DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:
IRM 2300-06C
C4
11 Oct 18

From: Director, Command, Control, Communications and Computers (C4)

Subj: ENTERPRISE INFORMATION TECHNOLOGY SERVICE MANAGEMENT SERVICE ASSET CONFIGURATION MANAGEMENT PROCESS GUIDE

Ref: (a) MCO 5271.1B

Encl: (1) IRM-2300-06C

1. PURPOSE. The purpose of the Enterprise Information Technology Service Management (E-ITSM) Service Asset Configuration Management Process Guide is to update the previously defined foundation for process implementation and execution across the Marine Corps Enterprise Network (MCEN). Process implementation and execution at lower levels (e.g., Regional, Local, and Programs of Record) must align with and adhere to directives and schema documented within this guide. This guide enables USMC Information Technology (IT) activities through promoting standardization of work instructions and operating procedures across a continuum of document specificity.

2. CANCELLATION. IRM-2300-06B

3. AUTHORITY. The information promulgated in this publication is based upon policy and guidance contained in reference (a).

4. APPLICABILITY. This publication is applicable to the Marine Corps Total Force.

5. SCOPE.

a. Compliance. Compliance with the provisions of this publication is required unless a specific waiver is authorized.

b. Waivers. Waivers to the provisions of this publication will be authorized by Director, Command, Control, Communications and Computers (C4).

6. SPONSOR. The sponsor of this technical publication is HQMC C4, Network, Plans and Policy Division (CP).

C. O. URBINA
By direction


# Enterprise IT Service Management
# Service Asset and Configuration Management
# Process Guide

***Release Date:***
***11 October 2018***

# Document Approval / Major Revision Change History Record

This table is used for initial release and subsequent revisions. Major revisions are indicated by the number to the left of the decimal point while minor revisions are indicated by the number to the right. Major revisions are required when the intent or process is changed rendering the prior version obsolete or when the number of minor releases total twenty (20). Changes to this document shall be recorded, described and approved using the table below:

| Release Date (MM/DD/YY) | Release No. | Approvals | | Change Description |
|---|---|---|---|---|
| | | Author | Process Owner/Approver | |
| 09/21/09 | 0.1 | Printed Name | Printed Name | Draft Release |
| 11/24/09 | 1.0 | Printed Name | Printed Name | Initial Release |
| 12/03/09 | 1.1 | Printed Name | Printed Name | Updated as per RFAs post CR |
| 06/18/10 | 2.0 | Printed Name | Printed Name | Updated as per CRMs from the follow-on Task Order 13, CDRL L0012 |
| 08/24/10 | 3.0 | Printed Name | Printed Name | Updated as per CRMs from the follow-on Task Order 13, CDRL L0012 |
| 12/17/10 | 4.0 | Printed Name | Printed Name | Updated as per CRMs from the follow-on Task Order 13, CDRL L0012 |
| 02/17/11 | 5.0 | Printed Name | Printed Name | Updated as per CRMs from the follow-on Task Order 13, CDRL L0012 |
| 04/14/11 | 6.0 | Printed Name | Printed Name | Updated as per CRMs from the follow-on E-ITSM Task Order, CDRL L3005 |
| 04/04/13 | 7.0 | Printed Name | Printed Name | Updated as per Process Owner review for MCATS Tasker |
| 04/21/2014 | 7.1 | Printed Name | Printed Name | Draft changes – to expand existing CfM PG to become SACM PG and incorporate DML in appendix |
| 08/06/2014 | 8.0 | Printed Name | Printed Name | Process Owner Update |
| 01/11/2018 | 9.0 | Printed Name | Printed Name | Updated by Process Owner: DML Appendix C removed pending revision; CSF/KPI Measures revised; Roles and Responsibilities updated |

## Table of Contents

## List of Tables



## List of Figures

# 1.0 INTRODUCTION

## 1.1 Purpose

The purpose of this process guide is to establish a documented and clear foundation for process implementation and execution across the Marine Corps Enterprise Network (MCEN). Process implementation and execution at lower levels (e.g., regional, local, and Programs of Record) must align and adhere to directives and schema documented within this guide. The use of this guide enables USMC Information Technology (IT) activities through promoting standardization of work instructions and operating procedures across a continuum of document specificity as represented in Figure 1-1.

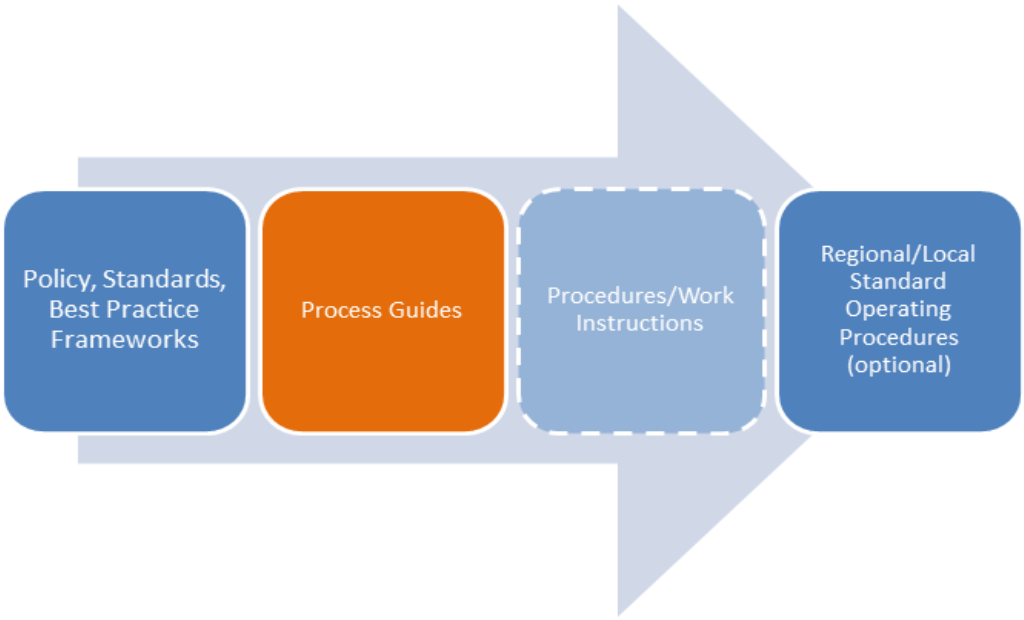



***Figure 1-1 Process Document Continuum***

## 1.2 Scope

This document covers all services provided in support of the MCEN for both the Secret Internet Protocol Router Network (SIPRNET) and the Non-Secure Internet Protocol Router Network (NIPRNET). Information remains relevant for the global operations and defense of the Marine Corps Enterprise Network (MCEN) as managed by Marine Corps Cyberspace Operations Group (MCCOG), including all Regional Network Operations and Security Centers (RNOSC) and Marine Air Ground Task Force Information Technology Support Center (MITSC) assets and supported Marine Expeditionary Forces (MEF), Supporting Establishments (SE) organizations, and Marine Corps Installation (MCI) commands.

Table 1-1 depicts the various layers of document design. Each layer has discrete entities, each with its own specific authority when it comes to promulgating documentation. This enterprise process operates at Level B. Sub-processes such as procedures and work instructions are not included within the scope of this document.

**Table 1-1 Document Design Layers**

| | ENTITIES | DOCUMENTS GENERATED |
|---|---|---|
| LEVEL A | Federal Govt<br>DoD<br>DoN<br>CMC/HQMC | Statutes/Laws<br>DoD Issuances<br>DoN Policies<br>Marine Corps Orders/IRMSs |
| LEVEL B | HQMC C4<br>MCCOG<br>MCSC | MCOs<br>IRMs (Process Guides)<br>Directives<br>MARADMINs |
| LEVEL C | RNOSC<br>MITSC | Regional Procedures<br>Work Instructions |
| LEVEL D | MCBs<br>POSTS<br>STATIONS | Locally Generated SOPs |

## 1.3 Process and Document Control

This document will be reviewed semi-annually for accuracy by the Process Owner with designated team members. Questions pertaining to the conduct of the process should be directed to the Process Owner. Suggested Changes to the process should be directed to USMC C4 CP in accordance with MCO – 5271.1c Information Resource Management (IRM) Standards and Guidelines Program.

# 2.0 PROCESS OVERVIEW

## 2.1 Purpose, Goals, and Objectives

The purpose of Service Asset and Configuration Management (SACM) is to identify, control, and document service assets and configuration items (CI) while protecting their integrity throughout the service lifecycle. Service Assets are defined as any capability or resource of a service provider, and CIs are defined as any component (including IT, services, hardware, software, documentation, etc.) that needs to be managed in order to deliver an enterprise IT service. This process establishes details of how the service assets and CIs have been configured and includes their relationships. SACM provides other Service Management processes with up-to-date information about the status of the services assets, CIs, and the IT infrastructure.

The goals of the SACM process are to:

- Support the organization by providing accurate and reliable information on inventory of all service assets (software, hardware, etc.) to provide visibility on ownership and internal and external dependencies.
- Account for, manage, and protect the integrity of service assets and CIs through the service lifecycle by working with the Change Management process to ensure that only authorized components are used and that only authorized changes are made.
- Minimize the number of quality and compliance issues caused by improper (incorrect or inaccurate) configurations of services assets and CIs.

The primary objectives of the SACM process are to:

- Maintain an accurate and complete Configuration Management System (CMS) to ensure configuration information is available to other USMC Enterprise IT Service Management (E-ITSM) processes for effective decision-making (i.e., for authorization of change, release, incident, problem, and capacity management activities).
- Define and control of the components of services and infrastructure to maintain accurate configuration information on historical, planned (future), and current state of the services and the infrastructure.
- Support the agreed IT service provision by managing, storing, controlling, and providing information about service assets and CIs throughout their lifecycle.

## 2.2 Scope of SACM Process

The scope of the SACM process includes managing the accuracy and reliability of configuration and relationship data for service assets and CIs from their inception to retirement, by providing a logical model to identify, control, maintain, verify, and report on service assets and resources comprising an IT infrastructure, as well as their constituent components and relationships.

The SACM scope also includes managing the lifecycle of service assets (with associated costs from the purchase, installation, and use) to retirement with attention to providing financial accountability and governance. Additionally, the scope involves management of registered media assets, such as software installation disks, backups, disk images, and release packages, all which are part of a Definitive Media Library (DML).

The SACM process scope does NOT include Responsible Officer (RO) responsibilities and processes, or data and property accountability systems, nor does it include the Defense Reutilization and Marketing Office (DRMO) asset disposal process or system.

The Service Asset portion of the SACM process maintains information about those assets in terms of their source, value, location, who controls them, etc. It manages the information about the entire life cycle of service assets, from procurement, through usage and maintenance, through disposition. The Configuration Management part of this process works closely with the design architecture of services, drawing relationships between CIs which is vital for resolving incidents, tracking changes, releases, finding the root cause of problems, and charting the technical service catalog.

The difference between a service asset and a CI is often confusing because some items appear in both the IT Asset Management (ITAM) database and the Configuration Management Database (CMDB). This is because the systems may be referencing the same "object," but they are for completely different purposes. Only a system like the CMDB, enabled by the relationship record, can provide accurate impact analysis, cost rollups, or a big picture understanding, etc. Neither ITAM nor Inventory Management can provide the level of visibility into how a service is actually delivered that can be found in the CMDB. Understanding the goals of ITAM, Configuration Management, and Inventory Management is important to help compare and contrast the three disciplines.

The SACM process includes asset, inventory, and configuration activities, which are defined in the Section 4.0 Sub-Processes of this process guide. These activities align with the services assets that are entered into the CMDB as a CI along with its CI record. Additionally, the SACM process aligns with the stages of the ITAM lifecycle from the same perspective.

## 2.3 Relationships with Other Processes

The SACM process manages the service assets and CIs needed to provision all of the other E-ITSM processes. SACM and the data it controls, exists as the central element of a mature E-ITSM solution. As the single repository of configuration data and information for E-ITSM, the SACM process supports and interfaces with many other Service Management processes and activities.

While any one of the E-ITSM processes can operate in the presence of an undeveloped process, the efficiency and effectiveness of each is greatly enhanced by the maturity and integration of all E-ITSM processes. Figure 2-1 depicts key relationships that exist between the SACM process and current E-ITSM processes that underpin the USMC near-term objectives. Note: This figure is not all-encompassing and the relationships shown can be either direct or indirect.

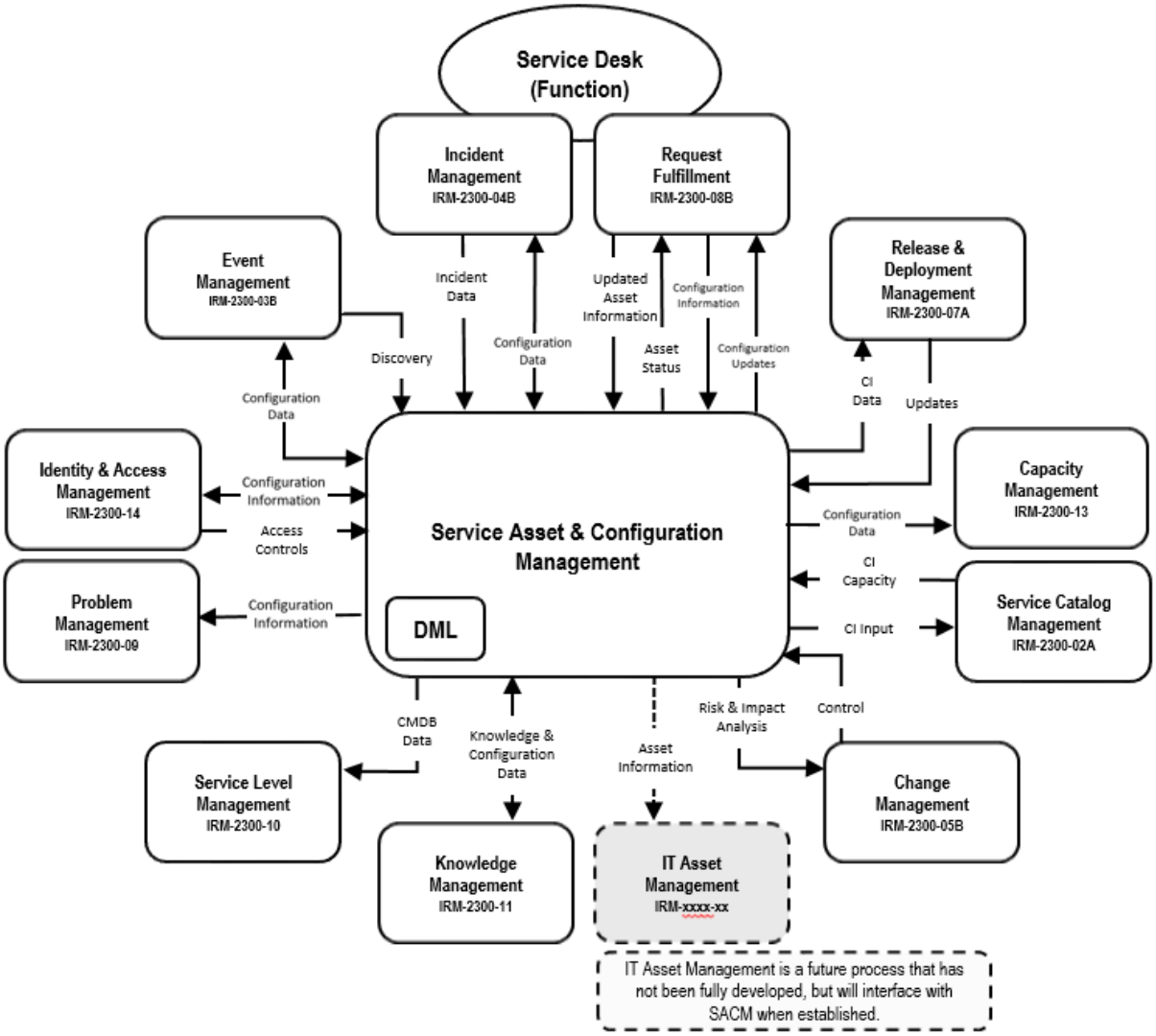



***Figure 2-1 SACM Relationships with other E-ITSM Processes***

The graphic above illustrates only an interface between processes at a high level and does not represent detailed dependencies. The following list describes some of the key inputs/outputs regarding the relationships between the SACM process and the other E-ITSM processes as illustrated in Figure 2-1.

- Problem Management (PbM)
  - Configuration Data: SACM provides baseline information required to aid with problem determination and resolutions (implement workarounds and fix known errors).
- Knowledge Management (KM)
  - Configuration Data: SACM configuration information enables effective decision support and reduces the risks that arise from the lack of proper control of the data.

- Service Level Management (SLM)
    - Configuration Data: Invoked when measuring the performance of the SACM process. Data from the CMDB enables measured and reported Change and/or Incident resolution achievements against service level targets in the form of Operational Level Agreements (OLA), Underpinning Contracts (UC), and Service Level Agreements (SLA) or Memorandums of Understanding/Agreement (MOU/MOA).

- Service Catalog Management (SCM)
    - The CMS maintained by the SACM process provides input on CIs that are part of the IT Services identified by the SCM process. The Service Catalog itself is stored and maintained as a CI within the CMS.
    - Service Definition: The Service Catalog is the definitive source of record for services that are present in the CMS. Service definition is a cornerstone of CMS architecture and contents; therefore, a high degree of coordination between the SACM process and the SCM process is required to ensure dependencies are effectively managed and service definitions stay in sync.
    - Technical Service Content: The Technical Service Catalog is produced by the SCM process directly from CMDB contents. This artifact details the technical or functional components that underpin IT services, and it exists as a report or as a filtered view of the CMDB.

- Release and Deployment Management (RDM)
    - Planning Content: The CMS and supporting processes provide invaluable information for the purposes of planning, preparing, designing, and controlling a release. For example, in the presence of an accurate CMS, the environment does not need to be inventoried to predict work effort and manpower required to propagate a large-scale enterprise release.
    - Additions and Updates: The CMS is updated as CIs are introduced or updated to ensure it accurately reflects the as-deployed environment.
    - Releases and distributes new versions of software with licenses and hardware with documentation.

- Incident Management (IM)
    - Configuration Data: The CMDB provides information to the Service Desk and to the Incident Management process for the purposes of troubleshooting, diagnosis, and resolution of incidents. By knowing which CIs, which CI relationships/dependencies, and the extent to which CIs are affected, incidents can be assessed for impact and prioritized accordingly.
    - Incident Data: Incidents are linked to CIs in the CMDB. This provides the Service Desk and other interested parties information regarding the history and disposition of CIs and associated services, systems, and applications.

