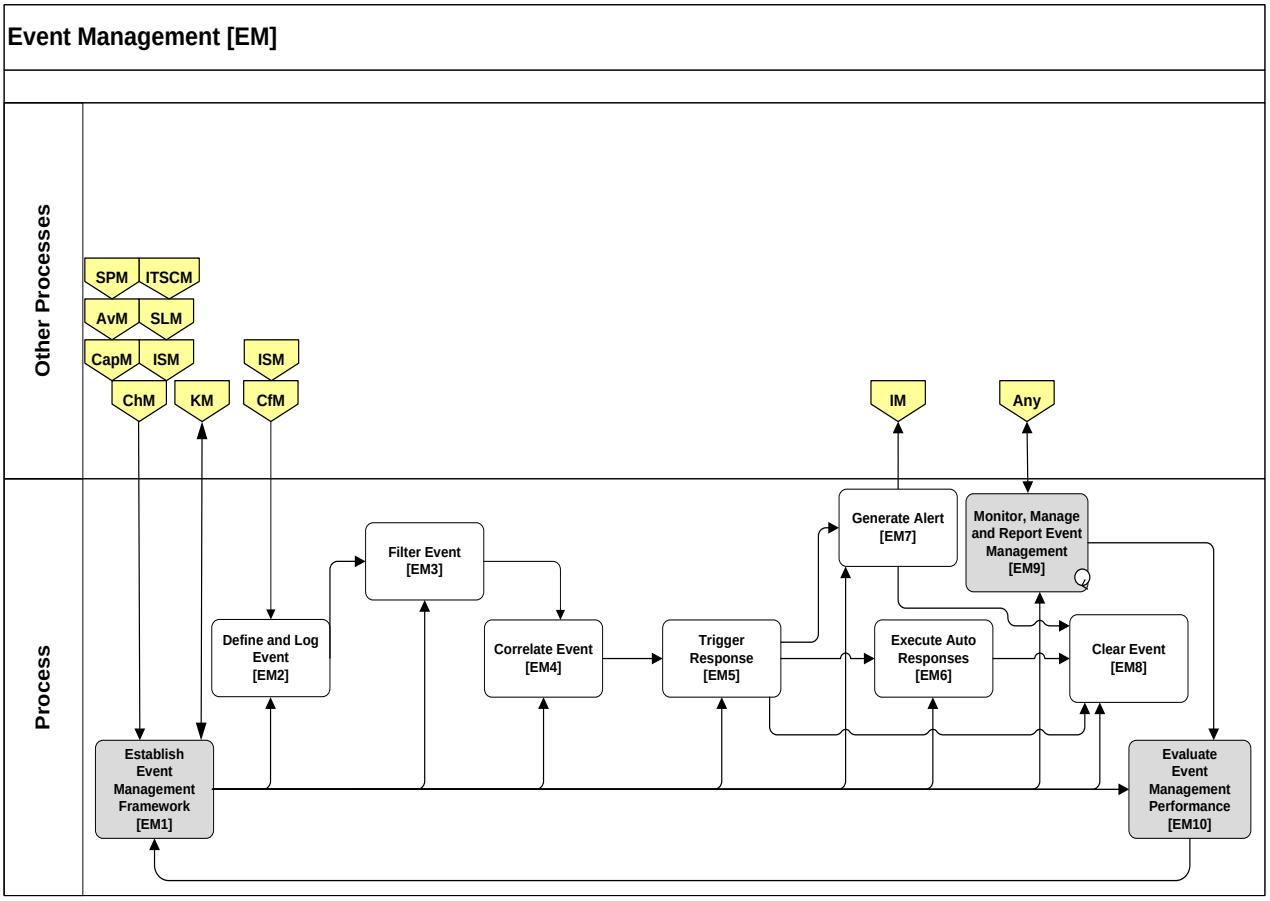
6.4.2.2 Scope

Event Management includes occurrences or actions that affect the ability to provide services. These may be related to: security, performance of CIs, component failure, facilities, capacity, or issues related to compliance and contracts or licensing. Event Management can be utilized to capture/display near real-time monitoring data enabling increased command and control of the IT Infrastructure and help shape Service Levels. Tool sets are pre-engineered to support automated monitoring and responses to events, including pre-populating an alarm event.

6.4.2.3 Process Benefits and Expected Outcomes

- Improved Situational Awareness (SA) of critical IT service and infrastructure components/systems
- Decreased labor costs due to automated responses to events
- Automation for escalating exception conditions to the Incident Management Process to engage automatically, which improves service availability
- Higher productivity staff through reduction of monitoring non-consequential events
- Ability to preclude incidents, increasing availability of services
- Quicker return to service due to notification from the source of the event
- Standardization in event notification, enables better responses from Operations
- Monitoring of IT should be service and mission focused
- Reduction in the TCO for monitoring resources

6.4.2.4 Process Workflow Guidance



Event Management Activity Level Workflow

6.4.2.5 Activities

[EM1] Establish Event Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "EM process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity which generates recommendations for changes and improvements to the EM process framework.

[EM2] Define and Log Requirements

This activity involves receipt of all predefined events detected into the Event Management System (EMS) monitoring the IT environment. When an event is actively or passively detected, it is the responsibility of those managing the device to ensure the event is defined and logged in an agreed format and that protocol is adhered to for handling the EMS.

[EM3] Filter Event

This activity determines if the event must be communicated or ignored based on predefined criteria.

[EM4] Correlate Event

This activity describes the tasks involved in reviewing service requests that were fulfilled in this activity. The command's predefined mission goals are applied to significant events to determine what actions are required. Events are correlated by the EMS to determine commonalities and appropriate response action.

[EM5] Trigger Response

After an event is detected, filtered and correlated, the appropriate and specific event notification / response activities are initiated. The response includes opening an incident, changing the status or severity of an event, dropping an event, or sending the event for automated recovery.

[EM6] Execute Auto Response

In this activity, a pre-defined automated response is initiated by the EMS (e.g. rebooting and/or restarting a device, initiating a batch job, etc.). These responses do not require human intervention.

[EM7] Generate Alert

This activity identifies those events requiring human intervention and provides necessary information to determine appropriate action. Additionally, this activity transmits the event information to Incident Management, which manages routing / escalation to the proper level for resolution.

[EM8] Clear Event

In this activity, the status of the event is confirmed as cleared and appropriate updating of event records is made.

[EM9] Monitor, Manage and Report Event Management

In this activity, all Event Management activity is monitored to determine whether suitable progress is being made. Unsatisfactory results are reported and may result in actions taken to address any issues.

[EM10] Evaluate Event Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Event Management process. It includes the capture of information on records, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Event Management process remains fit for purpose and identifies where changes to the process might be required.

6.4.3 Incident Management (IM)

6.4.3.1 Purpose

The purpose of Incident Management is to restore normal service operation as quickly as possible and minimize the adverse impact on mission partner operations, thus ensuring that the best possible levels of service quality, security, and availability are maintained. The focus is on reducing the duration and consequences of service outages from a mission partner perspective; not on finding the root cause of the incident.

6.4.3.2 Scope

The scope includes any disruption or potential disruption of service. The process allows for three different paths: Normal, Major, and Security related. Defining a major incident is an important aspect of Incident Management process definition. Those incidents that have the highest impacts and are most disruptive to the affected service components must be managed in a separate sub-process. Additionally, security incidents require a separate sub-process since these tend to occur as a result of activities intended to disrupt or degrade services, rather than as a result of human error or material failures. These have different reporting criteria and may or may not adversely affect one or more services. Other incidents are considered normal.

Connecting IM security incidents to CND/DCO Incident Management as outlined in DOD 8530 series and CJCS (Chairman of the Joint Chiefs of Staff) 6510 series:

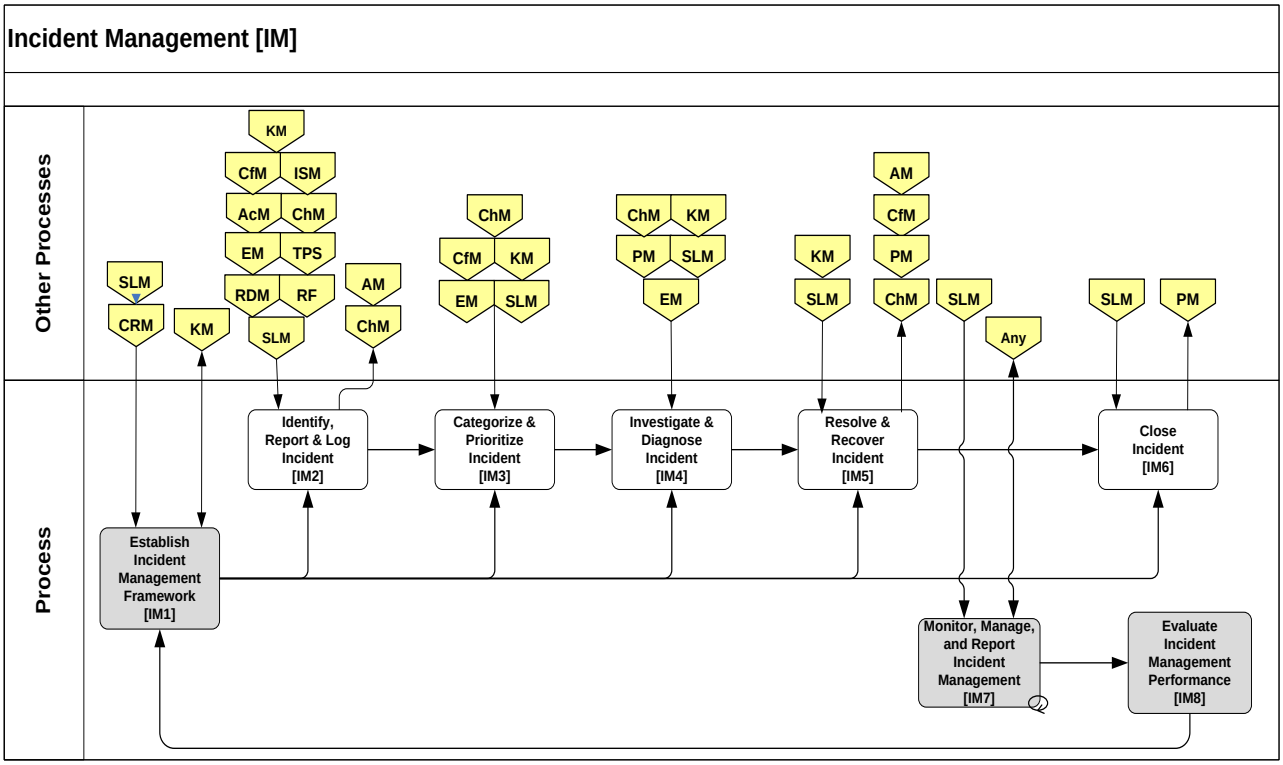
Computer Network Defense (CND, also known as Defensive Cyber Operations, DCO) activities under the categories of Detect, Identify, Initial Diagnosis, and Preliminary Response Actions are considered part of the IM process. Some activities under the categories of Investigate and Diagnosis, and Resolution and Recovery may also be considered part of IM, depending on scope.

6.4.3.3 Process Benefits and Expected Outcomes

- Incidents are recorded and categorized
- Ability to detect and resolve incidents more efficiently, which results in higher availability of the service to the mission partner.
- Ability to align IT activity to real-time business priorities. Incident Management includes the capability to identify mission partner priorities and dynamically allocate resources as necessary.
- Identification of potential improvements to services. This happens as a result of understanding what constitutes an incident and from being in contact with the activities of operational staff.
- Potential to identify needed service or training during the handling of incidents
- Improved information flow to mission partners regarding service restoration
- Basis of information for Problem Management. With standard recording techniques, there is better management of resources for problem resolution.

- A consistent flow for IM based on mission, policy, and process
- A single Incident Management process for use across the organization
- Better focus on restoring service as opposed to just performing root cause analysis
- A searchable base of incidents and workarounds to better resolve service outages
- A standard method of prioritization, categorization and escalation of incidents
- Incident models to allow for more efficient resolution of incidents
- Transparency into the status of incident resolution

6.4.3.4 Process Workflow Guidance



Incident Management Activity Level Workflow

6.4.3.5 Activities

[IM1] Establish Incident Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "IM process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for changes and improvements to the IM process framework.

[IM2] Identify, Report and Log Incident

The incident is identified and logged by the Service Desk resulting in creation of an Incident record.

[IM3] Categorize and Prioritize Incident

The incident is categorized and prioritized. Categorization is based on the systems, applications, service or segment affected, or the requestor's mission support role. Prioritization is based on urgency and impact. The record is assigned to an analyst for diagnosis and investigation. The path and procedures involved are based on how the incident is categorized, for instance Normal, Major or Security etc. If the incident is categorized as a request for service, it is transferred to the Request Fulfillment process as a Service Request. Incidents

exceeding a defined threshold of impact and urgency are categorized as Major Incidents and appropriate procedures are invoked.

[IM4] Investigate and Diagnose Incident

Incidents and all associated data are accessed to identify appropriate responses and actions, and to formulate Incident Resolution Plans. Actions may include identifying workarounds, recategorizing the incident based on further analysis, and updating Incident records.

[IM5] Resolve and Recover Incident

Actions necessary to resolve the incident and restore service are executed. Resolution and restorations may be in the form of existing workaround solutions, or alternatively creating a Request for Change to implement a new solution. It also prompts any action necessary to recover the service to approved Service Level Agreements (SLA), Operational Level Agreements (OLA) and/or Underpinning Contracts (UC).

