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

IN REPLY REFER TO:
2300/06B
CP

From: Commandant of the Marine Corps

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

Ref: (a) MCO 5271.1B

Encl: (1) IRM-2300-06B Enterprise Information Technology Service Management Service Asset Configuration Management Process Guide

1. PURPOSE. The purpose of the Enterprise Information Technology Service Management (ITSM) Service Asset Configuration Management 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.

2. CANCELLATION. 2300-06A.

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 the Director, Command, Control, Communications and Computers.

6. SPONSOR. The sponsor of this technical publication is HQMC C4 CP.

K. J. NALLY
Brigadier General
U.S. Marine Corps
Director, Command, Control,
Communications and Computers (C4)

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

DISTRIBUTION: PCN 18623000600

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

IN REPLY REFER TO:
2300/06B
CP

From: Commandant of the Marine Corps

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

Ref: (a) MCO 5271.1B

Encl: (1) IRM-2300-06B Enterprise Information Technology Service Management Service Asset Configuration Management Process Guide

1. PURPOSE. The purpose of the Enterprise Information Technology Service Management (ITSM) Service Asset Configuration Management 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.

2. CANCELLATION. 2300-06A.

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 the Director, Command, Control, Communications and Computers.

6. SPONSOR. The sponsor of this technical publication is HQMC C4 CP.

K. J. NALLY
Brigadier General
U.S. Marine Corps
Director, Command, Control,
Communications and Computers (C4)

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

DISTRIBUTION: PCN 18623000600

Enterprise IT Service Management
Service Asset and Configuration Management
Process Guide

Release Date:
DD MONTH YEAR

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	

Table of Contents

Section Title Page

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 IT activities through promoting standardization of work instructions and operating procedures across a continuum of document specificity as represented in Figure 1-1.

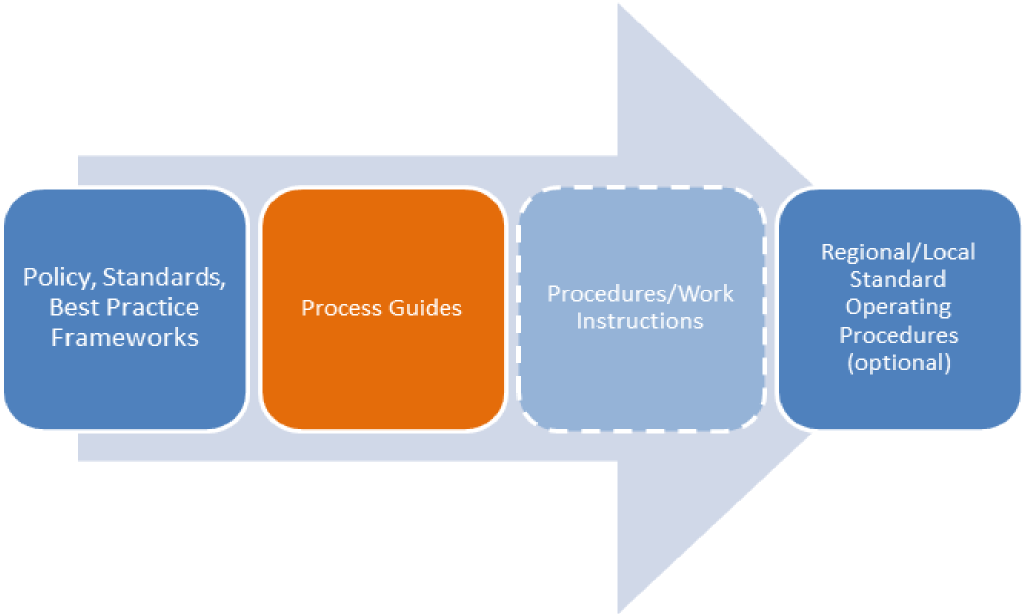

Policy, Standards, Best Practice Frameworks
Process Guides
Procedures/Work Instructions
Regional/Local Standard Operating Procedures (optional)

Figure 1-1. Process Document Continuum

1.2 Scope

The scope of 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 Network Operations and Security Center (MCNOSC) 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 their 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 DoD DoN CMC/HQMC	Statutes/Laws DoD Issuances DoN Policies Marine Corps Orders/IRMS
LEVEL B	HQMC C4 MCNOSC MCSC	MCOs IRMs (Process Guides) Directives MARADMINS
LEVEL C	RNOSC MITSC	Regional Procedures Work Instructions
LEVEL D	MCBs POSTS STATIONS	Locally Generated SOP’s

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 5271.1 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 the service assets and configurations items (CI) while protecting their integrity throughout the service lifecycle. 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 the 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 the service assets and resources comprising an IT infrastructure, as well as their constituent components and relationships. Service Assets are defined as any capability or resource of a service provider and CIs are defined as any component (include IT, services, hardware, software, documentation, etc.) that needs to be managed in order to deliver an enterprise IT service.

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

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

Within the SACM process, the Service Asset part of this 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. While the Configuration Management part of this process works closely with the design architecture of services. It draws 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. This is where it is important to understand the goals of ITAM, Configuration Management, and Inventory Management to help compare and contrast the three disciplines.

The SACM process does include 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 this 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.

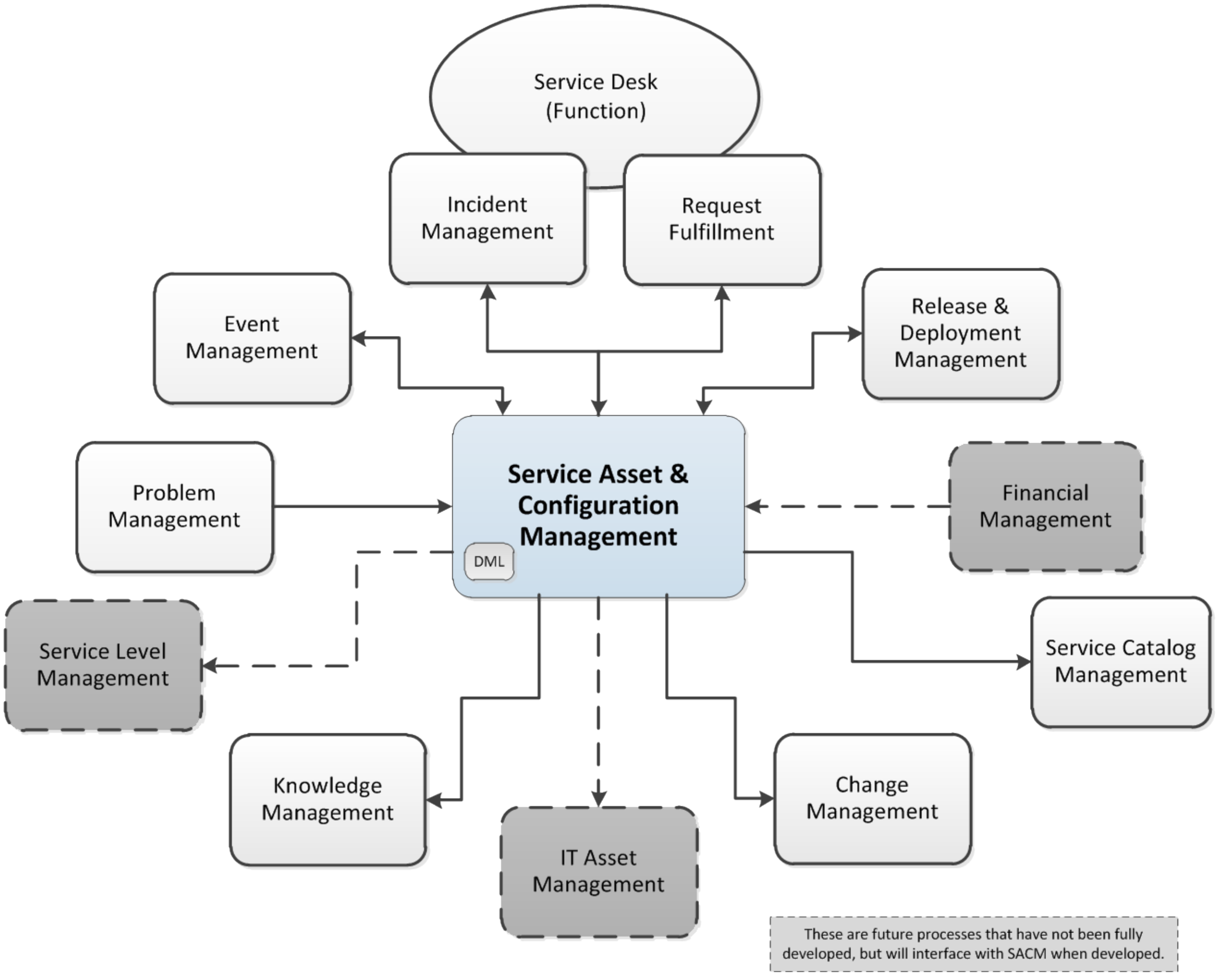

Service Desk
(Function)
Incident Management
Request Fulfillment
Event Management
Release & Deployment Management
Problem Management
Service Asset & Configuration Management
DML
Financial Management
Service Level Management
Service Catalog Management
Knowledge Management
IT Asset Management
Change Management
These are future processes that have not been fully developed, but will interface with SACM when developed.

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). This is a future process that has not been fully developed, but will interface with SACM when developed.

— 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, exists as a report or as a filtered view of the CMDB.

— Service Desk (SD)

- The Service Desk is not a process, but a function. Invoked when the helpdesk personnel request hardware and software information to assist with problem determination. The SACM process provides and maintains key diagnostic information and enables the provisioning of this data to the Service Desk which aids in the processing and resolution of Incidents, Problems, and Known Errors. This enables the Service Desk Agent to easily access information about assets a user refers to when they call for assistance (i.e., what kind of PC? which model?, etc.).

— 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. ITAM and SACM should share databases so that there is one source to retrieve information about IT managed assets and components. This is a future process that has not been fully developed, but will interface with SACM when developed.

— Financial Management (FM)

- Provides the business and IT with the quantification (in financial terms) of the value of IT services, the value of the assets underlying the provisioning of those services, and the qualification of operational forecasting. It includes all function and processes responsible for managing an IT service provider's budgeting, accounting and charging policies and activities. Exchanges information with Financial Management for IT Services regarding new cost and charging codes and other attributes. This is a future process that has not been fully developed, but will interface with SACM when developed.

— 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.

— Definitive Media Library (DML)

- The DML is not a process, but consists of one or more locations in which the definitive and approved versions of all software CIs are securely stored. The DML may also contain associated CIs such as software licenses and documentation. The DML is a single logical storage area even if there are multiple locations. All software in the DML is under the control of Change and Release Management and is recorded in the CMS. Only software from the DML is acceptable for use in a release. Detailed DML information and workflows are referenced in Appendix C of this process guide.

— Capacity Management (CpM) (not shown in Figure 2-1)

- The CMS maintained by SACM provides a Capacity Management Information System (CMIS) which is a virtual repository of all Capacity Management data and usually stored in multiple physical locations in the CMS. 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) (not shown in Figure 2-1)

- 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.

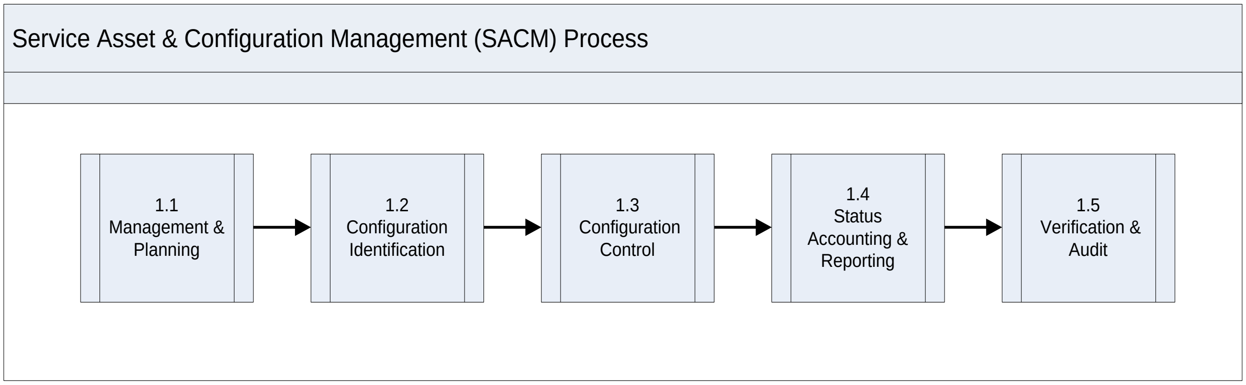

Service Asset & Configuration Management (SACM) Process
1.1 Management & Planning
1.2 Configuration Identification
1.3 Configuration Control
1.4 Status Accounting & Reporting
1.5 Verification & Audit

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	Defining the level of Configuration Management required for a service or a change project. 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 it. Additionally Management and Planning provides: • Descriptions of current and expected SACM tools (e.g., what you have and expect to find). • Related documentation such as existing SACM plans or plans from suppliers. • Listings of relevant documents and their interrelationships. • Policies describing SACM management activities. • Organizational responsibilities and authorities of relevant interested parties (stakeholders). • Qualifications and training of staff to support SACM process. • Criteria for the selection of CIs. • Frequency, distribution, and control of reports.

Number	Sub-Process	Description
1.2	Configuration Identification	Defines the selection and identification of CIs and their relationships. 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. Good selection and identification criteria include: • Regulatory requirements. • Criticality in terms of risks. • New or modified technology. • Interfaces with other CIs. • Procurement conditions. • Support and service considerations.
1.3	Configuration Control	Ensures there are adequate mechanisms to control CIs. 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. The organization defines how to accurately update CMDB records in the SACM Plan (Management & Planning sub-process), which would include: • Management authorizations and relationships of those in authority. • Procedures for control of changes to CI records within the CMDB. • 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. Reporting on changes to CIs throughout their lifecycle. Include 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. 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. 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. These reviews are defined in the SACM Plan (Management & Planning sub-process) and should include: • A list of audits planned (including schedules). • Audit procedures to be used. • Authorizations required (within and without IT). • Description of report and expected contents. • Configuration care and feeding.

2.4.1 Process Description

The SACM process manages the lifecycle of the 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 (IMAC) on IT operational service assets and manages the data that is configured between the stocking of and disposing 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 refresh 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 unique 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, "CCIR are tools for the commander to reduce information gaps generated by uncertainties that he may have concerning his own force, the threat, and/or the environment. 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. CCIR 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 others 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) is an attribute. 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 a 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 their lifecycle and 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 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.

2.5.13 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 Library (DSL) consistent with the CMDB.

2.5.14 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.

2.5.15 Discovery

Discovery is a manual or automated process by which CIs are identified, recorded, stored, and then updated in the CMS/CMDB. This is commonly use 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.)

2.5.16 Defense Property Accountability System

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).

2.5.17 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 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.

2.5.19 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.

2.5.20 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 NMCI Naming Standards D400.11939.01 v11.0 dated 10 Dec 2010 document provides naming standards for Microsoft Active Directory components, domain name service, servers, Client Data seats, printers, file shares, public folders, users, groups, network equipment and circuits.

The following Table 2-2 describes an example of a naming convention for a server:

Table 2-2. NMCI Naming Convention Example

Naming Convention of a Server : DDDDSSSSFF##AB	
Identifier	**Description**
DDDD	Represents a four-digit domain identifier corresponding to the service and region of the domain.
SSSS	Represents the site identifier
FF	Represents a two-letter function identifier from NMCI Server Function Identifiers
##	Represents a two-digit unique identifier. Lead zeros should be included for 01 through 09. To support the possibility of a site having more than 99 servers of a single function, it is allowed to use three digits as the unique identifier
A	<F> identifies a nonclustered failover server for the BlackBerry solution <N> identifies that this is a physical node in a cluster <Q> identifies this is a Classroom File server <S> identifies this is a Staging server <V> identifies that this is a Virtual server
B	Is an optional alpha identifier to identify a clustered or load-balanced server, used only if the previous <**V**> option is used.
Server Example: ***NADSSDNIDC01***	

2.5.21 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.

2.5.22 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. email service). 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).

2.5.23 Service Asset

A Service Asset is any resource or capability of a service provider. Resources could be infrastructure, application, or data. Capabilities include people, organization, management and their knowledge. In essence, every single 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 a IT service. Service assets can be one of the following types: Management, Organization, Process, Knowledge, People, Information, Applications, Infrastructure, and Financial Capital.

2.5.24 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).

2.5.25 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, Delete, In Inventory, On Loan, Disposed, Reserved, 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.

2.5.26 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.

2.5.27 Software License Management

SW license management consists of processes, business rules, and supporting technology that identify the standards for which Commercial off the Shelf (COTS) and Government off the Shelf (GOTS) applications will be managed.

2.5.28 Information Technology Strategic Sourcing (ITSS)

ITSS is a project management team within MCSC PMM-110 charged with ensuring quality, consistency and value in the procurement of USMC enterprise hardware and software assets. ITSS consists of Marine Corps Hardware Suite (MCHS), Marine Corps Software Enterprise License Management System (MCSELMS), and the enterprise Staging and Warehousing capability. ITSS optimizes the IT supply base while reducing Total Cost of Ownership (TCO) and improving mission delivery. Life-cycle information in the CMDB is used to evaluate asset performance and value while establishing requirements for vendor purchases. The CMDB manages information on the assets procured by ITSS and subsequently managed and maintained by the asset's parent MITSC and/or Program of Record (PoR). ITSS provides SACM with the contract information related to the hardware and enterprise software purchases. The contract information is stored within the overall CMS as a Contract Database detailing contracts, their length, what services are provided by suppliers and any associated CIs.

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 managing 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 action taken to improve it. 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 (should be close to 1:1).

In developing CSFs it is essential to recognize that a CSF is the reason to do things, it is a purpose, 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 this is what a KPI is, a sign that is either heading towards or away from a CSF.

The following Table 2-3 describes the SACM process recommended CSF's and KPIs to be monitored, measured, and analyzed. These measures are based on best practices and can be evaluated for future expansion.

Table 2-3. 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	Improved accuracy in budgets and charges for the assets utilized by each USMC organization	Attracting and justifying funding for SACM since the practice typically out of sight to the USMC leadership
		2	Increase in the re-use and redistribution of under-utilized resources and assets	Reduces the risk concerning lack of commitment and support from USMC leadership who may not understand the key role of SACM
		3	Reduction in the use of unauthorized hardware and software, non-standard and variant builds	Reduces the risk of inaccurate exchange of information and high cost associated with increase complexity of the unauthorized components in the environment
		4	Reduced number of exceptions reported during audits	Reduces the risk of the CMS becoming out date
2	Supporting efficient and effective service management processes by providing accurate configuration information at the right time	5	Percentage improvement in the maintenance scheduling over the life of an asset	Improves the short term efficiency (costs) and long term effectiveness (asset utilization)
		6	Improve speed for incident management to identify faulty CIs and restore service	Reduces the risk of technical staff circumventing the SACM process and procedures
		7	Reduction in the average time and cost of diagnosing and resolving incidents and problems, by type	Improves the short term asset efficiency (reduces costs)
		8	Improve ratio of used licenses against paid-for licenses	Improves the controls and efficient use of licenses
		9	Improvement in time to identify poor-performing and poor-quality assets	Improves the return on investments and availability of the USMC network
		10	Reduction in risks due to early identification of unauthorized change	Reduces the risk of technical staff circumventing the SACM process and procedures
		11	Reduce percentage of change not completed successfully or causing errors because of poor impact assessment, incorrect data in the CMS, or poor version control	Reducing the lifecycle for implementing improvements into the USMC networks
3	Establishing and maintaining an accurate and complete CMS	12	Reduction in business impact of outages and incidents caused by poor configuration management	Improves the availability of the USMC network
		13	Increase quality and accuracy of configuration information	Improve asset baselines used to assess impact on the USMC networks
		14	Improve audit compliance	Reduces the risk of the CMS becoming out dated

CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Benefits
		15	Shorter audits as quality configuration information is easily accessible	Reduces the risk of the CMS becoming out dated
		16	Fewer errors caused by people working with out-of-date information	Reduces the risk of inaccurate exchange of information and high cost implementing change
		17	Improve Software License compliance	Reduce the risk of Software License violations

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 MCIE.