- IT Asset Management (ITAM)

- ITAM maintains all information regarding technology assets, including leased and purchased assets, licenses and inventory (including location) from the time an asset is received until its retirement.

- Event Management (EM)
  - Configuration Data: The CMDB provides target and scope (CI relationships and dependencies) information necessary to architect and engineer service monitoring as well as establish correlation rules to help minimize redundant alerts.

- Request Fulfillment (RqF)
  - Configuration Data: SACM provides data for request for information, advice, frequently asked questions, etc., to the requestor.
  - Control: To keep information current, CI data and history are updated via the Change Management process during record updates of a service request.

- Change Management (ChM)
  - Invoked when a change request to implement a new component or affect an existing component configuration is executed.
  - Risk and Impact Analysis Content: The CMS depicts relationships between services and CIs, enabling risk and impact analysis for the purposes of Request for Change (RFC) evaluation.
  - Control: To keep information current the CI data and history is updated by both ChM to SACM and vice versa. SACM provides the infrastructure data required to assess customer impact of an IT infrastructure component failure and aids identification of the CI owners and associated user(s). Status of changes, especially completion, is an input to SACM, keeping the CMDB current.

- Capacity Management (CpM)
  - The CMS maintained by SACM provides a Capacity Management Information System (CMIS) which is a virtual repository of all Capacity Management data and is usually stored in multiple physical locations in the CMS. It provides capacity data to populate CI record attributes regarding capacity, i.e., storage, memory, etc. Configuration information is also made available to Capacity Management concerning growth estimates based on the CMDB.

- Access Management (AM)
  - Provides information on CIs. The (CMS) can be used for data storage and interrogated to determine current access details.

## 2.4 High-Level Process Model

The SACM process consists of five distinct sub-processes: (1) Management and Planning, (2) Configuration Identification, (3) Configuration Control, (4) Status Accounting and Reporting, and (5) Verification and Audit, as illustrated in Figure 2-2.

SACM is a process that underpins all other E-ITSM processes. It is used to identify and control service assets and CIs, and to govern the performance of periodic audits used to verify the accuracy and completeness of the SACM data.

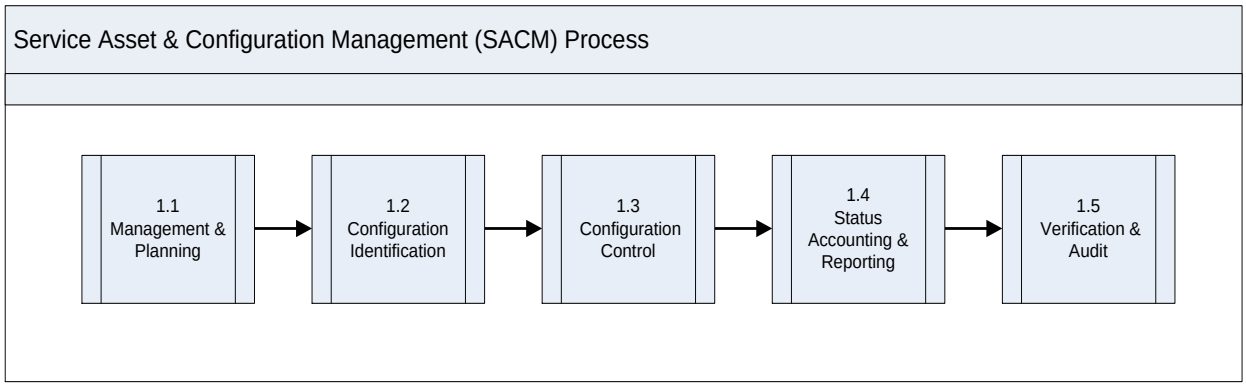



***Figure 2-2 High-Level SACM Process Model***

The following Table 2-1 provides a high-level description of each of the SACM sub-processes. The sub-process "Number" is hyperlinked to its detailed description and workflow activities in Section 4.0, Sub-Processes.

**Table 2-1 SACM Sub-Process Descriptions**

| Number | Sub-Process | Description |
|---|---|---|
| 1.1 | Management and Planning | Defines the level of Configuration Management required for a service or a change project.<br><br>Involves making decisions about what needs to be controlled within a product configuration, how controlled configurations are changed, and what amount of effort is expended to manage configurations, with the decisions formalized in a SACM Plan. The sub-process also takes into consideration how the succeeding four sub-processes will be managed and what resources are necessary to achieve them.<br><br>Additionally, Management and Planning provides:<br>• Descriptions of current and expected SACM tools (e.g., what you have and expect to find).<br>• Related documentation such as existing SACM plans or plans from suppliers.<br>• Listings of relevant documents and their interrelationships.<br>• Policies describing SACM management activities.<br>• Organizational responsibilities and authorities of relevant interested parties (stakeholders).<br>• Qualifications and training of staff to support SACM process.<br>• Criteria for the selection of CIs.<br>• Frequency, distribution, and control of reports. |

| Number | Sub-Process | Description |
|---|---|---|
| 1.2 | Configuration Identification | Defines the selection and identification of CIs and their relationships.<br><br>Identification includes assigning unique identifiers and version numbers to CIs, applying labels to CIs as appropriate, identifying and assigning CI Owners, and entering the CI into the appropriate databank (CMDB, DML, etc.) in the CMS. For service-level CIs, the selection of resource-level CIs and the descriptions of their interrelationships should describe the services' structure.<br><br>Good selection and identification criteria include:<br>• Regulatory requirements.<br>• Criticality in terms of risks.<br>• New or modified technology.<br>• Interfaces with other CIs.<br>• Procurement conditions.<br>• Support and service considerations. |
| 1.3 | Configuration Control | Ensures there are adequate mechanisms to control CIs.<br><br>Maintains that only authorized and identifiable CIs are accepted and recorded, from receipt to disposal. It safeguards that no CI is added, modified, replaced, or removed without appropriate controlling documentation through the Change Management process.<br><br>The organization defines how to accurately update CMDB records in the SACM Plan (Management & Planning sub-process), which would include:<br>• Management authorizations and relationships of those in authority.<br>• Procedures for control of changes to CI records within the CMDB.<br>• Methods to communicate changes from physical CIs to their CMDB records. |
| 1.4 | Status Accounting and Reporting | Maintains the status of CIs as they progress through their discrete states.<br><br>Reports on changes to CIs throughout their lifecycle. Includes methods to track CIs from ordering to depreciation, and disposal. Unlike the Configuration Control sub-process, Status Accounting provides historical records for the CIs, which includes baselines, linked Incidents, Problems, Known Errors, etc.<br><br>Additionally, this sub-process includes the methods for collecting, recording, processing, and maintaining status accounting records. The SACM Plan (Management & Planning sub-process), provides the definition of the content and format for all configuration status accounting reports. |

| Number | Sub-Process | Description |
|---|---|---|
| 1.5 | Verification and Audit | Checks that the physical CIs exist, records in the CMS match the real world, and that documentation is accurate.<br><br>A series of reviews to verify the presence (including physical) and configuration of CIs with their respective records within the CMDB. It ensures that the accuracy of CI information residing on CMDB is reviewed, and an audit over a sample size is conducted by both internal and external parties regularly.<br><br>These reviews are defined in the SACM Plan (Management & Planning sub-process) and should include:<br>• A list of audits planned (including schedules).<br>• Audit procedures to be used.<br>• Authorizations required (within and without IT).<br>• Description of report and expected contents.<br>• Configuration care and feeding. |

### 2.4.1 Process Description

The SACM process manages the lifecycle of service assets (i.e., hardware, software, including licensing and documentation) and associated costs from their purchase, installation, and use, to retirement. SACM is responsible for identifying, recording, tracking, controlling, reporting, and auditing by performing supporting process activities that maintain the integrity of these items throughout the life cycle of a project, including their versions, fundamental components, and relationships.

SACM governs the four aspects of the installation, movement, addition, and change on IT operational service assets and manages the data that is configured between the stocking of and disposal of these service assets. CIs managed within the scope of SACM will follow IT asset and property management requirements as defined in Federal Acquisition Regulations (FAR), Defense Federal Acquisition Regulation Supplement (DFARS), DoD, DoN, and USMC Directives.

The SACM process delivers a configuration model of the services, IT assets, and infrastructure by recording relationships between these CIs, which enable other E-ITSM processes to access valuable information to:

- Assess the impact of proposed changes.
- Assess the impact and cause of incidents and problems.
- Plan and design new or changed services.
- Plan technology refreshes and software upgrades.
- Plan release and deployment packages and migrate service assets to different locations.
- Create real-time service asset visibility, including software changes (data protection, software license management and regulatory compliance).
- Assume accountability and control for all service assets.
- Create links between service assets, financial, and contractual information to enable IT spend expenditures.

This process guide provides guidance and information to the USMC managers and personnel responsible in specific SACM roles for executing activities within the SACM process. The SACM

Process Guide will be used by the USMC organizations for planning, identifying, status accounting, controlling, maintaining, and verifying service assets and CIs including their versions, components, and relationships. Additionally, the process guide will provide reference to management and IT staff with a need to understand how the SACM process works within their IT organization.

## 2.5 Key Concepts

The following section describes key concepts that are relevant to the SACM process:

### 2.5.1 Commander's Critical Information Requirements

Commander's Critical Information Requirements (CCIR) are the commander's "need to know immediately" information and response requirements. From MCWP 3 40.2 Information Management, "are tools that can be used to focus large volumes of available data to permit the efficient flow of quality information through the information hierarchy". They define the information required by the commander to better understand the battle-space, identify risks, and to make sound, timely decisions in order to retain the initiative. CCIRs focus the staff on the type and form of quality information required by the commander, thereby reducing information needs to manageable amounts.

All commands are required to produce command-specific CCIR guidance with detailed IT service management requirements and are required to adhere to the current CCIR guidance of their superior commands. Common CCIR categories are Enterprise Service Management, Network Defense, Content Management, and MCEN, but other categories may be applicable based upon the commander's requirements**.**

### 2.5.2 Asset Accountability

Asset Accountability includes accurate record keeping and inventory of all IT assets owned by the USMC throughout the full life cycle. This requires adherence to public law, policy and regulation to ensure control of property, documents or funds. This includes fiduciary duties, responsibilities, and obligations necessary for protecting USMC interests.

### 2.5.3 Asset Management

Asset Management is a generic activity or process responsible for tracking and reporting the value and ownership of assets throughout their lifecycle. From an IT asset perspective, this process typically involves gathering a detailed inventory of an organization's IT asset (hardware, software, etc.) and then using that information to make informed decisions about IT-related purchases and redistribution.

### 2.5.4 Attribute

An attribute is a piece of information about a CI (e.g., name, location, version number, and cost). CIs are recorded in a CMDB and maintained as part of a CMS.

### 2.5.5 Audit

An audit ensures there is conformity between the documented baselines (e.g., agreements, interface control documents) and the actual business environment to which they refer. It verifies the physical existence of CIs in the organization or in the DML and spares stores, the functional

and operational characteristics of CIs, and it confirms records in the CMS match the physical infrastructure.

### 2.5.6 Baseline

A baseline is the configuration of a service, product, or infrastructure that has been formally reviewed and agreed, which thereafter serves as the basis for further activities and can be changed only through formal Change Management procedures. A configuration baseline is used as a basis for future builds, releases, and changes.

### 2.5.7 Change Advisory Board

A Change Advisory Board (CAB) is a group of people that support the assessment, prioritization, authorization and scheduling of changes. The CAB is usually made up of representatives from all areas within the IT service provider: the business, and third parties such as suppliers. All service asset and CI changes or additions to the CMDB must go through the formal E-ITSM Change Management process and be approved by the CAB prior to implementation.

### 2.5.8 Configuration Control

Configuration Control ensures that there are adequate control mechanisms over CIs while maintaining a record of changes to CIs, versions, location and custodianship/ownership. This is the activity responsible for ensuring that adding, modifying or removing a CI is properly managed, for example by submitting an RFC or Service Request.

### 2.5.9 Configuration Item

A Configuration Item (CI) is a component or service asset that needs to be managed in order to deliver an IT service. Information about each CI is recorded in a configuration record within the CMS and is maintained throughout its lifecycle by SACM. CIs are under the control of Change Management. CIs may vary widely in complexity, size, and type, ranging from an entire service or system including all hardware, software, documentation, and support staff to a single software module or a minor hardware component. CIs may be grouped and managed together.

### 2.5.10 Configuration Management Database

The Configuration Management Database (CMDB) is a large central logical repository used to store configuration records throughout the CI's lifecycle. The database makes that information accessible to other service processes. The CMDB resides in the CMS and stores attributes of service assets and CIs to include relationships with other CIs.

### 2.5.11 Configuration Management System

The Configuration Management System (CMS) is a set of tools and databases (i.e., CMDB, DML) that are used to manage the IT organization's configuration data. The CMS includes information about Incidents, Problems, Known Errors, Changes and Releases; and may contain data about Employees, Suppliers, Locations, Business Units, Customers, and Users. Then CMS includes tools for collecting, managing, updating, and presenting data about CIs and their relationships. The purpose of the CMS is to support SACM as it is maintained by SACM and used by all E-ITSM processes.

### 2.5.12 Decommissioned Assets

Assets are decommissioned for a number of reasons to include: when a service is retired and the assets used are no longer needed, when a technology refresh has replaced old assets, or when hardware failure resulted in the replacement of old assets. Assets must be decommissioned in a proper manner following the USMC disposal regulatory requirements.

### 2.5.13 Defense Property Accountability System (DPAS)

DPAS is one of the mandated property management systems used to support DoD property accountability and financial requirements. DPAS allows users to: account for real and personal property, heritage assets, and manage their assets (maintenance scheduling, redistributions, allowances).

### 2.5.14 Definitive Spares

The Definitive Spares are components and assemblies that are maintained, in a secure area, at the same revision level as the systems within the controlled test or live environment. Details of these components, their locations, respective builds, and contents should be comprehensively recorded in the CMS. Spares can be used in a controlled manner when needed for additional systems or in the recovery from incidents.

### 2.5.15 Definitive Media Library

The Definitive Media Library (DML) is the secure library (i.e., physical and electronic media storage repository) into which definitive authorized versions of all media CIs are stored and protected. The DML stores master copies of versions that have passed quality assurance checks. The DML should include definitive copies of purchased software (along with software license documents or information), as well as software developed on site. Master copies of controlled documentation for a system are also stored in the DML in electronic form. The DML is a foundation for Release and Deployment Management as information exchanged in order to keep the definitive software consistent with the CMDB.

### 2.5.16 Discovery

Discovery is both a manual and automated process by which CIs are identified, recorded, stored, and then updated in the CMDB. This is commonly used with a toolset that collects data on a network or service and records any changes made to the IT assets (i.e., changes made to memory, software versions, storage, etc.)

### 2.5.17 Fixed Asset Management (FAM)

FAM maintains the asset register and is usually carried out by the overall business, rather than by the IT organization.

### 2.5.18 Global Combat Support System - Marine Corps (GCSS-MC)

Global Combat Support System - Marine Corps (GCSS-MC) serves as a foundation for all logistics information required by the Marine Forces and the Supporting Establishment. GCSS-MC is the primary technology enabler for the Marine Corps Logistics Modernization strategy. Future capabilities include warehousing, distribution, logistics planning, decision support, depot maintenance, and improvement of asset visibility through integration with emerging technologies.

### 2.5.19 Hardware Asset Management

Hardware (HW) Asset Management (AM) consists of managing the physical components of computers and computer networks, from purchase request through disposal. Common HW AM business practices include request and approval, procurement, life cycle management, monitoring/auditing and disposal processes, which are enabled by discovery and service management tool capabilities. Additionally, HW AM includes financial asset data capture and metrics measurements which are key components that aid in making business decisions.

### 2.5.20 Labeling

All physical device CIs should be labeled with the configuration identifier so that they can be easily identified. Plans should be made to label CIs and to maintain the accuracy of their labels. Items need to be distinguished by unique, durable identification. Physical non-removable asset tags (labels) should be attached to all hardware CIs; cables/lines should be clearly labeled at each end and at any inspection points. All software CIs should be labeled with a software identification tag (SWID) utilizing ISO/IEC Standard 19770-2 or a comparable method to easily identify licensed USMC software. Plans should be made to label the CIs and to maintain accuracy of their labels. Publisher stock keeping unit (SKU) numbers (manufacturer part numbers) should be clearly identified in all contracts and within the CMDB.

### 2.5.21 Naming

Naming conventions have been established and applied to the identification of CIs, configuration documents and changes, as well as to baselines, builds, releases, and assemblies. CIs should be uniquely identifiable by means of the identifier and version. The naming convention includes the management of: (1) hierarchical relationships between CIs within a configuration structure, (2) subordinate relationships in each CI, (3) relationship between CIs and their associated documents, (4) relationship between CIs and changes, and (5) relationships between CIs, incidents, problems, and known errors. The Marine Corps Naming Standard for Applications and Systems provides naming standards for Microsoft Active Directory components (server farm site identifiers, organizational units, sites, servers, workstations, printers, service accounts, user accounts, contacts, groups, and group policies), Exchange, Distributed Files System, VMWare, Threat Management Gateway, NETAPP, Network Circuits Devices and Wiring, Solution Documentation, and Site Codes.

### 2.5.22 Relationships

Relationships in SACM are a link between two or more CIs that identifies a dependency or connection between them. For example, applications may be linked to the servers they run on. IT Services can have one or more relationships to the CIs that contribute to them.

### 2.5.23 Service

A service is set of related components provided in support of one or more business processes. The service will comprise a range of CI types but will be perceived by customers and users as a self-contained, single, coherent entity (e.g., Enterprise Messaging). A service is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks. Services facilitate outcomes by enhancing the performance of associated tasks and reducing the effect of constraints (e.g., email, provisioning, and financial management).

### 2.5.24 Service Asset

A service asset is any resource or capability of a USMC service providing organization. Resources could be infrastructure, application, or data. Capabilities include people, organization, management and their knowledge. In essence, every aspect of a service is considered a service asset. The service assets of a service provider include anything that could contribute to the delivery of an IT service. Service assets can be one of the following types: management, organization, process, knowledge, people, information, applications, and infrastructure, and financial capital.

### 2.5.25 Service Provider

A Service Provider is an organization supplying services to one or more internal customers or external customers. The term service provider is often used as an abbreviation for IT Service Provider. Service provider activities may include: (Monitoring of servers, networks, etc., administration of server or network devices, maintenance of hardware).