[IM6] Close Incident

This activity ensures all required incident documentation is complete, including details of cause, expended effort for resolution and outcome. A review of the incident's original categorization against available root cause information is used to determine categorization accuracy. This activity obtains stakeholder agreement with resolution activity and status.

[IM7] Monitor, Manage and Report Incident Management

This activity supports continuous monitoring and analysis of operational results data and comparison with service achievement reporting to identify Incident Management trends and issues. Incident Management information is used to generate detailed service component reporting as well as a perspective on overall service availability.

[IM8] Evaluate Incident Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Incident Management process. It includes the capture of information on records, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Incident Management process remains fit for purpose and identifies where changes to the process are required.

6.4.4 Problem Management (PM)

6.4.4.1 Purpose

The purpose of Problem Management is to prevent problems and incidents from happening, to eliminate recurring incidents and to minimize the impact of incidents that cannot be prevented. Problem Management includes the activities required to diagnose the root cause of incidents, determining the resolution to those problems and providing workarounds to Incident Management.

6.4.4.2 Scope

A problem is defined as a cause of one or more incidents. The cause is not usually known at the time a problem record is created, and the Problem Management process is responsible for further investigation. Problem Management has aspects of both reacting to problems and proactively identifying and solving problems and known errors before more incidents occurs.

Problem Management finds trends in incidents, groups those incidents into problems, identifies the root causes of problems, and initiates Request for Change (RFC) against those problems. Also, Problem Management maintains information about problems and the workarounds and resolutions to reduce the number and impact of incidents over time. This process has a strong interface with Knowledge Management, and tools such as the Known Error Database (KEDB). Although Incident Management and Problem Management are separate processes, they are closely related and typically use the same tools, and have similar categorizations, impact and priority coding systems. This ensures effective communication when dealing with incidents and problems that are related. Problem Management also ensures the resolution is implemented through appropriate control procedures such as Change Management and Release and Deployment Management.

Connecting PM to CND/DCO Incident Management as outlined in DOD 8530 series and CJCS (Chairman of the Joint Chiefs of Staff) 6510 series:

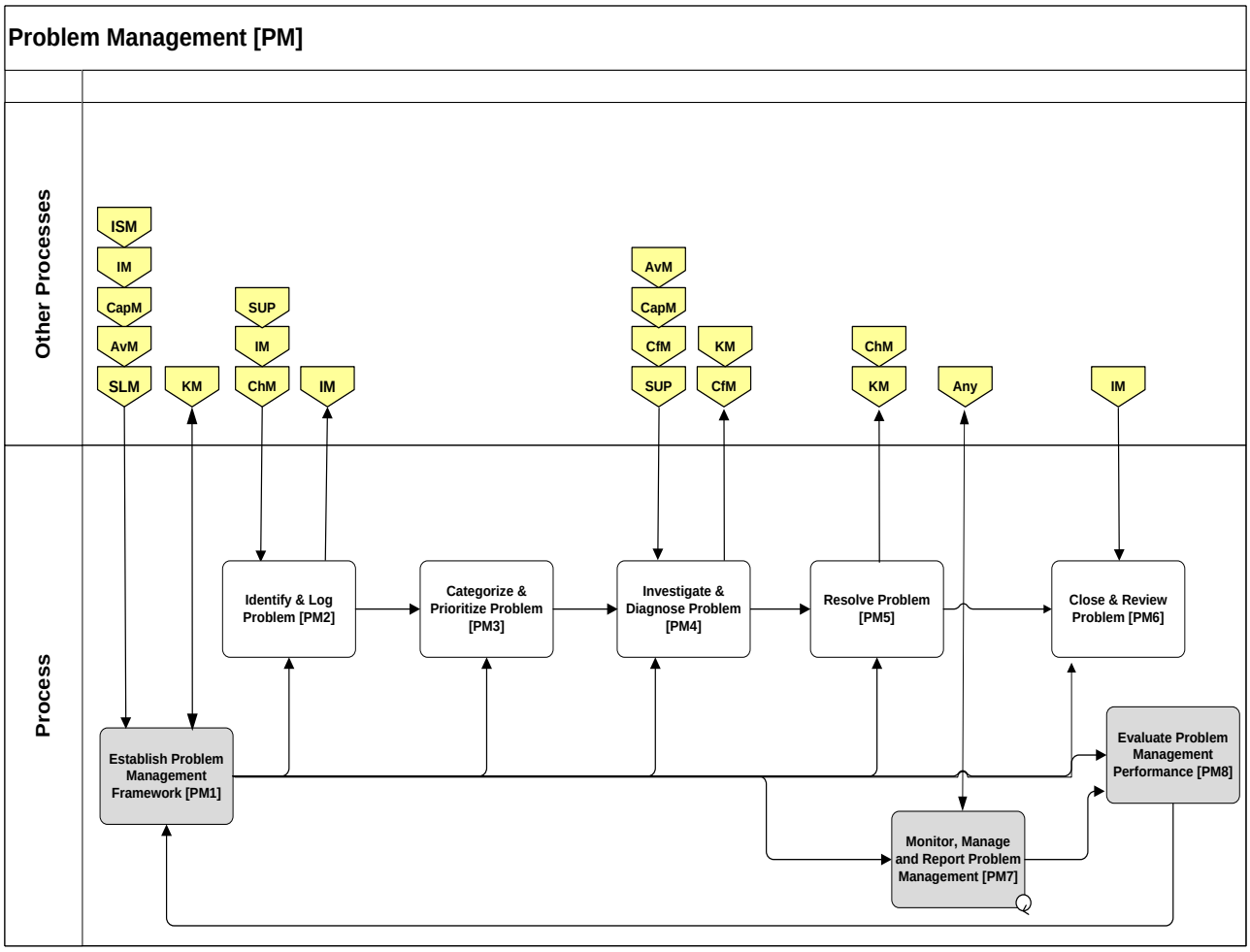
Computer Network Defense/Defensive Cyber Operations (CND/DCO) activities under the category of Post-Incident Analysis, as well as some activities under the categories of Investigate and Diagnosis, and Resolution and Recovery are considered part of the PM process.

6.4.4.3Process Benefits and Expected Outcomes

- Incident trends are identified and proactively investigated as a problem
- Higher availability of IT services
- Higher productivity of business and IT staff
- Reduced expenditure on workarounds or fixes that do not work
- Reduction in cost of effort in fire-fighting or resolving repeat incidents
- Reduces the chance of having to invoke the business continuity plan
- A Known Error Database (KEDB) reduces time to resolution and allows learning from historical data

- A structured process based on prioritization schemes to allocate resources for solving problems
- Ability to distinguish between restoring service (IM) and root cause analysis (PM) which will create higher availability of services
- Better integration of supporting processes

6.4.4.4 Process Workflow Guidance



Problem Management Activity Level Workflow

6.4.4.5 Activities

[PM1] Establish Problem Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "PM process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for changes and improvements to the PM process framework.

[PM2] Identify and Log Problem

This activity ensures problems are identified through resource monitoring, trend recording and analysis.

[PM3] Categorize and Prioritize Problem

Problems are classified to support active analysis, problem resolution, and post-problem forensic review. This activity also classifies problem severity and potential impact to enterprise operations and goals.

[PM4] Investigate and Diagnose Problem

This activity includes Root Cause Analysis, creating workarounds, and recording Known Errors. If a workaround is identified and approved for deployment, this activity ensures the workaround is known to be effective, and sufficient evidence exists to support the Root Cause Analysis. A Known Error Record is created or updated that describes problem diagnosis and lists available approved workarounds. This activity also updates the problem record to indicate the diagnosed problem.

[PM5] Resolve Problem

This activity includes the search for a solution, steps planned to implement the solution and eliminate known errors, and tracks infrastructure changes. Once the resolution has been documented in the problem and known error records, the activity culminates in Request for Change or Project Proposal submissions.

[PM6] Close and Review Problem

The Problem record is closed, known error records are updated, and major problems are reviewed for performance quality, process adherence, and lessons learned. Prior to closing, each problem record is checked to ensure completeness and accuracy of detail. Major problems are reviewed and results are disseminated through enterprise communication (including extended enterprise stakeholders such as vendors), staff training and service review.

[PM7] Monitor, Manage and Report Problem Management

This activity ensures all service requests are effectively and efficiently managed throughout the process life cycle. All request data and status changes are examined for consistency and recorded in Problem Management records.

[PM8] Evaluate Problem Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Problem Management process. It includes the capture of information, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Problem Management process remains fit for purpose and identifies where changes to the process are required.

6.4.5 Request Fulfillment (RF)

6.4.5.1 Purpose

The purpose of the Request Fulfillment process is to fulfill service requests from users and route each request to the appropriate process for handling within accepted service levels. Request Fulfillment is responsible for the entire lifecycle of the request.

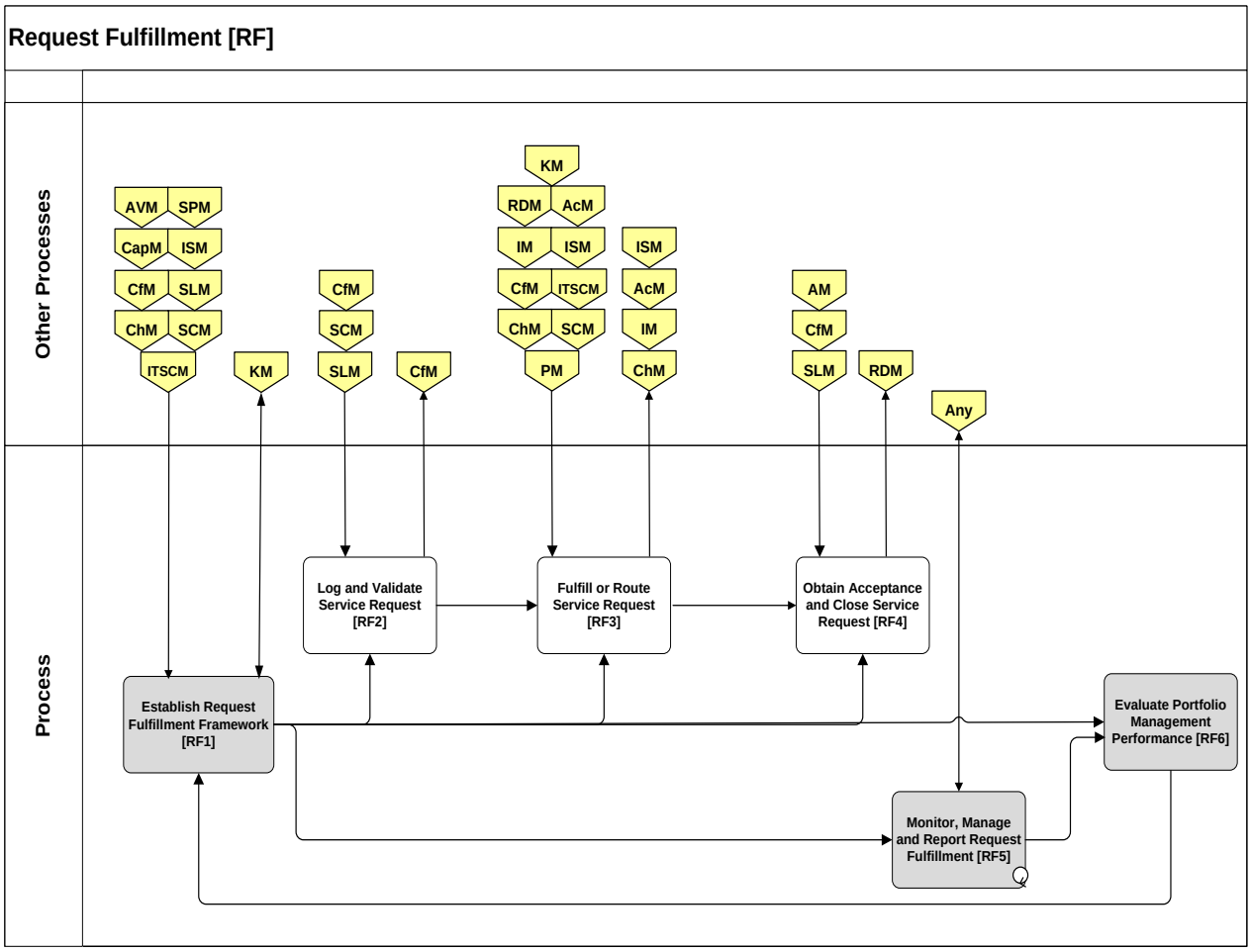
6.4.5.2 Scope

Request Fulfillment encompasses fulfillment of service requests within agreed service levels. Requests can come from a mission partner by direct communication or automated menu system. This process interacts at the process framework level of other specific processes to determine which types of service requests should be handled by which processes, e.g., Request for Changes interacts with the Change Management process. Request Fulfillment is responsible for the entire lifecycle of the request.

6.4.5.3 Process Benefits and Expected Outcomes

- Service improvement through repeatable and measured fulfillment
- The Service Desk better prioritizes requests by separating incidents from service requests
- Service requests are prioritized
- Mission partners have quick and easy access to standard services
- Service requests which have not progressed according to accepted service level timelines and thresholds are escalated
- Standard process for financial approvals of standard services requests
- Information regarding the status and progress of service requests is communicated to interested parties

6.4.5.4 Process Workflow Guidance



Request Fulfillment Activity Level Workflow

6.4.5.5 Activities

[RF1] Establish Request Fulfillment Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "RF process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for changes and improvements to the RF process framework.