While the goal is to have a single SACM Process Owner and SACM Process Manager at the enterprise level, the USMC will initially use a shared process ownership framework. There will be a SACM Process Owner and SACM Process Manager for the acquisition sector inclusive of all USMC IT PORs, as well as a SACM Process Owner and SACM Process Manager for the operational sector inclusive of all other USMC organizations at the enterprise, regional, and local levels.

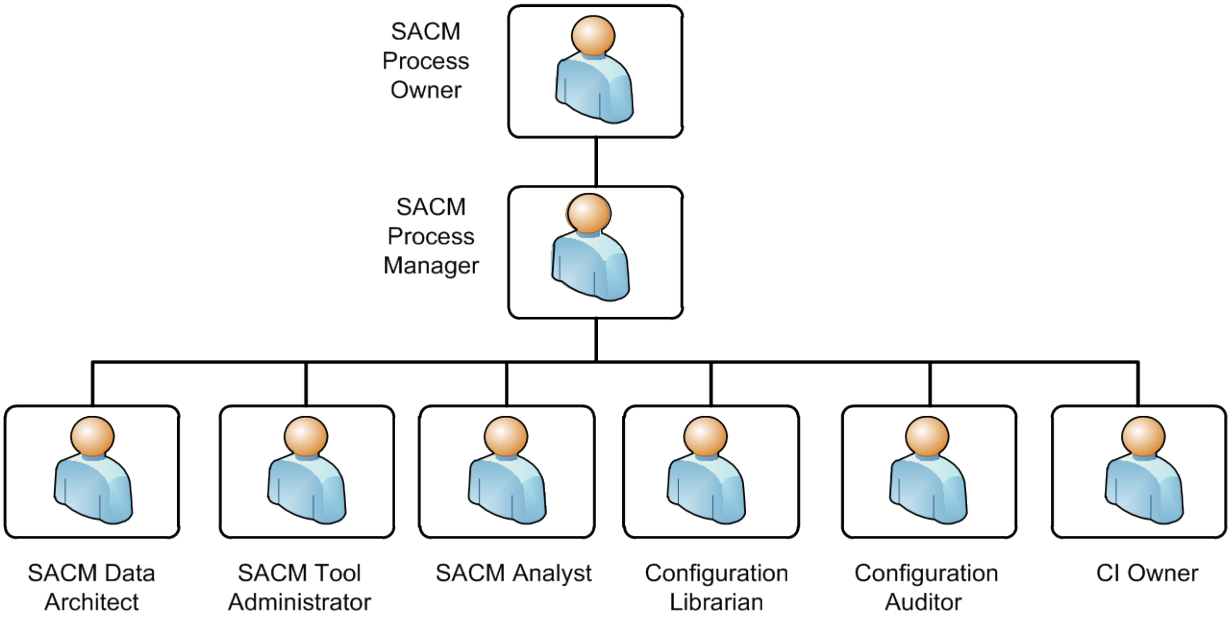
The additional and following roles will support the SACM process:

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

It is important to note that roles and job titles are two different things, but are often confused with each other. Position titles or job titles and position descriptions will vary from organization to organization, however, individuals holding whichever title can perform one or more of the required E-ITSM process roles.

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.



SACM Roles represents process roles, not head count or resource requirements.

Figure 3-1. SACM Process Roles

Table 3-1. SACM Process Roles and Responsibilities

Role Description	Role 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. 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. 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. • Ensures the process is followed by the organization. • Ensures the SACM process and working practices are effective and efficient. • Ensures all stakeholders are sufficiently involved in the SACM process. • Decision maker on any proposed enhancements to the process and development of process improvement plans. • Agrees with and documents the scope for the process, incorporating the policy for determining which service assets should be treated as CIs. • Adjudicates when new CI types are requested by SACM Process Managers. • Ensures tight integration between SACM and other related processes. • 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.
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.	• Perform the Process Manager role for the SACM process. • Implements the service asset management policy and standards.

Role Description	Role Responsibilities
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. 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. There is a Service Asset Manager for each level of the environment.	• Support the scope of the SACM process, including items that are to be controlled, and information that is to be recorded. • Management of the assets that are under control of IT. • Plans population of the service assets; manages the service assets in CMDB, central libraries and tools; ensures regular housekeeping of the Asset database or register. • Identifies and classifies service assets that will be regarded as CIs. • 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. • Ensure all data relating to SACM is available when required. • Evaluates existing service asset management systems and the design, implementation and management of new/ improved systems for efficiency and effectiveness. • Prepares and manages SACM tools and processes. • Manages the evaluation service asset management tools. • Develops service asset management standards and Service asset management plans and procedures. • Ensures that the service asset management methods and processes are properly approved and communicated to staff before being implemented. • Arranges recruitment and training of SACM staff. • Proposes interfaces with network management, computer operations, logistics, finance, and administration functions. • Coordinate key interfaces between SACM and other processes, in particular, Change Management, Release and Deployment Management and Knowledge Management. • 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. 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. 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. There is a Configuration Manager for each level of the environment.	• Perform the Process Manager role for the SACM process. • Implements the SACM policy and standards. • Support the scope of the SACM process, including items that are to be controlled, and information that is to be recorded. • Management of the CIs that are under control of SACM. • Identifies and classifies service assets that will be regarded as CIs. • Ensure all data relating to SACM is available when required. • Prepare and manage SACM tools and sub-processes. • Coordinate key interfaces between SACM and other processes, in particular, Change Management, Release and Deployment Management and Knowledge Management • Evaluates existing CMS. • Develops configuration management standards, SACM plans and procedures. • Ensures that changes to the SACM methods and processes are properly approved and communicated. • Arranges recruitment and training of SACM staff. • Manages the evaluation of CM tools. • Manages the SACM plan, principles and processes and their implementation. • Ensures CIs are uniquely identified with naming conventions and that staff complies with identification standards for object

Role Description	Role Responsibilities
	types, environments, processes, lifecycles, documentation, versions, formats, baselines, releases and templates. • Proposes interfaces with network management, computer operations, logistics, finance, and administration functions. • Plans population of the CMS; manages CMS, central libraries, tools, common codes and data; ensures regular housekeeping of the CMS. • 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. 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. • Ensures the correct roles and responsibilities are defined in the SACM plan/procedures. • Assist with procurement of IT assets when requested. • Works with other SACM roles to tag and track all IT assets and to identify their locations and owners. • Receives IT assets and ensures delivery to correct locations. • Coordinate IT asset setup and teardown activities when requested. • Proposes/concurs with the SACM Manager on CIs to be uniquely identified with naming conventions. • Ensures developers and configuration system users comply with identification standards for object types, environments, processes, life cycles, documentation, versions, formats, baselines, releases, and templates. • Liaises with Configuration Librarian on population of asset and CMS. • Performs configuration audits to ensure physical inventory is consistent with the CMDB/CMS, initiating corrective action through Change Control. • Accepts baselined products from third parties for distribution. • Builds system baselines for promotion and release. • Maintains project status information and status accounting records and reports. • 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. The SACM Configuration Analysts 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. • Assists with the development of SACM standards, plans, and procedures. • Determines construction of the CMS, including CI types, naming conventions, attributes and relationships • Supports the creation of the SACM process, activities, and procedures to include CI registration procedures, access controls, and privileges. • Ensures the correct roles and responsibilities are defined in the SACM plan/procedures. • Proposes/concurs with the SACM Manager on CIs to be uniquely identified with naming conventions. • Ensures developers and configuration system users comply with identification standards for object types, environments, processes, life cycles, documentation, versions, formats,

Role Description	Role Responsibilities
	baselines, releases, and templates. • Liaises with Configuration Librarian on population of asset and CMS. • Performs configuration audits to ensure physical inventory is consistent with the CMDB/CMS, initiating corrective action through Change Control. • Uses the CMDB/CMS to help identify other CIs affected by a fault which is affecting a CI. • Creates and populates project libraries and the CMDB/CMS. • Accepts baselined products from third parties for distribution. • Builds system baselines for promotion and release. • Maintains project status information and status accounting records and reports. • Assists SACM Process Manager in report definition as required. • 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. • 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. • Analyzes data requirements to establish, modify, or maintain CMS object/data models. • Evaluates potential solutions, analyzing and modeling changes to the CMS/CMDB information model. • Uses appropriate tools, including logical models of configuration classes, attributes, and relationships, to contribute to the development of the information model for the CMS. • Produces detailed specifications and maps or translates these into designs for implementation in the CMS. • Consults on technical aspects of SACM (including requests for changes, deviations from specifications, etc.). • 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. The Configuration Librarian manages the Definitive Media Library activities, from population through positioning of controlled items for deployment actions. 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.	• Control the receipt, identification, storage, and withdrawal of all support CIs via Authorized or Approved RFCs. • Provide information on the status of CIs. • Number, record, store, and distribute SACM DML issues. • Assist SACM Analyst in Configuration Identification activities. • Assist SACM Manager to prepare the SACM Plan. • Create and manage the identification scheme for the CM libraries and DML. • Creates and manages libraries or other storage areas to hold CIs • Assists in the identification of products and CIs. • Maintains current status information on CIs. • Accepts and records the receipt of new or revised configurations into the appropriate library.

Role Description	Role Responsibilities
	• Archives superseded CI copies. • Safeguards and holds the master copies. • Administers configuration control sub-process: • Issues copies of products for review, change, correction, or information when authorized to do so. • Maintains a record of all copies issued. • Notifies holders of any changes to their copies. • Collects and retains information that will assist in the assessment of what CIs are impacted by a change to a product. • Produces configuration status accounting reports. • Assists in conducting configuration audits.
Configuration Auditor	
The Configuration Auditor is responsible for planning and executing audits of configuration data and validating CMS/CMDB accuracy. The Configuration Auditor is responsible for assessing and analyzing requests for verification and audits. The Configuration Auditor consults regularly with the SACM Service Asset Analyst, SACM Configuration Analyst and occasionally with the Configuration Librarian, and the CI Owner when performing SACM verifications and audits.	• Assesses and analyzes requests for SACM Verifications and Audits. • Verifies the integrity of the physical business environment as specified in requirements and configuration baseline documents. • Plans the business environment audit based on documents such as the following: requirements specifications, physical design, interface or implementation documents, release notes, service level agreements, and supplier contracts. • Utilizes CMS and Auto-discovery Tools to discover, preview and report about the physical data center environment. • Compares physical data against CMS information. • Plans audit to verify CMS information against the physical environment. • Generates CMS baseline reports. • Verifies conformance and highlights non-conformance and variations within the Draft Audit Report. • Creates a risk and gap analysis, assessing value of reconciliation. • Completes Verification and Audit Report. • Publishes the Verification and Audit Report and notifies interested groups. • Establishes and updates regular schedule of CMS verifications and 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 timely and accurately. The CI Owner is a POC whenever question 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. This role applies to anyone who performs the function for	• 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. • Owns technology roadmaps, CMS load plans, and end of life plans for specific CIs. • Engages in the planning activities involved in introducing, modifying, or retiring CIs. • Work with other CI Owners required to carry out CMS load tactics and ongoing Change, Configuration, and Release and Deployment responsibilities. • Works with CIs assigned to maintain. • Registers new CIs upon approval. • Manage the receipt, identification, storage and removal of all CIs. • Preserve status information on CIs.

Role Description	Role Responsibilities
defining, documenting the generic attributes (e.g. manufacture, model, version, catalog items, etc.) of one or more specific types	• Archive out of date CIs. • Identifies, records, stores, and distributes issues connected with the SACM process. • Transfers ownership of a CI. • Generates and view reports of the CIs assigned. • 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. • Ensures that appropriate CI documentation is available and current. • Communicates CI information or changes as appropriate to ensure awareness. • Conducts periodic reviews of assigned CIs to ensure that information is still appropriate and make changes as required. • Ensures completeness and integrity of information collected to conduct daily operations. • 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. 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. • Recommends improvement opportunities. • Evaluates tools, monitors performance and capacity of the CMS/CMDB. • Liaises with Capacity Management regarding volumes, trends and requirements. • Undertakes standard housekeeping and fine tuning within the Change Control process. • Supports requests for tool changes necessitated from Reporting and Audit / Reconciliation efforts. • Monitors/analyzes service asset/configuration data and compliance activities to identify trends, discover anomalies, and ensure proper management of the SACM process. • 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.

Table 3-2. RASCI Model for SACM by Process Role

SACM Sub-Process	SACM Process Owner	SACM Process Manager (Configuration)	SACM Process Manager (Service Asset)	SACM Analyst (Configuration)	SACM Analyst (Service Asset)	SACM Data Architect	Configuration Librarian	Configuration Auditor	CI Owner	SACM Tools Administrator
Management & Planning	AR	R	R	S	S	C	C	C	S	C
Configuration Identification	A	R	R	S	S	R	S	C	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	R	C	S

4.0 SUB-PROCESSES

The E-ITSM SACM process consists of five (5) sub-processes as shown in Figure 4-1. This process is responsible for 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

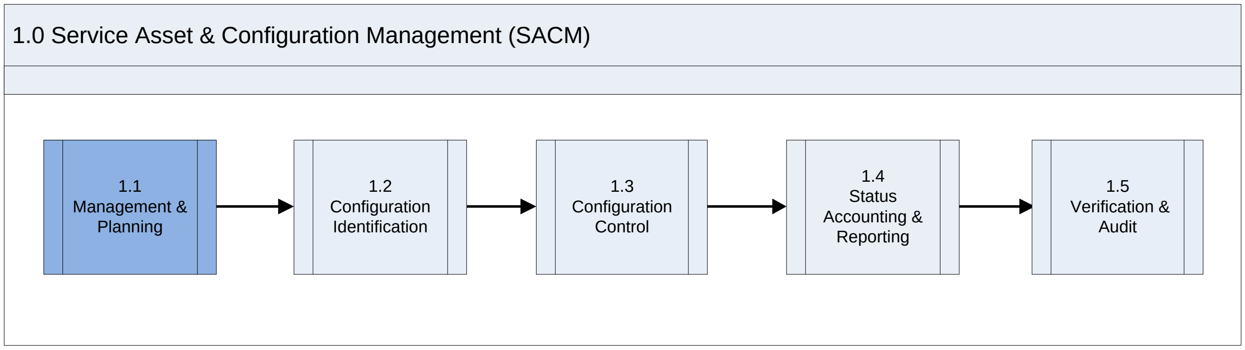

1.0 Service Asset & Configuration Management (SACM)
1.1 Management & Planning
1.2 Configuration Identification
1.3 Configuration Control
1.4 Status Accounting & Reporting
1.5 Verification & Audit

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 engage 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.

It is important to note that 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 should define the following:

- Purpose, scope, objectives of SACM.

- Related policies, standards, and processes specific to the support group.
- SACM roles and responsibilities.
- CI naming conventions.
- 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:

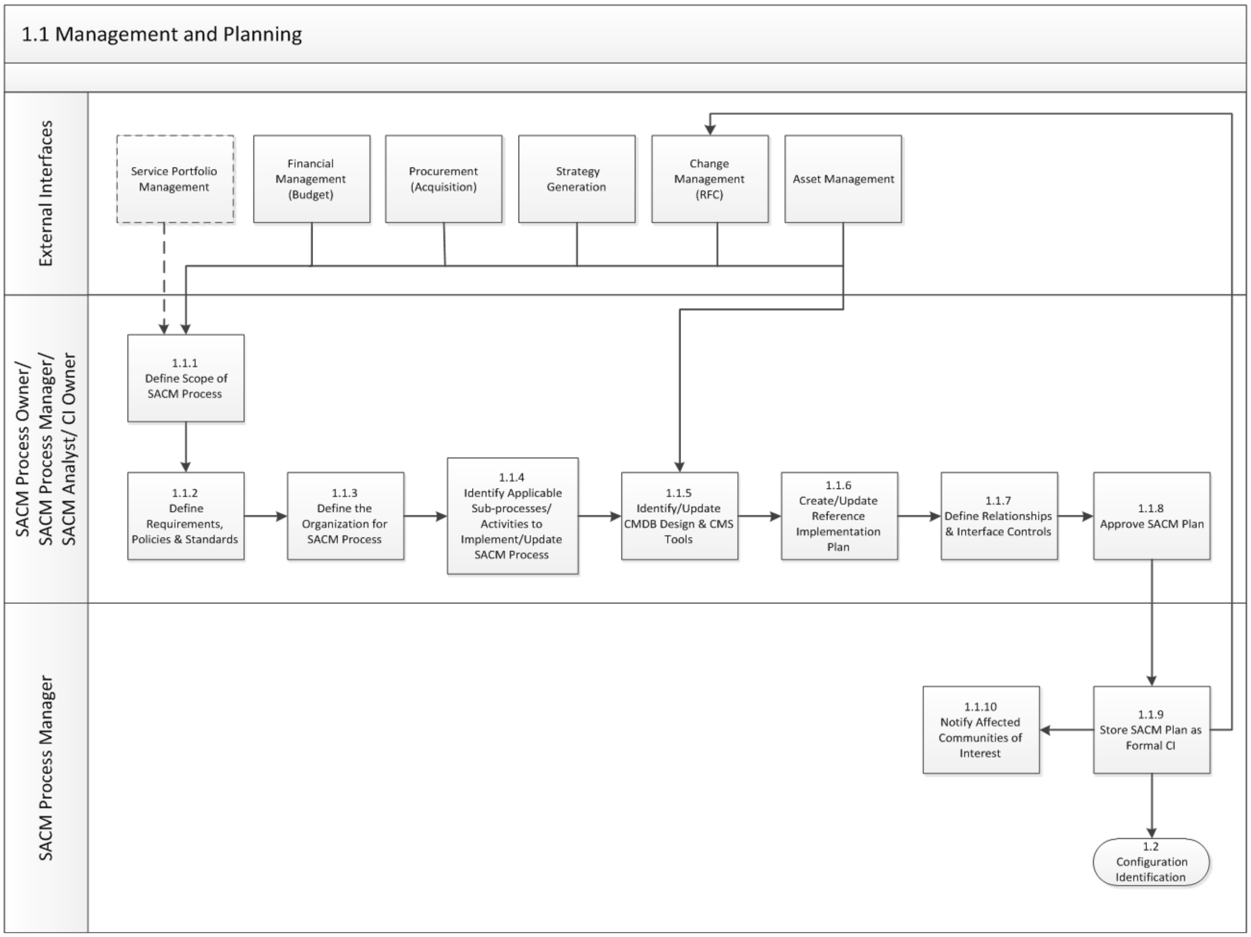

1.1 Management and Planning
External Interfaces
Service Portfolio Management
Financial Management (Budget)
Procurement (Acquisition)
Strategy Generation
Change Management (RFC)
Asset Management
SACM Process Owner/ SACM Process Manager/ SACM Analyst/ CI Owner
1.1.1 Define Scope of SACM Process
1.1.2 Define Requirements, Policies & Standards
1.1.3 Define the Organization for SACM Process
1.1.4 Identify Applicable Sub-processes/ Activities to Implement/Update SACM Process
1.1.5 Identify/Update CMDB Design & CMS Tools
1.1.6 Create/Update Reference Implementation Plan
1.1.7 Define Relationships & Interface Controls
1.1.8 Approve SACM Plan
SACM Process Manager
1.1.9 Store SACM Plan as Formal CI
1.1.10 Notify Affected Communities of Interest
1.2 Configuration Identification