### 2.5.26 Status Accounting

Each service asset or CI will have one or more discrete states through which it can progress. The significance of each state should be defined in terms of what use can be made of the asset or CI in that state. There will typically be a range of states relevant to the individual asset or CIs. (Examples of a lifecycle state are Received, Being Assembled, Deployed, In Repair, Down, End of Life, Transferred, Deleted, In Inventory, On Loan, Disposed, Reserved, and Return to Vendor).

The way CIs move from one state to another should be defined and at each lifecycle status change the CMS should be updated with the reason, date time stamp and person that did the status change.

### 2.5.27 Software Asset Management (SAM)

SAM involves managing and optimizing the purchase, deployment, maintenance, utilization and disposal of SW applications within the enterprise by aligning to E-ITSM best practices. This provides for effective management, control, and protection of SW assets throughout all stages of the life cycle, while reducing IT costs and limiting license ownership and use risks.

### 2.5.28 Software License Management

Software license management consists of standard processes, business rules, and supporting technology that identify the standards for which Commercial off the Shelf (COTS) and Government off the Shelf (GOTS) software will be tracked, controlled and managed in order to enforce and ensure compliance with software license contracts.

### 2.5.29 Verification

Verification is a method that is common to SACM, systems engineering, design engineering, manufacturing, and quality assurance. An activity that ensures that a new or changed IT service, process, plan or other deliverable is complete, accurate, reliable and matches its design specification.

## 2.6 Quality Control

### 2.6.1 Metrics, Measurements, and Continual Process Improvement

Continual Service Improvement (CSI) depends on accurate and timely process measurements and relies upon obtaining, analyzing, and using information that is practical and meaningful to the process at hand. Measurements of process efficiency and effectiveness enable the USMC to track performance and improve overall end user satisfaction. Process metrics are used as measures of how well the process is working, whether or not the process is continuing to improve, or where improvements should be made. When evaluating process metrics, the direction of change is more important than the magnitude of the metric.

Effective day-to-day operation and long-term management of the process requires the use of metrics and measurements. Reports need to be defined, executed, and distributed to enable the management of process-related issues and initiatives. Daily management occurs at the process manager level. Long-term trending analysis and management of significant process activities occurs at the process owner level.

### 2.6.2 Critical Success Factors with Key Performance Indicators

The essential components of any measurement system are Critical Success Factors (CSFs) and Key Performance Indicators (KPIs). Both CSFs and KPIs establish the baseline and mechanism for tracking performance. CSFs are those important factors that must be done well within the process. KPIs can then be defined and measured against the process to ensure each CSF is met.

The performance of SACM should be monitored, reported on, and acted upon for improvement. SACM is the central support process facilitating the exchange of information with other E-ITSM processes. However, SACM must be measured for its contribution to these other processes within the lifecycle and the overall KPIs that directly affect the USMC.

The following metrics include those that management will use near-term to measure the effectiveness and efficiency of the SACM implementation and its evolution, as opposed to metrics to measure the process effectiveness:

- Percentage of unauthorized CIs introduced into the IT infrastructure.
- Percentage of failed changes due to incorrect data in the CMDB, or poor version control.
- Percentage accuracy of CIs when compared to the live environment.
- Ratio of used licenses against paid-for licenses.

In developing CSFs it is essential to recognize that a CSF is the reason to do things. It is a purpose and a strategic ambition that should be linked to other desired strategic outcomes that lead to success. To know whether the organization is heading in the right direction, indicators are needed, and a KPI is a sign that demonstrate progress toward or away from a CSF.

459 Table 2-2 describes the SACM process recommended CSFs and KPIs to be monitored, measured,
460 and analyzed. These measures are based on best practices and can be evaluated for future
461 expansion.

462 **Table 2-2 SACM Process Critical Success Factors with Key Performance Indicators**

| CSF # | Critical Success Factors | KPI # | Key Performance Indicators | Benefits |
|---|---|---|---|---|
| 1 | Accounting for, managing, and protecting the integrity of service assets and CIs throughout the service lifecycle | 1 | Reduction of retired and / or disposed assets missing date of disposal<br><br>**Calculation:** Report generated of number of assets, by hardware type, designated as retired or disposed without an associated disposal date. Monthly end-over-end report showing trends over a period of time. | Improved accuracy for the service asset lifecycle by reducing the risks associated with assets disposition being improperly tagged |
| | | 2 | Reduction of deployed assets missing installation date<br><br>**Calculation:** Report generated of number of assets, by hardware type, designated as deployed without an associated deployed date. Monthly end-over-end report showing trends over a period of time. | |
| | | 3 | Reduction of assets missing UIC & ownership information<br><br>**Calculation:** Report generated of number of assets, by hardware type, missing UIC & ownership information. Monthly end-over-end report showing trends over a period of time. | |
| 2 | Supporting efficient and effective service management processes by providing accurate configuration information at the right time | 4 | Reduction in the use of unauthorized hardware<br><br>**Calculation:** Report generated of number of assets, by MITSC, discovered by network scanning tools that are missing from CMDB. Monthly end-over-end report showing trends over a period of time. | Reduces the risk of technical staff circumventing the SACM process and procedures |
| | | 5 | Reduced number of exceptions reported during audits.<br><br>**Calculation:** Report generated of number of assets, by MITSC, on the network but not marked in a deployed status. Monthly end-over-end report showing trends over a period of time. | |
| | | 6 | Reduction in risks due to early identification of unauthorized change<br><br>**Calculation:** Report generated of number of assets, by MITSC, discovered by network scanning tools that are missing from CMDB. Monthly end-over-end report showing trends over a period of time. | |

| CSF # | Critical Success Factors | KPI # | Key Performance Indicators | Benefits |
|---|---|---|---|---|
| 3 | Establishing and maintaining an accurate and complete CMS | 7 | Increase in quality and accuracy of configuration information<br><br>**Calculation:** Reports generated, by MITSC, capturing assets missing location, disposal/deployment dates, and UIC information. Monthly end-over-end report showing trends over a period of time. | Reduces the risk of the asset database becoming outdated while improving asset baseline impact analysis on USMC networks |
| | | 8 | Improved audit compliance<br><br>**Calculation:** Report generated of number of assets, by MITSC, discovered by network scanning tools that are missing from CMDB. Monthly end-over-end report showing trends over a period of time. | |
| | | 9 | Reduction in errors caused by people working with out-of-date information<br><br>**Calculation:** Report of assets being discovered and updated by network discovery tools (SCCM, MEMs, etc.) Monthly end-over-end report showing trends over a period of time. | |

463

# 3.0 ROLES AND RESPONSIBILITIES

Each E-ITSM process has roles and responsibilities associated with design, development, execution, and management of the process. A role within a process is defined as a set of responsibilities. There will be instances where roles are combined and a person will be responsible for multiple roles. This is based on factors such as the area or responsibility, size of user base, and/or size of the process support team, which will dictate exactly which roles require a dedicated person(s) and the total number of persons performing each role. The SACM Process Owner role serves as the authoritative process point of contact for any higher headquarters (DoN or DoD) or adjacent organization engagement or coordination. The Process Owner or delegated representatives will provide oversight of the SACM process and ensure the process is executed throughout the classified and unclassified environments in the Marine Corps Information Environment (MCIE).

Best Practices indicate that process ownership should reside with a single individual to ensure clear accountability. The Process Owner role exists at the enterprise level and is critical for the successful design and ongoing management and support of the process. Management (i.e., responsibility) of the SACM process is shared; a single process manager exists at the Enterprise level, and SACM Managers exist at the MITSCs. There will be instances where roles are combined or a person is responsible for multiple roles. Factors such as Area of Responsibility (AoR), size of user base and size of the process support team dictate exactly which roles require a dedicated person(s) and the total number of persons performing each role.

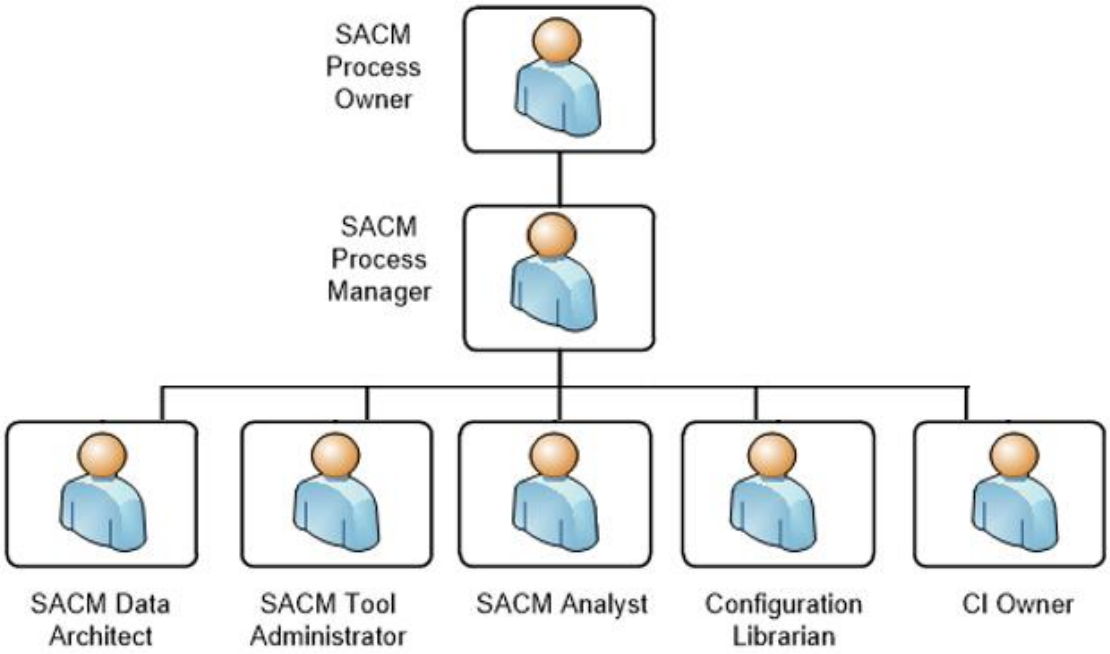
The following additional roles will support the SACM process:

- SACM Data Architect
- SACM Tool Administrator
- SACM Analyst
- Configuration Librarian
- CI Owner

Position titles or job titles and position descriptions will vary from organization to organization; however, individuals can perform one or more of the required E-ITSM process roles regardless of title.

## 3.1 Roles

Figure 3-1 depicts the hierarchy of the SACM Process Roles, while Table 3-1 provides a description for each of the SACM Process Roles and Responsibilities.




496

497 ***Figure 3-1 SACM Process Roles***

498 **Table 3-1 SACM Process Roles and Responsibilities**

| Role Description | Responsibilities |
|---|---|
| **SACM Process Owner** | |
| The Process Owner owns the process and the supporting documentation for the process. The primary functions of the Process Owner are oversight and continuous process improvement.<br><br>The Process Owner oversees the process, ensuring that the process is followed by the organization. When the process is not being followed or is not working well, the Process Owner is responsible for identifying and ensuring required actions are taken to correct the situation. In addition, the Process Owner is responsible for the approval of all proposed changes to the process, and development of process improvement plans.<br><br>The Process Owner may delegate specific responsibilities to another individual within their span of control, but remains ultimately accountable for the results of the SACM process. | • Provides leadership and accountability for the process and all of its sub-processes.<br>• Ensures the process is followed by the organization.<br>• Ensures the SACM process and working practices are effective and efficient.<br>• Ensures all stakeholders are sufficiently involved in the SACM process.<br>• Makes decisions on any proposed enhancements to the process and development of process improvement plans.<br>• Agrees with and documents the scope for the process, incorporating the policy for determining which service assets should be treated as CIs.<br>• Adjudicates when new CI types are requested by SACM Process Managers.<br>• Ensures tight integration between SACM and other related processes.<br>• Liaises with E-ITSM Process Owners to ensure there is an integrated approach to the design and implementation of SACM, Change Management, Release and Deployment Management and Knowledge Management and other processes as applicable. |

| Role Description | Responsibilities |
|---|---|
| **SACM Process Manager (Service Asset Manager)** | |
| The Service Asset Manager owns responsibility to implement SACM and works with the Process Owner on the implementation and continuous improvement.<br><br>Works collaboratively with the Configuration Manager to develop and implement the specific SACM plans and sub-processes, and procedures for the infrastructure. The Service Asset Manager focuses on the lifecycle of the IT Assets.<br><br>The Service Asset Manager is the direct interface for SACM with Incident, Problem, Change, Release, Operations Management, Service Level, Capacity, Finance, and all other project and process teams as required for proper maintenance and control of the IT Asset data.<br><br>There is a Service Asset Manager for each level of the environment. | • Performs the Process Manager role for the SACM process.<br>• Implements the service asset management policy and standards.<br>• Supports the scope of the SACM process, including items that are to be controlled, and information that is to be recorded.<br>• Manages assets in accordance with this instruction.<br>• Plans population of service assets; manages the service assets in CMDB, central libraries and tools; ensures regular housekeeping of the Asset database or register.<br>• Identifies and classifies service assets that will be regarded as CIs.<br>• Ensures service assets are uniquely identified with naming conventions and that staff complies with identification standards for object types, environments, processes, lifecycles, documentation, versions, formats, baselines, releases and templates.<br>• Ensures all data relating to SACM is available when required.<br>• Evaluates existing service asset management systems and the design, implementation and management of new/ improved systems for efficiency and effectiveness.<br>• Prepares and manages SACM tools and processes.<br>• Manages the evaluation service asset management tools.<br>• Develops service asset management standards and Service asset management plans and procedures.<br>• Ensures that the service asset management methods and processes are properly approved and communicated to staff before being implemented.<br>• Arranges recruitment and training of SACM staff.<br>• Proposes interfaces with network management, computer operations, logistics, finance, and administration functions.<br>• Coordinates key interfaces between SACM and other processes, in particular, Change Management, Release and Deployment Management and Knowledge Management.<br>• Provides reports, including management reports. |
| **SACM Process Manager (Configuration Manager)** | |
| The Configuration Manager owns responsibility to implement SACM and works with the process owner on the implementation and continuous improvement.<br><br>Works collaboratively with the Service Asset Manager to develop and implement the specific SACM plans and processes for the infrastructure. The Configuration Manager focuses on the CI attributes and relationships maintained in the CMDB.<br><br>The Configuration Manager is the direct interface for SACM with Incident, Problem, Change, Release, Operations Management, Service Level, Capacity, Finance, and all other project and process teams as required for proper maintenance and control of the CMDB data. | • Performs the Process Manager role for the SACM process.<br>• Implements the SACM policy and standards.<br>• Supports the scope of the SACM process, including items that are to be controlled, and information that is to be recorded.<br>• Manages the CIs that are under control of SACM.<br>• Identifies and classifies service assets that will be regarded as CIs.<br>• Ensures all data relating to SACM is available when required.<br>• Prepares and manages SACM tools and sub-processes.<br>• Coordinates key interfaces between SACM and other processes, in particular, Change Management, Release and Deployment Management and Knowledge Management<br>• Evaluates existing CMS.<br>• Develops configuration management standards, SACM plans and procedures. |

| Role Description | Responsibilities |
|---|---|
| There is a Configuration Manager for each level of the environment. | • Ensures that changes to the SACM methods and processes are properly approved and communicated.<br>• Arranges recruitment and training of SACM staff.<br>• Manages the evaluation of CM tools.<br>• Manages the SACM plan, principles and processes and their implementation.<br>• Ensures CIs are uniquely identified with naming conventions and that staff complies with identification standards for object types, environments, processes, lifecycles, documentation, versions, formats, baselines, releases and templates.<br>• Proposes interfaces with network management, computer operations, logistics, finance, and administration functions.<br>• Plans population of the CMS; manages CMS, central libraries, tools, common codes and data; ensures regular housekeeping of the CMS.<br>• Provides reports, including management reports. |
| **SACM Analyst (Service Asset)** | |
| The SACM Service Asset Analyst focuses on the tracking and control of service assets in the IT infrastructure.<br><br>The SACM Analyst also collaborates with the SACM Configuration Analyst to train SACM staff in SACM principles, processes, and procedures. | • Supports the creation of the SACM process, activities, and procedures to include CI registration procedures, access controls, and privileges.<br>• Ensures the correct roles and responsibilities are defined in the SACM plan/procedures.<br>• Assist with procurement of IT assets when requested.<br>• Works with other SACM roles to tag and track all IT assets and to identify their locations and owners.<br>• Receives IT assets and ensures delivery to correct locations.<br>• Coordinates IT asset setup and teardown activities when requested.<br>• Proposes/concurs with the SACM Manager on CIs to be uniquely identified with naming conventions.<br>• Ensures developers and configuration system users comply with identification standards for object types, environments, processes, life cycles, documentation, versions, formats, baselines, releases, and templates.<br>• Liaises with Configuration Librarian on population of asset and CMS.<br>• Performs configuration audits to ensure physical inventory is consistent with the CMDB/CMS, initiating corrective action through Change Control.<br>• Accepts baselined products from third parties for distribution.<br>• Builds system baselines for promotion and release.<br>• Maintains project status information and status accounting records and reports.<br>• Assists SACM Manager in report definition as required. |
| **SACM Analyst (Configuration Management)** | |
| The SACM Configuration Analyst focuses on the attributes and relationships of the CIs maintained in the CMDB.<br><br>The SACM Configuration Analyst collaborates with the SACM Service Asset Analyst to train Asset and Configuration Management specialists and other staff in Asset and Configuration Management principles, processes, and procedures. | • Supports the scope of the SACM processes and function that items that are to be controlled, and the information that is to be recorded.<br>• Assists with the development of SACM standards, plans, and procedures.<br>• Determines construction of the CMS, including CI types, naming conventions, attributes and relationships |