[RF2] Log and Validate Service Request

All reported service requests must be logged in a ticket management system with relevant details (user contact information, asset information, etc.) and are categorized, prioritized and assigned to the appropriate team for fulfillment. If the request does not meet established criteria for fulfillment, it is rejected and the user notified.

[RF3] Fulfill or Route Service Request

The Service Request is analyzed to determine the appropriate team to perform the fulfillment activities. If the request is resolved within Request fulfillment, the user is contacted to verify resolution. Upon user satisfaction, The Service Request record is updated and closed. If the request is transferred to another process, all relevant information and documentation is routed to the appropriate team and the receiving process is notified about the assigned request item. Request Fulfillment retains ownership of the Service Request and tracks fulfillment progress through user acceptance and closure.

[RF4] Obtain Acceptance and Close Service Request

This activity examines the work history of a Service Request with a '*Resolved*' status. It ensures that all required documentation is complete, including resolution details, effort expended and outcome. A review of appropriate classification and prioritization is conducted and stakeholder agreement with resolution activity and status is obtained for formal closure.

[RF5] Monitor, Manage and Report Request Fulfillment

This activity ensures all service requests are effectively and efficiently managed throughout the process life cycle. All request data and status changes are examined for consistency and recorded in Service Request records.

[RF6] Evaluate Request Fulfillment Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Request Fulfillment process. It includes the capture of information, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Request Fulfillment process remains fit for purpose and identifies where changes to the process might be required.

6.5 Continual Service Improvement (CSI) Domain

To successfully achieve the mission of the Department Of Defense (DoD) all Military Services and Defense Agencies must align their strategic plans, development efforts, and operational efforts. It is critical that all agencies and mission partners share information to provide capabilities and services that enable joint war fighting. It is imperative to constantly look for ways to improve services. With technology changing so quickly and providing more and improved features, it is necessary to improve services not only to gain a competitive edge, but in many instances simply to better protect the war-fighter, DoD data and to stay current.

CSI combines techniques, practices, principles and methods from quality management and change management to achieve improvement in processes, service delivery and quality.

Domain Metrics

Metrics are actionable measures for decisions related to improving the performance of a process and guiding resource allocation. Metrics must be viewed in an overall context of the DESMF. As processes are improved, current metrics are reviewed and analyzed to ensure continued or newly developed measures are in place.

6.5.1 Purpose

CSI combines practices, methods and principles from quality management and service measurement practices. The purpose of CSI is to ensure services provided within DoD remain aligned with mission objectives and the ever-changing needs of the consumer. This must be accomplished in concert with improving and maintaining quality and performance of services. This is accomplished through two cooperative objectives. Agencies and mission partners should measure and plan for the improvement of the service management processes that support the strategy, design, transition and operations of these services. Secondly, Agencies and mission partners should measure and plan for improvement in performance of current services.

6.5.2 Scope

The scope of CSI encompasses all DoD services, internal and external, and the service management processes that support those services.

6.5.3 Benefits and Expected Outcomes of CSI

- Service Owners and Process Owners have a process for understanding ways to improve their areas of accountability
- Improved Return on Investment (ROI) and Return on Value (ROV)
- Quality of services improves
- Quicker recognition of performance issues, allowing for less costly resolutions

- Ensures that services remain aligned to mission
- Better information for planning
- A standardized method for measuring services and processes
- Standardized process for monitoring and reporting on technology metrics, process metrics and service metrics

6.6 Domain Relationships Table

This table provides an overview of relationships between the domains previously described. To read the table the domains in the columns are the 'FROM' domain providing information to the domains represented in the rows. For example, the Service Design (SD) domain (SD column – From) provides 'Capacity numbers' "TO" the SS (Service Strategy) domain (SS row).

From To	Service Strategy (SS)	Service Design (SD)	Service Transition (ST)	Service Operations (SO)	Continual Service Improvement (CSI)
SS		Capacity numbers Service Level Agreements (SLA)	Change Information Effectiveness of strategy moving into production Financial information from assets	Feedback on strategy for production services Usage measure-ments Mission partner interfaces for requirements Financial reporting	Measurement of Strategy processes Cost information related to efficiency recommendation
SD	Strategic Security Policy Service Portfolio		Configuration Item (CI) information for capacity and design Move service to	Usage measure-ments Performance related	Measurement of Service Design processes Recommenda-tions

From To	Service Strategy (SS)	Service Design (SD)	Service Transition (ST)	Service Operations (SO)	Continual Service Improvement (CSI)
	information Service Catalog Financial costs of services Demand Strategy		production Test services Collaborative effort on Service Design Package (SDP)	statistics Incidents related to design failure	related to performance of services Reports on Service Level Management (SLM) information
ST	Guidance for change approval Financial guidance for service implementa-tions Budget information	Service specifica-tions Deploy-ment and test support Specifica-tions for evaluation		Deployment support ASI Support Access to facilities	Measurement of Service Transition processes Analysis of Knowledge Management information
SO	Intent of services	Event manage-ment alert	Releases		Measurement of Service Operations

From To	Service Strategy (SS)	Service Design (SD)	Service Transition (ST)	Service Operations (SO)	Continual Service Improvement (CSI)
	Budget information Governance	criteria Services operating procedures Access manage-ment information OLA/SLA information	Change information Fulfillment of Problem Management		processes Analysis of performance issues Trending information
CSI	Overall Strategy Targets	SLM information Design Specifications from SDP	Changes in architecture Changes in services to measure	Mission partner satisfaction reports Raw data related to service and infrastructure	

7 Supporting Functions

A function is described as a team, organization unit or group of people that specialize to perform certain activities or types of work. They typically have the similar skill sets and resources to carry out their duties to achieve specific outcomes. The function is responsible for defining the standards and procedures to be followed when operating within the function. The table below identifies the functions described in the DESMF, their primary and secondary Domains, and the processes with which they are most closely associated. It is a challenge to include functions in this framework, as these functions already exist, have been in existence for some time, and already have processes and procedures with some level of effectiveness. In addition, there are many standards that exist to guide individual functions outside those most commonly referenced in this document. The benefit gained in this document by the functions, is the understanding of standardized integrated processes and how functions fit into the overall service management framework as services are delivered to DoD mission partners.

7.1 Roles and Responsibilities within Functions

While all functions have unique roles and responsibilities, they also have two roles in common: Function Owner and Function Manager.

The **Function Owner** has the following responsibilities:

- Make sure the functions design includes the policies of the processes that are performed as part of the function
- Ensure that the function follows the governance guidelines of the appropriate governing bodies
- Ensure the integration of various processes utilized in the function
- Coordinate with the various Domain Owners with relation to their processes
- Coordinate with Process Owners to suggest improvements to their processes

The Function Owner must have the authority to direct members across Domains. Therefore, Function Owners must be a senior level manager.

The **Function Manager** is responsible to the Function Owner and performs day-to-day operational and managerial tasks demanded by the function. The Function Manager does not necessarily fall into the Function Owner's chain of command. The Function Manager has the following responsibilities:

- Monitor the function, using qualitative and quantitative Key Performance Indicators (KPI) and make recommendations for improvement
- Play a key role in developing requirements for and maintaining the function's tools
- Escalate questions related to the function
- Identify training requirements of all support staff and ensure proper training is provided to meet the requirements

- Provide metrics and reports to management and mission partners in accordance with outlined procedures and agreements

Figure 7.0 - Functions Relationship Table

Function	Primary Domain	Primary Domain Processes	Secondary Domain(s)	Secondary Domain Processes
Service Desk	Operations	1. Incident Management 2. Request Fulfillment 3. Event Management 4. Problem Management 5. Access Management	Transition	1. Configuration Management 2. Change Management
Application Management	Operations	1. Request Fulfillment 2. Incident Management 3. Problem Management	Transition Strategy	1. Release and Deployment Management 1. Service Portfolio Management
Engineering	Design	1. Service Level Management 2. Capacity Management	Operations Transition	1. Event Management 2. Problem Management 1. Service Validation & Testing
IT Operations Management	Operations	1. Event Management 2. Incident Management 3. Problem Management 4. Access Management	Design	1. Service Level Management 2. IT Service Continuity Management 3. Information Security Management
Technical Management	Operations	1. Incident Management 2. Problem Management 3. Event Management	Design Transition	1. Capacity Management 2. Availability Management 1. Service Validation & Testing 2. Knowledge Management

7.2 Service Desk

7.2.1 Purpose

As the single primary point of contact, the Service Desk is the interface between the user and the service. If there is an issue whether it be an unclear Event or Alert message, an Incident or Problem, or an Access issue, the user is going to contact the Service Desk for assistance if the issue cannot be resolved through self-help methods.

The purpose of the Service Desk is to:

- Be primary contact point for all calls, questions, service requests, complaints, and remarks
- Be primary provider of ongoing monitoring and management of mission partner satisfaction through appropriate communication channels
- Manage the incident lifecycle

As other processes mature, the Service Desk becomes more involved in areas such as Configuration Management, but the primary purposes above remain the same.

7.2.2 Scope

There are different concepts of operation, environments established and therefore differing scopes for Service Desk support. The scope of the Service Desk is also sometimes determined by the Service Level Agreements (SLAs) that were defined during mission partner negotiations.

7.2.3 Benefits and Expected Outcomes of a Service Desk

- Mission partner satisfaction – the mission partner is generally better served and better satisfied through the establishment of a single point of contact for all incidents and service requests.
- Decreases in overall business impact of incidents – Incidents are handled more efficiently through the Service Desk due to consistent use of process, procedures, and tools for resolution.
- Cost reduction – Service Desk construct reduces duplicative efforts through better communication and shared knowledge during incident resolution.
- Better C2 – Single point of information flow ensures consistency in reporting to decision makers during service outages.
- Reduction in redundancy and better implementation of global solutions through greater knowledge sharing.
- Increased mission partner satisfaction though quicker resolution, better communication, and stricter adherence to SLAs.
- Reduction in service outages and overall time to restore services.

7.2.4 Relationship to other Functions

- **Application Management** - Provides second tier support during incident resolution, especially as it relates to the business applications and systems.
- **Engineering** - Provides third tier support during incident resolution, especially as it relates to the IT infrastructure and systems
- **IT Operations Management** - Provides second tier support during incident resolution, especially as it relates to the services monitored through operations. Will relay to Service Desk any issues related to productions activities, job scheduling, and operational failures
- **Technical Management** – Provides second level support during incident resolution, especially as it relates to the IT infrastructure

7.2.5 Relationship to Processes

- **Access Management** - Provides support in granting access to mission partners and users
- **Change Management** – Participate in Change Advisory Boards (CABs) and track changes against incidents
- **Configuration Management** – Service Desk personnel may also be designated to fill the role of Configuration Management Librarian if appropriately trained
- **Event Management** – Provides support when there is an event.
- **Incident Management** – Primary executer of the incident management process and procedures. Takes ownership of all incidents
- **Problem Management** – Participates in problem resolution and trend analysis
- **Request Fulfillment** – Primary point of contact for coordinating mission partner requests for services as well as informational requests
- **Service Level Management** – Performs requests in conjunction with established SLAs and OLAs. Service Desk monitoring is also used to inform SLM of SLA breaches.

7.3 Application Management

7.3.1 Purpose

The purpose of Application Management is to support the lifecycle of applications (requirements, development, build, deployment, operation, optimization, and retirement) that enhance the Department of Defense (DoD) ability to provide services in support of its mission.

7.3.2 Scope

The scope of Application Management encompasses the lifecycle of all applications, provided by a vendor or developed in-house, from understanding the strategic goals of DoD and its mission partners to the retirement or discontinued use of the application. This includes ensuring that the applications sustain the services in the production environment. Basically, this covers any software, other than operating systems and firmware that resides on the IT Infrastructure in support of DoD services.

7.3.3 Benefits and Expected Outcomes of Application Management

- Much greater focus on software and software development in support of service
- More efficient incident resolution related to applications issues
- Reduced cost of service implementations through better control of application configuration items
- Better visibility into the Application Management processes resulting in lower risks and higher quality
- A standard set of processes for deployment of software
- Centralized control of software licensing, control of software versioning, and the management of a definitive software library
- Better applications portfolio management through centralization and consistent analysis of software options and consolidation of software options
- Better at meeting cost, quality, schedule, and performance goals.

7.3.4 Relationship to other Functions

- **Engineering** – Application Management provides specifications and maintenance information for the new or changed services
- **IT Operations** - Provides event management requirements to IT Operations, and guidance on operational management of the technology
- **Service Desk** – Coordinates with Application Management on any issues related to application incidents
- **Technical Management** – provides specifications to Technical Management for applications performance configuration and storage requirements

7.3.5 Relationship to Processes

- **Capacity Management** – Determines resources required from infrastructure components for Capacity Management
- **Configuration Management** – Records application CI's and changes to CI fields as they relate to deployment
- **Event Management** – Provides required alerts for IT Operations
- **Incident Management** – Provides resources for resolution of application incidents
- **Information Security Management** – Identifies security information for access to vendor software, and for any security bypasses used by purchased software, especially software used for monitoring
- **IT Service Continuity Management** – Plans for recovery services as related to applications
- **Problem Management** – Provides resources for resolution of application problems
- **Service Level Management** – Provides performance throughput information
- **Service Portfolio Management** – provides requirements and prioritization of application development efforts
- **Service Validation and Testing** – Provides testing of changes and services as related to applications, as part of the required segregation of duties.
- **Strategy Generation Management** - Provides requirements, needs and wants from stakeholders
- **Supplier Management** – supports and often manages suppliers of software

7.4 Engineering

7.4.1 Purpose

Engineering designs, builds, and maintains services and products, to include supporting systems and infrastructure, (hardware and software,) that allows the Department Of Defense (DoD) to successfully accomplish its mission. The systems and services must perform and function as required by the mission partner, allow for standardized integration into the architecture, meet agreed levels of reliability and availability, maintain data integrity, and be secure.