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

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

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)* 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. Plan for an integrated SACM though its full lifecycle. The scope definition includes: • Applicable Services (New/Updated) • Environments and Infrastructure (New/Updated) • Geographical Locations (New/Updated) Strategy Generation for the USMC may include: • ESRVG (Governance Board) • C4 - Plans and Policy • PMO - Programmatic Strategy • CDNI - Requirements • UMG (Unification Management Group) and ESG - ITSM strategy **Roles**: SACM Process Owner, SACM Process Manager, SACM Analyst, CI Owner **Inputs**: • Program Initiation/ Contract Portfolio, Customer Portfolio, Organizational Policy, Service Management Plan, from Strategy Generation • Financial Information (Contract requirements) from Financial Management • ITAM Scope (HW/SW/Licensing) from Asset Management • Acquisition Data from Procurement **Output**: • SACM Scope

1.1 Management and Planning		
Creates/Implements a SACM Plan		
Number	**Activity**	**Description**
1.1.2	Define Requirements, Policies & Standards .	Identify the policies, requirements, contractual requirements. Link to other Service Management Policies, strategies, E-ITSM policies, USMC directives). Link to requirements for the CMS. Include policies and standards: • Applicable Policies • Industry Standards (ISO/IEC 20000, ISO/IEC 19770-1 • Internal standards relevant to SACM (hardware standards, desktop standards, software & licensing Summarize requirements for accountability, traceability, auditability (depth and breadth for SACM process). **Roles**: SACM Process Owner, SACM Process Manager, SACM Analyst, CI Owner **Input**: • SACM Scope **Output**: • 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. **Roles**: SACM Process Owner, SACM Process Manager, SACM Analyst, CI Owner **Input**: • SACM Policies and Standards **Output**: • 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. To include: • Configuration Identification • Version Management • Interface Management • Supplier Management • Configuration Control (Change Management) • Release and Deployment • Build Management • Establishing and maintaining configuration baselines • Maintaining the CMS • Reviewing the integrity of configurations and the CMS (verification and audit) **Roles**: SACM Process Owner, SACM Process Manager, SACM Analyst, CI Owner **Input**: • SACM Organization Structure **Output**: • SACM Sub-processes and Activities
1.1.5	Identify/Update CMDB Design & CMS Tools	Conduct CMDB design workshop as applicable. Identify or update the software tools that will be used to create or automate CMS and leverage the Asset Management Database. **Roles**: SACM Process Owner, SACM Process Manager, SACM Analyst, CI Owner **Inputs**: • ITAM System Details from Asset Management • SACM Sub-processes and Activities **Outputs**: • CMS Software Tools updated or identified • 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.). Build SACM catalog, product catalog, DSL entries. When implementing the plans, define the structures and foundation *(sites, location, owners)* data that will be used during Configuration Identification. **Roles**: SACM Process Owner, SACM Process Manager, SACM Analyst, CI Owner **Inputs**: • CMS Software Tools updated or identified • CMDB Design **Output**: • 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. Include relationship management and control of suppliers and sub-contractors. **Roles**: SACM Process Owner, SACM Process Manager, SACM Analyst, CI Owner **Input**: • SACM Reference Implementation Plan **Output**: • Draft SACM Plan
1.1.8	Approve SACM Plan	Review and approve new or updated SACM Plan. **Roles**: SACM Process Owner (Review & Approve), SACM Process Manager, SACM Analyst, CI Owner (Review) **Input**: • Draft SACM Plan **Output**: • 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. 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. **Role**: SACM Process Manager **Input**: • Approved SACM Plan **Output**: • 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. **Role**: SACM Process Manager **Input**: • Approved SACM Plan **Output**: • Notification of SACM Plan

4.2 Configuration Identification

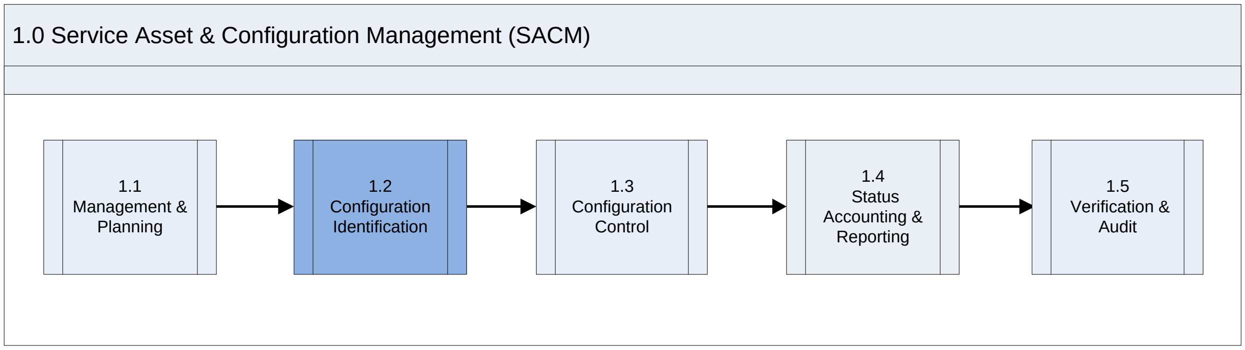

1.0 Service Asset & Configuration Management (SACM)
1.1 Management & Planning
1.2 Configuration Identification
1.3 Configuration Control
1.4 Status Accounting & Reporting
1.5 Verification & Audit

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.

Configuration Identification process enables the following:

- Identify and register CIs.
- Assign unique labels.
- Record relationship information.
- Identify and designate baselines of 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).

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

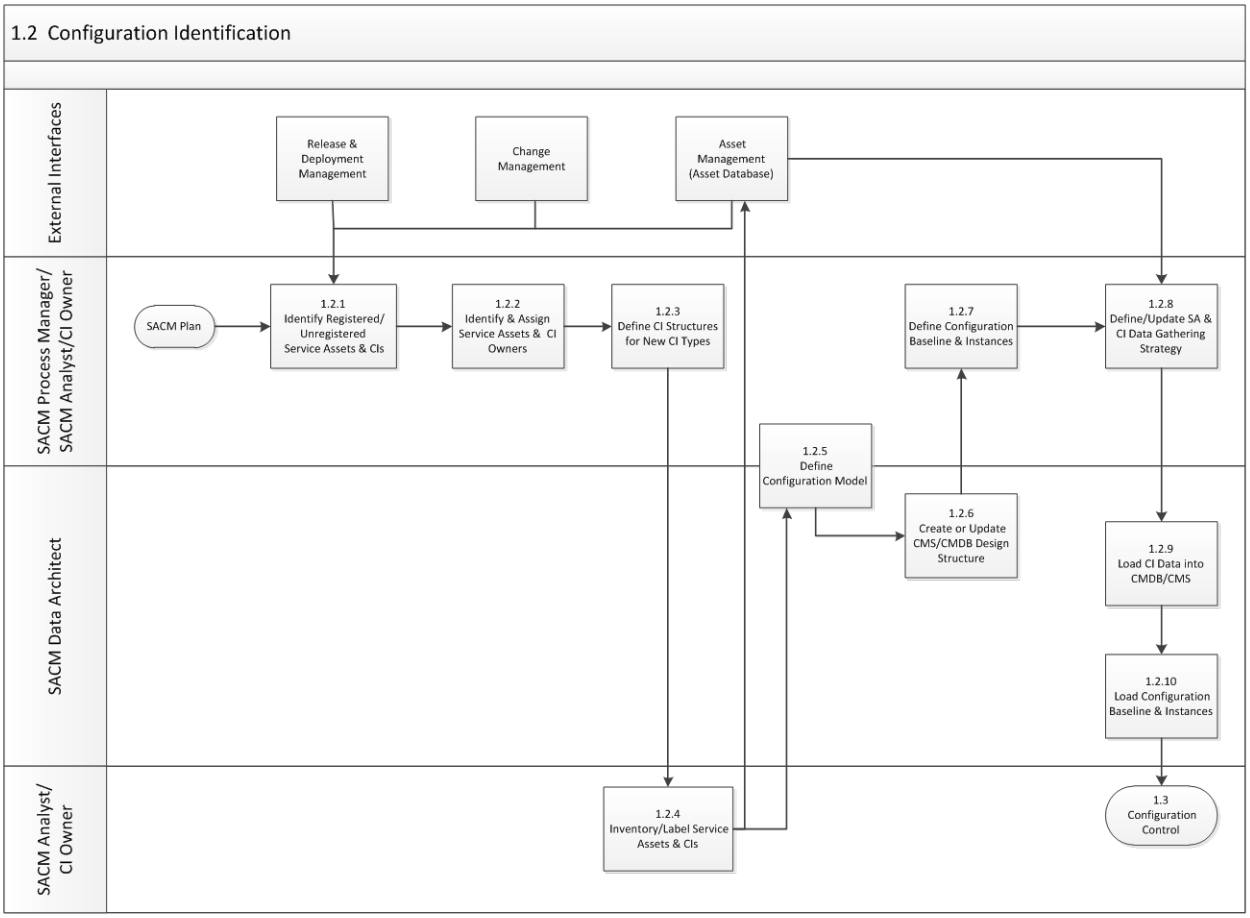

1.2 Configuration Identification
External Interfaces
SACM Process Manager/ SACM Analyst/CI Owner
SACM Data Architect
SACM Analyst/ CI Owner
Release & Deployment Management
Change Management
Asset Management (Asset Database)
SACM Plan
1.2.1 Identify Registered/ Unregistered Service Assets & CIs
1.2.2 Identify & Assign Service Assets & CI Owners
1.2.3 Define CI Structures for New CI Types
1.2.7 Define Configuration Baseline & Instances
1.2.8 Define/Update SA & CI Data Gathering Strategy
1.2.5 Define Configuration Model
1.2.6 Create or Update CMS/CMDB Design Structure
1.2.9 Load CI Data into CMDB/CMS
1.2.10 Load Configuration Baseline & Instances
1.2.4 Inventory/Label Service Assets & CIs
1.3 Configuration Control

Figure 4-4. Configuration Identification Sub-Process Workflow

The following Table 4-2 describes the Configuration Identification sub-process activities illustrated in Figure 4-4:

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	The first time an item is to be placed under this sub-process it starts with a need that is defined in the SACM plan. A change to a CI starts with a change request to place a CI under SACM. 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 which are new and need to be registered.

1.2 Configuration Identification		
Identifies CIs		
Number	**Activity**	**Description**
		Roles: SACM Process Manager, SACM Analyst, CI Owner **Inputs**: • ITAM • Release & Deployment (Build & procure to rectify deviances from specifications for CI) • Change Management o Capabilities o Resources • SACM Plan (Requirements Design, Maintenance, Release, Deployment, Operations Plan) • Scheduled CMDB Review (Requirements Design, Maintenance, Release, Deployment, Operations Plan) **Outputs:** • Unregistered service asset and CIs identified • 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 the appropriate Service Asset and CI Owners unregistered CIs that have been identified. 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. **Roles**: SACM Process Manager, SACM Analyst, CI Owner **Input**: • Unregistered service asset and CIs identified **Output**: • 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. The Configuration Structures describes the relationship and position of CIs for both infrastructure and services. **Roles**: SACM Process Manager, SACM Analyst, CI Owner **Inputs**: • Registered service assets and CIs identified • Identified Service Asset and CI Owners **Output**: • 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. **Roles**: SACM Analyst, CI Owner

1.2 Configuration Identification		
Identifies CIs		
Number	Activity	Description
		Input: • CMS/CMDB Structure Definition **Outputs**: • Inventoried and Labeled service assets and CIs • 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. The Configuration Model is used to: • Plan technology refreshes and software upgrades • Plan release and deployment packages • Migrate services to different locations • Assess impact of proposed changes • Assess impact of incidents and problems • Plan, design, and change new or existing services **Roles**: SACM Process Manager, SACM Analyst, CI Owner, SACM Data Architect **Input**: • Inventoried and Labeled service assets and CIs **Output**: • 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. 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. 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). CMDB Objects include: • CI Instances • CI Relationship Types (parent, child, etc.) • CI Categories/Baselines **Role**: SACM Data Architect **Input**: • Configuration Model defined

1.2 Configuration Identification		
Identifies CIs		
Number	**Activity**	**Description**
		Output: • 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). This activity allows you to build a service component from a defined set of inputs. 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. **Roles**: SACM Process Manager, SACM Analyst, CI Owner **Input**: • CMS/CMSD design structure **Output**: • 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. **Roles**: SACM Process Manager, SACM Analyst, CI Owner **Inputs**: • Defined Configuration Baseline and Instances • Service Asset and CI data from Asset Management / CMS databases **Output**: • 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). **Role**: SACM Data Architect **Inputs**: • Service Asset and CI Data Strategy • Defined Configuration Baseline and Instances **Output**: • 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). 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 a Footprint). Enables Problem Management to analyze 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.). **Role**: SACM Data Architect **Input**: • Service Asset and CI data loaded into CMDB/CMS **Output**: • Configuration Baseline (CI identification, naming, labeling, data and documentation baseline)

4.3 Configuration Control

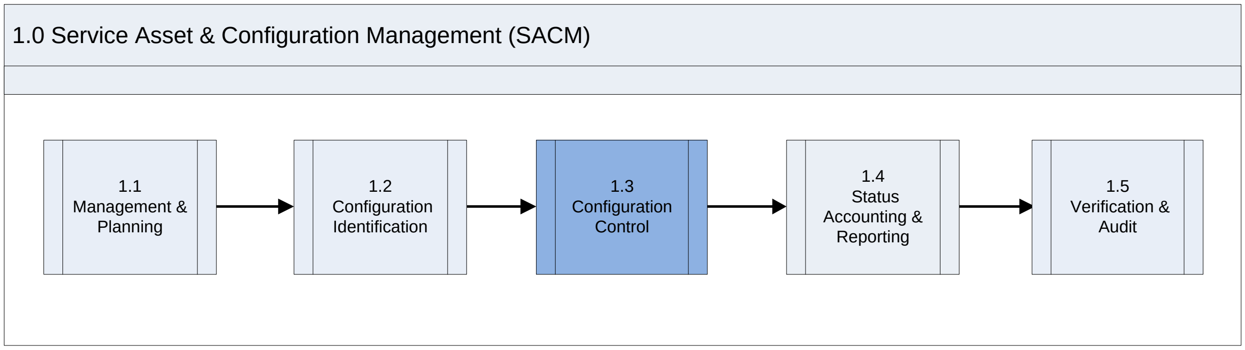

1.0 Service Asset & Configuration Management (SACM)
1.1 Management & Planning
1.2 Configuration Identification
1.3 Configuration Control
1.4 Status Accounting & Reporting
1.5 Verification & Audit

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 is put in place to confirm 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 an appropriate controlling documentation or procedure being followed.

Policies and procedures should be in place to cover the following:

- Version control of software, hardware, image builds, and releases.
- Access control to facilities, storage areas, and CMS, including user roles.
- Establishing 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 statistic can provide managers and other stakeholders' 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.

- Maintaining compliance while significantly reducing overall software costs.

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

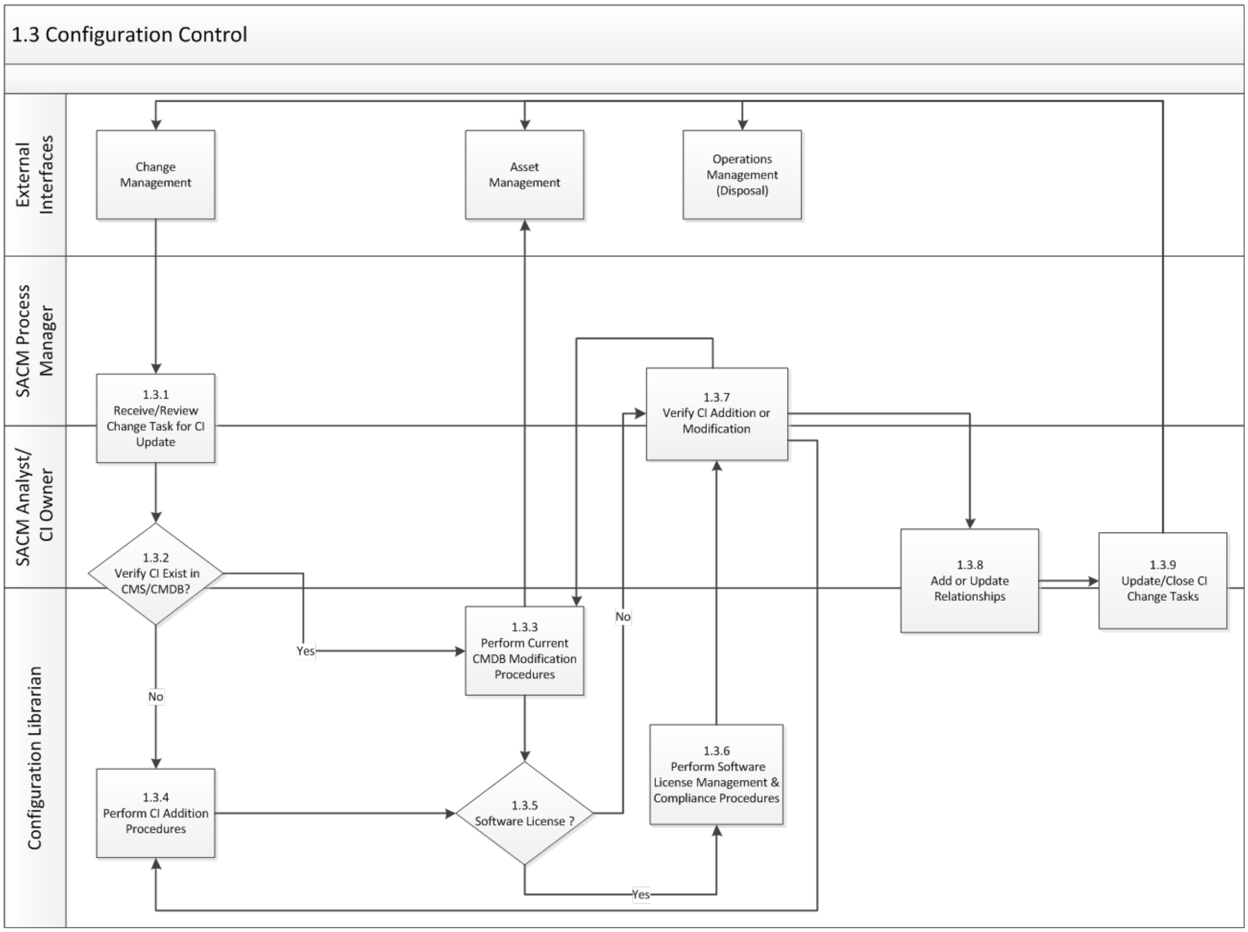

1.3 Configuration Control
External Interfaces
SACM Process Manager
SACM Analyst/ CI Owner
Configuration Librarian
Change Management
Asset Management
Operations Management (Disposal)
1.3.1 Receive/Review Change Task for CI Update
1.3.2 Verify CI Exist in CMS/CMDB?
Yes
No
1.3.3 Perform Current CMDB Modification Procedures
1.3.4 Perform CI Addition Procedures
1.3.5 Software License ?
Yes
No
1.3.6 Perform Software License Management & Compliance Procedures
1.3.7 Verify CI Addition or Modification
1.3.8 Add or Update Relationships
1.3.9 Update/Close CI Change Tasks