| Role Description | Responsibilities |
|---|---|
| | • Supports the creation of the SACM process, activities, and procedures to include CI registration procedures, access controls, and privileges.<br>• Ensures the correct roles and responsibilities are defined in the SACM plan/procedures.<br>• Proposes/concurs with the SACM Manager on CIs to be uniquely identified with naming conventions.<br>• Ensures developers and configuration system users comply with identification standards for object types, environments, processes, life cycles, documentation, versions, formats, baselines, releases, and templates.<br>• Liaises with Configuration Librarian on population of asset and CMS.<br>• Performs configuration audits to ensure physical inventory is consistent with the CMDB/CMS, initiating corrective action through Change Control.<br>• Uses the CMDB/CMS to help identify other CIs affected by a fault which is affecting a CI.<br>• Creates and populates project libraries and the CMDB/CMS.<br>• Accepts baselined products from third parties for distribution.<br>• Builds system baselines for promotion and release.<br>• Maintains project status information and status accounting records and reports.<br>• Assists SACM Process Manager in report definition as required.<br>• Supports CI Owners in Configuration Identification process and in support of Configuration Control activities. |
| **SACM Data Architect** | |
| The SACM Data Architect is primarily responsible for Configuration Identification. The SACM Data Architect consults regularly with the SACM Configuration Analyst and the Configuration Librarian during the SACM Identify Configuration process. | • Develops and maintains the configuration identification architecture, including categorization, attributes, relationships, and naming conventions.<br>• Develops and maintains specialist knowledge of object-oriented analysis, design, and modeling techniques and principles, and a detailed knowledge of IT service, system, infrastructure, and CMS/CMDB architectures.<br>• Analyzes data requirements to establish, modify, or maintain CMS object/data models.<br>• Evaluates potential solutions, analyzing and modeling changes to the CMS/CMDB information model.<br>• Uses appropriate tools, including logical models of configuration classes, attributes, and relationships, to contribute to the development of the information model for the CMS.<br>• Utilizes CMS and auto-discovery tools to discover, preview and report about the physical data center environment.<br>• Compares physical data against CMS information.<br>• Assesses and analyzes requests for SACM Verifications and Audits.<br>• Verifies the integrity of the physical business environment as specified in requirements and configuration baseline documents.<br>• Plans audit to verify CMS information against the physical environment.<br>• Generates CMS baseline reports.<br>• Verifies conformance and highlights non-conformance and variations within the Draft Audit Report. |

| Role Description | Responsibilities |
|---|---|
| | • Creates a risk and gap analysis, assessing value of reconciliation.<br>• Produces detailed specifications and maps or translates these into designs for implementation in the CMS.<br>• Consults on technical aspects of SACM (including requests for changes, deviations from specifications, etc.).<br>• Ensures relevant technical strategies, policies, standards and practices are applied correctly. |
| **Configuration Librarian** | |
| The Configuration Librarian is the custodian and guardian of all master copies of software, assets and documentation CIs registered within SACM.<br><br>The Configuration Librarian manages the Definitive Media Library activities, from population through positioning of controlled items for deployment actions.<br><br>The Configuration Librarian collaborates with the Change Manager as actions proposed for changes to controlled DML items are controlled via the Change Management process and the Request for Change (RFC) only. | • Controls the receipt, identification, storage, and withdrawal of all support CIs via Authorized or Approved RFCs.<br>• Provides information on the status of CIs.<br>• Numbers, records, stores, and distributes SACM DML issues.<br>• Assists SACM Analyst in Configuration Identification activities.<br>• Assists SACM Manager to prepare the SACM Plan.<br>• Creates and manages the identification scheme for the CM libraries and DML.<br>• Creates and manages libraries or other storage areas to hold CIs<br>• Assists in the identification of products and CIs.<br>• Maintains current status information on CIs.<br>• Accepts and records the receipt of new or revised configurations into the appropriate library.<br>• Archives superseded CI copies.<br>• Safeguards and holds the master copies.<br>• Administers configuration control sub-process:<br>• Issues copies of products for review, change, correction, or information when authorized to do so.<br>• Maintains a record of all copies issued.<br>• Notifies holders of any changes to their copies.<br>• Collects and retains information that will assist in the assessment of what CIs are impacted by a change to a product.<br>• Produces configuration status accounting reports.<br>• Assists in conducting configuration audits. |
| **CI Owner** | |
| The CI Owner is responsible to all stakeholders for the CIs to which it's assigned. A CI Owner is designated by the SACM Configuration Manager to manage one or more classes of CIs and assist the SACM Configuration Manager in ensuring necessary CI updates are completed in a timely and accurate manner.<br><br>The CI Owner is a POC whenever questions regarding the completeness or accuracy of a particular CI arises. The CI Owner is responsible for monitoring assigned CIs and ensuring that policies are followed, standards are implemented, and control objectives are met. This responsibility includes oversight of CI quality, continual improvement, and compliance with organizational mandates and performance targets.<br><br>This role applies to anyone who performs the function for defining, documenting the generic attributes (e.g. | • Owns, defines, and documents the generic (common) attributes for specific CI types, including identifying which CI attributes should be available with specific status within the CI lifecycle.<br>• Owns technology roadmaps, CMS load plans, and end of life plans for specific CIs.<br>• Engages in the planning activities involved in introducing, modifying, or retiring CIs.<br>• Works with other CI Owners required to carry out CMS load tactics and ongoing Change, Configuration, and Release and Deployment responsibilities.<br>• Works with CIs assigned to maintain.<br>• Registers new CIs upon approval.<br>• Manages the receipt, identification, storage and removal of all CIs.<br>• Preserves status information on CIs.<br>• Archives out of date CIs. |

| Role Description | Responsibilities |
|---|---|
| manufacture, model, version, catalog items, etc.) of one or more specific types. | • Identifies, records, stores, and distributes issues connected with the SACM process.<br>• Transfers ownership of a CI.<br>• Generates and views reports of the CIs assigned.<br>• Under the direction of the SACM Manager, ensures that all Stakeholders (Enterprise wide) responsible for performing CI management and administrator procedures understand and are capable of performing their roles.<br>• Ensures that appropriate CI documentation is available and current.<br>• Communicates CI information or changes as appropriate to ensure awareness.<br>• Conducts periodic reviews of assigned CIs to ensure that information is still appropriate and make changes as required.<br>• Ensures completeness and integrity of information collected to conduct daily operations.<br>• Assists in audits of CIs for compliance with documented procedures. |
| **SACM Tools Administrator** | |
| The SACM Tools Administrator evaluates proprietary Asset and Configuration Management tools and recommends those that best meet the organization's budget, resource, timescale, and technical requirements.<br><br>This role also directly or indirectly customizes proprietary tools to produce effective SACM environments in terms of databases and software libraries, workflows, and report generation. | • Monitors the performance and capacity of existing SACM/CMS.<br>• Recommends improvement opportunities.<br>• Evaluates tools, monitors performance and capacity of the CMS/CMDB.<br>• Liaises with Capacity Management regarding volumes, trends and requirements.<br>• Undertakes standard housekeeping and fine tuning within the Change Control process.<br>• Supports requests for tool changes necessitated from Reporting and Audit / Reconciliation efforts.<br>• Monitors/analyzes service asset/configuration data and compliance activities to identify trends, discover anomalies, and ensure proper management of the SACM process.<br>• Liaises with other functions in IT service to establish quality improvement in the SACM process. |

## 3.2 Responsibilities

E-ITSM processes will span organizational boundaries; therefore, the sub-processes, including associated activities, procedures, and work instructions, will be mapped to roles within the process. These roles are then mapped to job functions, IT staff, and departments. For the purpose of this document, only the SACM sub-processes are mapped to the respective SACM process roles.

Roles are accountable or responsible for an activity, and they can also provide support or be consulted or informed about something. The RASCI model provides a useful way of defining and communicating roles and responsibilities.

The following RASCI descriptions further define the level of role involvement:

- **R**esponsible – Completes the process or activity; responsible for action/implementation. The degree of responsibility is determined by the role with the 'A'. There may be multiple "R" roles for a process activity; however there must be at least one.

- **A**ccountable – Approves or disapproves the process or activity. Individual who is ultimately answerable for the task or a decision regarding the task. Individual with final decision authority. Typically, the Process Owner is accountable for a process, and there must be only one "A" specified for per process activity.
- **C**onsulted – Gives needed input about the process or activity. Prior to final decision or action, these subject matter experts or stakeholders are consulted. Two-way communication is assumed.
- **S**upport – Provides resources or a supporting role in the process or activity. Resources allocated to responsible. Unlike consulted, which may provide input to the task, support helps complete the task.
- **I**nformed – Needs to be informed after a decision or action is taken. May be required to take action as a result of the outcome. One-way communication is assumed.

This section includes a RASCI model to depict how each sub-process maps to a SACM process role, highlighting when that role is responsible, accountable, supported, consulted, and/or informed. All roles associated with each sub-process and its activities are listed across the top of the chart in columns, with the sub-processes listed to the left in rows. Table 3-2 displays the RASCI model for the SACM process roles.

530

531 **Table 3-2 RASCI Model for SACM by Process Role**

| SACM Process Activities | SACM Process Owner | SACM Process Manager (Configuration) | SACM Process Manager (Service Asset ) | SACM Analyst (Configuration) | SACM Analyst (Service Asset) | SACM Data Architect | Configuration Librarian | CI Owner | SACM Tools Administrator |
|---|---|---|---|---|---|---|---|---|---|
| Management & Planning | AR | R | R | S | S | C | C | S | C |
| Configuration Identification | A | R | R | S | S | R | S | C | S |
| Configuration Control | A | R | R | R | R | C | S | S | |
| Status Accounting & Reporting | A | R | R | R | R | S | S | S | C |
| Verification & Audit | A | R | R | S | S | S | C | C | S |

*Legend:*
*Responsible (R) – Completes the process or activity*
*Accountable (A) – Authority to approve or disapprove the process or activity*
*Support(S) – Supports process or activity*
*Consulted (C) – Experts who provide input*
*Informed (I) – Notified of activities*

*Note: Any role that is designated as Responsible, Accountable, Consulted, or Supporting is not additionally designated as Informed because being designated as Responsible, Accountable, Consulted, or Supporting already implies being in an Informed status. A role is designated as Informed only if that role is not designated as having any of the other four responsibilities.*

*Note: Only one role can be accountable for each process activity.*

532

# 4.0 SUB-PROCESSES

The E-ITSM SACM process consists of five (5) sub-processes as shown in Figure 4-1. This process involves planning, identifying, controlling, recording, tracking, reporting, auditing, and verifying information about the service assets and CIs required to deliver an IT Service (including their relationships). This section will provide an overview, including the high-level workflow and description of each sub-process within the SACM process.

## 4.1 Management and Planning

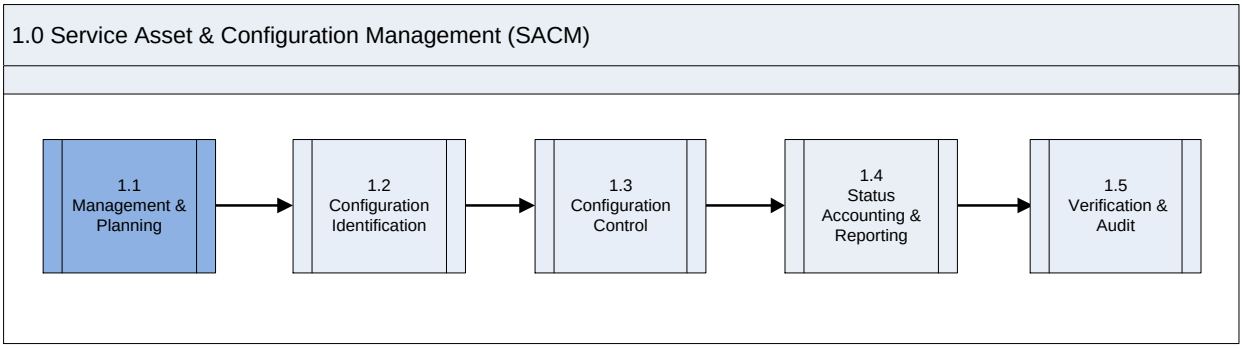



***Figure 4-1 SACM Process Overview – Management and Planning Sub-Process***

The Management and Planning sub-process highlighted in Figure 4-1 represents the core SACM activity and its relationships to the other SACM sub-processes. The inputs to Management and Planning consist of the authorization to initiate the SACM Program, communications with all of the other SACM sub-processes, and selected information and performance measurements received from the SACM Status Accounting sub-process. This sub-process and its activities are further facilitated by the degree of management support provided, the working relationships established with such other interfacing E-ITSM processes and USMC organizations, to include Engineering and Logistics. It is further enabled by the resources and facilities assigned to the function, including such resources as automated tools, connectivity to a shared data environment, and other infrastructure elements.

The SACM process management team, collaborating with key stakeholders, engages in the planning, decision making, and management efforts regarding the level of service asset and configuration management required for a selected service or project that is either new to a baseline or delivering changes to an existing baseline, and how this level will be achieved. The output from this sub-process consists of a SACM Plan that provides the planning details and the resultant documented SACM process that determines the extent of allocation of the SACM process functional activities.

Management and Planning does not perform these activities; it collaborates with SACM's additional four sub-processes to plan and manage as described below:

- Configuration Identification Sub-Process
  - Plan and manage how IT Assets and CIs are to be selected, grouped, classified, and defined by appropriate characteristics to ensure that they are manageable and traceable throughout their lifecycle.
  - Plan and manage the approach to identification, uniquely naming and labeling all the IT Assets or service components of interest across the service lifecycle and the relationships between them.
  - Plan and manage the roles and responsibilities of the owner or custodian for CI type at each stage of its lifecycle, e.g., the service owner for a service package or release at each stage of the service lifecycle.

- Configuration Control Sub-Process
  - Plan and manage requirements for supporting SACM tools and their system and data architectures.
  - Plan and manage control mechanisms over CIs while maintaining a record of changes to CIs, versions, location, and custodianship/ownership.
  - Plan and manage configuration control policies and procedures for the addition, modification, replacement, or removal of CIs.
  - Plan and manage control policies and procedures for software licenses, service asset versions, software and hardware versions, images/builds and releases, access, builds, promotions, migrations of electronic data and information, audits, deployments, and maintenance of the CMDB and DML.

- Status Accounting and Reporting Sub-Process
  - Plan and manage CI states through which it can/will progress. Includes planning the significance of each state in terms of what use can be made of the asset or CI in that state.
  - Plan and manage how CIs will move from one state to another.
  - Plan and manage why, when, and how the CMS should be updated at each lifecycle stage.
  - Plan and manage reporting mechanisms, scope, structures, and frequencies.

- Verification and Audit Sub-Process
  - Plan and manage how documented baselines maintain conformity to the environment to which they refer.
  - Plan and manage what (scope), when (frequency), and how audits are conducted.
  - Plan and manage audit remediation policies, to include Plan or Action and Milestone (POA&M) generation and approval authorities.

Infrastructure and services should have an up-to-date SACM Plan, which can stand alone or form part of other planning documents.

The SACM Plan defines the following:

- Purpose, scope, objectives of SACM.

- Related policies, standards, and processes specific to the support group.
- SACM roles and responsibilities.
- CI naming conventions as a related document (Marine Corps Naming Standard for Applications and Systems).
- Schedule and procedures for performing SACM activities.
- SACM system design including scope and key interfaces.
- Planning for Configuration Baselines, and Major Releases, Audits, etc.
- Archiving and CI retention Periods.
- SACM process to provide the following services:
    - Define the CIs that comprise related service(s) and infrastructure.
    - Control changes to configurations.
    - Record and report status of CIs.
    - Verify the completeness and correctness of CIs according to the requirements for accountability, traceability, and auditability.
- Configuration Control (access, protection, version, build, and release controls).
- Interface control process for identifying, recording, and managing CIs and information at the common boundary of two or more organizations (for example, system interfaces and releases).
- Planning and establishing the resources to bring assets and configurations under control and maintain the CMS.
- Management of suppliers and subcontractors performing SACM.

The following workflow in Figure 4-2 illustrates the activities in the Management and Planning sub-process:

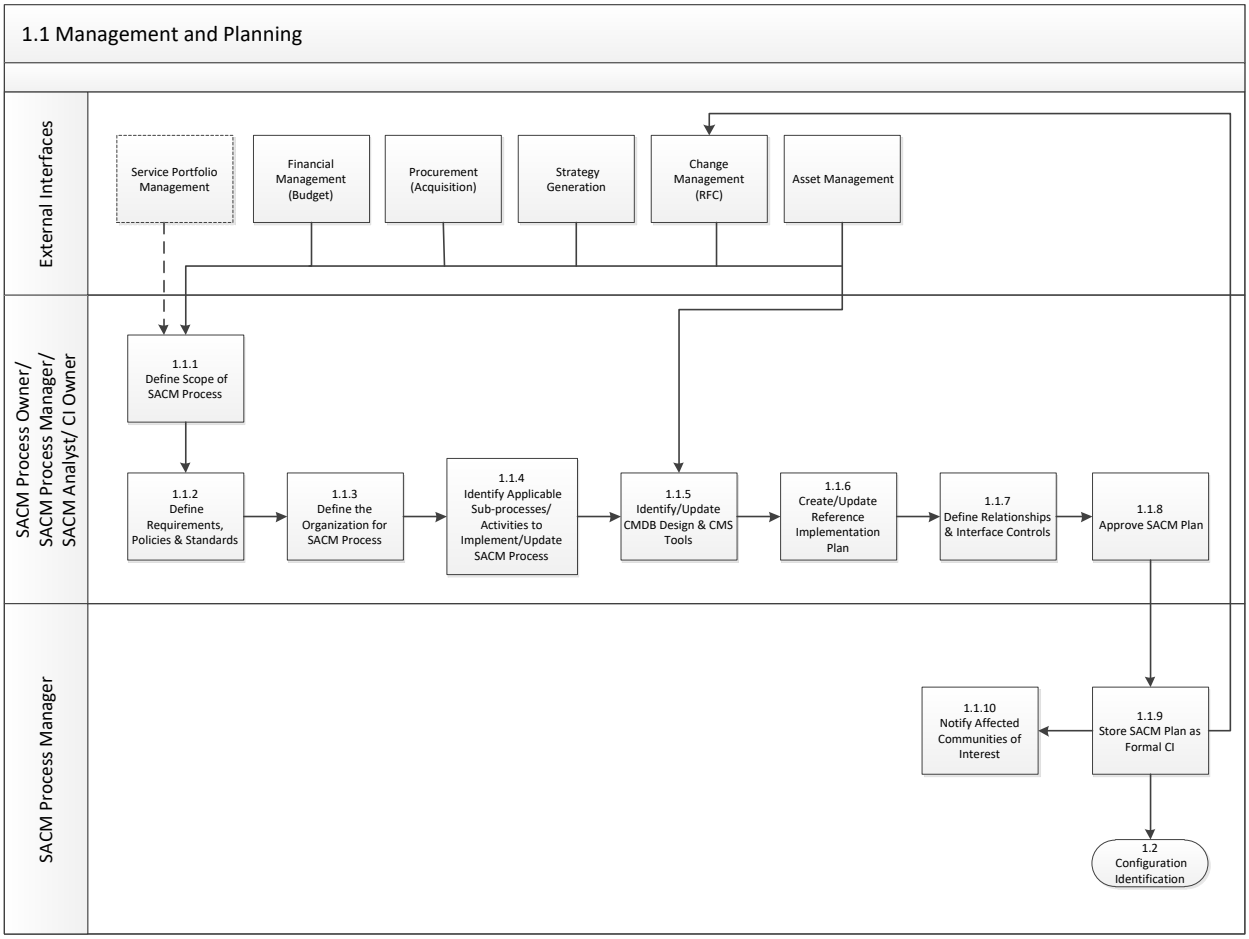



***Figure 4-2 Management and Planning Sub-Process Workflow***

Table 4-1 describes the Management and Planning sub-process activities illustrated in Figure 4-2:

637 **Table 4-1 Management and Planning Sub-Process Description**

| 1.1 Management and Planning | | |
|---|---|---|
| **Creates/Implements a SACM Plan** | | |
| **Number** | **Activity** | **Description** |
| 1.1.1 | Define Scope of SACM Process | SACM begins with the definition of the scope *(which CIs will be tracked)* and the IT infrastructure that needs to be covered by this process. The appropriate depth *(number and level of CIs to maintain)* and breadth *(level of detail to be tracked on CIs)* of the SACM process is based on organizational requirements. This includes updates to the SACM scope such as a new program/project/service.<br><br>Plan for an integrated SACM though its full lifecycle.<br><br>The scope definition includes:<br>• Applicable Services (New/Updated)<br>• Environments and Infrastructure (New/Updated)<br>• Geographical Locations (New/Updated)<br><br>Strategy Generation for the USMC may include:<br>• C4 - Plans and Policy<br>• PMO - Programmatic Strategy<br>• CDNI - Requirements<br><br>**Roles**: SACM Process Owner, SACM Process Manager, SACM Analyst, CI Owner<br><br>**Inputs**:<br>• Program Initiation/ Contract Portfolio, Customer Portfolio, Organizational Policy, Service Management Plan, from Strategy Generation<br>• Financial Information (Contract requirements) from Financial Management<br>• ITAM Scope (HW/SW/Licensing) from Asset Management<br>• Acquisition Data from Procurement<br>**Output**:<br>• SACM Scope |

| 1.1 Management and Planning | | |
|---|---|---|
| **Creates/Implements a SACM Plan** | | |
| **Number** | **Activity** | **Description** |
| 1.1.2 | Define Requirements, Policies & Standards<br><br>. | Identify the policies, requirements, and contractual requirements.<br>Link to other Service Management Policies, strategies, E-ITSM policies, USMC directives).<br>Link to requirements for the CMS.<br><br>Include policies and standards:<br>• Applicable Policies<br>• Industry Standards (DESMF, ISO/IEC 20000, ISO/IEC 19770-1)<br>• Internal standards relevant to SACM (hardware standards, desktop standards, software & licensing<br><br>Summarize requirements for accountability, traceability, auditability (depth and breadth for SACM process).<br><br>**Roles**: SACM Process Owner, SACM Process Manager, SACM Analyst, CI Owner<br><br>**Input**:<br>• SACM Scope<br>**Output**:<br>• SACM Policies and Standards |
| 1.1.3 | Define the Organization for SACM Process | Define the organizational structure for the SACM process, define the roles and responsibilities and determine the authorization for establishing baseline, changes, and releases of this process.<br><br>**Roles**: SACM Process Owner, SACM Process Manager, SACM Analyst, CI Owner<br><br>**Input**:<br>• SACM Policies and Standards<br>**Output**:<br>• SACM Organization Structure |

| 1.1 Management and Planning | | |
|---|---|---|
| **Creates/Implements a SACM Plan** | | |
| **Number** | **Activity** | **Description** |
| 1.1.4 | Identify Applicable Sub-processes /Activities to Implement/Update SACM Process | Based on the defined scope of the SACM process, identify and select the applicable sub-processes and activities to implement or update the SACM process.<br><br>To include:<br>• Configuration Identification<br>• Version Management<br>• Interface Management<br>• Supplier Management<br>• Configuration Control (Change Management)<br>• Release and Deployment<br>• Build Management<br>• Establishing and maintaining configuration baselines<br>• Maintaining the CMS<br>• Reviewing the integrity of configurations and the CMS (verification and audit)<br><br>**Roles**: SACM Process Owner, SACM Process Manager, SACM Analyst, CI Owner<br><br>**Input**:<br>• SACM Organization Structure<br>**Output**:<br>• SACM Sub-processes and Activities |
| 1.1.5 | Identify/Update CMDB Design & CMS Tools | Conduct CMDB design workshop as applicable.<br><br>Identify or update the software tools that will be used to create or automate CMS and leverage the Asset Management Database.<br><br>**Roles**: SACM Process Owner, SACM Process Manager, SACM Analyst, CI Owner<br><br>**Inputs**:<br>• ITAM System Details from Asset Management<br>• SACM Sub-processes and Activities<br>**Outputs**:<br>• CMS Software Tools updated or identified<br>• CMDB Design |

| 1.1 Management and Planning | | |
|---|---|---|
| **Creates/Implements a SACM Plan** | | |
| **Number** | **Activity** | **Description** |
| 1.1.6 | Create/Update Reference Implementation Plan | Create or update a reference implementation plan, (should include data migration and loading, training and knowledge transfer plan, etc.).<br><br>Build SACM catalog, product catalog, DML entries.<br><br>When implementing the plans, define the structures and foundation *(sites, location, owners)* data that will be used during Configuration Identification.<br><br>**Roles**: SACM Process Owner, SACM Process Manager, SACM Analyst, CI Owner<br><br>**Inputs**:<br>• CMS Software Tools updated or identified<br>• CMDB Design<br>**Output**:<br>• SACM Reference Implementation Plan |
| 1.1.7 | Define Relationships & Interface Controls | Define relationship management and interface controls. For example: with Financial Asset Management, with projects, with development and testing, with customers, with service providers interfaces (SPI), with operations including the service desk.<br><br>Include relationship management and control of suppliers and sub-contractors.<br><br>**Roles**: SACM Process Owner, SACM Process Manager, SACM Analyst, CI Owner<br><br>**Input**:<br>• SACM Reference Implementation Plan<br>**Output**:<br>• Draft SACM Plan |
| 1.1.8 | Approve SACM Plan | Review and approve new or updated SACM Plan.<br><br>**Roles**: SACM Process Owner (Review & Approve), SACM Process Manager, SACM Analyst, CI Owner (Review)<br><br>**Input**:<br>• Draft SACM Plan<br>**Output**:<br>• Approved SACM Plan |

| 1.1 Management and Planning | | |
|---|---|---|
| **Creates/Implements a SACM Plan** | | |
| **Number** | **Activity** | **Description** |
| 1.1.9 | Store SACM Plan as a formal CI | Submit SACM Plan through Change Management process for configuration control as an approved CI.<br><br>The SACM Plan is a living document that is in place to impose control on a project, but may be updated for additions and changes as appropriate.<br><br>**Role**: SACM Process Manager<br><br>**Input**:<br>• Approved SACM Plan<br>**Output**:<br>• RFC to store SACM Plan as a formal CI |
| 1.1.10 | Notify Affected Communities of Interest | Notify the affected communities of interest / stakeholders of the new or updated SACM Plan.<br><br>**Role**: SACM Process Manager<br><br>**Input**:<br>• Approved SACM Plan<br>**Output**:<br>• Notification of SACM Plan |

## 4.2 Configuration Identification

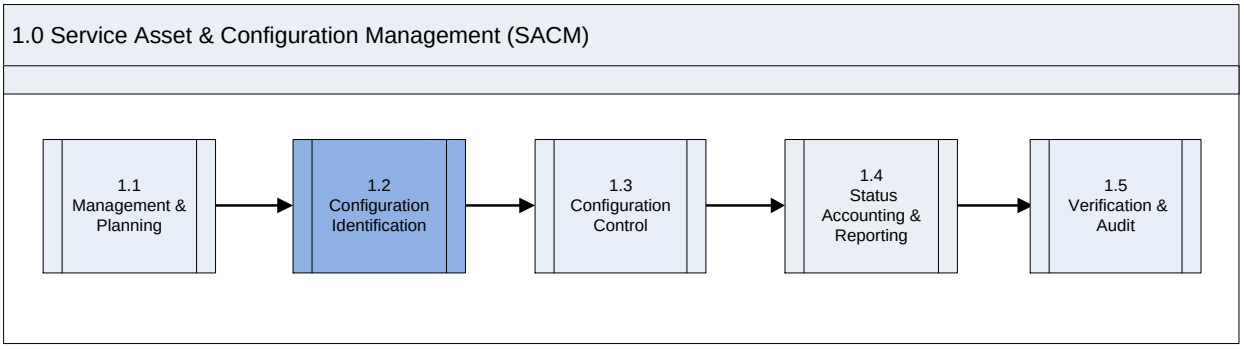



***Figure 4-3 SACM Process Overview – Configuration Identification Sub-Process***

The Configuration Identification sub-process highlighted in Figure 4-3 identifies and registers IT assets, service components and other items which will be under the control of SACM. The classes and types of CIs are selected, grouped, classified, defined, and named including the appropriate characteristics (e.g., warranties for a service) to ensure they are manageable and traceable throughout their lifecycle. The CIs and their components have been determined according to documented criteria established within the SACM Plan created in the SACM Management and Planning sub-process. As such, CIs identified include hardware, software and licenses, services, and documentation components of (and supporting) the USMC infrastructure.

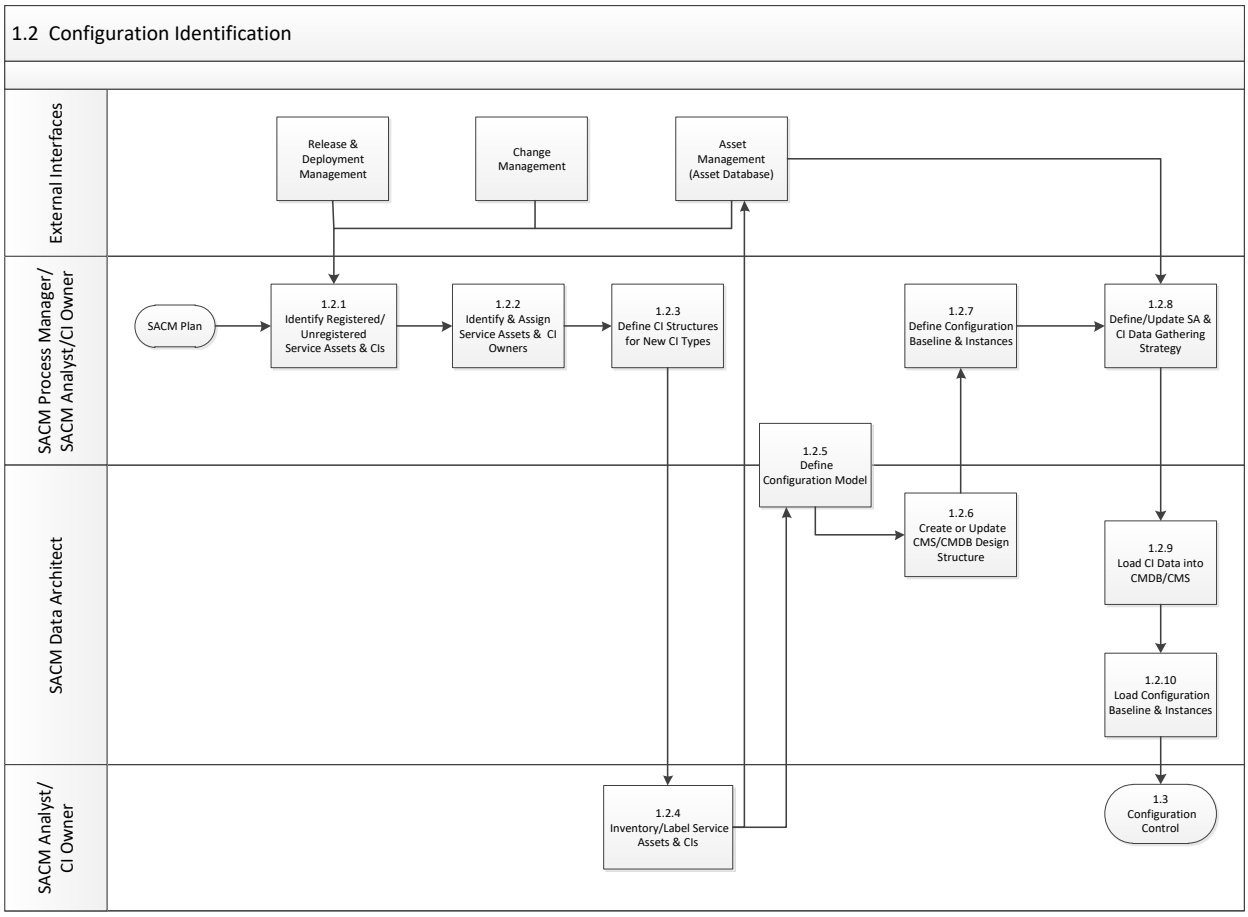
The Configuration Identification process enables:

- Identification and registration of CIs.
- Assignment of unique labels.
- Recording relationship information.
- Identification and designation of baselines for one or more CIs.
- Efficient data storage and retrieval.

Configuration Identification is responsible for collecting information about CIs and their relationships, and for loading this information into CMS/CMDB. Configuration Identification is also responsible for labeling the CIs, which enables the corresponding configuration records to be found.

A CI can only be registered if the CI type is known and a Configuration Management policy is available for these types. Existing types must match the attributes that need to be managed and allow for designation of a person who is responsible for maintaining the CI. All CIs must be assigned to an owner, (that is a reference to an organizational entity), and to an administrator (the group responsible for managing the CI during its lifecycle).

665 The following workflow in Figure 4-4 illustrates the activities in the Configuration Identification
666 sub-process:



667

668 ***Figure 4-4 Configuration Identification Sub-Process Workflow***

669 Table 4-2 describes the Configuration Identification sub-process activities illustrated in Figure 4-
670 4:

671 **Table 4-2 Configuration Identification Sub-Process Description**

| 1.2 Configuration Identification | | |
|---|---|---|
| **Identifies CIs** | | |
| **Number** | **Activity** | **Description** |
| 1.2.1 | Identify Registered/Unregistered Service Assets and CIs | Placing an item under this sub-process for the first time starts with a need that is defined in the SACM plan.<br><br>A change to a CI starts with a change request to place a CI under SACM.<br><br>Gather or discover CIs using a various means such as a physical inspection, leveraging the Asset Management Database, DPAS (manual/external interface), or CMDB, and using discovery tools to identify IT assets/CIs that are already registered and those that are new and need to be registered. |

| 1.2 Configuration Identification | | |
|---|---|---|
| **Identifies CIs** | | |
| **Number** | **Activity** | **Description** |
| | | **Roles**: SACM Process Manager, SACM Analyst, CI Owner<br><br>**Inputs**:<br>• ITAM<br>• Release & Deployment (Build & procure to rectify deviances from specifications for CI)<br>• Change Management<br>  ○ Capabilities<br>  ○ Resources<br>• SACM Plan (Requirements Design, Maintenance, Release, Deployment, Operations Plan)<br>• Scheduled CMDB Review (Requirements Design, Maintenance, Release, Deployment, Operations Plan)<br>**Outputs:**<br>• Unregistered service asset and CIs identified<br>• Registered service assets and CIs identified |
| 1.2.2 | Identify & Assign Service Assets & CI Owners | Appropriate staff is consulted in order to identify and assign unregistered CIs to the appropriate Service Asset and CI Owners.<br><br>This is a CI type owner with authorities for creating, authorizing, modifying or deleting the CIs of this type, as appropriate. Normally assigned access rights in the CMS and relevant sub-systems.<br><br>**Roles**: SACM Process Manager, SACM Analyst, CI Owner<br><br>**Input**:<br>• Unregistered service asset and CIs identified<br>**Output**:<br>• Identified Service Asset and CI Owners for unregistered CIs |
| 1.2.3 | Define CI Structures for New CI Types | Identify the structure or “template” for new CI types. Define and set attributes for CI Types, Relationships, etc.<br><br>The Configuration Structure describes the relationship and position of CIs for both infrastructure and services.<br><br>**Roles**: SACM Process Manager, SACM Analyst, CI Owner<br><br>**Inputs**:<br>• Registered service assets and CIs identified<br>• Identified Service Asset and CI Owners<br>**Output**:<br>• CMS/CMDB Structure Definition |
| 1.2.4 | Inventory/Label Service Assets & CIs | Service Asset and CI Owners will inventory and label the service assets and CIs (with unique identifiers as defined in the Naming Convention procedures) for which they are responsible.<br><br>**Roles**: SACM Analyst, CI Owner |

| 1.2 Configuration Identification | | |
|---|---|---|
| **Identifies CIs** | | |
| **Number** | **Activity** | **Description** |
| | | **Input**:<br>• CMS/CMDB Structure Definition<br>**Outputs**:<br>• Inventoried and Labeled service assets and CIs<br>• Updates to ITAM |
| 1.2.5 | Define Configuration Model | This is a model of services, assets, and infrastructure that records the relationships between CIs. It is meant to be a single common representation used by all areas of E-ITSM and other functions, such as finance, suppliers, etc.<br><br>The Configuration Model is used to:<br>• Plan technology refreshes and software upgrades<br>• Plan release and deployment packages<br>• Migrate services to different locations<br>• Assess impact of proposed changes<br>• Assess impact of incidents and problems<br>• Plan, design, and change new or existing services<br><br>**Roles**: SACM Process Manager, SACM Analyst, CI Owner, SACM Data Architect<br><br>**Input**:<br>• Inventoried and labeled service assets and CIs<br>**Output**:<br>• Configuration Model defined |
| 1.2.6 | Create or Update CMS/CMDB Design Structure | Using the Change Management process, facilitate additions or modifications to the CMDB Architecture and CMDB Objects.<br><br>Note: This activity is NOT focused on individual CIs or individual relationship instances. For example, this is NOT about creating an individual relationship between server ABC and router XYZ, but a higher overall level CMS/CMDB design structure.<br><br>Establish the template and structure (fields) that will be managed and controlled by the SACM Analysts for each CI instance (an occurrence that is a specific realization/recognition of any object).<br><br>CMDB Objects include:<br>• CI Instances<br>• CI Relationship Types (parent, child, etc.)<br>• CI Categories/Baselines<br><br>**Role**: SACM Data Architect<br><br>**Input**:<br>• Configuration Model defined<br>**Output**: |

| 1.2 Configuration Identification | | |
|---|---|---|
| **Identifies CIs** | | |
| **Number** | **Activity** | **Description** |
| | | • CMS/CMDB design structure (created or updated) |
| 1.2.7 | Define Configuration Baseline & Instances | The Configuration Baseline is the configuration of a service asset or infrastructure that has been formally reviewed and approved (must go through formal Change Management process).<br><br>This activity allows you to build a service component from a defined set of inputs.<br><br>Provides basis for a configuration audit or desired state (e.g., pre-changed state in the event a change must be backed out). Provides Snapshot to mark milestones in development of a service.<br><br>**Roles**: SACM Process Manager, SACM Analyst, CI Owner<br><br>**Input**:<br>• CMS/CMSD design structure<br>**Output**:<br>• Configuration Baseline and Instances define |
| 1.2.8 | Define/Update SA & CI Data Gathering Strategy | Identify the resources (people and tools (e.g., discovery tools)) that will be used to gather service asset and CI data.<br><br>**Roles**: SACM Process Manager, SACM Analyst, CI Owner<br><br>**Inputs**:<br>• Defined Configuration Baseline and Instances<br>• Service Asset and CI data from Asset Management / CMS databases<br>**Output**:<br>• Service Asset and CI Data Strategy |
| 1.2.9 | Load CI Data into CMDB/CMS | Load the available/collected service asset and CI data into the CMDB (Registration of CI information into the CMDB).<br><br>**Role**: SACM Data Architect<br><br>**Inputs**:<br>• Service Asset and CI Data Strategy<br>• Defined Configuration Baseline and Instances<br>**Output**:<br>• Service Asset and CI data loaded |
| 1.2.10 | Load Configuration Baseline & Instances | The Configuration Baseline is captured (a baseline is a snapshot of the current CMS/CMDB).<br><br>A snapshot describes the current state of a CI or environment and may be generated using a discovery tool. The snapshot is recorded in the CMS and remains a fixed historical record (referred to as a Footprint).<br><br>Enables Problem Management to analyze the historical state that existed at the time an incident occurred. |

| 1.2 Configuration Identification | | |
|---|---|---|
| **Identifies CIs** | | |
| **Number** | **Activity** | **Description** |
| | | Allows for a system restore if needed (as a result of a change or in support of security scanning software, etc.).<br><br>**Role**: SACM Data Architect<br><br>**Input**:<br>• Service Asset and CI data loaded into CMDB/CMS<br>**Output**:<br>• Configuration Baseline (CI identification, naming, labeling, data and documentation baseline) |