7.4.2 Scope

The scope of Engineering encompasses the entire lifecycle of the enterprise architecture. This includes from understanding the strategic goals of DoD and its mission partners, to the design, construction, and testing of new and changed services, deployments into production, and ensuring that the services are maintainable in the production environment. Engineering may also need to take a role in the event a service is retired or discontinued.

7.4.3 Benefits and Expected Outcomes of Engineering

- Improved management - By defining processes for all of engineering projects to follow, schedules and budgets are better controlled, and higher quality is achieved
- Reduction in turnover impact – Standardized processes lessens the impact of staff turnover, and handing projects off to different teams
- Quality Assurance – Standardization of engineering processes ensures quality and compliance to various internal and external regulations
- Better C2 – Information flow is consistent with other functions through the service lifecycle
- Engineering projects should have governance and Domain phase gates for more consistent approvals and communication
- All engineering projects should have a holistic view of DoD services

Engineering should work with the user community to establish a rigorous requirements process that establishes a user approved baseline set of requirements; provides for requirements traceability to originating documents and to the various CIs, architectures, and test scenarios; and incorporates CM into the establishment of new requirements along with changes to existing requirements. This will enable better requirements definition up front in the planning and design phases.

7.4.4 Relationship to other Functions

Application Management - Provides the software development and ongoing activities related to software that support the services designed in Engineering

IT Operations - Provides event management requirements to engineering. Reports back to engineering on performance and trending analysis for service related issues

Service Desk – Coordinates with Engineering on any issues related to changes to productions services and projected support related items from new and changed services

Technical Management – Engineering provides specifications and maintenance information for the new or changed services in order to allow Technical Management to perform their custodial duties related to the infrastructure. Technical Management provides current configuration data to Engineering

7.4.5 Relationship to Processes

- **Business Relationship Management** - Provides requirements, needs and wants from stakeholders
- **Change Management** – Approval of the service design package triggers engineering activities
- **Configuration Management** – Responsible for recording new infrastructure CIs and changes to CI fields as they relate to the new and changed services
- **Event Management** – Provides required alerts for IT Operations
- **Information Security Management** – Defines event management parameters related to security breaches. Defines security requirements for services
- **IT Service Continuity Management** – Plans for recovery of new and changed services
- **Service Level Management** – Provides engineering with requirements related to availability, capacity, and disaster recovery
- **Service Portfolio Management** – Determines strategy and priority for engineering projects
- **Service Validation and Testing** – Provides testing of changes and services, as part of the required segregation of duties.

7.4.6 Additional Resources

Many systems engineering process standards and models exist that describe best practices in accomplishing systems engineering. Some of the many sources available are listed below:

• ISO/IEC 15288, Systems Engineering-System Life Cycle Processes

• ANSI/EIA 632, Processes for Engineering a System

• IEEE 1220, Application and Management of the Systems Engineering Process

• EIA 731, Systems Engineering Capability Model

• CMMI, Capability Maturity Model Integration

• Defense Acquisition Guidebook, Chapter 4

• AFI 63-1201, Life Cycle Systems Engineering

- IEEE/EIA 12207, Software Life Cycle Processes
- Air Force Weapon System Software Management Guidebook

7.5 IT Operations

7.5.1 Purpose

The purpose of IT Operations is to ensure alignment of three primary areas of responsibility with the DoD mission and services. These areas are:

- Management of the day-to-day activities supporting the IT infrastructure
- Operations Control
- Facilities Management

7.5.2 Scope

IT Operations encompasses all hardware (owned or deployed on behalf of DoD), all software that runs on the infrastructure, and all network components. It includes monitoring and reacting to events that impact the environment, job scheduling, performing backups and restores, output management and IT Service Continuity Management (ITSCM) activities. Command Centers, Data Centers, and outsourced facilities fall within the management scope of IT Operations.

7.5.3 Benefits and Expected Outcomes of IT Operations

- Continuous monitoring of services - Outages and performance degradation of services can be mitigated more efficiently through earlier detection
- Better conflict resolution – Centralized operations eliminates conflicting computer resources through holistic scheduling of events in the environment
- Cost reduction – IT Operations construct reduces duplicative efforts
- Better C2 – Single point of information flow ensures consistency in distribution of changing operational priorities
- Agencies and mission partners will better align IT Operations to DoD mission goals
- IT Operations should have SLAs, recognized cost of services, and agreement of requirements for moving new and changed services into production
- IT Operations is represented throughout the service lifecycle

7.5.4 Relationship to other Functions

- **Application Management** - Provides guidance to IT operations about how best to carry out the ongoing operational management of applications
- **Engineering** - Provides event management alerts. Assists in establishing monitoring and documentation for services
- **Service Desk** – Coordinates with IT Operations on any issues related to productions activities, job scheduling, and operational failures

- **Technical Management** – Provides technical knowledge and expertise related to managing the IT infrastructure

7.5.5 Relationship to Processes

- **Access Management** - Provides support in granting access to mission partners and users as it relates to facilities
- **Change Management** – Coordinate maintenance and modifications to infrastructure components
- **Configuration Management** – Responsible for recording new infrastructure CIOs and changes to CI fields, such as location
- **Event Management** – Primary human responder to alerts
- **Incident Management** – Monitors for, records, and coordinates with the Service Desk for all infrastructure and job scheduling incidents
- **Information Security Management** – Assigns facilities and physical security processes and policies. Designs event management parameters related to security breaches
- **IT Service Continuity Management** – Primary executer of ITSCM plans. Primary tester of ITSCM plans
- **Problem Management** – Participates in problem resolution and trend analysis
- **Service Level Management** – Monitors and reports on events as related to SLAs. Owns recovery of infrastructure within SLA parameters. Function is prominent in OLAs

7.6 Technical Management

7.6.1 Purpose

The purpose of Technical Management is to provide expertise and knowledge to build and maintain the infrastructure throughout the lifecycle of services to include design, testing, implementation, operations, and retirement. Technical Management ensures that the DoD has access to the right resources to manage technology in alignment with mission objectives and strategic goals.

7.6.2 Scope

The scope of Technical Management covers the lifecycle of the infrastructure, from understanding the strategic goals of DoD and its mission partners, to the design, construction, and testing of changes in support of the mission, to the deployments into production, while ensuring that the infrastructure supports the services in the production environment. Technical Management will take a role in the event a service is discontinued, or the infrastructure to maintain service levels requires upgrades or replacement to infrastructure components.

7.6.3 Benefits and Expected Outcomes of a Technical Management Function

- Individual infrastructure service components are managed more effectively because staff are adequately trained and skilled
- More efficient incident resolution related to infrastructure issues
- Reduced cost of service implementations through better control of infrastructure configuration items
- Better Financial Management and understanding of the relationship of high cost infrastructure to service.
- Structure should exist to set goals and plans for the technical department in business expertise and technology
- Establishment of training programs to move technicians into management

7.6.4 Relationship to other Functions

- **Application Management** – provides specifications to technical management for infrastructure support requirements.
- **Engineering** – Technical Management provides specifications and maintenance information for the new or changed services
- **IT Operations** - Provides event management requirements to IT Operations, and guidance on operational management of the technology
- **Service Desk** – Coordinates with Technical Management on any issues related to infrastructure incidents

.

7.6.5 Relationship to Processes

- **Business Relationship Management** - Provides requirements, needs and wants from stakeholders
- **Capacity Management** – Determines resources required from infrastructure components for capacity management
- **Configuration Management** – Responsible for recording new infrastructure CIs and changes to CI fields as they relate to infrastructure upgrades
- **Event Management** – Provides required alerts for IT Operations
- **Incident Management** – Provides resources for resolution of infrastructure incidents
- **Information Security Management** – Identifies security information for access to infrastructure components and firmware
- **IT Service Continuity Management** – Plans for recovery of new and changed services as related to infrastructure
- **Problem Management** – Provides resources for resolution of infrastructure problems
- **Service Level Management** – Provides performance throughput information.
- **Service Validation & Testing** – Provides testing of changes and services as related to infrastructure, as part of the required segregation of duties
- **Supplier Management** – supports and often manages suppliers of infrastructure components

8 References

ISO/IEC 20000® – an international standard that promotes the adoption of an integrated process approach to effectively deliver managed services to meet business and mission partner requirements; ISO/IEC 20000 is well recognized as the world-wide standard for IT Service Management.

COBIT® (Control Objectives for Information and related Technology) - a business-oriented set of standards for guiding management in the sound use of information technology; COBIT® originates from the Information Systems Audit and Control Association (ISACA).

ITIL® (Information Technology Information Library) – a globally recognized framework representing the most widely accepted best practices approach to IT Service Management in the world.

LSS (Lean Six Sigma) - a business management strategy focusing on the reduction of errors and variation through the use of quality management and statistical methods.

CMM (Capability Maturity Model) – a standard used to identify relative process maturity; the standard is used to benchmark process maturity and is used to aid organizational process-improvement

JCIDS (Joint Capabilities Integration and Development System) – Manual identified in the Appendix, provides further details regarding the DOTMLPF-P.

ITSM CoP (ITSM Community of Practice) – Located on the Defense Enterprise Portal, the ITSM CoP is available to anyone with a .mil email address and allows access to ITSM artifacts and news, including the DESMF and associated supplements.

APAN (All Partners Access Network) - an unclassified network allowing information exchange and collaboration between the United States Department of Defense (DoD) and any external country, organization, Agency or individual that does not have ready access to traditional DoD systems and networks (non .mil email addresses). APAN provides access to the DESMF, allowing industry partners to participate in its development.

NPRM (Navy Process Reference Manual) - a model developed by the U.S. Navy; based on industry best practices including ITIL, ISO 20k, and COBIT 5.0. It covers 34 ITSM processes. Outcomes listed in DESMF 2.0 were leveraged from the NPRM. Please refer to the document for additional info.

9 Acronyms

AcM	Access Management
AM	Asset Management
AOR	Area of Responsibility
APAN	All Partners Network
AV	All Viewpoint
AvM	Availability Management
BCL	Business Capability Lifecycle
BPF	Business Process Framework
BRM	Business Relationship Management
C&A	Certification and Accreditation
CA	Change authority
CAB	Change Advisory Board
CapM	Capacity Management
CC/S/A's	Combatant Commands/Services/Agencies
CDRL	Contract Deliverable Requirements List
CEP	Chief Engineering Panel
CfM	Configuration Management
ChM	Change Management
CI	Configuration items
CJCS	Chairman of the Joint Chiefs of Staff
CMM	Capability Maturity Model
CND	Computer Network Defense
CNSS	Committee on National Security Systems
COBIT	Control Objectives for Information and related Technology

CONOPS	Concept of Operations
COOP	Continuity of Operations
CPC	Common Process Control
CSF	Critical Success Factors
CSI	Continual Service Improvement
CV	Capability Viewpoint (CV)
DAMS	Defense Acquisition Management System
DC	Design Coordination
DCO	Defensive Cyber Operations
DCR	DOTMLPF-P Change Request/Recommendation
DESMF	Department of Defense Enterprise Service Management Framework
DFARS	Department of Defense Federal Acquisition Regulation Supplement
DISA	Defense Information Services Agency
DIV	Data and Information Viewpoint
DM	Demand Management
DML	Definitive Media Library
DoD CIO	Department of Defense Chief Information Office
DoDAF	Department of Defense Architecture Framework
DODI	DOD Instruction
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership & education, Personnel, Facilities & Policy
EM	Event Management
EMS	Event Management System
eTOM	enhanced Telecom Operations Map
EXCOM	Executive Committee
FAR	Federal Acquisition Regulation

FIPS PUB	Federal Information Processing Standards Publication
FM	Financial Management
GIS	Geospatial Information Services
ICD	Initial Capabilities Document
IM	Incident Management
IPT	Integrated Project Teams
ISACA	Information Systems Audit and Control Association
ISM	Information Security Management
ISMS	Information Security Management System
IT	Information Technology
ITESR	DoD IT Enterprise Strategy and Roadmap
ITIL	Information Technology Infrastructure Library
ITSCM	IT Service Continuity Management
ITSM	Information Technology Service Management
ITSM CoP	ITSM Community of Practice
ITSMO	ITSM Office
JCAs	Joint Capability Areas
JCIDS	Joint Capabilities Integration and Development System
JIE	Joint Information Environment
KEDB	Known Error Database
KM	Knowledge Management
KPI	Key Performance Indicator
LSS	Lean Six Sigma
MAC	Mission Assurance Category
MTRS	Mean Time to Restore Service

NIST	National Institute of Standards & Technology
NMS	National Military Strategy
NRPM	Navy Process Reference Manual
NSS	National Security Strategy
OCM	Organizational Change Management
OLA	Operational Level Agreement
OMB	Office of Management and Budget
OV	Operational Viewpoint
PM-	Problem Management
PV	Project Viewpoint
QDR	Quadrennial Defense Review
RF	Request Fulfillment
RFC	Request for Change
ROI	Return on Investment
ROV	Return on Value
RMF	Risk Management Framework
SA	Situational Awareness
SCD	Supplier and Contract Database
SCM	Service Catalog Management
SD	Service Design
SDP	Service Design Package
SEC	NIST - Information Security Management process acronym
SGM	Strategy Generation Management
SIP	Service Improvement Plan
SKMS	Service Knowledge Management System

SLA	Service Level Agreements
SLM	Service Level Management
SLR	Service Level Requirements
SME	Subject Matter Expert
SMP	DoD Strategic Management Plan
SO	Service Operations
SPM	Service Portfolio Management
SS	Service Strategy
ST	Service Transition
StdV	Standards Viewpoint
SUP	Supplier Management
SV	Systems Viewpoint
SvcV	Services Viewpoint
SVT	Service Validation and Testing
SWOT	Strengths, Weaknesses, Opportunities and Threats
TCO	Total Cost of Ownership
TPS	Transition Planning and Support
TQM	Total Quality Management
UC	Underpinning Contract

10 Glossary

In most cases, the definitions provided in the ITIL V3 glossary are used. The definitions in this glossary supersede those in the ITIL glossary.