Figure 4-6. Configuration Control Sub-Process Workflow

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

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. **Roles**: SACM Process Manager, SACM Analyst, CI Owner **Input**: • RFC to register New CI or update current CI data **Output**: • Reviewed Change Task
1.3.2	Verify CI Exist 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? **Roles**: SACM Analyst, CI Owner, Configuration Librarian **Input**: • Reviewed Change Task **Outputs**: • CI does exist - Modification required to current CI • 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. 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. **Role**: Configuration Librarian **Inputs**: • Modification required to current CI (Reviewed/Verified RFC to modify existing CIs in CMS/CMDB) • From SACM Process Manager - CMS/CMDB Modification not successful **Outputs**: • Modified CI in CMS/CMDB • 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. Activities for normal every-day addition of new CMDB objects to include initial bulk loading of CIs. CMDB Objects include: • CI Instances • CI Relationship Instances • CI Architecture Building-block types/categories/baselines • CI Relationship Types **Role**: Configuration Librarian **Inputs**: • New CI Required • From SACM Process Manager - CMS/CMDB Addition not successful **Output**: • 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. **Role**: Configuration Librarian **Inputs**: • New Registered CI • Modified CI in CMS/CMDB **Outputs**: • Software License Required • 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. 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. **Role**: Configuration Librarian **Input**: • Reviewed RFC for additional software license or update to current software licensing **Outputs**: • Assigned Software License • RFC for Harvesting Software License to Change Management • 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. 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. Focus particular attention on Change tasks to create/modify CMDB architecture building-blocks or that relate to a Normal Change. **Roles**: SACM Process Manager, SACM Analyst, CI Owner **Inputs**: • Registered CI (from Perform CI Addition RFC) • Modified CI (from Perform Current CMDB Modification RFC) • Removed CI (Deregistered) from CMS/CMDB **Outputs**: • CMS/CMDB Addition/Modification not successful • Verified CMS/CMDB Addition/Modification
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. **Roles**: SACM Analyst, CI Owner, Configuration Librarian **Input**: • Verified CMS/CMDB Addition/Modification (Registered/updated CIs) **Output**: • CI Relationships established or updated

1.3 Configuration Control		
Controls Updates/Changes to CIs & Relationships		
Number	**Activity**	**Description**
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. **Roles**: SACM Analyst, CI Owner, Configuration Librarian **Input**: • CI Relationships updated (from Add or Update relationship) **Outputs**: • Closed Change Task o Feeds back into Change Management • Decommissioned /Deregistered CI o Feeds into ITAM/CI needs to be removed o Feeds into Operations Management/Decommissioned service asset and CI

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:

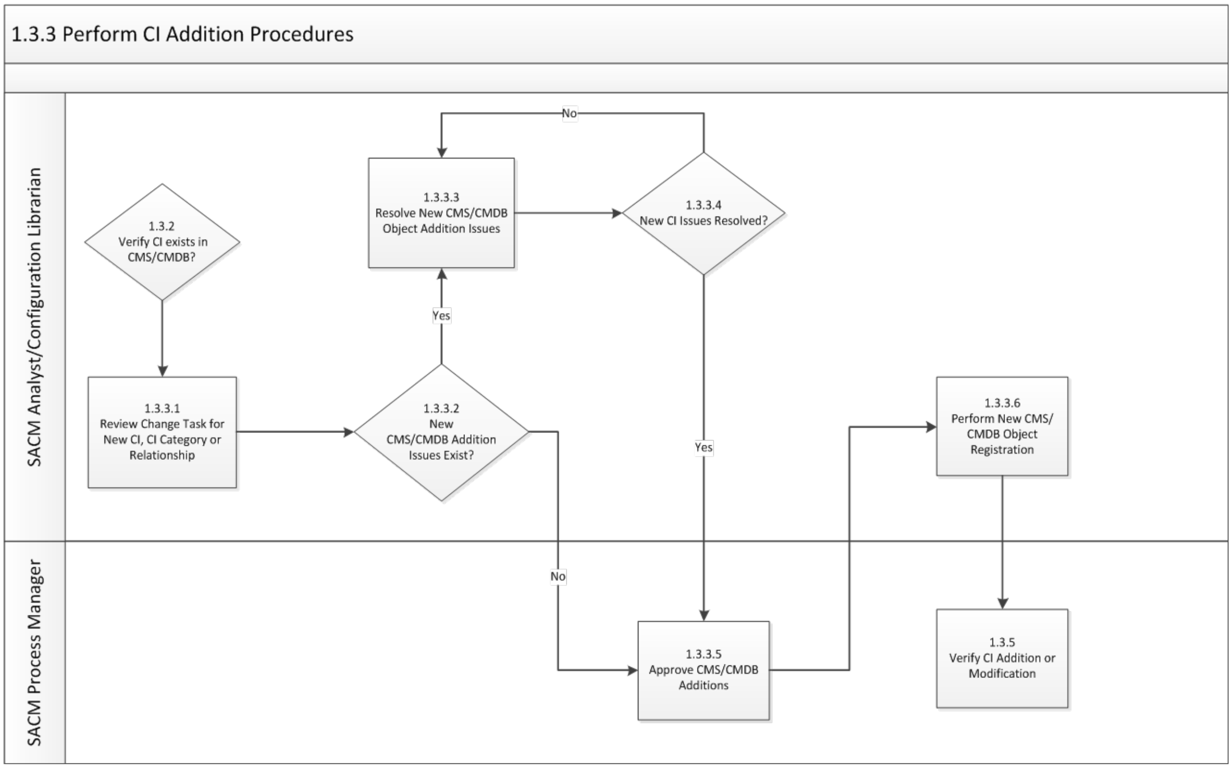

1.3.3 Perform CI Addition Procedures
SACM Analyst/Configuration Librarian
SACM Process Manager
1.3.2 Verify CI exists in CMS/CMDB?
1.3.3.1 Review Change Task for New CI, CI Category or Relationship
1.3.3.2 New CMS/CMDB Addition Issues Exist?
Yes
No
1.3.3.3 Resolve New CMS/CMDB Object Addition Issues
1.3.3.4 New CI Issues Resolved?
No
Yes
1.3.3.5 Approve CMS/CMDB Additions
1.3.3.6 Perform New CMS/ CMDB Object Registration
1.3.5 Verify CI Addition or Modification

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. **Roles**: SACM Analyst, Configuration Librarian **Input**: • New CI required **Output**: • Reviewed Change Task

1.3.3 Perform CI Addition Procedures		
Number	**Activity**	**Description**
1.3.3.2	Do New CMS/CMDB Addition issues exist?	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. **Roles**: SACM Analyst, Configuration Librarian **Input**: • Reviewed Change Task **Outputs**: • Issues Exist - begin remediation activities • 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. **Roles**: SACM Analyst, Configuration Librarian **Input**: • Issues Exist (Any data gathered to assist in resolving the issue) **Outputs**: • Issues Resolved - The Process Manager will review/approve the CMS/CMDB additions • Issues Not Resolved- continue to resolve issues before adding CI Object to the CMDB
1.3.3.4	New CI Issues Resolved?	If the issues regarding adding a new CI, CI Category, or Relationship are resolved, the CMS/CMDB can be modified accordingly. If the issues have not been resolved, work continues to resolve data issues using necessary resources. **Roles**: SACM Analyst, Configuration Librarian **Input**: • Resolution Results **Outputs**: • Issues Resolved - The Process Manager will review/approve the CMS/CMDB addition • 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. **Role**: SACM Process Manager **Input**: • Issues Resolved (Resolution results) **Output**: • 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. CMDB Objects include: • CI Instances • CI relationship instances • CI architecture building-block types/categories/baselines • CI relationship types **Roles**: SACM Analyst, Configuration Librarian **Input**: • CMS/CMDB Addition Approved **Output**: • Newly registered CI in CMS/CMDB

4.3.2 Configuration Control – Activity: 1.3.4 Perform CI Addition Procedures

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

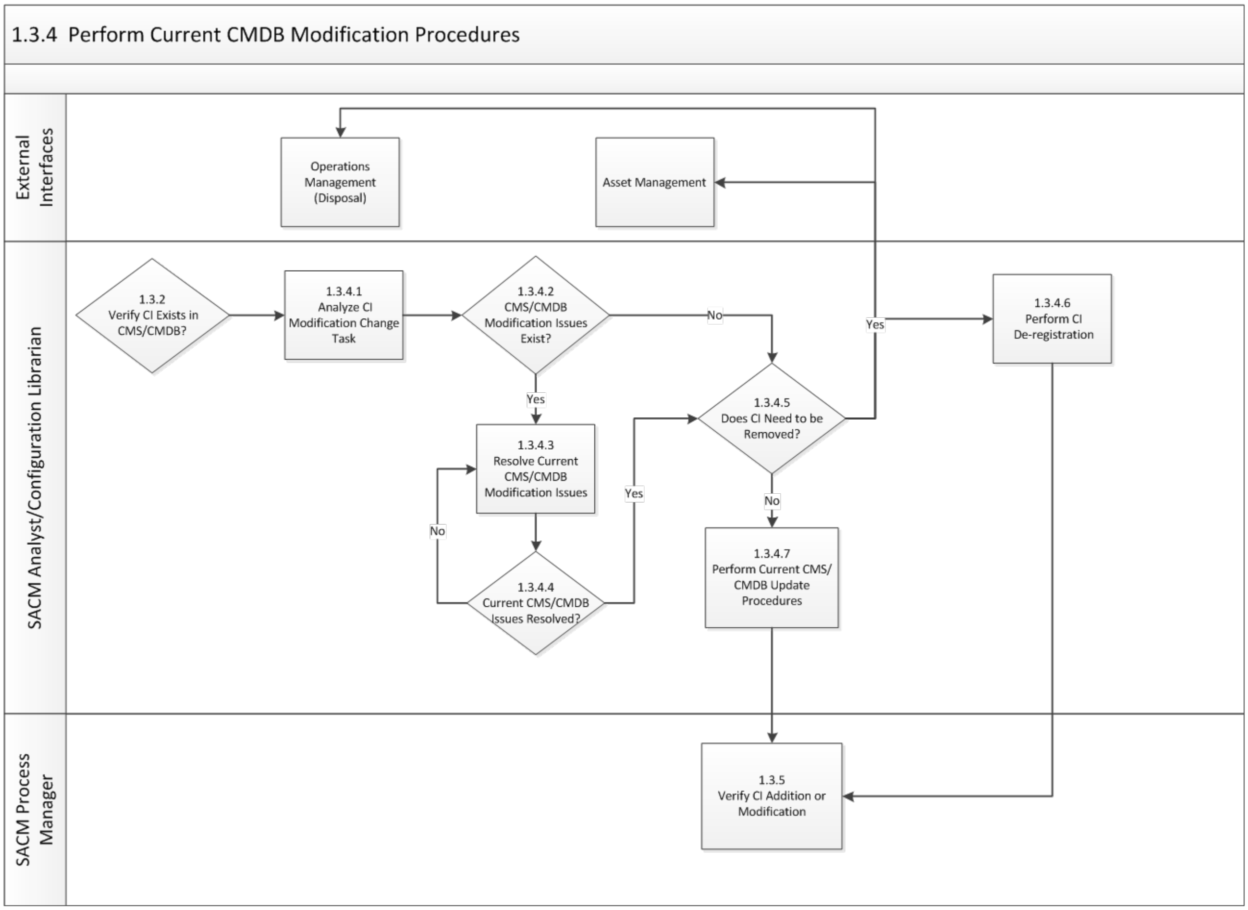

1.3.4 Perform Current CMDB Modification Procedures
External Interfaces
SACM Analyst/Configuration Librarian
SACM Process Manager
Operations Management (Disposal)
Asset Management
1.3.2 Verify CI Exists in CMS/CMDB?
1.3.4.1 Analyze CI Modification Change Task
1.3.4.2 CMS/CMDB Modification Issues Exist?
No
Yes
1.3.4.3 Resolve Current CMS/CMDB Modification Issues
No
1.3.4.4 Current CMS/CMDB Issues Resolved?
Yes
1.3.4.5 Does CI Need to be Removed?
Yes
No
1.3.4.6 Perform CI De-registration
1.3.4.7 Perform Current CMS/ CMDB Update Procedures
1.3.5 Verify CI Addition or Modification

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. **Role**: SACM Analyst, Configuration Librarian **Inputs**: • Verification that the CI does exist in the CMDB • Modification required to current CI **Output**: • Reviewed Change Task
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. **Roles**: SACM Analyst, Configuration Librarian **Input**: • Reviewed Change Task **Output**: • Issues Exist - Attempt to resolve the modification issues • 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. Procedures performed to resolve any issues that were discovered when attempting to modify the current CMS/CMDB. **Roles**: SACM Analyst, Configuration Librarian **Input**: • Issues Exist (Resolution needed in order to complete the modification) **Output**: • Modification Resolution
1.3.4.4	Current CMS/CMDB Issues Resolved?	If not, continue resolution attempts. **Roles**: SACM Analyst, Configuration Librarian **Input**: • Modification Resolution **Output**: • Issues Not Resolved- continue resolution attempts • Issues Resolved - CI can now either be modified or removed.

1.3.4 Perform Current CMDB Modifications Procedures		
Number	**Activity**	**Description**
1.3.4.5	Does CI Need to be Removed?	If any CIs need to be removed from the CMDB, the CIs are identified for de-registration. Asset Management and Operations Management are notified of the Decommissioned service asset and CI. **Roles**: SACM Analyst, Configuration Librarian **Input**: • Issues Resolved • Issues Do Not Exist **Output**: • CI Needs to be Removed (De-register) • CI Does Not Need to be Removed
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. The status is modified to archived/de-commissioned as appropriate. **Roles**: SACM Analyst, Configuration Librarian **Input**: • CI Needs to be Removed **Outputs**: • Removed CI (De-registration) from CMS/CMDB • 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. **Roles**: SACM Analyst, Configuration Librarian **Input**: • CI Does Not Need To Be Removed **Output**: • Modified CI

4.3.3 Configuration Control – Activity: 1.3.6 Software License Management and Compliance Procedures

The following workflow in Figure 4-9 illustrates the steps in the Activity - 1.3.6 Software License Management and Compliance Procedures:

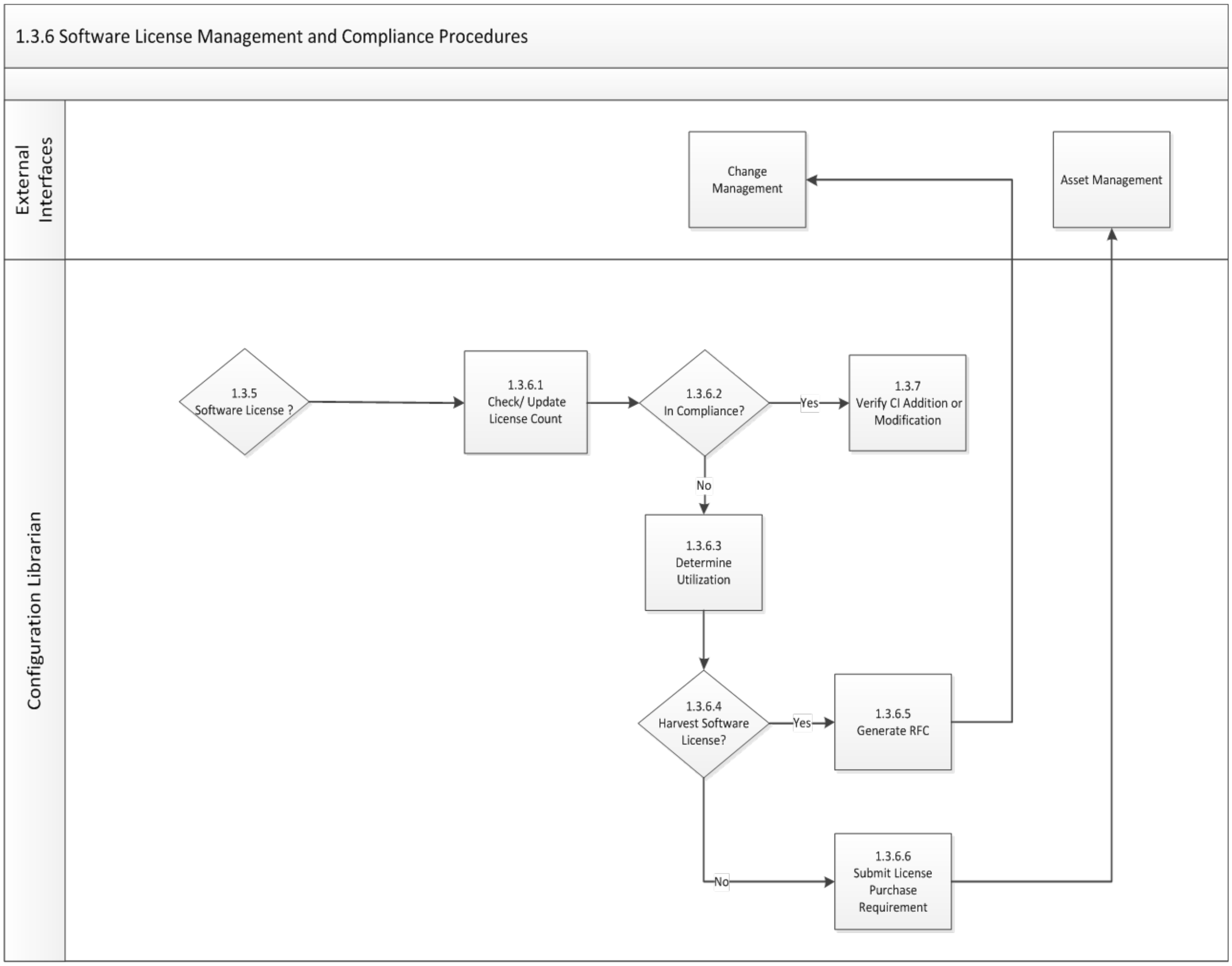

1.3.6 Software License Management and Compliance Procedures
External Interfaces
Configuration Librarian
Change Management
Asset Management
1.3.5 Software License ?
1.3.6.1 Check/ Update License Count
1.3.6.2 In Compliance?
Yes
1.3.7 Verify CI Addition or Modification
No
1.3.6.3 Determine Utilization
1.3.6.4 Harvest Software License?
Yes
1.3.6.5 Generate RFC
No
1.3.6.6 Submit License Purchase Requirement

Figure 4-9. 1.3.6 Software License Management and Compliance Procedures

The following Table 4-6 describes the Activity - 1.3.6 Software License Management and Compliance Procedures illustrated in Figure 4-9:

Table 4-6. Software License Management and Compliance Procedures Description

1.3.6: Software License Management and Compliance Procedures		
Number	**Activity**	**Description**
1.3.6.1	Check/Update License Count	The CMS is reviewed to determine the number of available Software Licenses. If available, a Software License can be assigned and the CMS can be updated. **Role**: Configuration Librarian **Input**: • RFC for Software License **Output**: • Review of CMS to determine if there are Software Licenses available
1.3.6.2	In Compliance?	After reviewing the CMS for assigned licenses, the Configuration Librarian must ensure that the organization is still in compliance with the license agreement. If there are sufficient licenses, the license can be assigned. If not, the compliance issues must be resolved before completing the software license request. **Role**: Configuration Librarian **Inputs**: • RFC for Software License • DML review **Outputs**: • Software License assigned • Resolve license compliance issues through RFC or purchase request
1.3.6.3	Determine Utilization	Are all the Software Licenses being effectively used? Usage of the software can be analyzed and reviewed. If there are no licenses available, then a decision can be made to give a non-utilized license to another user. **Role**: Configuration Librarian **Inputs**: • RFC for software license • Review of DML for available licenses **Output**: • Utilization report identifying software usage

1.3.6: Software License Management and Compliance Procedures		
Number	**Activity**	**Description**
1.3.6.4	Harvest Software License?	Based on utilization of the software licenses, there may be licenses that are not in use. These unused licenses can be "harvested" and assigned to another user to complete the RFC. **Role**: Configuration Librarian **Inputs**: • RFC for software license • Review of software usage for software license utilization **Outputs**: • Harvest Software License • Do not Harvest Software License- Submit purchase request for new/additional software licenses
1.3.6.5	Generate RFC	Generate a RFC to harvest the software license and assign it to another user. **Role**: Configuration Librarian **Inputs**: • RFC for Software License • Software Utilization Report • Software License Harvest Review **Output**: • RFC to Harvest Software License
1.3.6.6	Submit License Purchase Requirement	If all licenses are being utilized, a purchase order for the new license must be submitted to begin the procurement process. **Role**: Configuration Librarian **Inputs**: • RFC for Software License • Software Utilization Report • Software License Harvest Review **Output**: • Software License purchase request/requirement to Asset Management to begin procurement process