672
673

## 4.3 Configuration Control

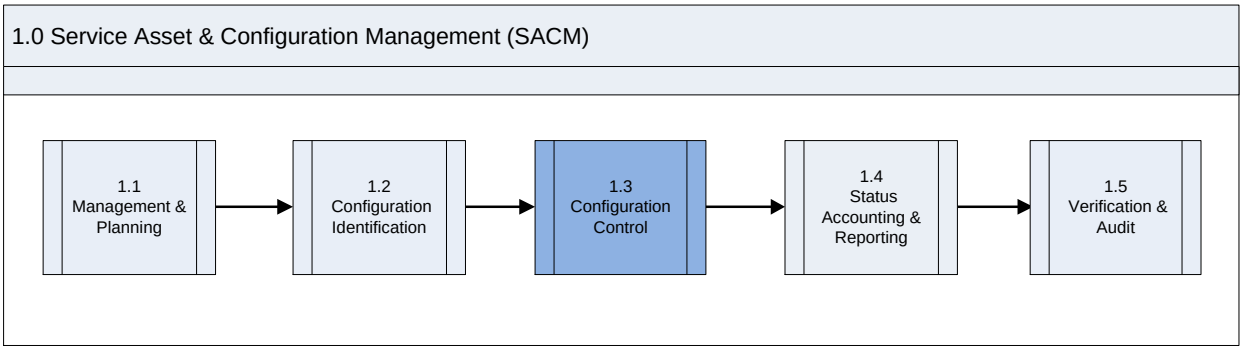



***Figure 4-5 SACM Process Overview – Configuration Control Sub-Process***

The Configuration Control sub-process highlighted in Figure 4-5 is an important part of the SACM process since it confirms that only identifiable and authorized CIs are recorded in the CMDB. Configuration Control ensures that there are adequate control mechanisms over CIs while maintaining a record of changes to CIs, versions, statuses, location, and ownership. This sub-process ensures that no CI is added, modified, replaced, or removed without appropriate controlling documentation or procedures in place.

Policies and procedures should cover the following:

- Version control of software, hardware, image builds, and releases.
- Access control to facilities, storage areas, and CMS, including user roles.
- Establishment of configuration baseline of CIs before supporting a release in a manner that can be used for subsequent evaluation against actual deployment.
- Promotion and/or migration of electronic data and information (including software license management and compliance), maintaining the integrity of the definitive media library DML and CMS within the overarching Service Knowledge Management System (SKMS).

Configuration Control applies the best practice for software license management and compliance with the ability to gain a single view into the control and maintenance of the software licenses across the enterprise. It is imperative to leverage and analyze accurate usage statistics to ensure the completeness of data matches the software vendor's license management results. Additionally, usage statistics can provide managers and other stakeholders with granular insight into their organizations' actual software usage. This can enable IT departments to establish shared license pools with prioritized resource allocation so users with high-priority needs can "reserve" a fixed number of shared licenses, ensuring software availability.

Software license management and compliance is about:

- Knowing what software you have installed.
- Knowing what software licenses have been purchased.
- Knowing that the installations don't exceed the license purchases.
- Knowing what software is being used.
- Knowing the details of the organization’s software license usage rights and restrictions.
- Knowing the number of underutilized software.
- Knowing what hardware assets the software is installed on.

- Maintaining compliance while significantly reducing overall software costs.

The following workflow in Figure 4-6 illustrates the activities in the Configuration Control sub-process:

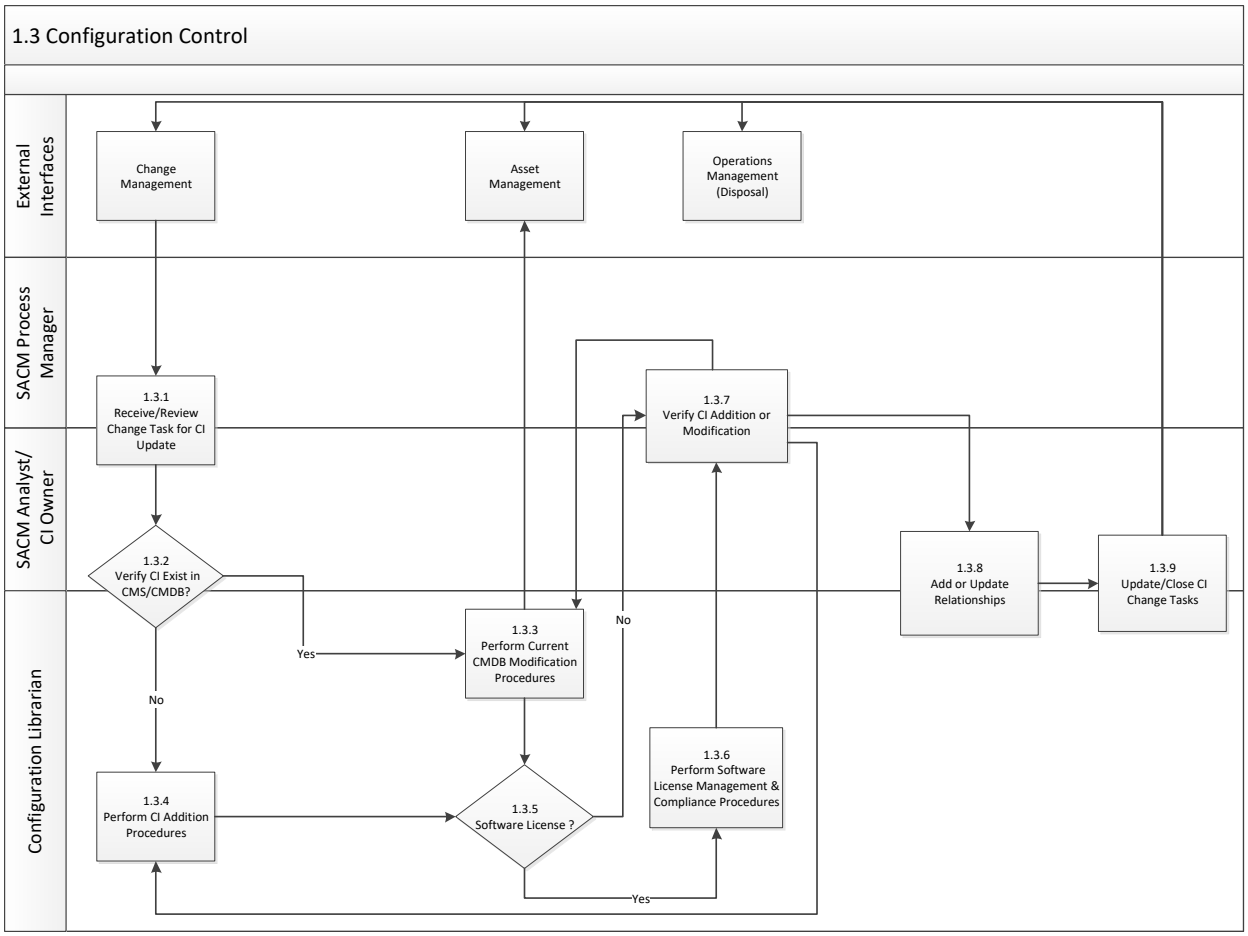



***Figure 4-6 Configuration Control Sub-Process Workflow***

713 The following Table 4-3 describes the Configuration Control sub-process activities illustrated in
714 Figure 4-6:

715 **Table 4-3 Configuration Control Sub-Process Description**

| 1.3 Configuration Control | | |
|---|---|---|
| **Controls Updates/Changes to CIs & Relationships** | | |
| **Number** | **Activity** | **Description** |
| 1.3.1 | Receive/Review Change Task for CI Update | A task is received from Change Management to make registration/updates to the CI data. The task is reviewed for scope and impact as well as for any issues in implementing the change.<br><br>**Roles**: SACM Process Manager, SACM Analyst, CI Owner<br><br>**Input**:<br>• RFC to register New CI or update current CI data<br>**Output**:<br>• Reviewed Change Task |
| 1.3.2 | Verify CI Exists in CMS/CMDB | Verify if the CI exists in the CMS/CMDB. Decision point to determine if a new CI needs to be added or a current CI needs to be modified.<br><br>**Roles**: SACM Analyst, CI Owner, Configuration Librarian<br><br>**Input**:<br>• Reviewed Change Task<br>**Outputs**:<br>• CI does exist - Modification required to current CI<br>• CI does not exist - New CI Required - the Configuration Librarian will complete the procedures to add the new CI to the CMDB |
| 1.3.3 | Perform Current CMDB Modification Procedures | Based on the modification activities in the Change task, updates to the CI data in the CMDB will be performed.<br><br>Procedures to modify existing CMDB data, primarily CI instances and instances of CI relationships. Also includes modifying CMDB architecture building block types/categories/baselines and relationship types.<br><br>**Role**: Configuration Librarian<br><br>**Inputs**:<br>• Modification required to current CI (Reviewed/Verified RFC to modify existing CIs in CMS/CMDB)<br>• From SACM Process Manager - CMS/CMDB Modification not successful<br>**Outputs**:<br>• Modified CI in CMS/CMDB<br>• Removed CI (Deregistered) from CMS/CMDB |

| 1.3 Configuration Control | | |
|---|---|---|
| **Controls Updates/Changes to CIs & Relationships** | | |
| **Number** | **Activity** | **Description** |
| 1.3.4 | Perform CI Addition Procedures | Based on the activities in the Change task, new CI additions in the CMDB will be performed.<br><br>Activities for normal everyday addition of new CMDB objects to include initial bulk loading of CIs.<br><br>CMDB Objects include:<br>• CI Instances<br>• CI Relationship Instances<br>• CI Architecture Building-block types/categories/baselines<br>• CI Relationship Types<br><br>**Role**: Configuration Librarian<br><br>**Inputs**:<br>• New CI Required<br>• From SACM Process Manager - CMS/CMDB Addition not successful<br>**Output**:<br>• New Registered CI |
| 1.3.5 | Software License? | Is a Software License required from the CI modification or addition? Decision point to further determine if the Software License is available or if an additional license(s) needs to be purchased.<br><br>**Role**: Configuration Librarian<br><br>**Inputs**:<br>• New Registered CI<br>• Modified CI in CMS/CMDB<br>**Outputs**:<br>• Software License Required<br>• Software License Not Required |

| 1.3 Configuration Control | | |
|---|---|---|
| **Controls Updates/Changes to CIs & Relationships** | | |
| **Number** | **Activity** | **Description** |
| 1.3.6 | Perform Software License Management & Compliance Procedures | Based on the activities in the Change task, Software License Management procedures for additional software license or update to current software licensing will be performed.<br><br>The Configuration Librarian will review the CMS (DML) and assign a software license or work with Change Management to revise software license assignment or Asset Management to acquire new software licenses.<br><br>**Role**: Configuration Librarian<br><br>**Input**:<br>• Reviewed RFC for additional software license or update to current software licensing<br>**Outputs**:<br>• Assigned Software License<br>• RFC for Harvesting Software License to Change Management<br>• Software License Purchase Request/Requirement to Asset Management (for procurement) |
| 1.3.7 | Verify CI Addition or Modification | Upon completion of CMDB modifications (new CI, de-registration, and CI updates), review the CMS/CMDB to verify that the modifications are accurate and met the RFC and policy scope.<br><br>This task ensures that the CI status has been updated in the CMS/CMDB and that all CMS/CMDB objects associated with the task have been added or modified.<br><br>Focus particular attention on Change tasks to create/modify CMDB architecture building blocks or that relate to a Normal Change.<br><br>**Roles**: SACM Process Manager, SACM Analyst, CI Owner<br><br>**Inputs**:<br>• Registered CI (from Perform CI Addition RFC)<br>• Modified CI (from Perform Current CMDB Modification RFC)<br>• Removed CI (Deregistered ) from CMS/CMDB<br>**Outputs**:<br>• CMS/CMDB Addition/Modification not successful<br>• Verified CMS/CMDB Addition/Modification |

| 1.3 Configuration Control | | |
|---|---|---|
| **Controls Updates/Changes to CIs & Relationships** | | |
| **Number** | **Activity** | **Description** |
| 1.3.8 | Add or Update Relationship | Upon verified completion of the CI data load/update, relationships between the CI and other CIs in the CMS/CMDB will be established or updated.<br><br>**Roles**: SACM Analyst, CI Owner, Configuration Librarian<br><br>**Input**:<br>• Verified CMS/CMDB Addition/Modification (Registered/updated CIs)<br>**Output**:<br>• CI Relationships established or updated |
| 1.3.9 | Update/Close CI Change Tasks | Ensure that the Change Task(s) are updated with all relevant details, including any issues, and closed.<br><br>**Roles**: SACM Analyst, CI Owner, Configuration Librarian<br><br>**Input**:<br>• CI Relationships updated (from Add or Update relationship)<br>**Outputs**:<br>• Closed Change Task<br>  ○ Feeds back into Change Management<br>• Decommissioned /Deregistered CI<br>  ○ Feeds into ITAM/CI needs to be removed<br>  ○ Feeds into Operations Management/Decommissioned service asset and CI |

716

717

### 4.3.1 Configuration Control – Activity: 1.3.3 Perform CI Addition Procedures

The following workflow in Figure 4-7 illustrates the steps in the Activity - 1.3.3 Perform CI Addition Procedures:

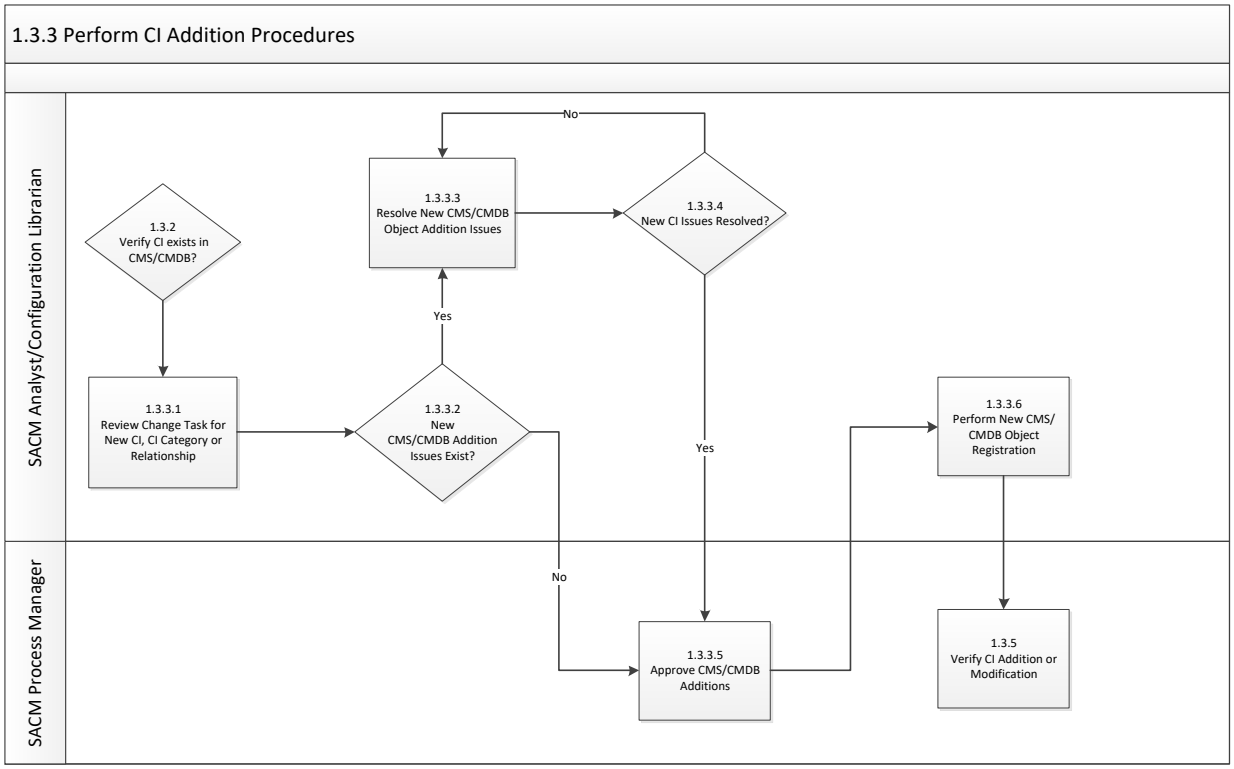



***Figure 4-7 1.3.3 Perform CI Addition Procedures***

The following Table 4-4 describes the Activity - 1.3.3 Perform CI Addition Procedures illustrated in Figure 4-7:

**Table 4-4 Perform CI Addition Procedures Description**

| 1.3.3 Perform CI Addition Procedures | | |
|---|---|---|
| **Number** | **Activity** | **Description** |
| 1.3.3.1 | Review Change Task for New CI, CI Category or Relationship | The request to add new elements to the CMS/CMDB is reviewed and analyzed.<br><br>**Roles**: SACM Analyst, Configuration Librarian<br><br>**Input**:<br>• New CI required<br>**Output**:<br>• Reviewed Change Task |

| 1.3.3 Perform CI Addition Procedures | | |
|---|---|---|
| **Number** | **Activity** | **Description** |
| 1.3.3.2 | Check for CMS/CMDB Addition issues | If there are any issues in adding the new CI, the SACM Process Manager will assign a SACM Analyst to resolve the issue. If there are no issues, the request can be approved.<br><br>**Roles**: SACM Analyst, Configuration Librarian<br><br>**Input**:<br>• Reviewed Change Task<br>**Outputs**:<br>• Issues Exist - begin remediation activities<br>• Issues Do Not Exist - begin new CMS/CMDB addition |
| 1.3.3.3 | Resolve New CMS/CMDB Object Addition Issues | The SACM Analyst and additional roles as necessary, will attempt to resolve any issues with adding a CI to the CMS/CMDB.<br><br>**Roles**: SACM Analyst, Configuration Librarian<br><br>**Input**:<br>• Issues Exist (Any data gathered to assist in resolving the issue)<br>**Outputs**:<br>• Issues Resolved - The Process Manager will review/approve the CMS/CMDB additions<br>• Issues Not Resolved- continue to resolve issues before adding CI Object to the CMDB |
| 1.3.3.4 | Ensure that New CI Issues are Resolved | If the issues regarding adding a new CI, CI Category, or Relationship are resolved, the CMS/CMDB can be modified accordingly.<br><br>If the issues have not been resolved, work continues to resolve data issues using necessary resources.<br><br>**Roles**: SACM Analyst, Configuration Librarian<br><br>**Input**:<br>• Resolution Results<br>**Outputs**:<br>• Issues Resolved - The Process Manager will review/approve the CMS/CMDB addition<br>• Issues Not Resolved - Continue to resolve issues before adding CI Object to the CMDB |
| 1.3.3.5 | Approve CMS/CMDB Additions | Once the issue (if any) has been resolved, the requested addition to the CMS/CMDB can be approved.<br><br>**Role**: SACM Process Manager<br><br>**Input**:<br>• Issues Resolved (Resolution results)<br>**Output**:<br>• CMS/CMDB Addition Approved |

| 1.3.3 Perform CI Addition Procedures | | |
|---|---|---|
| **Number** | **Activity** | **Description** |
| 1.3.3.6 | Perform New CMS/CMDB Object Registration | Perform procedures for adding a new CMS/CMDB object.<br><br>CMDB Objects include:<br>• CI Instances<br>• CI relationship instances<br>• CI architecture building-block types/categories/baselines<br>• CI relationship types<br><br>**Roles**: SACM Analyst, Configuration Librarian<br><br>**Input**:<br>• CMS/CMDB Addition Approved<br>**Output**:<br>• Newly registered CI in CMS/CMDB |

726

727

### 4.3.2 Configuration Control – Activity: 1.3.4 Perform CI Modification Procedures

The following workflow in Figure 4-8 illustrates the steps in the Activity - 1.3.4 Perform Current CMDB Modification Procedures:

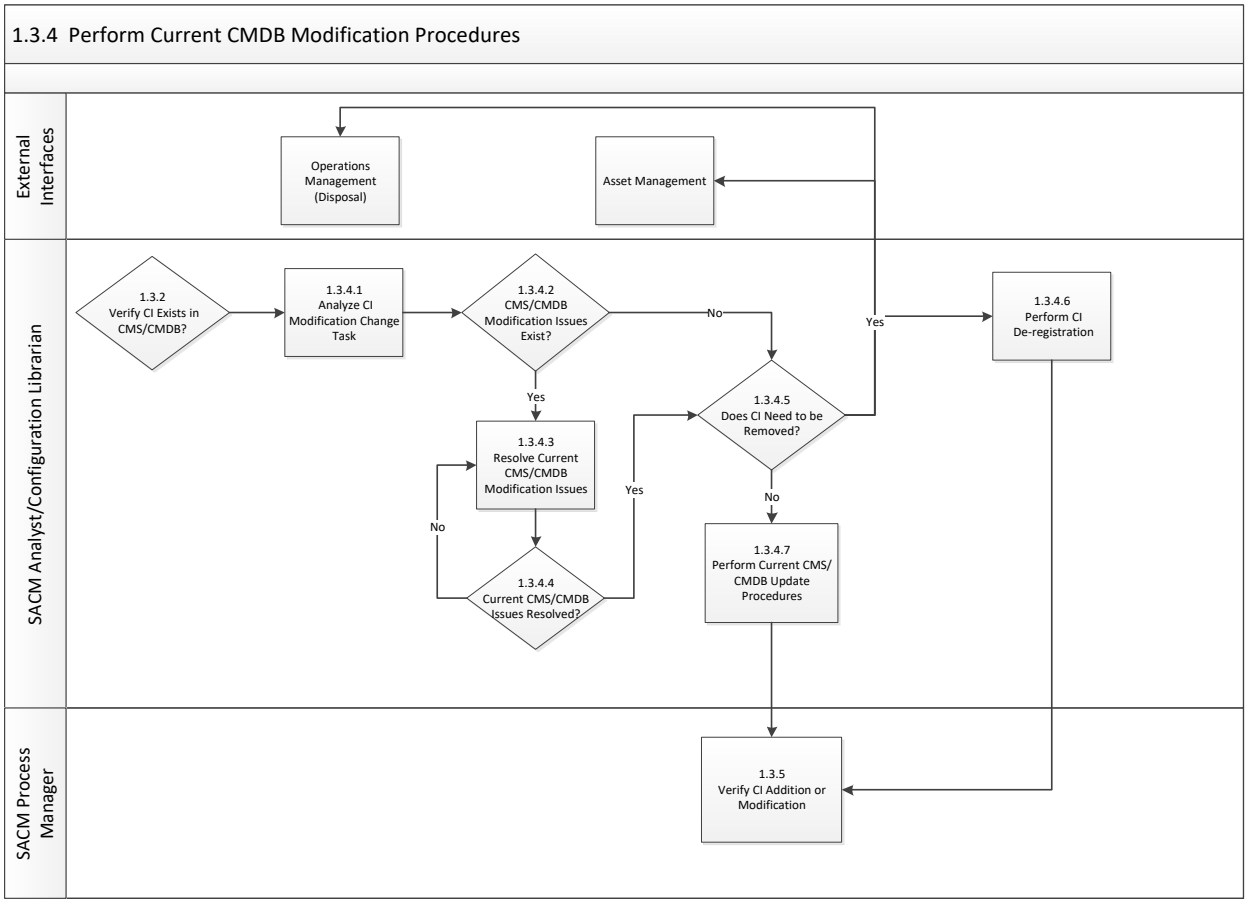



***Figure 4-8 1.3.4 Perform Current CMDB Modification Procedures***

The following Table 4-5 describes the Activity - 1.3.4 Perform Current CMDB Modification Procedures illustrated in Figure 4-8:

**Table 4-5 Perform Current CMDB Modifications Procedures Description**

| 1.3.4 Perform Current CMDB Modifications Procedures | | |
|---|---|---|
| **Number** | **Activity** | **Description** |
| 1.3.4.1 | Analyze CI Modification Change Task | Change Task is reviewed and analyzed to determine if there are any issues preventing the modification from being completed.<br><br>**Role**: SACM Analyst, Configuration Librarian<br><br>**Inputs**:<br>• Verification that the CI does exist in the CMDB<br>• Modification required to current CI<br>**Output**:<br>• Reviewed Change Task |

| 1.3.4 Perform Current CMDB Modifications Procedures | | |
|---|---|---|
| **Number** | **Activity** | **Description** |
| 1.3.4.2 | Do CMS/CMDB Modification issues exist? | If there are any issues with the CMDB modification, an attempt is made to resolve them, additional resources may be necessary.<br><br>**Roles**: SACM Analyst, Configuration Librarian<br><br>**Input**:<br>• Reviewed Change Task<br>**Output**:<br>• Issues Exist - Attempt to resolve the modification issues<br>• Issues Do Not Exist - Continue with the CMS/CMDB Modification |
| 1.3.4.3 | Resolve Current CMS/CMDB Modification issues | The SACM Analyst and additional roles/resources as necessary, will attempt to resolve any issues with modifying a current CI in the CMS/CMDB.<br><br>Procedures performed to resolve any issues that were discovered when attempting to modify the current CMS/CMDB.<br><br>**Roles**: SACM Analyst, Configuration Librarian<br><br>**Input**:<br>• Issues Exist (Resolution needed in order to complete the modification)<br>**Output**:<br>• Modification Resolution |
| 1.3.4.4 | Current CMS/CMDB Issues Resolved? | If not, continue resolution attempts.<br><br>**Roles**: SACM Analyst, Configuration Librarian<br><br>**Input**:<br>• Modification Resolution<br>**Output**:<br>• Issues Not Resolved- continue resolution attempts<br>• Issues Resolved - CI can now either be modified or removed. |
| 1.3.4.5 | Determine If CI Needs to be Removed | If any CIs need to be removed from the CMDB, the CIs are identified for de-registration.<br><br>CIs are removed only in the event of administrative or technical error.<br><br>**Roles**: SACM Analyst, Configuration Librarian<br><br>**Input**:<br>• Issues Resolved<br>• Issues Do Not Exist<br>**Output**:<br>• CI Needs to be Removed (De-register)<br>• CI Does Not Need to be Removed |

| 1.3.4 Perform Current CMDB Modifications Procedures | | |
|---|---|---|
| **Number** | **Activity** | **Description** |
| 1.3.4.6 | Perform CI De-registration | If the task is to de-register the CI from IT Infrastructure, the requested CI or CI instances are removed from the CMDB. A removal of a CI is considered a modification.<br><br>The status is modified to archived/de-commissioned as appropriate.<br><br>**Roles**: SACM Analyst, Configuration Librarian<br><br>**Input**:<br>• CI Needs to be Removed<br>**Outputs**:<br>• Removed CI (De-registration) from CMS/CMDB<br>• CMS/CMDB Update (De-registration) |
| 1.3.4.7 | Perform Current CMS/CMDB Update Procedures | Procedures to modify the CI in the CMDB are performed.<br><br>**Roles**: SACM Analyst, Configuration Librarian<br><br>**Input**:<br>• CI Does Not Need To Be Removed<br>**Output**:<br>• Modified CI |

736

737

## 4.4 Status Accounting and Reporting

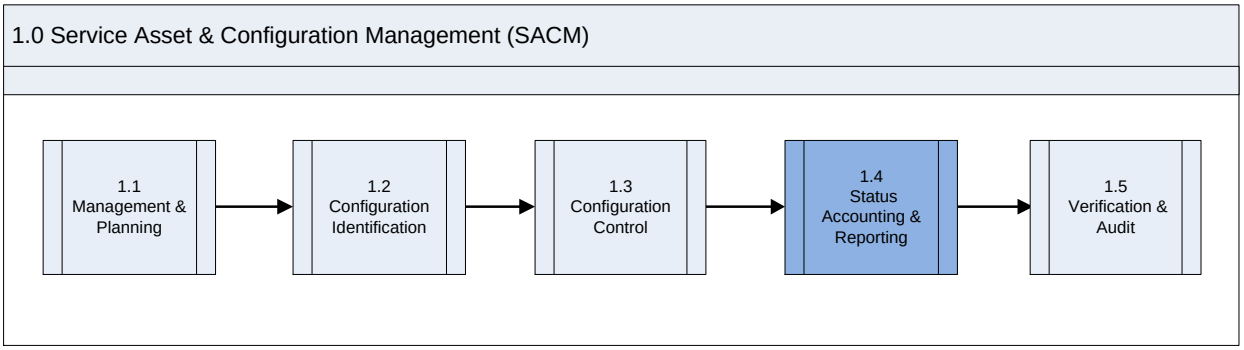



***Figure 4-9 SACM Process Overview – Status Accounting and Reporting Sub-Process***

The Status Accounting and Reporting sub-process highlighted in Figure 4-10 ensures that all service asset and configuration data and documentation is recorded as each service asset and CI progresses through its lifecycle from test to production to retirement. These lifecycle transactions are integrated with E-ITSM Change Management process and Release and Deployment Management process activities to achieve a high degree of accuracy.

Status Accounting and Reporting is the recording and reporting of information needed to manage configuration issues effectively, including a record of approved configuration documentation and identification numbers, the status of proposed changes and variances to the configuration, the implementation status of approved changes and the configuration of units of the CI in the operation inventory as required.

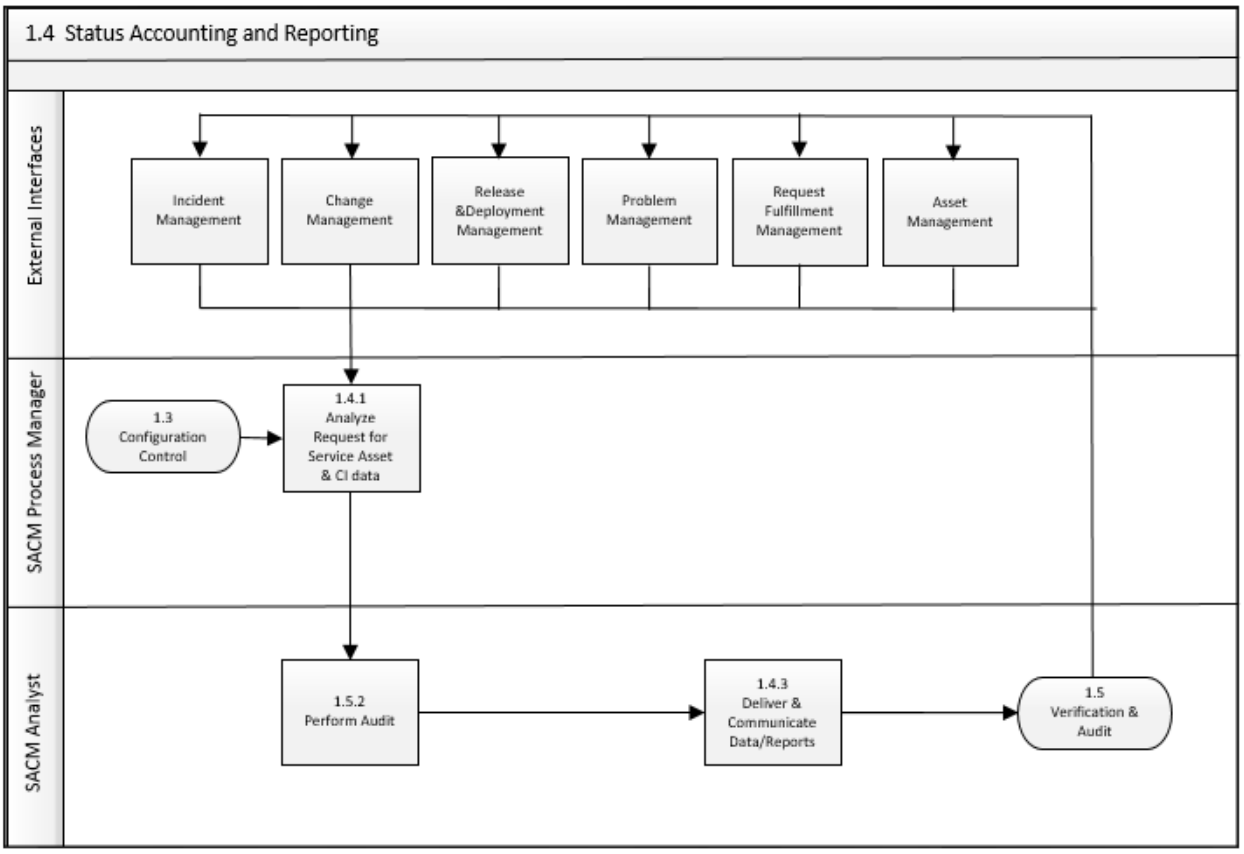
Status Accounting and Reporting is the process of recording state changes to a CI record. Some common states are: ordered, received, in acceptance test, live, under change, withdrawn, or disposed. All state changes must be recorded so the CMDB always has an accurate representation of the IT infrastructure. Status Accounting answers the following questions: (1) What happened? (2) Who did it? (3) When did it happen? and (4) What else will be affected?

Status reports should be produced on a regular basis, listing all CIs under control, their current version, change history, and include IT asset information (lease renewals, licensing, maintenance, etc.). There are two types of reports: reports accounting for the lifecycle status of CIs as defined by CI type, and other SACM reports in support of services throughout the service lifecycle.

Typical activities in this sub-process include:

- Maintaining configuration records through the service lifecycle.
- Managing the recording, retrieval and consolidation of the current configuration status and the status of all preceding configuration to confirm information correctness.
- Making the status of items under SACM available throughout the lifecycle.
- Recording changes to the CIs from receipt to disposal.