Configuration Item: Any component or other service asset that needs to be managed in order to deliver an IT service. Information about each configuration item is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by service asset and configuration management. Configuration items are under the control of change management. They typically include IT services, hardware, software, products buildings, people and formal documentation such as process documentation and service level agreements. (Source: ITIL V.3 2011)

Feature: A configuration or add-on to a product, something that may be selected from that products list of characteristics to enable functions or capabilities, often associated with additional cost for the service or product. (Source: HP Cloud Support Model, DISA ITSM Instruction)

Policies are formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of processes, standards, roles, activities, IT Infrastructure etc.

P**rocedure** is a document containing steps that specify how to achieve an activity. Procedures are defined as a part of processes. As such, a change to a procedure does not necessarily change a process, just as a change to a process does not necessitate a policy change.

Process is a structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. A process may include any of the roles, responsibilities, tools and management controls required to reliably deliver the outputs.

Product: A CI or collection of CI's that have physical characteristics, are manufactured, and are used to deliver a capability or function or series of capabilities and functions. A product is often a subset of a service, but never vice versa. In addition to this a product may be utilized by one or more services and must be fit for purpose for all services utilizing the product. (Source: HP Cloud Support Model, DISA ITSM instruction)

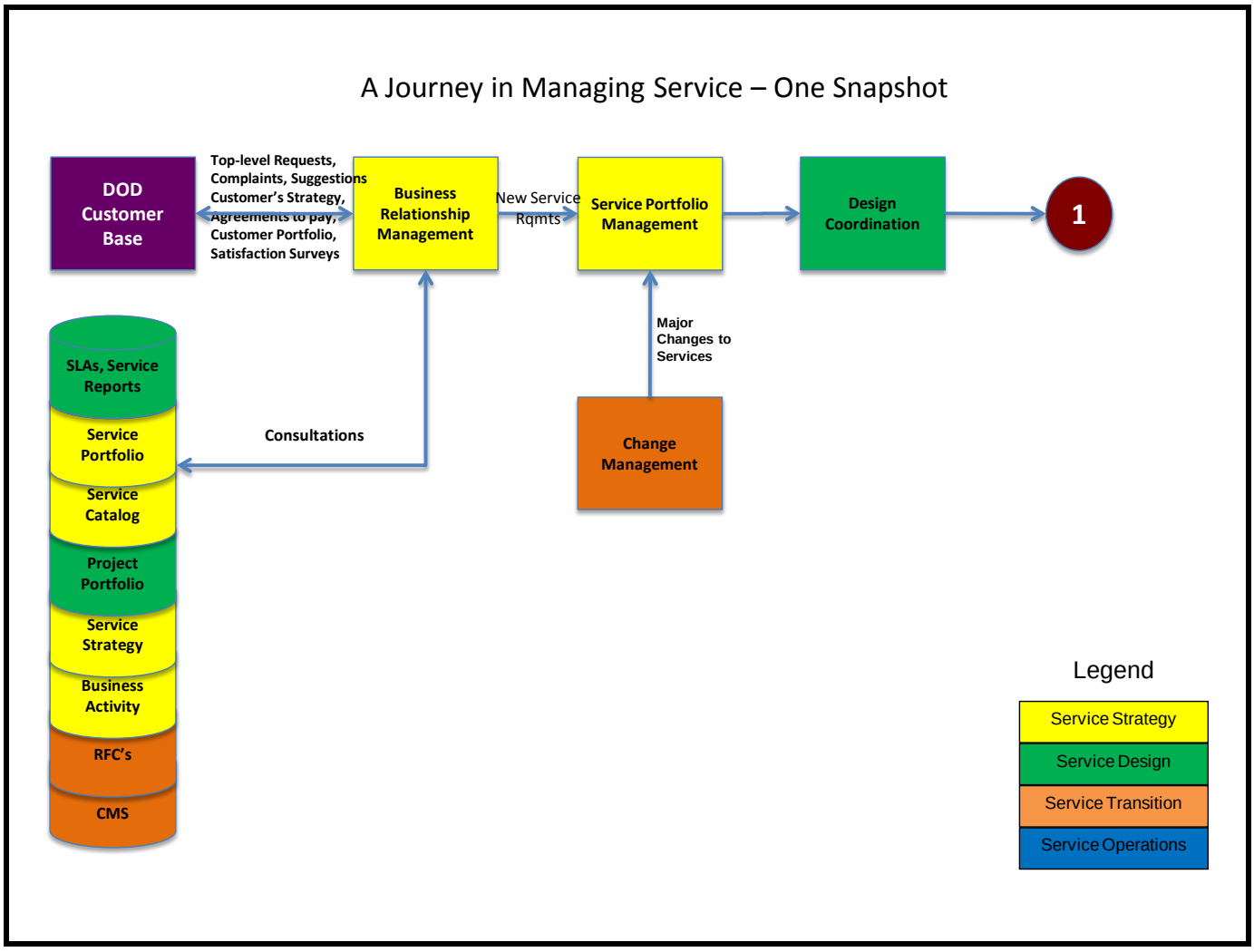
Service: A service is a means of delivering value comprised of people, processes and technology perceived by Customers and Users as a self-contained, single, coherent entity that enables them to achieve mission objectives and functions. (Source: ISO 20000, COBIT 5, ITIL V.2 & 3)

Vital Business Function: A Function of a Business Process which is critical to the success of DISA. Vital Business Functions are supported by critical business services -- those services the business depends upon. Vital Business Functions are an important consideration of Business Continuity Management, IT Service Continuity Management and Availability Management.

Appendix A: "DESMF - A Journey in Managing Service – DISA Perspective"

A framework this involved, complex and intermingled with other frameworks, methodologies and standards is difficult to articulate and illustrate pictorially. This excerpt provides dialogue and a graphical representation of one "snapshot" of the interaction between ITSM Service Domains and processes from the DISA perspective. This supporting verbiage and the illustrations are not meant to be an all inclusive rationalization of the framework, but rather a substantiation of the dichotomy that exists between the simplicity of process to process interaction and the multi-process orchestration that is paramount when implementing this framework. The circled numbers correlate to graphics.

A Journey in Managing Service



Leading up to:

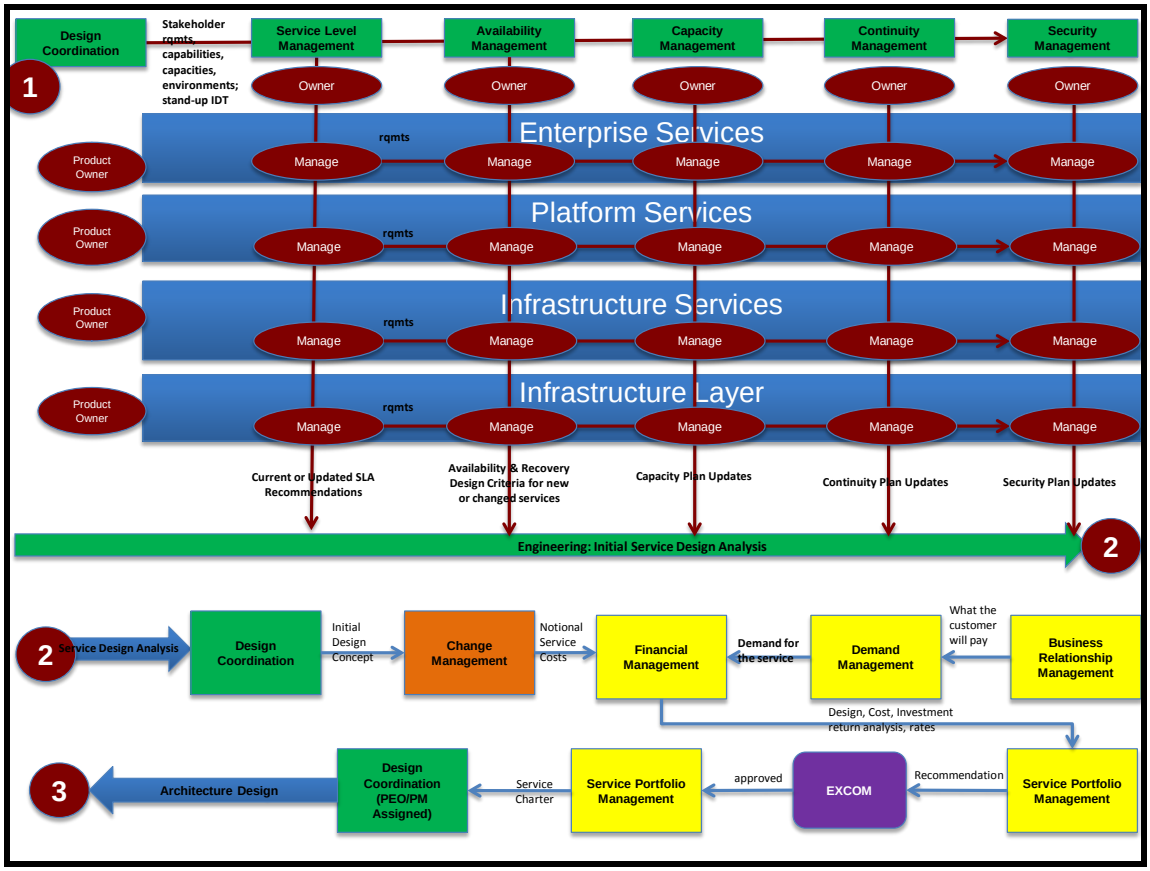
Mission partner needs and requirements are the driving forces from which DISA garners strategy and allocates investments to support. The Service Portfolio is the repository of all services. Services that are available to mission partners are shown on the Service Catalog. The remainder of the services is under consideration to either be provided or retired.

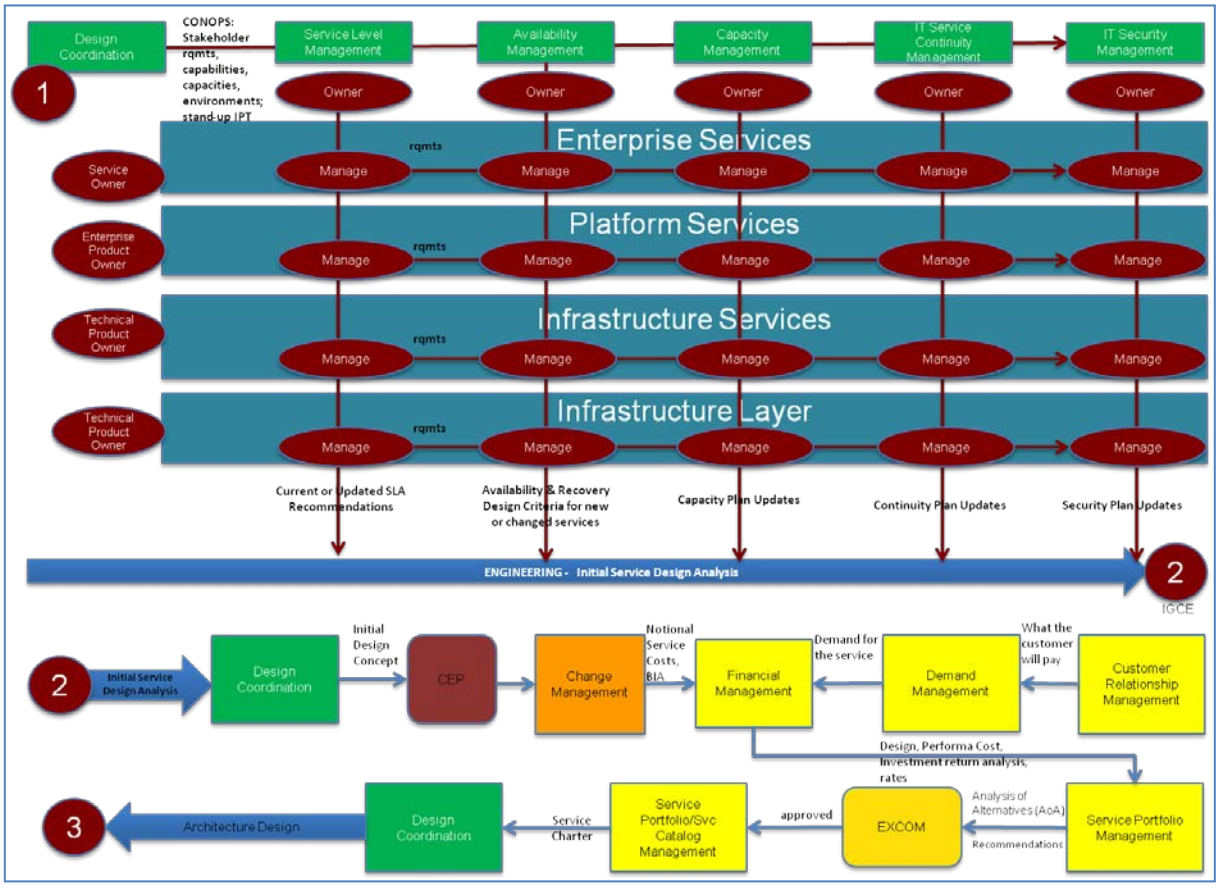
The Change Management process can launch the Service Portfolio Management process if and when there's a request for a major change to an existing service. When the decision has been made to create a new service or make a major change to an existing service, Design Coordination is initiated and is responsible for coordinating all service design activities, processes and resources.