4.4 Status Accounting and Reporting

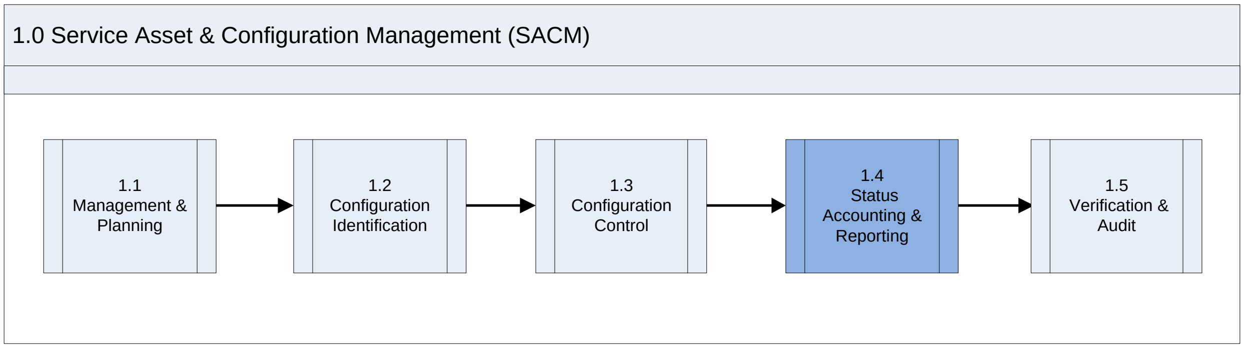

1.0 Service Asset & Configuration Management (SACM)
1.1 Management & Planning
1.2 Configuration Identification
1.3 Configuration Control
1.4 Status Accounting & Reporting
1.5 Verification & Audit

Figure 4-10. 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:

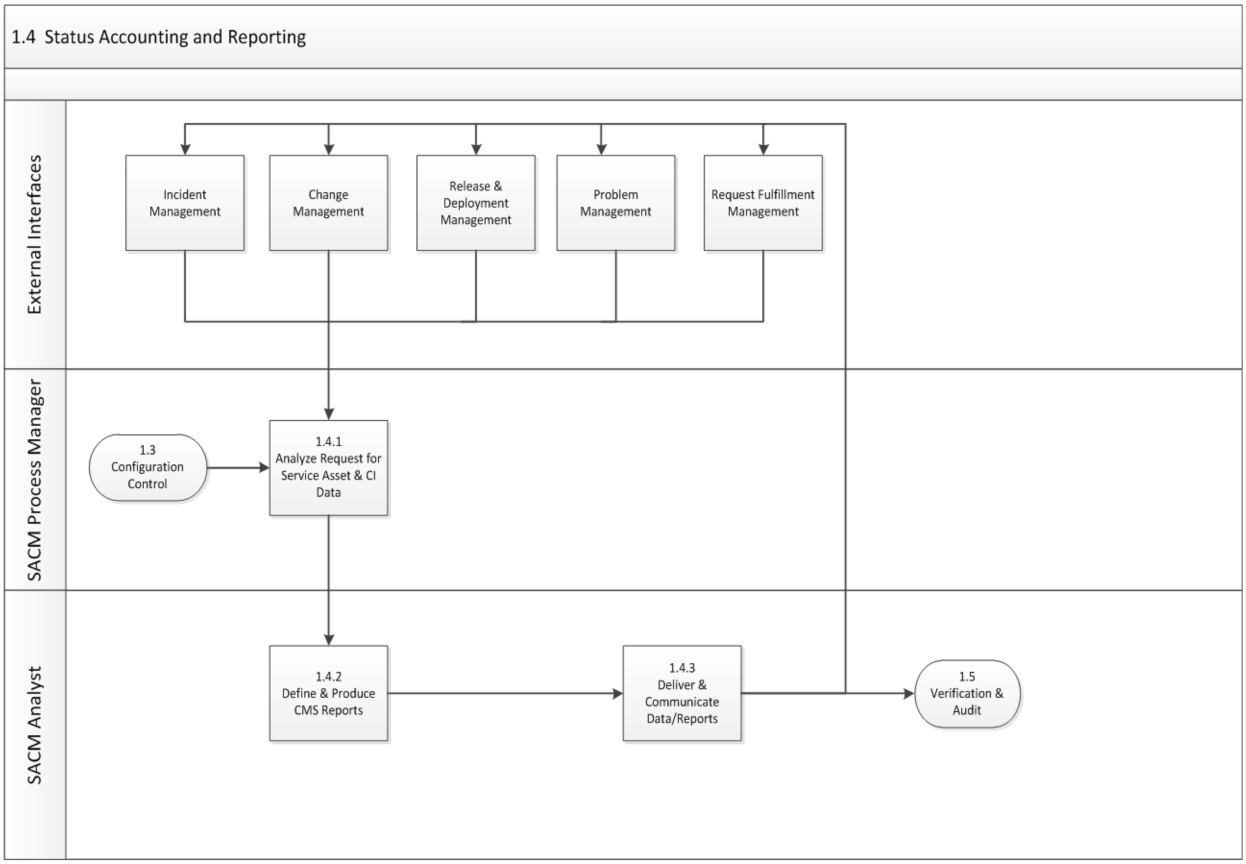

1.4 Status Accounting and Reporting
External Interfaces
SACM Process Manager
SACM Analyst
Incident Management
Change Management
Release & Deployment Management
Problem Management
Request Fulfillment Management
1.3 Configuration Control
1.4.1 Analyze Request for Service Asset & CI Data
1.4.2 Define & Produce CMS Reports
1.4.3 Deliver & Communicate Data/Reports
1.5 Verification & Audit

Figure 4-11. Status Accounting and Reporting Sub-Process Workflow

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

Table 4-7. 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. This activity is triggered by a request for service asset and CI data or to generate periodic status reports (from Configuration Control). • Review a request for a report on a CI, type, or attribute • Validate distribution authority • Determine if this request is to produce an ongoing standard report **Role**: SACM Process Manager **Inputs**: • Automated Discovery reports • Returns from CMS query • Service Asset, CI data, and Status data from CMS **Output**: • 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. • Define and build report. • Design a report that meets the needs of the requester. • Create the report. 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. 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. 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. 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. **Role**: SACM Analyst **Input**: • Service Asset and CI data (from queried databases and discovery reports) **Output**: • 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. • Deliver the report to the requester. • Validate the report with the requester. • Exceptions/anomalies detected (Exception Reports) will be provided to Verification & Audit. 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. **Role**: SACM Analyst **Input**: • Generated service asset and CI data report **Output**: • Completed service asset and CI data report

4.5 Verification and Audit

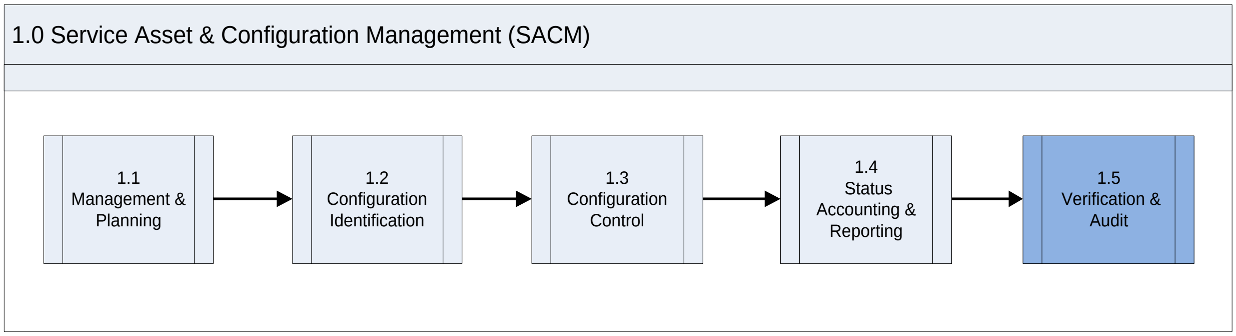

1.0 Service Asset & Configuration Management (SACM)
1.1 Management & Planning
1.2 Configuration Identification
1.3 Configuration Control
1.4 Status Accounting & Reporting
1.5 Verification & Audit

Figure 4-12. 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 to 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.

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

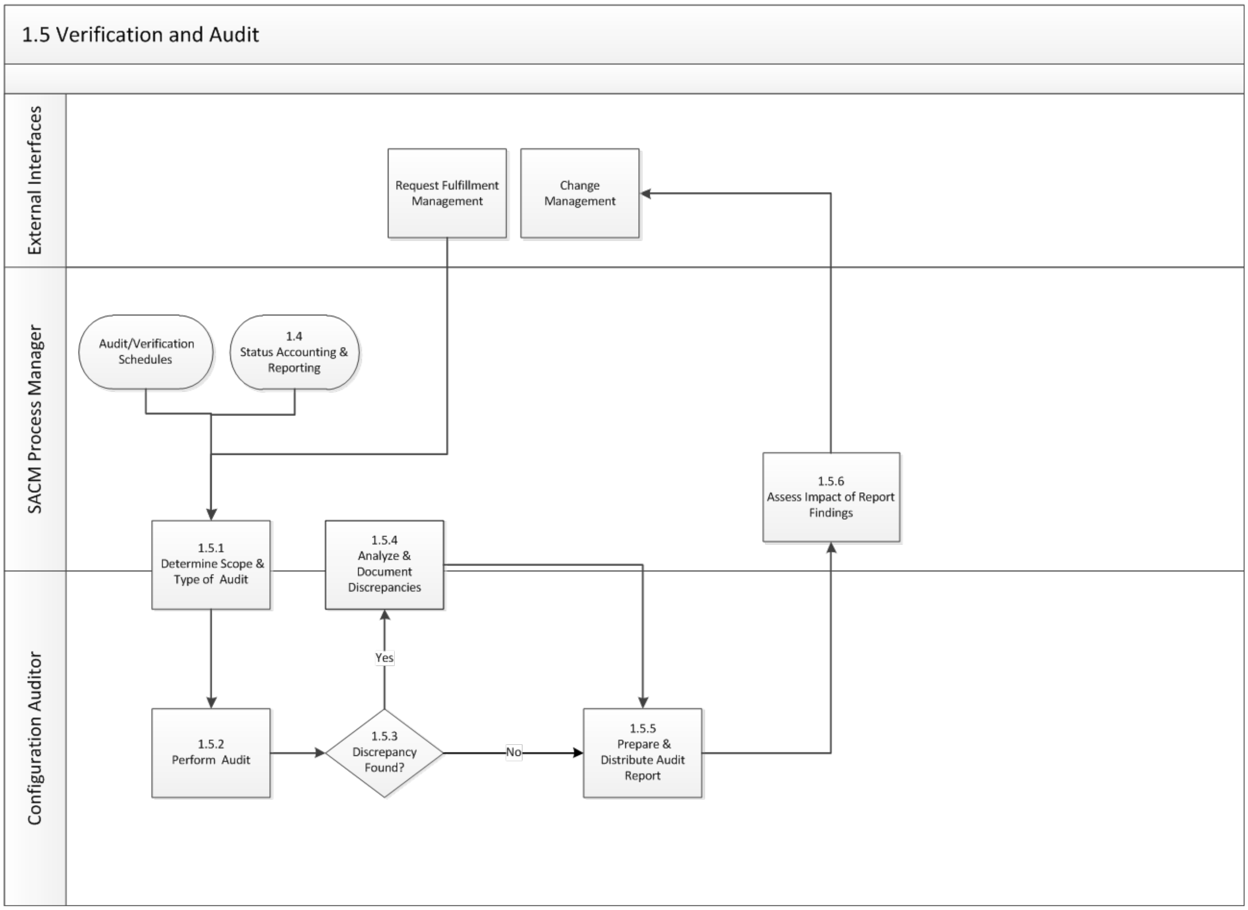

1.5 Verification and Audit
External Interfaces
SACM Process Manager
Configuration Auditor
Request Fulfillment Management
Change Management
Audit/Verification Schedules
1.4 Status Accounting & Reporting
1.5.6 Assess Impact of Report Findings
1.5.1 Determine Scope & Type of Audit
1.5.4 Analyze & Document Discrepancies
Yes
1.5.2 Perform Audit
1.5.3 Discrepancy Found?
No
1.5.5 Prepare & Distribute Audit Report

Figure 4-13. Verification and Audit Sub-Process Workflow

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

Table 4-8. 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. 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. Configuration Audits occur: • Shortly after changes to the CMS. • Software License Compliance needs. • Before /after changes to IT services or infrastructure. • Before a release or installation to ensure the environment is as expected. • Following the recovery from disasters and after a “return to normal” (in this case, the audit should be included in contingency plans). • At planned intervals per the SACM Plan, annually at a minimum. • At random intervals. • In response to the detection of any unauthorized CIs. **Roles:** SACM Process Manager, Configuration Auditor **Inputs**: • Scheduled Audit • Verification Scheduled • Ad Hoc audit request **Output**: • 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). The Configuration Auditor will perform the audit with assistance as needed from the CI Owner to establish reports on the CMDB, service assets, CIs, and Infrastructure baselines. A comparison is done between infrastructure and CMS using a Physical and/or Discovery tool audit. **Role**: Configuration Auditor **Input**: • Scope, Definition, and Type of Audit **Output**: • Verification and Audit Results (will be reviewed for discrepancies)
1.5.3	Discrepancy Found?	Determine if there is a discrepancy found in the results of the audit performed. **Role**: Configuration Auditor **Input**: • Audit Results **Outputs**: • Discrepancy Found – Discrepancies will be analyzed and document with the SACM Process Manager • 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. A key component of the verification and audit activities is the reconciliation between the managed and discovered inventories and configurations. **Roles**: SACM Process Manager, Configuration Auditor **Input**: • Audit Results - Discrepancies Found **Outputs**: • Documented Discrepancies • 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. **Role**: Configuration Auditor **Inputs**: • Discrepancy Analysis Results (Findings from audit) • Audit Results – no discrepancies **Outputs**: • Discrepancy Analysis Results- These results will be used to prepare the Audit Report • Audit Report- after the Configuration Auditor 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. 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. Document and communicate the remediation required to meet the baseline requirements of the reference model. Any updates to the CMDB should be performed through Change Management. If updates to the CMDB are required, RFCs are prepared. **Role:** SACM Process Manager (other process roles may be consulted) **Input**: • Audit Report **Outputs**: • Impact findings accessed • Feedback to determine if an update to the SACM Plan is needed

Appendix A – ACRONYMS

The official list of E-ITSM acronyms can be found on the Enterprise Information Technology Service Management site (https://eis.usmc.mil/sites/irm/ITSM/default.aspx). The link to the document is referenced below:

https://eis.usmc.mil/sites/irm/ITSM/Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Firm%2FITSM%2FDocuments%2FE%2DITSM%20Acronym%20List&FolderCTID=0x0120001918760B7D35A5478C0474985E3ACBCD&View={9CD820B3-EF85-4D2C-BD0C-A255AEE9E40D}

Appendix B – 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.
Back-out Plan	A Back-out Plan is developed in the Release planning phase. This plan provides a recovery plan to return to the original configuration or process if the release fails to achieve the planned outcome.
Backup	Backup is copying data to protect against loss of integrity or availability of the original data.
Change Schedule	A Change Schedule is a document that lists all approved changes and their planned implementation dates.
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 Plan	Document defining how configuration management will be implemented (including policies and procedures) for a particular acquisition or program. (Source: MIL HDBK-61A)
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.

Term	Definition
Early Life Support	Early Life Support (ELS) involves Technical Management or IT Operations providing support for a new or changed IT service for a period of time after it is released. During ELS, the IT service provider may review the KPIs, service levels, and monitoring thresholds and provide additional resources for incident management and problem management (when implemented).
EM System	The EM System (EMS) is comprised of tools which monitor CIs and provide event notifications. It is a combination of software and hardware which provides a means of delivering a message to a set of recipients. The EMS often requires real-time interaction, escalation, and scheduling.
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.
Escalation	Escalation is an activity that obtains additional resources when needed to meet service-level targets or customer expectations.
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.
Event Correlation	Event correlation involves associating multiple related events. Often, multiple events are generated as a result of the same infrastructure fault. Events need correlation to prevent duplication of effort in resolving the original fault.
Exit and Entry Criteria (Pass/Fail)	These are criteria (defined well in advance and accepted by the stakeholders) defined at authorized points in the Release and Deployment Process to set expectations of acceptable/unacceptable results.
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.
Pilot	A Pilot is a limited deployment of an IT service, a release, or a process to the live environment. A pilot is used to reduce risk and to gain user feedback and acceptance.

Term	Definition
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.
Severity	Severity refers to the level or degree of intensity.
Service Design Package	A Service Design Package (SDP) is composed of document(s) defining all aspects of an IT service and its requirements through each stage of its lifecycle. An SDP is produced for each new IT service, major change, or IT service retirement.
Service Improvement Plan	A Service Improvement Plan (SIP) is a formal plan to implement improvements to a process or IT service.
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.
Service Level Agreement	A Service-Level Agreement (SLA) is an agreement between an IT service provider and a customer. The SLA describes the IT service; documents service-level targets, and specify the responsibilities of the IT service provider and the customer. A single SLA may cover multiple IT services or multiple customers.
Service Validation and Testing	Service Validation and Testing is the process responsible for validation and testing of a new or changed IT service. Service Validation and Testing ensures an IT service matches the design specification and will meet the needs of the business. Service Validation and Testing during release conducts testing in the pre-production Systems Integration Environment (SIE) and during deployment in the pilot production environment.
Single Point of Contact	A Single Point of Contact (SPOC) is an agreement used to assign a single, consistent way to communicate within an organization or unit. For example, the Service Desk will be the SPOC for a service provider.
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.
Throttling	Some events do not need to be acted on until they have occurred a number of times within a given time period. This is called Throttling. Once a repeated event has reached its limit for repetition, forward that event to be acted upon.
User Acceptance Testing	User Acceptance Testing is a testing activity conducted by the user intended to verify a CI, IT service, or process meets a specification. It is also used to validate whether agreed requirements have been met.
Work-around	Work-arounds for problems are documented in known error records and are intended to reduce or eliminate the impact of an incident or problem for which a full resolution is not yet available. Work-arounds for incidents that do not have associated problem records are documented in the incident record.
Work Instruction	The Work Instruction is a document containing detailed instructions that specify exactly what steps are followed to carry out an activity. A work instruction contains much more detail than a procedure and is only created if very detailed instructions are needed.

APPENDIX C – Definitive Media Library (DML)

The DML was developed independently as a stand-alone document titled Definitive Media Library Interim Operations Guide, dated 06 December 2013. As such, the DML is formatted and outlined similar to an E-ITSM process guide. It is included as an appendix in the SACM Process Guide to reference the critical role the DML has in this process and with regards to the solid solution it provides with the control of what media is released into the production environment.

1.0 DML INTRODUCTION

1.1 Background

USMC requires a DML capability to host the USMC certified solutions in support of approved Release and Deployment actions.

1.2 Scope

This integration of the DML in the SACM Process Guide is specific to Non-Secure Internet Protocol Router Network (NIPRNet) operations. The DML is critical in supporting the transition of enterprise solutions from development to production. DML manages only the documents and media which have been certified into production. Raw media resulting from procurement activities is stored separately from DML artifacts.

The DML has several internal repositories/instances in which the definitive, approved versions of Master Documentation CIs, Site and Applied Engineering Documentation, Pre-Production bundles, and Certified DML bundles are managed. The DML is a single logical storage area, even if there are multiple instances within the area. All changes to solutions in the DML must be approved or “certified” by Enterprise Change Management (ChM) processes. Only certified solutions from the DML are acceptable for deployment to the Production environment.