The following workflow in Figure 4-11 illustrates the activities in the Status Accounting and Reporting sub-process:




768

769 ***Figure 4-10 Status Accounting and Reporting Sub-Process Workflow***

770

771 Table 4-7 describes the Status Accounting and Reporting Sub-Process activities illustrated in
772 Figure 4-11.

773 **Table 4-6 Status Accounting and Reporting Sub-Process Description**

| 4.0 Status Accounting and Reporting | | |
|---|---|---|
| **Recording/Reporting on the Lifecycle of CIs** | | |
| **Number** | **Activity** | **Description** |
| 1.4.1 | Analyze Request for Service Asset and CI Data | Use the CMS, CMDB, DML, and Auto-Discovery tools to obtain current and historical service asset and CI data and status data.<br><br>This activity is triggered by a request for service asset and CI data or to generate periodic status reports (from Configuration Control).<br><br>• Review a request for a report on a CI, type, or attribute<br>• Validate distribution authority<br>• Determine if this request is to produce an ongoing standard report<br><br>**Role**: SACM Process Manager<br><br>**Inputs**:<br>• Automated Discovery reports<br>• Returns from CMS query<br>• Service Asset, CI data, and Status data from CMS<br>**Output**:<br>• Service Asset and CI data |

| 4.0 Status Accounting and Reporting | | |
|---|---|---|
| **Recording/Reporting on the Lifecycle of CIs** | | |
| **Number** | **Activity** | **Description** |
| 1.4.2 | Define and Produce CMS Reports | Based on the requirements and retrieved data, produce requested CMS reports.<br><br>• Define and build report.<br>• Design a report that meets the needs of the requester.<br>• Create the report.<br><br>This data may be gathered real-time based on the service asset and CIs stored in the CMS or sourced from a predefined CMS report.<br><br>It is best if reports are structured as exception reports so that the volume of data is limited to something that is manageable and actionable.<br><br>Multiple standard reports can be defined as business needs dictate, but output should result in a volume of data that is useable by those to whom it is distributed.<br><br>Reports may be scheduled to run at an agreed interval (e.g., daily, weekly, monthly, quarterly, etc.) and distributed to individuals with a known interest in CMS activities, or produced ad hoc based on demand.<br><br>**Role**: SACM Analyst<br><br>**Input**:<br>• Service Asset and CI data (from queried databases and discovery reports)<br>**Output**:<br>• Generated service asset and CI data report |
| 1.4.3 | Deliver and Communicate Report | The SACM Analyst moves the generated report to a designated website or distributed via email. Report contents are communicated as appropriate.<br><br>• Deliver the report to the requester.<br>• Validate the report with the requester.<br>• Exceptions/anomalies detected (Exception Reports) will be provided to Verification & Audit.<br><br>Additionally, these reports may be used to aid verification and audit activities, assess effectiveness of the SACM process, produce Software License Compliance data, or trigger archiving activities for CI data.<br><br>**Role**: SACM Analyst<br><br>**Input**:<br>• Generated service asset and CI data report<br>**Output**:<br>• Completed service asset and CI data report |

774

## 4.5 Verification and Audit

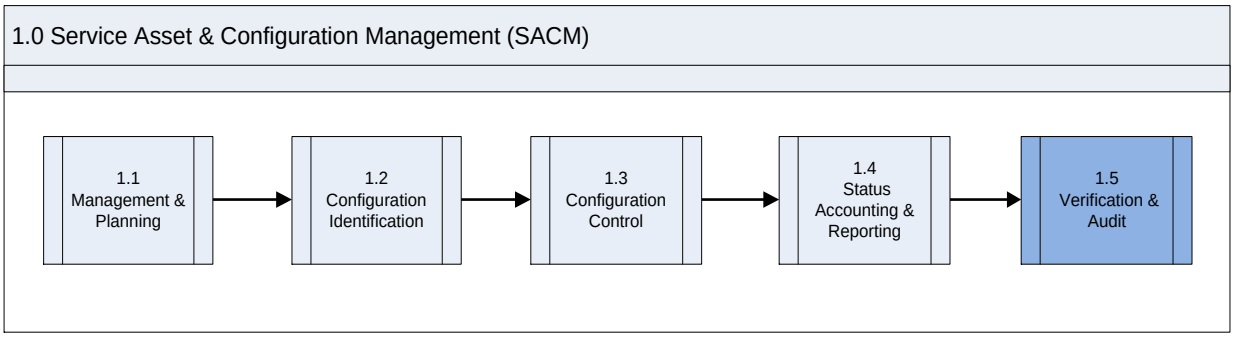



***Figure 4-11 SACM Process Overview – Verification and Audit Sub-Process***

The Verification and Audit sub-process highlighted in Figure 4-12 is responsible for ensuring that information in SACM is accurate and that all CIs are identified and recorded in the CMDB. This process can be conducted manually, or by using automated inventory and discovery tools.

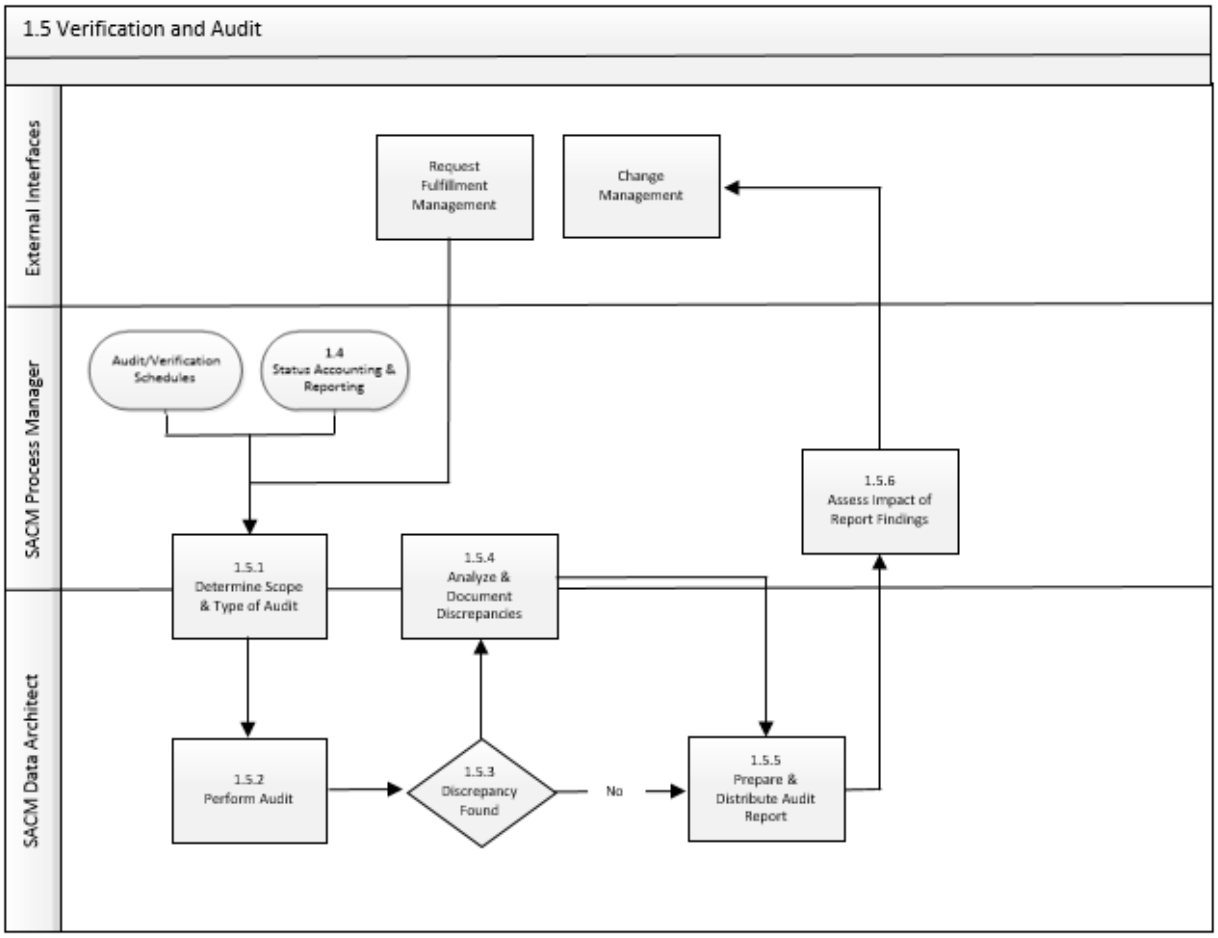
Verification includes routine checks that are part of other processes (for example, verifying the serial number of a desktop PC when a user logs an incident). Audit is a periodic, formal check. Verify and audit configuration regularly to ensure proper functioning of the entire SACM process, and for related E-ITSM processes.

The objective of Verification and Audit for the SACM process is to detect and manage all exceptions to configurations policies, processes, and procedures, including security and license use rights. The verification process ensures that configuration records are accurate and complete, and that any recorded changes are approved. Configuration audits help to maintain the integrity of the CMS.

The following activities include a series of reviews or audits:

- Ensure conformity between the documented baselines and the actual USMC environment.
- Verify the physical existence of CIs in the organization or in the DML.
- Verify functional and operational characteristics of CIs and check that the records in the CMS match the physical infrastructure.
- Check that release and configuration documentation is present before supporting a release.
- Verify Software Licensing usage to ensure compliance.

797 The following workflow in Figure 4-13 illustrates the activities in the Verification and Audit sub-
798 process:




799

800 ***Figure 4-12 Verification and Audit Sub-Process Workflow***

801 Table 4-8 describes the Verification and Audit sub-process activities illustrated in Figure 4-13:

802 **Table 4-7 Verification and Audit Sub-Process Description**

| 5.0 Verification and Audit | | |
|---|---|---|
| **Verify Configuration Changes/Perform Periodic Configuration Audits** | | |
| **Number** | **Activity** | **Description** |
| 1.5.1 | Determine Scope and Type of Audit | Plan and determine the portion of the CMS (CMDB/DML, etc.) and or service assets to be verified and audited.<br><br>Requirements are reviewed and validated regarding the need for the audit. Confirm and schedule resources to perform and participate in the audit. Identify the affected areas and inform the concerned parties.<br><br>Configuration Audits occur:<br>• Shortly after changes to the CMS.<br>• Software License Compliance needs.<br>• Before /after changes to IT services or infrastructure.<br>• Before a release or installation to ensure the environment is as expected.<br>• Following the recovery from disasters and after a "return to normal" (in this case, the audit should be included in contingency plans).<br>• At planned intervals per the SACM Plan, annually at a minimum.<br>• At random intervals.<br>• In response to the detection of any unauthorized CIs.<br><br>**Roles:** SACM Process Manager, SACM Data Architect<br><br>**Inputs**:<br>• Scheduled Audit<br>• Verification Scheduled<br>• Ad Hoc audit request<br>**Output**:<br>• Scope and Type of Audit |

| 5.0 Verification and Audit | | |
|---|---|---|
| **Verify Configuration Changes/Perform Periodic Configuration Audits** | | |
| **Number** | **Activity** | **Description** |
| 1.5.2 | Perform Audit | The procedures for auditing the CMS are represented by this activity - (refer to documented organizational audit procedures).<br><br>The SACM Analyst will perform the audit with assistance as needed from the CI Owner to establish reports on the CMDB, service assets, CIs, and Infrastructure baselines.<br><br>A comparison is done between infrastructure and CMS using a Physical and/or Discovery tool audit.<br><br>**Role**: SACM Data Architect<br><br>**Input**:<br>• Scope, Definition, and Type of Audit<br>**Output**:<br>• Verification and Audit Results (will be reviewed for discrepancies) |
| 1.5.3 | Note Discrepancies | Determine if there is a discrepancy found in the results of the audit performed.<br><br>**Role**: SACM Data Architect<br><br>**Input**:<br>• Audit Results<br>**Outputs**:<br>• Discrepancy Found – Discrepancies will be analyzed and document with the SACM Process Manager<br>• Discrepancy Not Found – Prepare & Distribute Audit Report |
| 1.5.4 | Analyze and Document Discrepancies | Analyze and document the identified audit discrepancies. Based on the findings of the audit, determine corrective action – if action should be taken to address audit finding (such as data or process issues). Any exceptions noted are documented. Provide proposed corrective actions.<br><br>A key component of the verification and audit activities is the reconciliation between the managed and discovered inventories and configurations.<br><br>**Roles**: SACM Process Manager, SACM Data Architect<br><br>**Input**:<br>• Audit Results - Discrepancies Found<br>**Outputs**:<br>• Documented Discrepancies<br>• Proposed Corrective Action |

| 5.0 Verification and Audit | | |
|---|---|---|
| **Verify Configuration Changes/Perform Periodic Configuration Audits** | | |
| **Number** | **Activity** | **Description** |
| 1.5.5 | Prepare & Distribute Audit Report | Upon completion of the audit, prepare the audit findings report, including documented discrepancies if any, and distributed to appropriate stakeholders.<br><br>**Role**: SACM Data Architect<br><br>**Inputs**:<br>• Discrepancy Analysis Results (Findings from audit)<br>• Audit Results – no discrepancies<br>**Outputs**:<br>• Discrepancy Analysis Results- These results will be used to prepare the Audit Report<br>• Audit Report- after the SACM Analyst completes the Audit Report, it will be sent to the SACM Process Manager to assess the impact on the CMS/CMDB and infrastructure. |
| 1.5.6 | Assess Impact of Report Findings | Results of the audit report are reviewed and a determination is made regarding the possible impacts. The audit data is communicated to stakeholders, along with a recommended course of action.<br><br>It is determined if the exceptions were due to process activity violations. A risk impact analysis of the exceptions is included. The recommended course(s) of action are prioritized.<br><br>Document and communicate the remediation required to meet the baseline requirements of the reference model.<br><br>Any updates to the CMDB should be performed through Change Management. If updates to the CMDB are required, RFCs are prepared.<br><br>**Role:** SACM Process Manager (other process roles may be consulted)<br><br>**Input**:<br>• Audit Report<br>**Outputs**:<br>• Impact findings accessed<br>• Feedback to determine if an update to the SACM Plan is needed |

803

# Appendix A – GLOSSARY

| Term | Definition |
|---|---|
| Asset Management | Asset Management is the process responsible for tracking and reporting the financial value and ownership of assets throughout their lifecycle. |
| Backup | Backup is copying data to protect against loss of integrity or availability of the original data. |
| Configuration Control | Configuration Control is a sub-process of Service Asset & Configuration Management. Configuration Control is a set of processes and approval stages required to change a CI attribute. Configuration Control encompasses the oversight to ensure that a CI is changed through the Change Management process. |
| Configuration Identification | A sub-process of Service Asset & Configuration Management, Configuration Identification is the selection, identification, and labeling of the configuration structures and CIs including their respective technical owner and the relationships between them. CIs become the manageable unit that is planned for release into a configuration controlled environment. The CIs consist of hardware, software, services, and documentation. |
| Configuration Item | A Configuration Item (CI) is any component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the Configuration Management System (CMS) and is maintained throughout its lifecycle by Service Asset & Configuration Management. CIs are under the control of Change Management. CIs typically include IT services, hardware, software, buildings, people, and formal documentation such as process documentation and SLAs. |
| CI Type | CI Type is a category used to Classify CIs. The CI Type identifies the required attributes and relationships for a configuration record. Common CI Types include: server, document, user, etc. |
| Configuration Management Database | A Configuration Management Database (CMDB) is a database used to store configuration records throughout their lifecycle. The Configuration Management System (CMS) maintains one or more CMDBs and each CMDB stores attributes of CIs and relationships with other CIs. |
| Configuration Management System | A Configuration Management System (CMS) is a set of tools and databases used to manage an IT service provider's configuration data. The CMS also includes information about incidents, problems, known errors, changes, and releases and may contain data about employees, suppliers, locations, units, customers and users. The CMS includes tools for collecting, storing, managing, updating, and presenting data about all CIs and their relationships. The CMS is maintained by Service Asset & Configuration Management and is used by all IT Service Management processes. |
| Deployment | Deployment is the activity responsible for movement of new or changed hardware, software, documentation, process, etc. to the live environment. Deployment is part of the Release and Deployment Management Process. |
| Deployment Readiness Test | A Deployment Readiness Test is conducted to ensure that the deployment processes, procedures, and systems can deploy, install, commission, and decommission the release package and resultant new or changed service in the production/deployment environment. |
| Deployment Verification Test | A Deployment Verification Test is conducted to ensure the service capability has been correctly deployed for each target deployment group or environment. |
| Environment | Environment is a subset of the IT infrastructure used for a particular purpose (e.g., live environment, test environment or build environment). It is possible for multiple environments to share a CI (e.g., test and live environments may use different partitions on a single mainframe computer). In the term physical environment, environment can be defined as the accommodation, air conditioning, power system, etc. Environment can be used as a generic term defined as the external conditions that influence or affect something. |
| Error | An Error is a design flaw or malfunction that causes a failure of one or more CI or IT services. A mistake made by a person or a faulty process that affects a CI or IT service is also an error. |

| Term | Definition |
|---|---|
| Event | An Event is a piece of data that provides information about one or more system resources. Most events are benign. Some events show a change of state which has significance for the management of a CI or IT service. The term 'event' is also used to define an alert or notification created by any IT service, CI, or monitoring tool. Events typically require IT operations personnel to take actions and often lead to incidents being logged. |
| Fault | Fault is the deviation from *normal* operation of a CI or a series of CIs. A fault is a design flaw or malfunction that causes a failure of one or more CIs or IT services. Fault is also referred to as an error. |
| Governance | Governance is the process of ensuring policies and strategy are actually implemented and that required processes are correctly followed. Governance includes defining roles and responsibilities, measuring, and reporting and taking actions to resolve any issues identified. |
| Key Performance Indicator | A Key Performance Indicator (KPI) is a metric used to help manage a process, IT service, or activity. Many metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the process, IT service, or activity. KPIs are selected to ensure that efficiency, effectiveness, and cost effectiveness are all managed. |
| Known Error | A Known Error is a problem that has a documented root cause and a work-around. Known errors are created and managed throughout their lifecycle by Problem Management. Known errors may also be identified by SIE or suppliers. |
| Monitoring | Monitoring is the process of repeated observation of a CI, IT service, or process to detect events and to ensure that the current status is known. |
| Notification | Notification is a communication that provides information. |
| Process | A 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. A process may define policies, standards, guidelines, activities, and work instructions, if needed. |
| Quality Assurance | Quality Assurance (QA) is the process responsible for ensuring the quality of a product and also ensuring it will provide its intended value. |
| Role | A Role refers to a set of connected behaviors or actions that are performed by a person, team, or group in a specific context. |
| Service Knowledge Management System | A Service Knowledge Management System (SKMS) is a set of tools and databases used to manage knowledge and information. The SKMS includes the Configuration Management System (CMS) as well as other tools and databases. The SKMS stores, manages, updates, and presents all information that an IT service provider needs to manage the full lifecycle of IT services. |
| Snapshot | A Snapshot is the baseline as captured by a discovery tool. A snapshot can also be called a benchmark. |
| Test | A Test is an activity that verifies that a CI, IT service, or process meets its specification or agreed requirements. |
| Test Environment | A Test Environment is a controlled environment used to test CIs, builds, IT services, and processes. |