1

Design Coordination is accountable for ensuring the consistent and effective design of the new or changed service. This is achieved through engaging Integrated Project Teams (IPT) which consists of members from all business units, i.e., Networking, Computing, Applications, Information Assurance, etc., as required, to complete the initial service design analysis.

Design Coordination activities include coordinating with other Service Design processes (Service Level Management, Availability and Capacity Management, IT Service Continuity and Information Security Management, etc.) and service and product owners to gather information about the infrastructure, technology stack, required resources, and functional area requirements for the service.





2

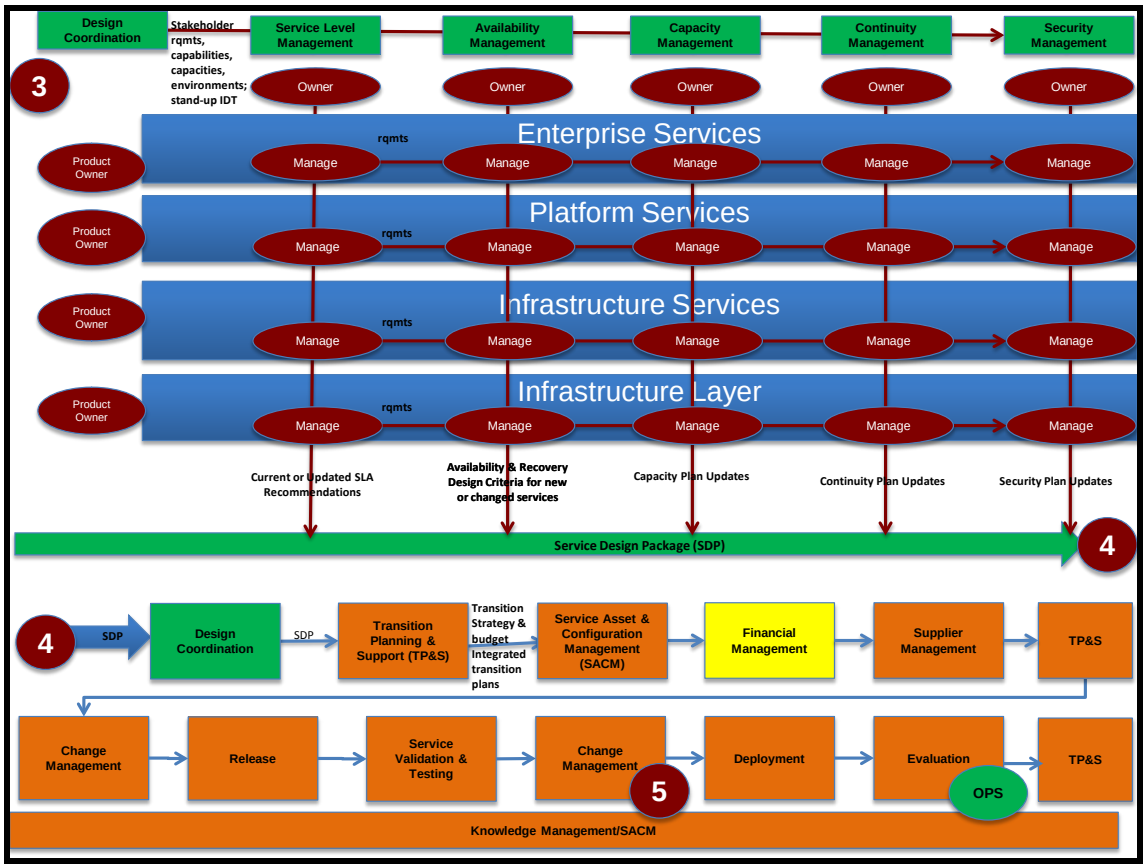
The Design Coordinator is responsible for presenting the initial design analysis or service solution to appropriate decision gates, i.e. Chief Engineering Panel (CEP) and Change Management, in order to ensure it conforms to strategic, architectural, governance and other Agency requirements.

Change Management is engaged from the aspect that information is accumulated and recorded which enable management reporting and phased documentation as the change progresses through its lifecycle. Congruently, Business Relationship Management, Demand Management and Financial Management processes have concepts about what the mission partner will pay and what the potential demand is for the service.

Service Portfolio Management assesses this information and recommendations are made to the EXCOM. The EXCOM approval results in the Service Portfolio and perhaps the Service Catalog (based on Service Catalog Management process) being updated.

3

Once the Service is chartered, Design Coordination reengages with required IPT members to fully design the service and produce a detailed Service Design Package (SDP). Details are fleshed out in great depth across the spectrum of needed support, ensuring the resources are considered and will be in place, when the service is deployed. This culminates in a very thorough and comprehensive Service Design Package (SDP) which has been vetted with processes from the other Domains.



4

Design Coordination presents the completed SDP to appropriate decision gates, i.e. Chief Engineering Panel (CEP) and prior to Service Transition Planning and Support. These two processes should be interfaced to ensure consistent overall plans and resource schedules.

Prior to releasing the service into the testing environment and employing the Service Validation and Testing process, various aspects of the service are refined through engaging other processes, such as Asset and Configuration Management, Financial and Supplier Management and Change Management.

Test results are supplied to appropriate decision gates, i.e. Change Management. If testing of the service renders positive and expected outcomes and meets the design specification and mission partner needs, the service is deployed into the production environment. Post implementation activities include a formal assessment of the new or changed service through the Change Evaluation process.

Service sustainment is accomplished through the Service Operations Domain which coordinates and carries out activities to deliver and manage the service at the agreed service levels.

All information about the service including the SDP is incorporated into the overall Service Knowledge Management System (SKMS).

In Conclusion:

This excerpt is one pathway from one perspective in the 'Journey in Managing Services'. Process relationships and integrations have many permutations and levels of abstraction, juxtapositions based on the uniqueness of the organization (size, culture, core competencies, process maturity level etc.) and service provided (number and/or complexity of services).

Appendix B: ISO/IEC 20000 Standards Information

ISO/IEC 20000, Information Technology Service Management comprises several volumes published as part of a comprehensive overhaul of the standard between 2004 and 2011. Parts 1 – 5 were used for this edition. They will be collectively referred to as ISO 20000-#, such as ISO 20000-1 for Part 1.

- ISO/IEC 20000-1:2011, Information Technology Service Management Part 1: Service Management System Requirements. Defines the Service Management System. It contains descriptions for general requirements; design and transition of new or changed services; and the requirements for service delivery, relationship, resolutions, and control processes. It contains specific "shall statements, for each topic, such as "All incidents shall be recorded."
- ISO/IEC 20000-2:2012, Information Technology Service Management Part 2: Code of Practice (ISO 20k-2) ISO 20k-2 has a similar structure to ISO 20k-1, but comprises the code of practice. It is a document with hundreds of "recommendations" a service provider should take into consideration when attempting to meet the requirements. ISO 20k-2 is similar in intention to ITIL v3, in that it describes a body of practice.

Other documents from ISO/IEC 20000 that will be or are integrated into the DESMF include:

- ISO/IEC 20000-3:2012, Information Technology Service Management Part 3: Guidance on Scope Definition and Applicability of ISO/IEC 20000-1 (ISO 20k-3). ISO 20k-3 describes how to appropriately scope ISO 20k compliance in a variety of service provider environments. It is extremely useful in creating "will/shall" accountability statements for use in multi-provider operations. This is a critical component for generating specific contract language to ensure contractor accountability to ITSM obligations, while allowing them the flexibility to execute tasks according to their own methods.
- ISO/IEC TR 20000-4:2010, Information Technology Service Management Part 4: Process Reference Model (ISO 20k-4). ISO 20k-4 is structured similarly to ISO 20k Parts 1 & 2. It contains a series of tables for each identified process or other area. The contents of each table identify the context, purpose, outcomes, and requirements traceability to other ISO 20k documents. It serves as a ready reference guide for directing and controlling activities within the Service Management System (SMS).
    - *For instances where spiral or iterative process development and implementation means that one or more processes may have to address an external dependency on another process that is not mature enough to fulfill the requirement, ISO 20000-4 provides guidance.*

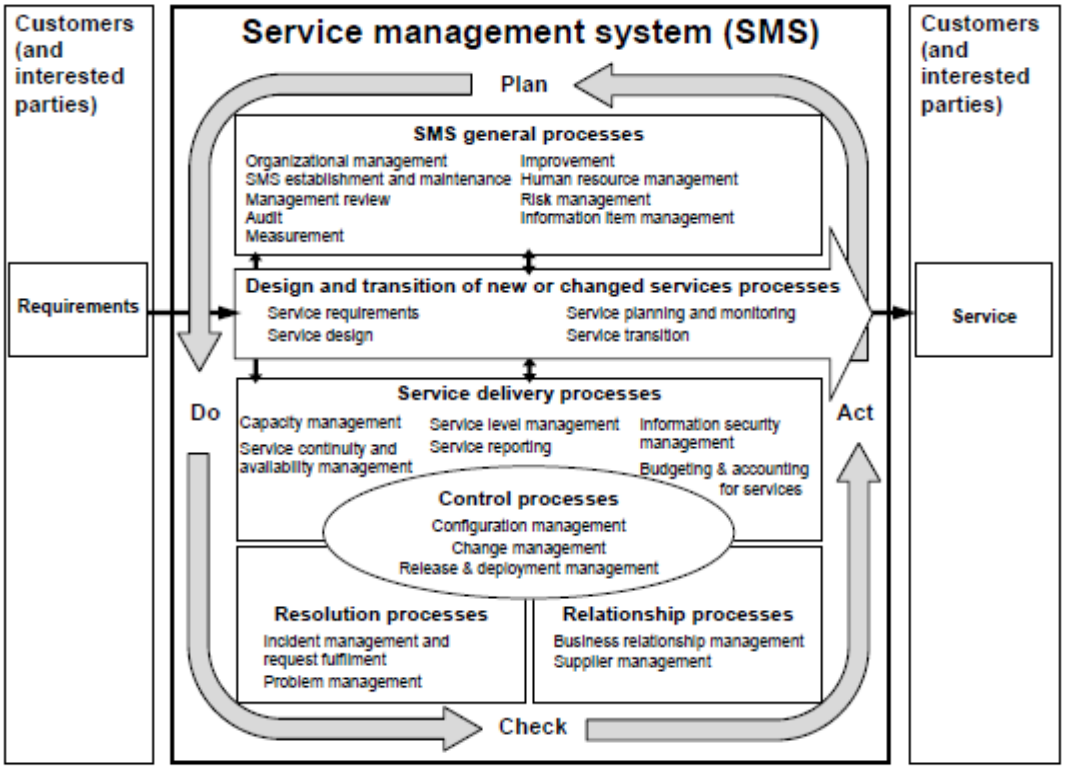


Figure 2 — Processes in the process reference model

- ISO/IEC TR 20000-5:2010, Information Technology Service Management Part 5: Exemplar Implementation Plan for ISO/IEC 20000-1 (ISO 20k-5). ISO 20k-5 contains detailed guidance for three-phased approach for implementing the SMS. It contains an extremely useful set of tables and checklists for the implementation program, and is mapped directly to the overall SMS that ISO 20k describes. It provides a very detailed and pragmatic starting point for ITSM implementation and improvement efforts.

Appendix C: DoD Architecture Framework (DoDAF)

The Department of Defense Architecture Framework (DoDAF) serves as the overarching, comprehensive framework and conceptual model enabling the development of architectures to facilitate the ability of Department of Defense (DoD) managers at all levels to make key decisions more effectively through organized information sharing across the Department, Joint Capability Areas (JCAs), Mission, Component, and Program boundaries. It is the Department's means for standardizing representation of architecture information. The DoDAF serves as one of the principal pillars supporting the DoD Chief Information Officer (CIO) in his/her responsibilities for development and maintenance of architectures required under the Clinger-Cohen Act. It also reflects guidance from the Office of Management and Budget (OMB) Circular A-130, and other Departmental directives and instructions. The current version, DoDAF V2.0 focuses on architectural data, rather than on developing individual products as described in previous versions. In general, data can be collected, organized, and stored by a wide range of architecture tools developed by commercial sources.

The purpose of DoDAF 2.0 is to support more effective decision-making by using consistent, model-based architectures that describe the relationships between mission- and operational requirements in terms of information, data, performers, and actions.

DoDAF is prescribed for the use and development of architectural models. Not all DoDAF-prescribed models need to be created. DoDAF V2.0 is "Fit-for-Purpose", based on decision-maker needs. DoDAF concentrates on data as the necessary ingredient for architecture development. Key process owners will decide which architecture models are required. However, regulations and instructions from both DoD and Chairman of the Joint Chiefs of Staff (CJCS) have particular presentation view requirements. In other words, if a model is created, it must be according to standard.