Items the DML instances include:

- Pre-Production solution bundles.
- Certified Solution bundles.
- Site and Applied Engineering Documentation.
- Master Documentation (relative to solution bundles).

2.0 DML Overview

2.1 Purpose, Goals, and Objectives

The purpose of a Definitive Media Library (DML) is to provide a secure repository (tool) in which USMC definitive, authorized versions of software media and documentation are managed (activity) by DML Librarians (people). Before any new or changed solution is released into the USMC operational environment, any such software is fully tested, quality assured, and RFC Approved via Enterprise Change Management.

The goal of the DML is to provide the areas for documentation and solutions ready for deployment and only contain master copies of controlled, solutions that have passed appropriate quality assurance checks.

The primary objectives of the DML are to:

- Support Engineering efforts to develop new solutions or updates to existing solutions by providing current, certified baselines.
- Support USMC Enterprise Release & Deployment Management as a foundation and the central repository for all deployable, certified solutions and documentation.

2.2 Relationships with Other Processes

DML activities, and support for the DML, are interrelated. The stakeholder interactions represented in Figure C-1 are shown because of the strength of the relationships and dependencies between them, such as changes to CI records occur with an Approved RFC, releases occur with an Approved RFC, etc. The dependencies exist between the processes; their strength is revealed when the processes are adhered to. As the single repository and certified area for all deployment solutions, the DML supports, and interfaces with, several service management processes and activities.

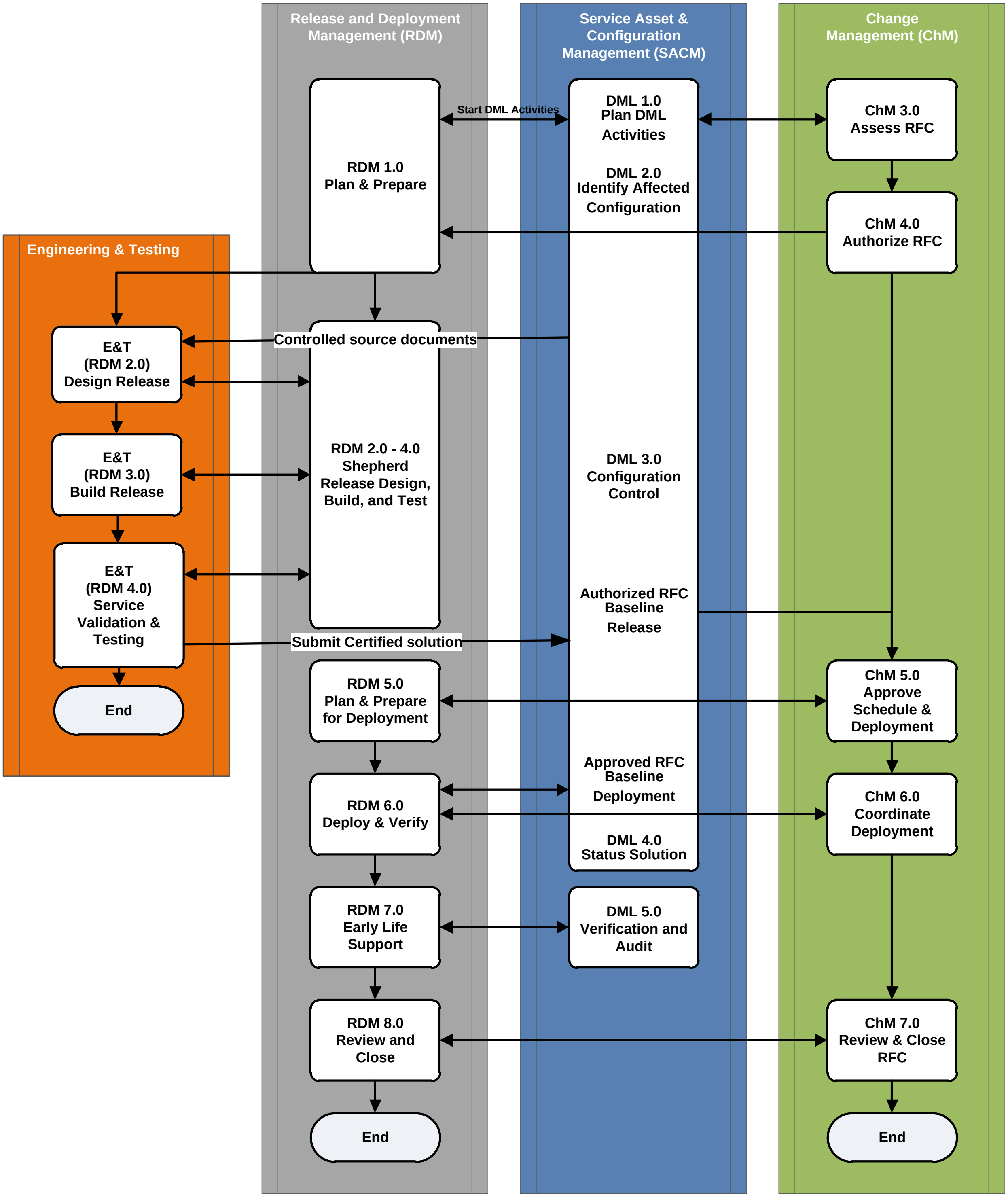

Release and Deployment Management (RDM)
Service Asset & Configuration Management (SACM)
Change Management (ChM)
Engineering & Testing
RDM 1.0 Plan & Prepare
Start DML Activities
DML 1.0 Plan DML Activities
DML 2.0 Identify Affected Configuration
ChM 3.0 Assess RFC
ChM 4.0 Authorize RFC
E&T (RDM 2.0) Design Release
Controlled source documents
E&T (RDM 3.0) Build Release
RDM 2.0 - 4.0 Shepherd Release Design, Build, and Test
DML 3.0 Configuration Control
E&T (RDM 4.0) Service Validation & Testing
Authorized RFC Baseline Release
Submit Certified solution
End
RDM 5.0 Plan & Prepare for Deployment
ChM 5.0 Approve Schedule & Deployment
Approved RFC Baseline Deployment
RDM 6.0 Deploy & Verify
ChM 6.0 Coordinate Deployment
DML 4.0 Status Solution
RDM 7.0 Early Life Support
DML 5.0 Verification and Audit
RDM 8.0 Review and Close
ChM 7.0 Review & Close RFC
End
End

Figure C-2-1. DML Stakeholder Interaction Model

The following represents a summarized brief of the stakeholder interactions (inputs or outputs) depicted in Figure C-2-1.

Change Management

- Assesses and Authorizes Change action.
- RFC Authorizes DML release of materials to Engineering.
- RFC Approves tested and validated Solution for Release.
- Closes RFC after final (when multiple are being implemented) Release Record(s) is Closed by RDM.

Engineering Management

- Requests DML materials for New or Changed Solution.
- Develops New or Changed Solution.
- Coordinates Solution Engineering and Testing with RDM.

DML Management

- Plans DML activities.
- Identifies New or Changed Solution as identified by RDM.
- Controls Solutions in and out of DML.
- Reports on the status of solutions in the DML and their control activities.
- Verifies and Audit DML Solution Baselines.

Release and Deployment Management

- Plans Release of the Solution Bundle.
- Oversees Engineering’s Test and Validation activities.
- Prepares and performs Deployment.
- Reviews and Manage Deployment.
- Closes Release Record(s).

2.3 DML Workflow Model

The DML workflow follows the Enterprise Service Asset & Configuration Management workflow, and consists of five distinct activities (i.e., (1) DML Planning, (2) DML Product Identification, (3) DML Control, (4) DML Status Accounting, and (5) DML Verification & Audit which interface with Stakeholder Processes and the DML to perform DML activities with the four DML repositories/instances (Pre-Production, DML, Master Documents, and Site & Applied Engineering Documents) boxed together in the DML Activity Interface Model in Figure C-2-2. The Master Copies of New Software repository resides outside of formal DML management as depicted.

The numbering within the formal process cells (ChM, RDM, and SACM) represents a specific Input/Output step within the referenced process where that process workflow interfaces with the specified DML repository workflow. The DML workflow cells are numbered to their respective activities and further defined in Table C-1 below.

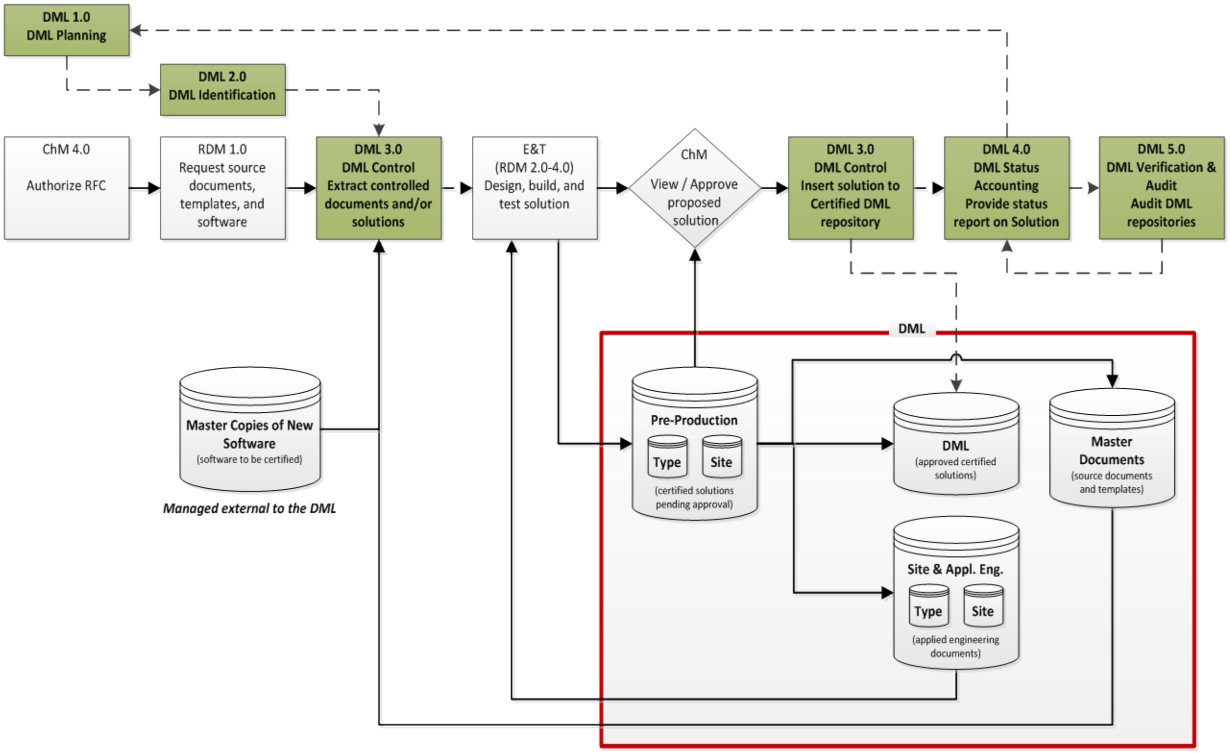

DML 1.0
DML Planning
DML 2.0
DML Identification
ChM 4.0
Authorize RFC
RDM 1.0
Request source documents, templates, and software
DML 3.0
DML Control
Extract controlled documents and/or solutions
E&T
(RDM 2.0-4.0)
Design, build, and test solution
ChM
View / Approve proposed solution
DML 3.0
DML Control
Insert solution to Certified DML repository
DML 4.0
DML Status Accounting
Provide status report on Solution
DML 5.0
DML Verification & Audit
Audit DML repositories
DML
Master Copies of New Software
(software to be certified)
Managed external to the DML
Pre-Production
Type
Site
(certified solutions pending approval)
DML
(approved certified solutions)
Master Documents
(source documents and templates)
Site & Appl. Eng.
Type
Site
(applied engineering documents)

Figure C-2-2. DML Workflow Model

Table C-2-1 below contains descriptions of each activity and its interface support to the DML. Each activity number is hyperlinked to its detailed description in Section 4.0, DML Activities.

Table C-2-1. DML Activity Descriptions

Number	Activity	Description
1.0	DML Planning	Is the initial activity within the DML activities. DML Planning represents the core DML activity and its relationships to the other DML activities. Inputs to DML Planning consist of communications criteria - standard on which a judgment or decision may be based - with all of the other DML activities regarding the planning of their individual and integrated division of work to broken out into specific tasks with deadlines, frequency – rate of occurrence - for, reporting, and selected information and performance measurements. The activity is facilitated by the degree of management support provided and the working relationships established with other interfacing activities such as Change Management, Engineering and Logistics, and Release Management. The resulting output of DML Planning is the supporting data and information relative to each of the DML activities and integrated support within the CMS (DML, CMDB, IP Share, etc.).
2.0	DML Product Identification	Defines how the new or enhanced solutions are to be selected, grouped, classified, and defined including the appropriate characteristics (e.g., warranties for a service, software license, etc.) to ensure they are manageable and traceable throughout their lifecycle. Define the roles and responsibility of the owner for a solution at each stage of its lifecycle. A key consideration of DML Product Identification is the naming convention provided by SACM. • Collaborate with Engineering to define and document criteria for selecting solutions and the components that compose them. • Select the solutions and their components according to documented criteria. • Assign SACM provided identifier and specify the relevant attributes to solutions. • Specify when each solution is placed under control of DML Control.
3.0	DML Control	The activity of extracting, or “checking-out”, identified products such as documents from the DML Master Source Documents repository based on an Authorized RFC from Change Management. The DML Librarian extracts the identified products via the Authorized RFC and provides to the requestor via defined Work Instructions. Requesting contents from the DML may also be to retrieve a copy of a solution/solution bundle to conduct the install of a device based on known configurations by Operations personnel either at the MCNOSC or the MITSC, and may not result in an RFC. The activity of inserting, or “checking-in” a developed/built solution into the DML Pre-Production repository based on, or aligned with, the original Authorized RFC from Change Management. . The DML Librarian takes the identified solution from the requestor and inserts the identified solution, via the Authorized RFC, into the DML Pre-Production repository. The activity of DML control is extended beyond the extract/insert controls to ensure there are adequate control mechanisms over solutions while maintaining a record of changes to solutions, versions, location and ownership. Ensures that no solution is added, modified, replaced, or removed without an appropriate controlling documentation or procedure being followed. The activity of extracting, or “checking-out”, the Certified solution from the DML Certified Solutions based on an Approved RFC from Change Management. These solutions are only those approved by Change Management as meeting the RFC requirements. The DML Librarian extracts the identified Certified solution, aligned with Approved RFC, and provides to RDM via defined Work Instructions

Number	Activity	Description
4.0	DML Status Accounting	The activity of providing the status accounting of activities at milestones related to the entrance of a product into the DML, and its progress/movement activities within the DML repositories. This status accounting is typically notification milestones such as when the solution is inserted into Pre-Production or extracted from Pre-Production repository and inserted into the Certified DML repository. While the actions are typically notifications, there is also reporting activities aligned with CMDB CIs related to Certified solutions. Based on an Authorized RFC, the submitting Engineering POC collaborates with the DML Librarian to provide notification of a built solution being inserted into the Pre-Production repository. Based on an Approved RFC, the DML Librarian notifies ChM, SACM, and RDM when solution is extracted from the Pre-Production repository and inserted into the DML repository. This is typically when the solution is ready for approved RDM deployment action.
5.0	DML Verification & Audit	The activity of auditing the contents of the DML repositories as well as the related CMDB CI records to verify CI-to-solution relationship accuracy. This is typically performed DML Librarian conducts the standard level of logical and physical audits on contents within the DML, as well as the records within the CMDB matching. As part of Post-Implementation Review (PIR), DML Librarian collaborates with RDM and ChM for the verification the release has been successfully implemented as requested. In the case of a failed deployment and PIR, notification from ChM and RDM must be provided back to the DML Librarian whereby the identified subject solution is frozen in the DML repository for further corrective action. Back out actions are not a DML action, however as the deployment pushed an electronic copy, there is no need for a “check-back”.

2.4 Key Concepts

In addition to those identified in the Enterprise SACM Process Guide, the following applies:

2.4.1 Solution Bundle

A solution bundle is a culmination of software, engineering documents or both for a product or series of products which has been certified for release into the operational environment. The difference between Solution Bundles and Release Packages is the release package may encompass a series of solution bundles within a release window. Solution bundles package and deploy custom features, site definitions, templates, software, and site related and applied engineering documentation.

2.5 Continual Service Improvement

Continual Service Improvement (CSI) depends on accurate and timely measurements and relies upon obtaining, analyzing, and using information that is practical and meaningful. Measurements of efficiency and effectiveness enable the USMC to track performance and improve overall end user satisfaction. Workflow metrics are used as measures of how well the workflow and/or its individual activities are working, whether or not the activity is continuing to improve, or where improvements should be made. When evaluating 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 workflow requires the use of metrics and measurements. Reports need to be defined, executed, and distributed to enable the managing of workflow-related issues and initiatives. Daily management occurs at the Process

Manager level. Long-term trending analysis and management of significant activities occurs at the Process Owner level.

The essential components of any measurement system are Critical Success Factors (CSFs), and Key Performance Indicators (KPIs) to achieve these CSFs.

2.5.1 Critical Success Factors (CSF) with Key Performance Indicators (KPI)

As with all activities and activities, the performance of DML activities should be monitored, reported on, and action taken to improve it.

CSFs are defined as activity-specific or service-specific goals that must be achieved if an activity, workflow, or IT service is to succeed. KPIs are the metrics used to measure performance or progress toward stated goals.

The following CSFs and KPIs can be used to judge the efficiency and effectiveness of the workflow. Achievement against KPIs should be monitored and used to identify opportunities for improvement, which should be logged in the CSI register for evaluation and possible implementation.

A threshold (target) is set by the SACM Process Owner as DML is a sub-set of SACM. The measurement is done on a monthly basis. Since the trend is what we are looking for, the metric becomes valuable not sooner than after 3 months. Also, not more than the last 13 months should be included in the report. Going back further would decrease the value of the information the report is providing.

Table C-2-2 describes the metrics to be monitored, measured, and analyzed.

Table C-2-2. DML Critical Success Factors with Key Performance Indicators

CSF #	Critical Success Factors	Key Performance Indicators	KPI Measure	Benefits
1	Improve DML Change	Percentage of failed Changes due to incorrect data in the CMDB/DML, or poor version control	# Failed Changes x 100 Total # of Changes	A decrease in percentage indicates an improvement in effectiveness and efficiency of DML Operations. A higher percentage of failed Changes indicate potentially a problem with updating the CMDB/DML after implementation of Changes, a Change process being circumvented, the execution of audit & verification procedures and/or poor verification of CI information before implementing Changes.
2	Improve DML Control	Percentage of unauthorized CIs introduced into DML solutions	# Unauthorized CIs x 100 Total # of CIs	A decrease in percentage indicates an improvement in effectiveness and efficiency of DML Operations. A higher percentage of unauthorized CIs indicate potentially the lack of DML Control, the lack of education and awareness and/or Change Management processes not being

CSF #	Critical Success Factors	Key Performance Indicators	KPI Measure	Benefits
				followed.
3	Improve DML Verification & Audit	Percentage accuracy of CI when compared to the live environment	# Errors in CI information x 100 Total # of CIs	A decrease in percentage indicates an improvement in effectiveness and efficiency of DML Operations. A lower percentage of accuracy of CIs indicates potentially a lack of control and CMDB/DML maintenance and relationships of Changes to the solutions, problems with the update procedures for the CMDB/DML and/or poor verification of CI information before implementing updates to the CMDB/DML.

3.0 DML Roles and Responsibilities

The DML has roles and responsibilities associated with execution and management of the DML activities.