DoDAF V2.0 Viewpoints

In DoDAF V2.0, architectural viewpoints are composed of data that has been organized to facilitate understanding. To align with ISO Standards, where appropriate, the terminology has changed from Views to Viewpoint (e.g., the Operational View is now the Operational Viewpoint).

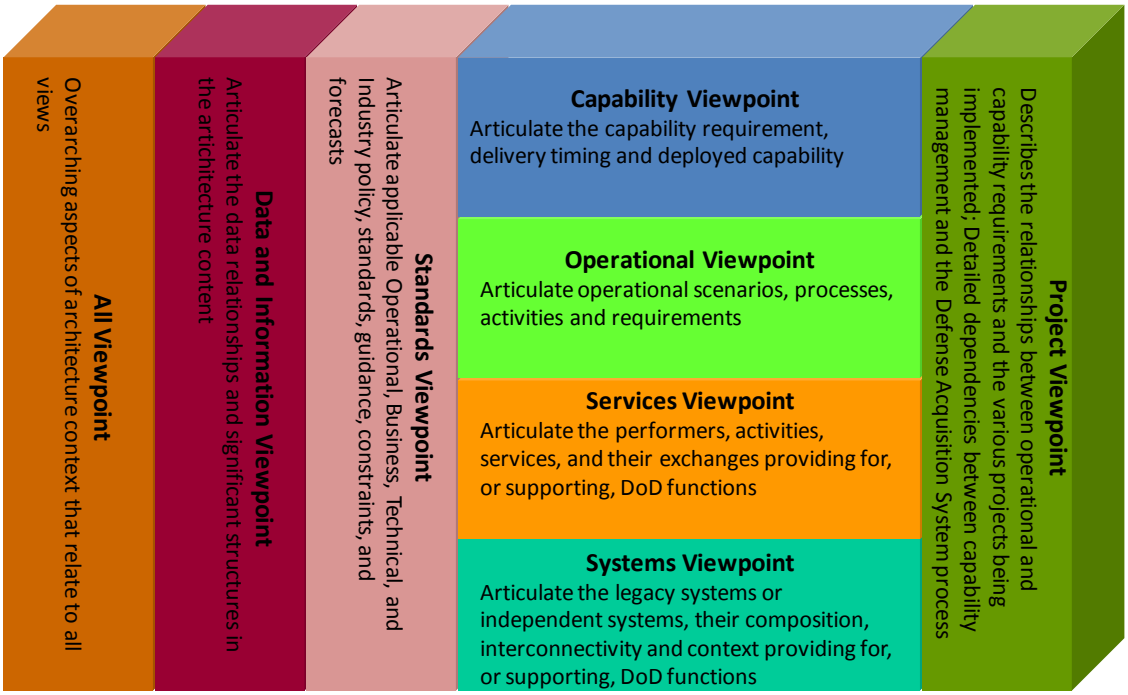


Figure 0-1 - Diagram of DoDAF V2.0 Viewpoints

Types of viewpoints include the following:

- **All Viewpoint (AV)** - Describes the overarching aspects of architecture context that relate to all viewpoints.
- **Capability Viewpoint (CV) (New in DoDAF V2.0)** - Articulates the capability requirements, the delivery timing, and the deployed capability.
- **Data and Information Viewpoint (DIV) (New in DoDAF V2.0)** - Articulates the data relationships and alignment structures in the architecture content for the capability and operational requirements, system engineering processes, and systems and services.
- **Operational Viewpoint (OV)** - Includes the operational scenarios, activities, and requirements that support capabilities.
- **Project Viewpoint (PV) (New in DoDAF V2.0)** - Describes the relationships between operational and capability requirements and the various projects being implemented. The Project Viewpoint also

details dependencies among capability and operational requirements, system engineering processes, systems design, and services design within the Defense Acquisition System process.

- **Services Viewpoint (SvcV) (New in DoDAF V2.0)** - Presents the design for solutions articulating the Performers, Activities, Services, and their Exchanges, providing for or supporting operational and capability functions.
- **Standards Viewpoint (StdV) (Renamed from Technical Standards View TV)** - Articulates the applicable operational, business, technical, and industry policies, standards, guidance, constraints, and forecasts that apply to capability and operational requirements, system engineering processes, and systems and services.
- **Systems Viewpoint (SV)** - Articulates, for Legacy support, the design for solutions articulating the systems, their composition, interconnectivity, and context providing for or supporting operational and capability functions.

The following viewpoints support the Service Management Lifecycle:

- AV-1 Overview and Summary Information
- AV-2 Integrated Dictionary
- CV-1 Capability Vision
- CV-2 Capability Taxonomy
- CV-3 Capability Phasing
- CV-4 Capability Dependencies
- CV-5 Capability to Organizational Development Mapping
- CV-6 Capability to Operational Activities Mapping
- CV-7 Capability to Services Mapping
- OV-1 High-Level Operational Concept Graphic
- OV-2 Operational Resource Flow Description
- OV-4 Organizational Resource Flow Matrix
- OV-5A Operational Activity Decomposition Tree
- OV-5B Operational Activity Model
- OV-6C Event-Trace Description

- SvcV-2 Systems Resource Flow Description
- SvcV-6 Systems Resource Flow Matrix
- StdV-1 (Final IT Standards Profile generated by the DISR online)
- StdV-2 Standards Forecast
- Svc-5 Operational Activity to Services Traceability Matrix
- Svc-7 Services Measures Matrix
- Svc-8 Services Evolution Description

Appendix D: Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities and Policy (DOTMLPF-P)

At the organization's discretion and if applicable, the Service Owner for each IT Service is responsible to include a requirements assessment within the Service Strategy of their service. The requirements assessment will include capability analysis of the Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities and Policy (DOTMLPF-P) areas to determine if a new service (as documented in an Initial Capabilities Document (ICD)) or revision of an existing service (as documented in a DOTMLPF-P Change Request (DCR)) is needed. The Service Strategy will be reviewed annually in support of the Program Evaluation Group (PEG) funding cycle to ensure each DOTMLPF-P area is compatible with the Joint Information Environment (JIE). If an ICD is created, the information will then be forwarded to the Service Design domain and the Design Coordinator to continue development. If a DCR is created to initiate an improvement, the recommendation will also be executed via a Service Improvement Plan (SIP), as part of the Continual Service Improvement (CSI) domain.

The following descriptions for each of the DOTMLPF-P areas is copied from paragraph 4b(2) of the Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS), JCIDS Manual, 19 Jan 2012. A hyperlink to this document is located in the Reference section.

(a) **Doctrine.** Fundamental principles that guide the employment of US military forces in coordinated action toward a common objective. Though neither policy nor strategy, joint doctrine serves to make US policy and strategy effective in the application of US military power. Joint doctrine is based on extant capabilities in accordance with reference z. Joint doctrine is authoritative guidance and will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise.

(b) **Organization.** A joint unit or element with varied functions enabled by a structure through which individuals cooperate systematically to accomplish a common mission and directly provide or support joint warfighting capabilities. Subordinate units and elements coordinate with other units and elements and, as a whole, enable the higher-level joint unit or element to accomplish its mission. This includes the joint staffing (military, civilian, and contractor support) required to plan operate, sustain, and reconstitute joint warfighting capabilities.

(c) **Training.** Training, including mission rehearsals, of individuals, units, and staffs using joint doctrine or joint tactics, techniques, and procedures to prepare joint forces or joint staffs to respond to strategic, operational, or tactical requirements considered necessary by the CCMDs to execute their assigned or anticipated missions.

(d) **Materiel.** All items (including ships, tanks, self-propelled weapons, aircraft, etc., and related spares, repair parts, and support equipment, but excluding real property, installations, and utilities) necessary to equip, operate, maintain, and support joint military activities without distinction as to its application for administrative or combat purposes. The letter "m" in the acronym is usually lower case since Joint DOTMPLF Change Recommendations (DCRs) do not advocate new materiel development, but rather advocate increased quantities of existing materiel capability solutions or use in alternate applications.

(e) **Leadership and Education.** Professional development of the joint leader is the product of a learning continuum that comprises training, experience, education, and self-improvement. The role of joint

professional military education is to provide the education needed to complement training, experience, and self-improvement to produce the most professionally competent individuals possible.

(f) **Personnel.** The personnel component primarily ensures that qualified personnel exist to support joint capability requirements. This is accomplished through synchronized efforts of joint force commanders and DOD components to optimize personnel support to the joint force to ensure success of ongoing peacetime, contingency, and wartime operations.

(g) **Facilities.** Real property consisting of one or more of the following: buildings, structures, utility systems, associated roads and other pavements, and underlying land. Key facilities are defined as command installations and industrial facilities of primary importance to the support of military operations or military production programs. A key facilities list is prepared under the policy direction of the Joint Chiefs of Staff.

(h) **Policy.** Any DOD, inter-agency or international policy issues that may prevent effective implementation of changes in the other seven DOTMLPF-P elemental areas.

Appendix E: NIST – Risk Management Framework (RMF) Applied to Information Security Management (SEC) [1]

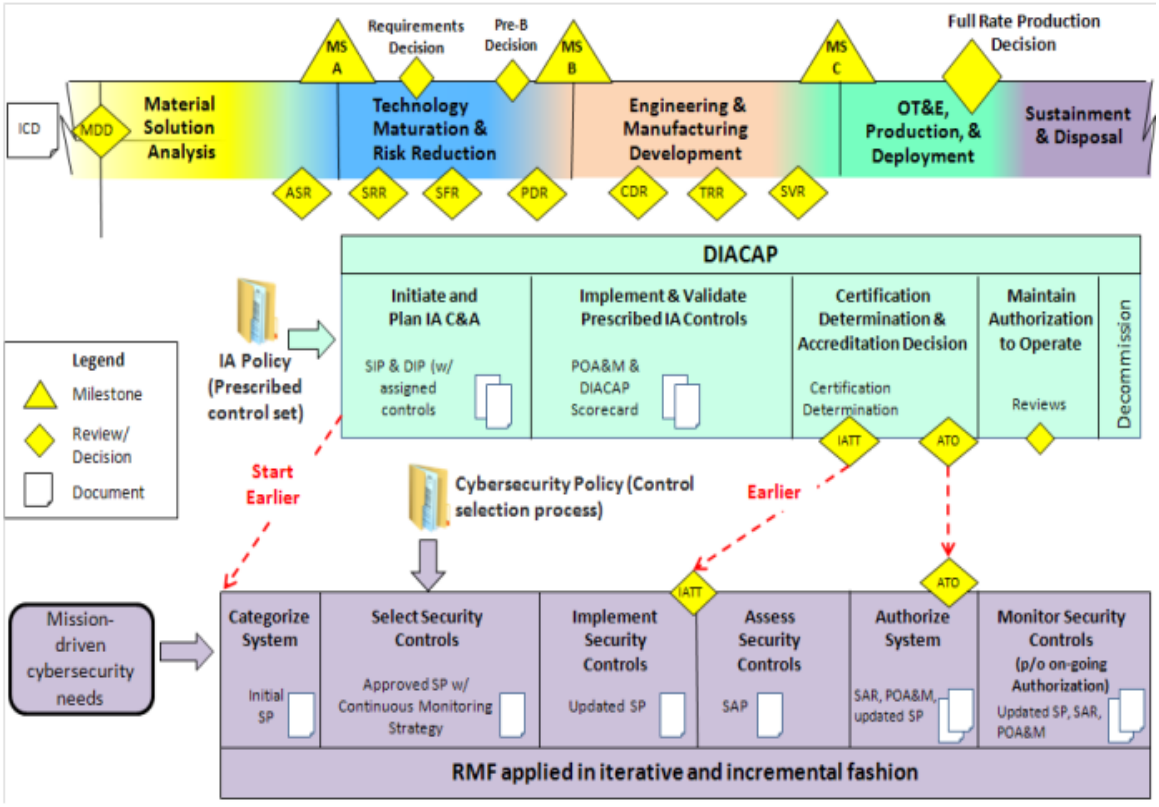
Purpose

For Information Security Management processes that come under NIST 800-53 requirements, this is a Process Workflow to consider. NIST Information Security Management ensures that security controls required to perform service management activities effectively protect information and information systems. The NIST Information Security Management activities delineated in the Process Workflow will correlate to the dashed circle in the figure below.

The figure below identifies (non-authoritative) relationships between RMF for DoD IT, DIACAP and the DoD 5000 Acquisition Framework. The figure is currently in DRAFT:

Information Security Management Activity Level Workflow

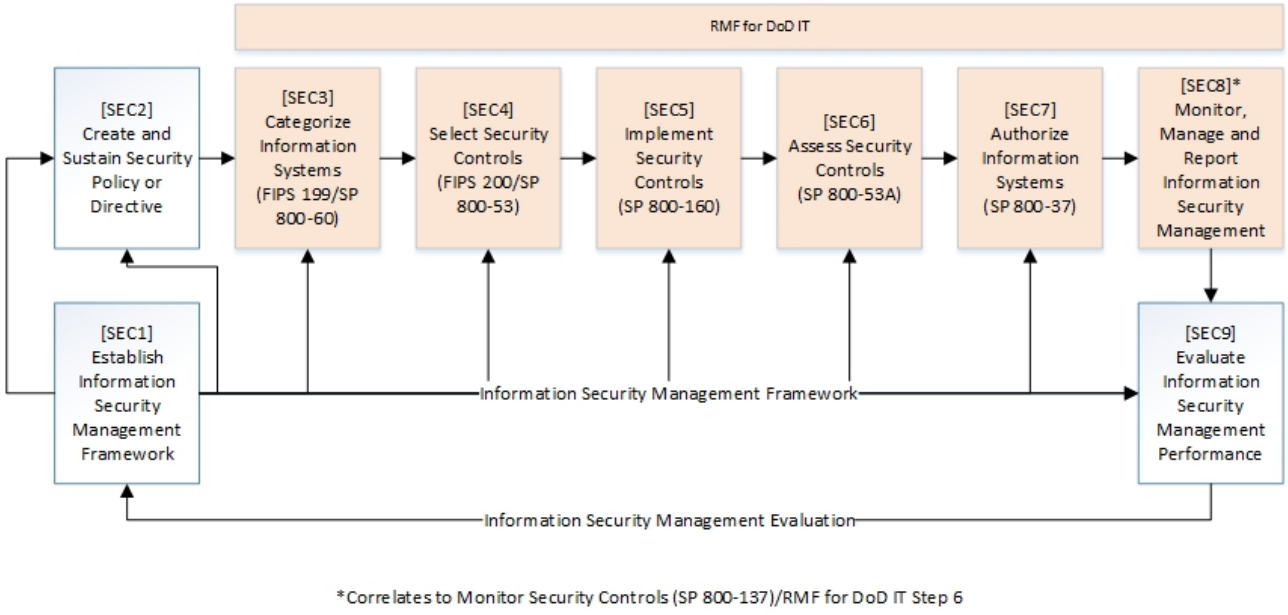
[1] Refer to DoD 8500 Series for authoritative requirements for Information Security Management



NIST – Information Security Management Outcomes

Information Security requirements are identified and established [SEC2]
Information Security risks are identified [SEC3] [SEC4]
Information Security risk is assessed [SEC4]
Assessment criteria for Information Security risks and risk appetite are identified [SEC3]
Information Security risk measures and controls are defined [SEC5]
Information Security risk measures and controls are applied [SEC5]
Information Security incidents are enumerated and recorded [SEC6]
Information Security concerns are communicated to stakeholders and interested parties [SEC8]
The impact of changes on Information Security are evaluated and reported [SEC8]

Activity Level Workflow



*Correlates to Monitor Security Controls (SP 800-137)/RMF for DoD IT Step 6

Activities[2]

[SEC1] Establish Information Security Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the "process framework" and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for making changes and improvements to the process framework. The process framework is a collection of information, not necessarily a single document.

[SEC2] Create and Sustain Security Policy or Directive

This activity incorporates the aims and objectives for the security that is to be established and operated in relation to IT services and resources. It maintains relevancy as circumstances change for both the IT service provider and its customer set. It works within the limits set for the security policy of the mission as outlined in public law, applicable DoD instructions and directives, modifying or extending its

[2] Activities assume transition from DIACAP to RMF for DoD IT

coverage to include aspects specific to information technology to enable compliance with existing regulations.

Referring to the following documents for additional guidance is encouraged:[3]

- OMB 2011 FISMA Reporting Guidance, Memorandum-11-33, regarding security reauthorization, "Continuous monitoring programs fulfill the three year security reauthorization requirement…"
- NIST SP 800-37, Revision 1, regarding security reauthorization, "…agencies are expected to conduct ongoing authorizations of information systems through the implementation of continuous monitoring programs."
- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments
- NIST SP 800-160, Security Engineering Guideline
- Update to NIST SP 800-53A, Revision 2, Guide for Assessing the Security Controls in Federal Information Systems and Organizations
- Federal Information Processing Standards Publication (FIPS PUB) 199, February 2004, Standards for Security Categorization of Federal Information and Information Systems*
- Federal Information Processing Standards Publication (FIPS PUB) 200, March 2006, Minimum Security Requirements for Federal Information and Information Systems*
- DoDi 8500.1, Information Assurance, Certified Current April 2007
- DoDi 8500.2, Information Assurance Implementation, February 2003
- CNSS Instruction 1253

[SEC3] Categorize Information Systems45

This activity involves categorizing information systems based on, at a minimum, FIPS 199 impact assessments.

Source: NIST 800-53 Rev. 4

---

[3] The list of references may not be exhaustive. DoD 8500 series is currently the authoritative source for DoD Information Assurance (IA) requirements.

[4]For [SEC3] through [SEC8], refer to the DoD 8500 Series for authoritative guidance.

[5] For National Security Systems, refer to CNSS Instruction 1253 for guidance on this activity.

This activity assigns or verifies the Mission Assurance Category (MAC) level and security classification level of information assets in order to support the Certification and Accreditation (C&A) of information systems.

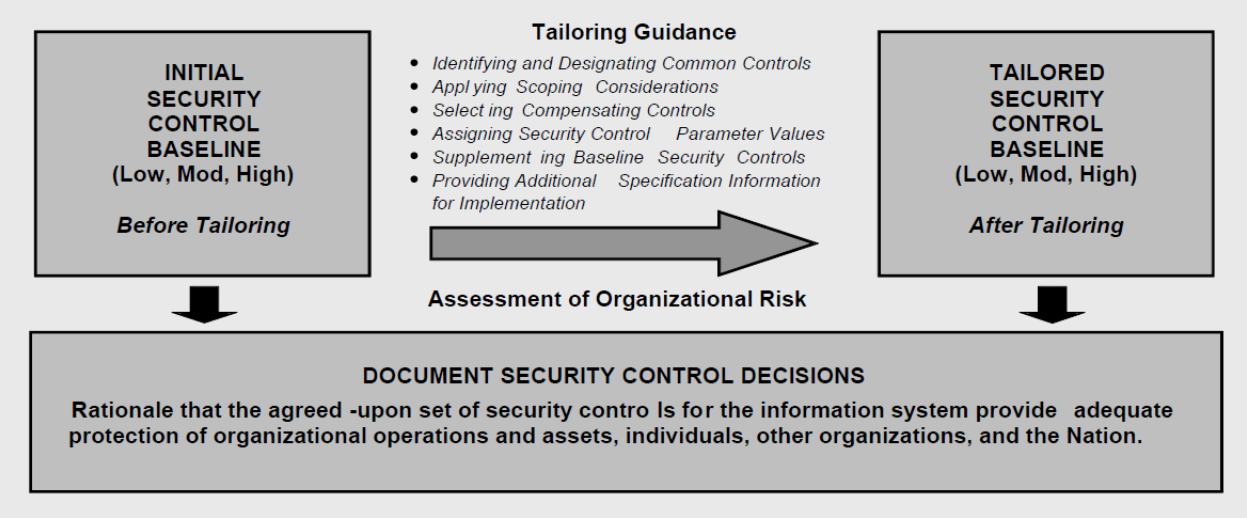
Refer to DoD 8500 series for current DoD requirements, as well as NIST Special Publication 800-60 for additional guidance.

[SEC4] Select Security Controls6

This activity involves selecting an initial set of baseline security controls based on the results of the security categorization and applying tailoring guidance (including the potential use of overlays).

The controls within NIST 800-53 are expected to replace, or have already replaced, the baseline controls listed in DoD 8500.2.

Once a baseline set of security controls are chosen, the tailoring process is used to modify and align the controls more closely with the conditions within an organization. These conditions may be related to the organization's mission, business, function, information systems, or environments of operation, which requires the use of a tailoring process.



[6] For National Security Systems, refer to CNSS Instruction 1253 for guidance on this activity.

Source: NIST 800-53

This activity identifies enterprise security threats, vulnerabilities and risks. It includes mitigation recommendations based on analysis and policy guidance from DOD Instruction (DODI) 8500 series.

An organizational assessment of risk validates the initial security control selection and determines if additional controls are needed to protect organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. The resulting set of security controls establishes a level of information security due diligence for the organization. [*Information security due diligence includes using all the appropriate information as part of an organization-wide risk management program to effectively use the tailoring guidance and inherent flexibility in NIST publications so that the selected security controls documented in organizational security plans meet the mission and business requirements of organizations.*]

A requirements definition approach and a gap analysis approach may be used in selecting security controls and control enhancements to supplement initial baselines. Organizations can select additional security controls and control enhancements from appendix F of NIST 800-53. Requirements definition focuses on defensive capability or cyber preparedness for new development. Gap analysis begins with an organizational assessment of current defensive capability or level of cyber preparedness. Gap analysis can apply to both information systems and external service providers.
Source: NIST 800-53 Rev. 4

[SEC5] Implement Security Controls

This activity involves implementing the security controls and documenting the design, development and implementation details of the controls.

Source: NIST 800-53 Rev. 4

This activity establishes the Security plan in compliance with DODI 8500 series, CJCS 6510 series, and SECNAV 5239 series. It defines and creates an appropriate security infrastructure and procedures, translates actions in the plan to security directives, and communicates them. It also makes Request for Change in the environment to realize the Security Plan.

[SEC6] Assess Security Controls

This activity involves assessing the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Source: NIST 800-53 Rev. 4

This activity executes prescribed information security controls and procedures throughout the enterprise by operating and activating protections within IT solutions and services. This activity monitors the full range of information security measures and capabilities, responds to service or authorization requests, and monitors real-time intrusion prevention/detection with established response criteria, in addition to noting information security violations and initiating incidents when required.

[SEC7] Authorize Information Systems

This activity involves authorizing information systems based on a determination of risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of the information system and the decision that this risk is acceptable.

Source: NIST 800-53 Rev 4

This activity has a strong relationship with [SEC6].

[SEC8] Monitor, Manage and Report Information Security Management [7]

This activity involves monitoring the security controls in the information system and environment of operation on an ongoing basis to determine control effectiveness, changes to the systems/environment, and compliance to legislation, Executive Orders, directives, policies, regulations, and standards.

Source: NIST 800-53 Rev. 4

This activity addresses review of security controls and mechanisms and determines whether they effectively implement security policies and procedures as described in DOD 8500 Series, and the SEC Security Plan. This activity manages documented information security violations. Security Assessments such as Blue or Red Team inspections and audits occur in this activity.

[SEC9] Evaluate Information Security Management Performance

This activity describes the tasks required to assess the efficiency and effectiveness of the Information Security Management process. It includes the capture of information on records, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure the Information Security Management process remains fit for purpose and identifies where changes to the process might be required.

[7] [SEC8] is synonymous with Step 6, monitor security controls in the RMF Framework.

Appendix F: The enhanced Telecom Operations Map (eTOM)

The enhanced Telecom Operations Map (eTOM) is a widely used Business Process Framework in the service provider industry because it provides important benefits, such as:

- It makes available a standard structure, terminology, and classification scheme for describing business processes and their constituent building blocks
- It supplies a foundation for applying enterprise-wide discipline to the development of business processes
- It provides a basis for understanding and managing portfolios of IT applications in terms of business process requirements
- It enables the creation of consistent and high-quality end-to-end process flows, with opportunities for cost and performance improvement, and for re-use of existing processes and systems
- Its use across the industry will increase the likelihood that off-the-shelf applications will be readily integrated into the enterprise, at a lower cost than custom-built applications.

The focus of eTOM is on business processes used service providers, the linkages between these processes, the identification of interfaces, and use of customer, service, resource, supplier, and other information by multiple processes.

Additional information concerning eTOM can be found at the TeleManagement Forum website:

http://www.tmforum.org/BusinessProcessFramework/1647/home.html

eTOM-ITIL Similarities and Differences

Although both eTOM and ITIL frameworks overlap in scope and have a similar approach of presenting a process view of the enterprise, there are also many differences between them. ITIL provides a framework of best practices guidance for IT service management. Just like eTOM, it is developed through consensus and is based on industry experience. Unlike the eTOM or ITIL however, ISO 20000 is a standard that has a basis in ITIL and provides standard practices for some ITIL practices against which certification can be assessed.

The table below compares and contrasts eTOM and ITIL.

eTOM to ITIL Mapping Table

	eTOM	ITIL
Context	• eTOM is a prescriptive catalogue of Process Element categories and a total business process framework for the ICT industry.	• ITIL is a set of non-prescriptive guidelines for IT/ICT Service Management.
Objective	• Provides a business process blueprint or service providers to streamline their end-to-end processes. • Enables effective communication and common vocabularies with the enterprise as well as with customers and suppliers.	• Aligns IT services with the current and future needs of the business and its customers. • Improves the quality of the IT services delivered. • Reduces long-term costs of service provision.
Scope	• Provides a top-down hierarchical view of business processes across the whole enterprise and does not address how these processes are supported by automation or human action. • Processes are developed through iterative decomposition. • Identifies the commonality of enterprise processes required among similar services for delivering high-quality, end-to-end service management. • Primary focus is service delivery to external customers.	• The ITIL processes represent flows in a number of key operational areas, with a strong orientation towards how these processes will map onto IT support environments. • Processes are developed through flows. • Offers advice and guidance on the implementation and continued delivery of service management. • Primary focus is serving internal IT customers.
Adoption	• eTOM was adopted as ITU international standards for the Telecom Sector, and primarily used by service providers in the ICT industry. ETOM is advanced by TM Forum: www.tmforum.org.	• ITIL is a set of best practices that is used by many companies worldwide and continues to be advanced by ITSMF local chapters: www.itsmf.com.
Implementation	• eTOM is a framework; the implementation will be different from organization to organization.	• ITIL is a framework. The implementation will be different from organization to organization.

Compliance	• eTOM compliance is achieved through certification of tools and applications that apply the eTOM processes to the product.	• ITIL is not a standard or set of regulations. Nothing can be deemed ITIL compliant. Processes and organizations *can* be assessed against ISO 20000.