3.1 Roles

The following abstract drawing (Figure C-3-1) depicts DML roles for the USMC, with their relationship to SACM roles, followed by a description of these roles (Table C-3-1).

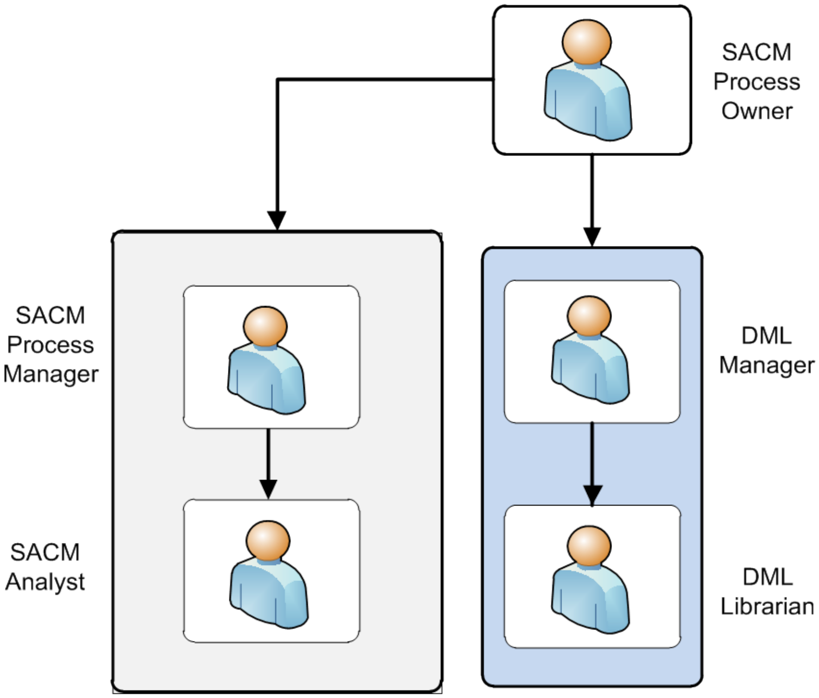


Figure C-3-1. DML Roles

Table C-3-1. DML Defined Roles and Responsibilities

Description	Overall Responsibility
Role #1 DML Manager	
The DML Manager is responsible for developing and implementing the specific DML work instructions aligned with defined DML activity and procedures. The DML Manager is the direct interface for DML with Change, Engineering, MITSC POCs, Configuration, and Release, all other project and activity teams as required for maintenance and control of the DML.	• The overall point person responsible for all DML activities and planning within the scope of the environment level for which responsibilities are defined. • Ensures the DML is accurate and directly interfaces with Change Management to ensure the activity is followed for solution changes. • Defines reports to support the DML activity with respect to Status Accounting and Verification & Audit activities. • Schedules and facilitates DML audits. • Participates in meetings representing DML. • Performs training, job shadowing, and knowledge transfer of DML

Description	Overall Responsibility
	activity upon availability of government resources. • Administers access management. • Implements and contributes to DML activity and workflow development.
Role #2 DML Librarian	
The DML Librarian performs the DML operations for extraction and insertion of products/solutions and the internal DML Control functions of processing various documents (i.e., installation documents, diagrams, software applications) and solutions control (moves between repositories, archives, etc.	• Maintains DML material inventory. • Researches and responds to management requests and produces reports. • Stores and distributes physical materials within a storage facility. • Maintains logs for inventory. • Checks-in and checks-out DML products per Authorized or Approved RFC. • Performs data entry into GFE SharePoint and Remedy CfM tools. • Performs records and forms management to include Remedy content management.

3.2 Responsibilities

These roles are then mapped to job functions, IT staff, and departments. The SACM Process Co-Owner is accountable for ensuring activity interaction by implementing systems that allow smooth activity flow.

The Responsible, Accountable, Support, Consulted, Informed (RASCI) model is a method for assigning the type or degree of responsibility that roles (or individuals) have for specific tasks. Table 4 displays the RASCI model for DML by activity roles.

- **R**esponsible – Completes the activity; responsible for action/implementation. The degree of responsibility is determined by the individual with the ‘A’.
- **A**ccountable – Approves or disapproves the activity. Individual who is ultimately answerable for the task or a decision regarding the task.
- **C**onsulted – Gives needed input about the activity. Prior to final decision or action, these subject matter experts or stakeholders are consulted.
- **S**upport – Provides resources or a supporting role in the activity. Resources allocated to responsible. Unlike consulted, who 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. This is one-way communication.

Table C-3-2 shows activity responsibilities by role.

Table C-3-2. DML Activity Responsibilities by Role Table

DML Activity	DML Manager	DML Librarian	EEVE Engineer	Change Manager	Configuration Manager	RDM Manager
DML Planning	S	R	CI	CI	CI	CI
DML Product Identification	S	R	CI	CI	CI	CI
DML Control	S	R	I	I	I	I
DML Status Accounting	S	R	I	I	I	I
DML Verification & Audit	S	R	CI	I	I	CI

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

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

Note: Only one role can be accountable for each activity. For the DML, the SACM Process Co-Owner is ultimately accountable.

4.0 DML Activities

The DML operation consists of five activities. As depicted, the DML activity is responsible for planning, identifying, controlling, recording/tracking/reporting, and auditing/verifying information about solutions required to deliver an IT Service (including their relationships).

4.1 DML Planning

DML Planning represents the core DML activity and its relationships to the other DML activities. Inputs to DML Planning consist of the authorization to initiate a new or updated DML certified solution, communications with all of the other DML activities, and selected information and performance measurements received from the DML Status Accounting activity. The activity is facilitated by the degree of management support provided and the working relationships established with other interfacing activities such as Change Management, Engineering, MITSC POCs, Configuration Management, and Release & Deployment Management.

The resulting output of DML Planning is the supporting data and information relative to each of the DML activities and a new or updated Certified solution.

The objectives of DML Planning are to set and document the following:

1. The source origination acceptance criteria,
2. The integration of the DML schedule with Change or Release schedule,
3. The Stakeholder interface responsibilities,
4. The DML activities, and
5. The Stakeholder reporting requirements.

The following workflow (Figure C-4-1) depicts the DML Planning activity:

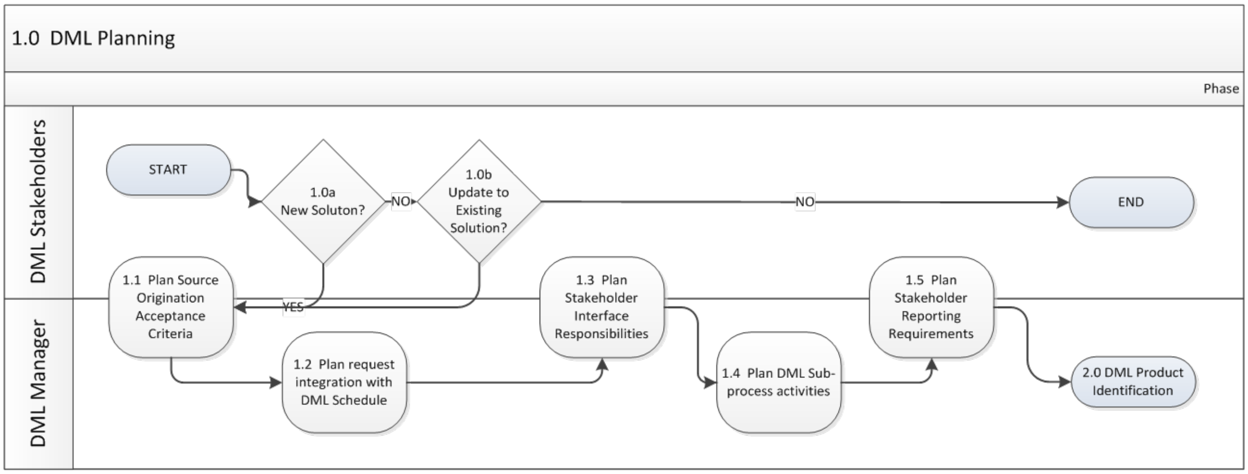

1.0 DML Planning
Phase
DML Stakeholders
DML Manager
START
1.0a New Soluton?
NO
1.0b Update to Existing Solution?
NO
END
YES
1.1 Plan Source Origination Acceptance Criteria
1.2 Plan request integration with DML Schedule
1.3 Plan Stakeholder Interface Responsibilities
1.4 Plan DML Sub-process activities
1.5 Plan Stakeholder Reporting Requirements
2.0 DML Product Identification

Figure C-4-1. DML Planning Workflow

Table C-4-1 describes the DML Planning activity steps as depicted in Figure C-4-1.

Table C-4-1. DML Planning Activity Descriptions

1.0 DML Planning		
Number	**Activity**	**Description**
1.1	Plan Source Origination Acceptance Criteria.	The DML Manager plans and documents the origination acceptance criteria with the originating source requestor based on status of proposed solution – either a new solution or an update to an existing solution under DML control. When the proposed solution is new, the DML Manager plans on the acceptance criteria with the originating source Requestor. This will include: • The document templates to be provided by Knowledge Management (or the E&T technical editing team), and • The raw media to be provided (once software license is recorded and entered within the CMDB) by the DML Librarian. When the proposed solution exists, the DML Manager plans on the acceptance criteria with the originating source Requestor. This includes: • The Source Documents to be provided by the DML Librarian, • The existing and/or new media/software by the DML Librarian, • The DML Librarian actions ensuring the Release Record contains relationships to the DML, CMDB, and other related CIs impacted by the RFC, • The artifacts received from an alternate source which are not delivered/shipped to be provided by the DML Librarian, and • The proper recording within the CMDB to follow extraction (check-out) procedures. Included in this planning step will be Activity 4.0 Status Accounting, Step 4.7 when an Audit Findings Report or DML Status Accounting Report indicates the need to remediate a finding or mitigate a risk through a change to a DML controlled solution. Source origination thus becomes the requirements from the subject report whereby acceptance planning ensues. Proceed to Step 1.2
1.2	Plan request integration with DML Schedule	The DML Manager plans and documents the integration of the Requestor's milestones and timelines into the DML Schedule of current and future DML activities. This will include: • The correlation between the RFC Change Calendar and/or the Release Record containing the expected delivery/release date with the DML Schedule for situational awareness and workload management, • The schedule mitigation when there is a conflict, and • The baselining of the new or updated DML Schedule. This activity is more prevalent when the DML is engaged in control of multiple, concurrent solution changes. Proceed to Step 1.3

1.0 DML Planning		
Number	**Activity**	**Description**
1.3	Plan Stakeholder Interface Responsibilities	The DML Manager plans and documents the stakeholder interface responsibilities during control of a solution in the DML. This will include: • The data attribute requirements for Source Document/Media requests from the Project Officer or Lead Engineer, • The communications mechanisms (face-to-face, phone, email, portal, Remedy, DCO) and frequency (agreed days and times, established meetings, ad hoc, formal milestones) between Engineering, DML Librarian, Configuration Manager, Change Manager, and Release & Deployment Manager, • The management of the proposed/agreed schedule of activities pertaining to the subject solution, • The location where the DML Librarian is to provide document templates, raw media, source documents, and existing and/or new media/software to, and • The access and permissions for the DML Librarian to the receiving location(s). Proceed to Step 1.4
1.4	Plan DML activities	The DML Manager plans and documents the identification, control, status accounting, and verification/audit activities to support the DML in a repeatable manner as well as in support of any request with specific needs. This will include: • DML Identification – The naming convention to be used for the new or updated solution as provided by SACM. • DML Control – The extraction (check-out) of documents and new or existing media/software, the insertion (check-in) of new or updated solutions, version control, intra-DML repository activities (solution progression between repositories), and the archiving post-release. • DML Status Accounting – The notification mechanisms between the DML Librarian to Engineering, Configuration Management, Change Management, and Release & Deployment Management when an extraction or insertion occurs, and when the solution is Approved to move from the Pre-Production repository to the Certified DML for Release and Deployment Management action. Notifications and receipt of notifications will be included in the Reporting Requirements. Also includes inputs from Step 4.7 for Status Accounting and Audit Reporting. • DML Verification & Audit – The review and verification that RFCs and Release Records have been properly Authorized by Change Management and that implemented changes are as Authorized. This also includes audit activities that (1) ensure that there is conformity between the documented DML baseline and the actual USMC environment, (2) verify the physical existence of CIs in the DML, (3) verify functional and operational characteristics of solutions and to check that the records in the CMS match the physical infrastructure, (4) check that the release and configuration documentation is present before progressing to the Certified DML repository for a release, and (5) recommended mitigation steps to Audit Findings within area of responsibility. Audit Findings will be included in Reporting Requirements, and recorded findings from Step 5.4 are provided to DML Status Accounting Step 4.7. Proceed to Step 1.5

1.0 DML Planning		
Number	**Activity**	**Description**
1.5	Plan Stakeholder Reporting Requirements	The DML Manager plans and documents the Stakeholder reporting requirements. This will include: • The scope of DML activities, • The scope of current, baselined solution bundles under DML control, • The scope of under-development and test and certified solution bundles ready for RDM, to include RFCs, • The Status Accounting notifications and receipt of notifications, and • The Audit Findings and recommended mitigation steps. Continue to Activity 2.0

4.2 DML Product Identification

DML Product Identification, in collaboration with DML Planning, defines how the physical and logical media, software, documentation, and source code CIs are to be selected, grouped, classified, defined, and named individually as well as collectively to a rollup (solution bundle) CI. This ensures they are manageable and traceable throughout their lifecycle.

A key consideration of DML Product Identification is uniquely naming and labeling all solution bundle components of interest across the solution and the relationship between them.

CIs include physical media, software, source code, and documentation components of (and supporting) the solution and/or solution bundle.

This DML activity defines the roles and responsibility of solution owners at each stage of solution lifecycles.

The solutions and their components are selected according to documented criteria established with DML Planning.

A unique identifier is assigned and specifies the relevant attributes for a solution and/or a solution component.

This activity also specifies when each CI is placed under control of DML Control, and identifies the owner responsible for each solution.

The following workflow (Figure C-4-2) depicts the DML Product Identification activity.

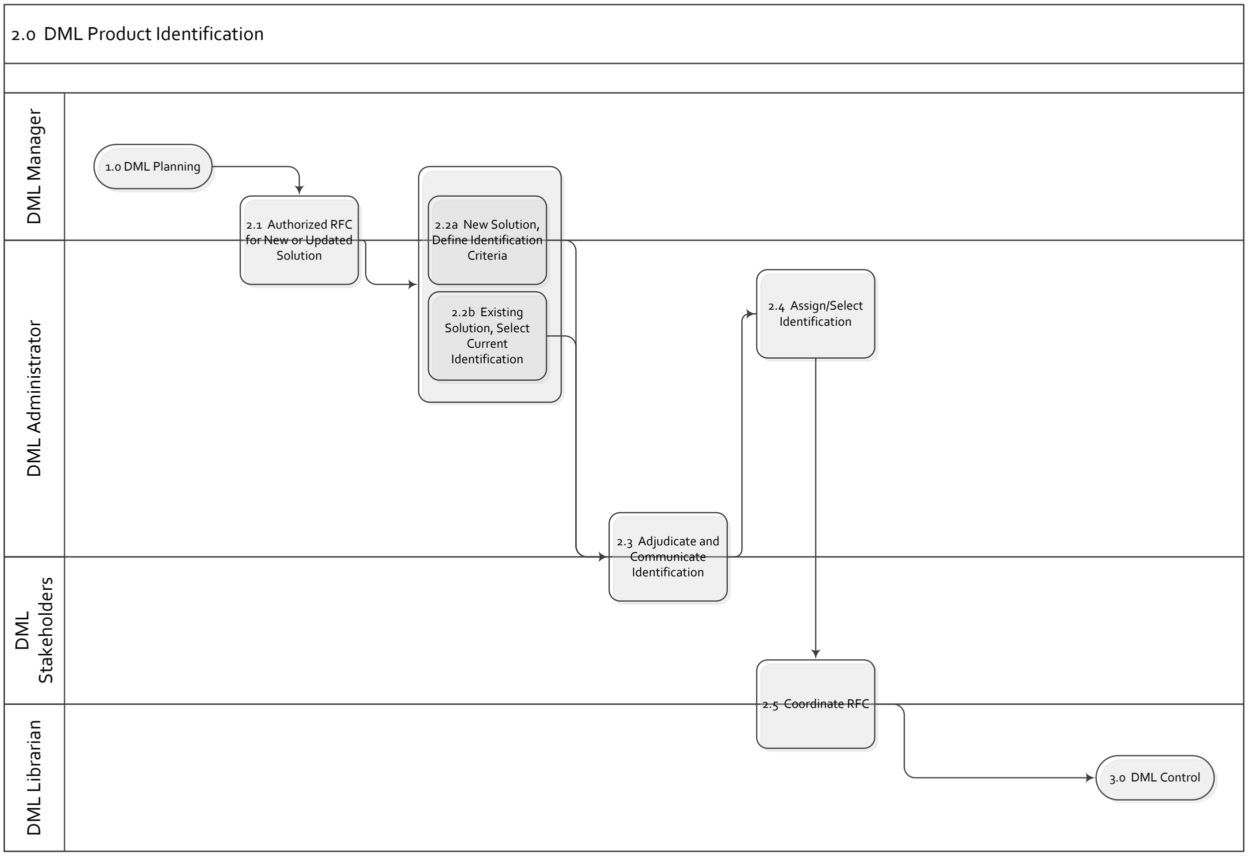

2.0 DML Product Identification
DML Manager
DML Administrator
DML Stakeholders
DML Librarian
1.0 DML Planning
2.1 Authorized RFC for New or Updated Solution
2.2a New Solution, Define Identification Criteria
2.2b Existing Solution, Select Current Identification
2.3 Adjudicate and Communicate Identification
2.4 Assign/Select Identification
2.5 Coordinate RFC
3.0 DML Control

Figure C-4-2. DML Product Identification Activity

Table C-4-2 describes the DML Product Identification activity steps as depicted in Figure C-4-2.

Table C-4-2. DML Product Identification Activity Descriptions

2.0 DML Product Identification		
Number	**Activity**	**Description**
2.1	Authorized RFC for New or Changed Solution	All changes are managed by the USMC Enterprise Change Management (ChM). Engineering (EEVE) submits a RFC for the proposed new solution or a change to an existing solution. Once Authorization is received from ChM, the change action may proceed. In this step, the DML Manager and the DML Librarian review the Authorized RFC to identify the existing solution and its components or prepare to create a new identification for a new solution. If New Solution, proceed to Step 2.2a. If Changed Solution, proceed to Step 2.2b.

2.0 DML Product Identification		
Number	**Activity**	**Description**
2.2a	New Solution Identification	When the proposed solution does not exist under DML control, a new identification convention is developed and applied. This may include controlled components with existing identifications that rollup to an eventual new solution bundle parent identification (CI). In this step, the DML Manager and DML Librarian collaborate with SACM as SACM creates a new solution identification. A New solution will also require a new Product Catalog entry, with pertinent solution data attributes populated such as Product Type, Product Name, Model/Version, and Origin. Proceed to Step 2.3
2.2.b	Changed Solution Identification	When the proposed solution exists under DML control and a change is proposed against its entirety or a component of the solution, the DML Librarian selects the current Product Catalog entry impacted. This will result in a next-version identification for this solution as well as any of its components that are changed. Proceed to Step 2.3
2.3	Adjudicate/Communicate Identification	Adjudicate solution modifications and the new or modified identification with the appropriate stakeholders, e.g. EEVE, and communicate identification to MITSCs, ChM, SACM, and RDM. Finalize RFC with ChM. Proceed to Step 2.4
2.4	Assign/Select Identification	When a new solution is identified for inclusion within the DML, a number of steps follow as applicable: • Creating specific naming conventions for the solution • Creating specific labeling conventions • Defining attributes for the solution • Defining lifecycle states for the solution and the transitions between states • Defining documentation for the solution • Defining relationships to other solution • Identification of solution Owners When an existing solution is identified from the DML, a similar number of steps will occur: • Creating specific next-version conventions for the solution • Creating specific next-version labeling conventions • Identifying current and newly identified attributes for the solution • Identifying current and new lifecycle states for the solution and the transitions between states • Defining next-version documentation for the solution • Identify current and new relationships to other solution Continue to Activity 3.0

4.3 DML Control

DML Control ensures that there are adequate control mechanisms over solution bundles and their CI components while maintaining a record of changes to CIs, versions, location, and ownership. The activity ensures that no solution or CI is added, modified, replaced, or removed without an appropriate controlling documentation or procedure being followed. Policies and procedures should be in place to cover the following features:

- Version control of software, documentation, solution builds, and releases,
- Access control between defined source and destination fileshares/drives,
- Establishing the solution baseline before supporting a release in a manner that can be used for subsequent evaluation against actual deployment, and
- Extraction and Insertion of electronic data and information, maintaining the integrity of the DML.

DML thus covers the activity of extracting, or “checking-out”, identified products (with direction from an Authorized RFC from a deployment POC) such as documents, templates, and source code from the DML Master Source Documents repository and/or DML Site & Applied Engineering repository based on an Authorized RFC from Change Management. These products are typically requested by Engineering to build a new or updated solution; however, MITSCs can also make requests for specific, site impacting (non-enterprise) products.

DML Control also includes the activity of inserting, or “checking-in” a developed/built solution (again, with direction from an Authorized RFC from the Engineering POC) into the DML Pre-Production repository based on, or aligned with, the original Authorized RFC from Change Management. These solutions are typically a package or bundle of solution source code, software, and documentation ready for test.

Once inserted, DML control involves the version control and solution/CI movement within the DML repositories, open communications between the DML staff and DML Stakeholders, and archiving actions.

Each installation or deployment should be authorized by a corresponding, approved production request for change (RFC) and the resulting RFC recorded in the CMDB as a relationship between the DML artifact and where it has been deployed.

The following workflow (Figure C-4-3) depicts the DML Control activity:

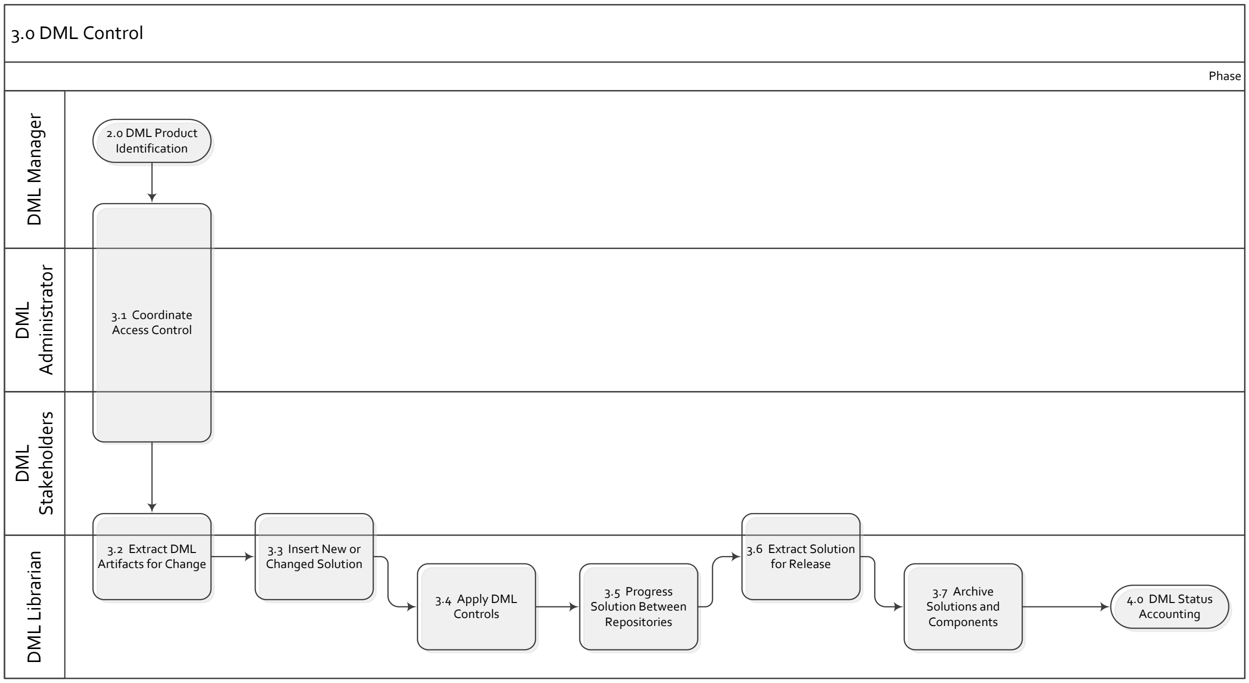

3.0 DML Control
Phase
DML Manager
DML Administrator
DML Stakeholders
DML Librarian
2.0 DML Product Identification
3.1 Coordinate Access Control
3.2 Extract DML Artifacts for Change
3.3 Insert New or Changed Solution
3.4 Apply DML Controls
3.5 Progress Solution Between Repositories
3.6 Extract Solution for Release
3.7 Archive Solutions and Components
4.0 DML Status Accounting

Figure C-4-3. DML Control Activity

Table C-4-3 describes the DML Control activity steps as depicted in Figure C-4-3.

Table C-4-3. DML Control Activity Descriptions

3.0 DML Control		
Number	**Activity**	**Description**
3.1	Coordinate Access Control	DML Manager coordinates access and permissions to the IP Share, Engineering fileshare/drive, and CMDB for use by the DML Librarian. This allows the DML Librarian to: • Provide RFC requested artifacts, • Position to the appropriate repository for change action, and • Provide CI record updates when required. Proceed to Step 3.2

3.0 DML Control		
Number	**Activity**	**Description**
3.2	Extract DML artifacts for change	For new solutions, from an Authorized RFC the DML Librarian extracts the requested/required DML artifacts such as: • Document templates (from Knowledge Management or the E&T technical editing team), and • Raw media (once software license is recorded and entered within the CMDB) and positions to the identified receiving repository for Engineering change action, and For existing solutions, either the project officer or the Lead Engineer will be identified as the requestor. Information required will include: • Requestor's Name • Functional IT Area • Name of Media • Version Number • Release Ticket Number • Request Date • Project Number • Organization • Priority (based upon the Release Ticket generated). If it is only a solution copy request, priority is Normal (1-2 Business Days), Low (3-5 Business Days). • Phone Number • Estimated Completion Date of Project (End Date within Release Management Record). This will be used if source documents, etc. are requested. • Delivery method (physical copy, soft copy—if soft copy is requested, need to define destination fileshare/drive if contents are too large to mail electronically) • Mailing address for physical copies which require shipment. • Number of copies required (if applicable). From an Authorized RFC the DML Librarian will extract: • Source documents, and • Existing and new media/software. The DML Librarian will then: • Update the Source Document Portal information, reflecting the artifact(s) in a checked out status, • verify the impacted items are related to the Release Record within the CMDB, Engineers may request to obtain copies of existing solutions as reference, but will not require a formal RFC for extraction. In the event only a copy of a solution is requested, the DML Librarian will verify receipt of the artifact(s) and close the request. No insert or re-insert action is required by the DML Librarian. Proceed to Step 3.3

3.0 DML Control		
Number	**Activity**	**Description**
3.3	Insert new or changed solution	Upon Engineering completion of change actions, the DML Librarian will: • Receive communication that the solution is ready to be inserted (checked-in) to the DML Pre-Production repository, • Coordinate with ChM to ensure the insert action is Authorized, • Coordinate with Engineering for accurate solution source fileshare/drive and file identification, • Perform the insert action from the Engineering repository to the DML Pre-Production repository, • Provide communication to DML Stakeholders of the insert action, to include solution new or next-version identification, date/time, and solution lifecycle state. Proceed to Step 3.4
3.4	Apply DML controls	With solutions and artifacts under DML Control, the DML Manager and DML Librarian will: • Control and update DML access control lists for accuracy and currency, • Control DML interfaces for security and integrity, • Control all solution and solution component requests via Authorized or Approved RFC relationships • Control all extract and insert actions via Authorized and Approved RFCs, • Review Release Records to contain relationships to the DML and other related solution components (CIs) impacted by the RFC, • Control artifacts received from an alternate source which are not delivered/shipped to ensure they are Authorized/Approved via the ChM Process, • Properly record regular and alternate source artifacts within the CMDB to follow extraction/check-out procedures, • Control new and next-version identification conventions for accuracy and currency, and • Control all solution logical moves between repositories. If the extract and delivery method required is a physical copy, the artifact(s) will be controlled via a download to a disk and provided to the requestor. • If a soft copy is requested, a copy of the artifact(s) will be controlled via extraction to the respective fileshare/drive defined by the requestor. The DML Librarian will monitor and control artifacts extracted based upon estimated completion date and follow up as necessary with requestor. Proceed to Step 3.5
3.5	Move solution between repositories	The activity of moving solutions, software, and documentation between DML repositories. This includes: • Approved RFC action to move a solution from DML Pre-Production repository to Certified DML repository, • Updated new and/or next-version secured (.PDF) documents into Master Documents, and archiving solutions. Proceed to Step 3.6

3.0 DML Control		
Number	**Activity**	**Description**
3.6	Extract solution for release	With an Approved RFC, the DML Librarian will: • Extract the identified Certified solution from the Certified DML repository, and • Insert to the identified Release & Deployment (RDM) destination fileshare/drive for RDM actions. No re-insert (check-in) is required as this is a copy which is retained in the Certified DML until notification of successful deployment. Upon successful notification, the DML Librarian performs Step 3.7 below. If/when ChM/RDM actions are deemed Emergency, a coordinated agreement between the DML Manager and RDM Owner will enable pre-approved RDM personnel access and permissions to extract the identified, Certified solution to the identified RDM destination fileshare/drive for RDM action. Proceed to Step 3.7
3.7	Archive solution and components	Once a Certified solution is deployed, and following a successful Post-Implementation Review, the DML Librarian will: • Receive communication from ChM/RDM that the PIR was successful, and • Archive the identified Certified solution bundle with its version identification. Continue to Activity 4.0

4.4 DML Status Accounting

DML Status Accounting is the bookkeeping activity of each DML solution entering or exiting DML control. DML Status Accounting is the activity of creating and organizing the knowledge base necessary for the performance reporting of the DML. In addition to facilitating control, the purpose of DML Status Accounting is to provide a highly reliable source of solution information to support all DML activities including systems engineering, software development and maintenance, logistic support, modification, and maintenance.

This activity involves tracking:

- What is requested for formal change or informal reference copy,
- What solution baselines are affected,
- What solution interfaces are occurring and active for the subject change,
- What is Authorized to be inserted (checked-in) to the DML,
- What Control activities occur within the DML,
- What solutions are Approved for RDM Action, and
- Audit findings

DML Status Accounting receives information from the other DML activities and related activities as the functions are performed. In addition to the use of automated DML management tools, the activity is aided or facilitated by documented DML operations and open communications. The outputs from this activity provide visibility into DML activity status and solution lifecycle information concerning the solution and its documentation.

The following workflow (Figure C-4-4) depicts the DML Status Accounting activity:

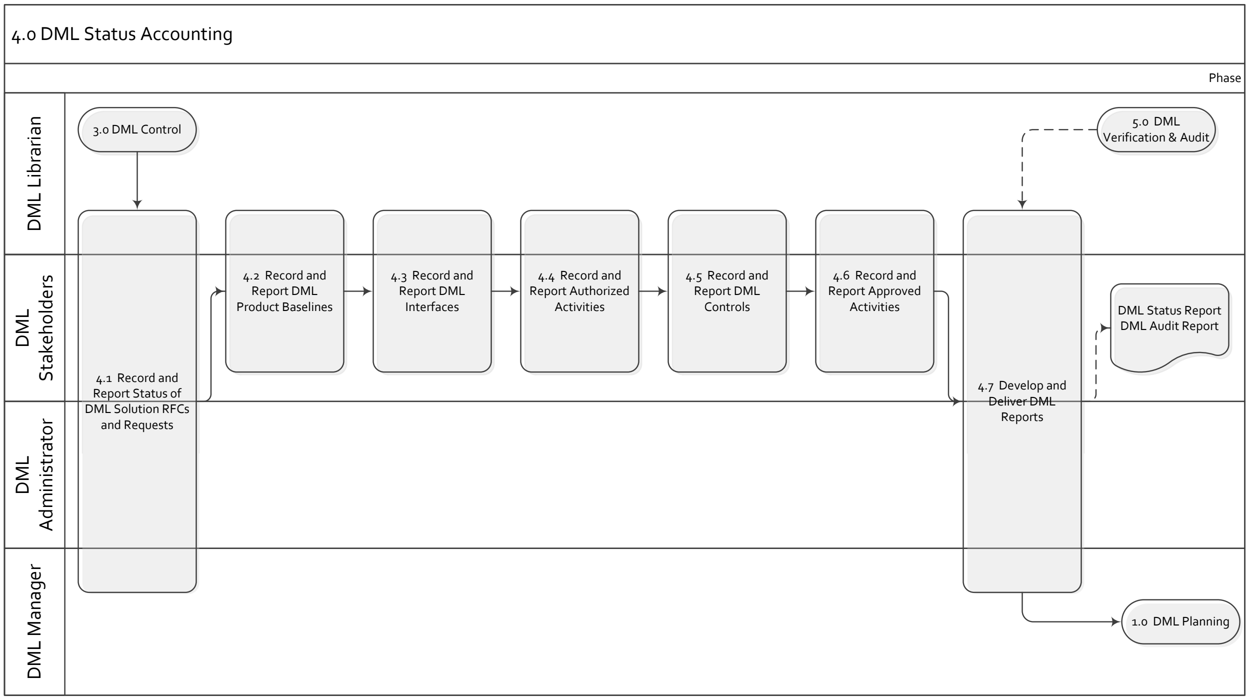

4.0 DML Status Accounting
Phase
DML Librarian
DML Stakeholders
DML Administrator
DML Manager
3.0 DML Control
5.0 DML Verification & Audit
4.1 Record and Report Status of DML Solution RFCs and Requests
4.2 Record and Report DML Product Baselines
4.3 Record and Report DML Interfaces
4.4 Record and Report Authorized Activities
4.5 Record and Report DML Controls
4.6 Record and Report Approved Activities
4.7 Develop and Deliver DML Reports
DML Status Report
DML Audit Report
1.0 DML Planning

Figure C-4-4. DML Status Accounting Activity

Table C-4-4 describes the DML Status Accounting activity steps as depicted in Figure C-4-4.

Table C-4-4. DML Status Accounting Activity Descriptions

4.0 DML Status Accounting		
Number	**Activity**	**Description**
4.1	Record and Report Status of DML Solution RFCs and Requests	Formal RFCs for New or Changes to solution bundles, and informal requests for solution copies and/or Source Documents as reference are recorded and tabulated for the given reporting period and built into the Status Report. This metric provides time-boxed data on Change activity per solution, document, and the DML in its entirety. Report data elements include and not limited to: • Requestor's Name • Organization • Mailing address • Request Date • Name of Documentation/Media • Name of Solution • Version Number • Release and/or RFC Record Number Proceed to Step 4.2
4.2	Record and Report DML Product Baselines	Product baselines are identified, monitored, and retrieved to record and report its comparison to a particular configuration, another baseline, and/or controlled CI components of the solution bundle. As a baseline is established at a fixed point in time (Certification), the retrieval is with regard to that point (identification of state). Report data elements include and not limited to: • The configuration of each Approved Certified solution bundle as it becomes operational, • The current Approved Source documentation and ID number associated with each solution bundle and/or associated CI, • Baseline change action, • Baseline Certification Approvals, • CIs bundled in Baselines, and • Comparison to another baseline (if applicable). Proceed to Step 4.3
4.3	Record and Report DML Interfaces	Physical, logical, and human interfaces are recorded and reported to support DML controls and integrity. • Physical interfaces include the physical storage cabinets • Logical interfaces include the IP Share, DML fileshares/drives, CMDB, and delivery destination fileshares/drives • Human interfaces include ChM, Engineering, SACM, DML, and RDM personnel interacting with the DML. Proceed to Step 4.4

4.0 DML Status Accounting		
Number	**Activity**	**Description**
4.4	Record and Report Authorized Activities	Specifically aligned with RFCs Authorizing the extraction of DML products to Engineering. This activity maintains the history and identification of DML product and workload. This includes and is not limited to: • Authorized Extractions, • Specific solution identifications, • RFC number, • Delivery Date/Time, • Engineering Contact, and • Destination fileshare/drive Notifications (email) to DML Stakeholders are included in this activity to set expectations of downstream activities and align with the DML Schedule. Authorized RFCs are those that allow the change action to occur in preparation of Validate & Test activities. Authorized RFCs do not establish the solution as ready for release. Proceed to Step 4.5
4.5	Record and Report DML Controls	Aligned with Authorization to release materials out of the DML for change or development actions, this activity records and reports the formal controls performed by the DML Librarian. This includes and is not limited to: • Authorized DML Insertion activities, • Archiving activities, • Specific solution bundle identifications, and • Date/Time of above activities. Notifications (email) to DML Stakeholders are included in this activity to set expectations of all activities and align with the DML Schedule. Proceed to Step 4.6
4.6	Record and Report Approved Activities	As an output from DML Controls, this activity records and reports all of the activities for solutions Approved for insertion into the DML Certified repository and hence ready for RDM action. This includes and is not limited to: • Approved Progression activities (Approved RFC movement from DML Pre-Production repository to DML Certified repository), • Specific solution identifications, • RFC number, • Release Record number, • Date/Time positioned into DML Certified repository, • RDM Contact, • Date/Time of extraction to RDM identified destination fileshare/drive, and • Confirmation of successful Post-Implementation Review (PIR) from ChM/RDM before Archiving. Notifications (email) to DML Stakeholders are included in this activity to set expectations of all activities and align with the DML Schedule. Provide recorded data as output to Step 4.7. Proceed to Step 4.7

4.0 DML Status Accounting		
Number	**Activity**	**Description**
4.7	Develop and Deliver DML Reports	As a result of DML Status Accounting recording (Inputs from Step 4.6), and DML Verification & Audit activities (Inputs from Step 5.4), the DML Librarian develops DML Status Reports and DML Audit Reports for delivery to DML Stakeholders. The DML Manager takes the Status and/or Audit data and develops report information pertinent to Stakeholder requirements and the DML. Notifications (email) to DML Stakeholders are included in this activity to set expectations of all activities and align with the DML Schedule. Report results are provided to DML Planning (Output to Activity 1.0, Step 1.1) for Action Planning. Continue to Activity 5.0

4.5 DML Verification & Audit

DML Verification & Audit is a series of reviews to verify the presence and configuration of certified solutions and their component CIs with their respective records within the CMDB and IP Share.

The DML Verification and Audit activity ensures that change and release records have been properly authorized by Change Management and that implemented/deployed changes are as Approved. Before a major release or change, DML Verification & Audit performs an audit of the specific solution to ensure it has the correct CMDB CI record data.

Included in the DML Verification & Audit activity is the:

- Verification of the initial configuration of a Certified solution CI,
- Verification of the solution bundle CI components,
- Verification of the incorporated Approved RFCs,
- Verification of the assurance the Certified solution meets its required performance,
- Verification of the documented requirements,
- Audit of verification records,
- Audit of physical product,
- Validation a Certified solution has achieved its performance requirements, and
- Validation a Certified solution meets its documentation.

The common objective is to establish a high level of confidence in the solution documentation used as the basis for DML control and support of the solution bundle throughout its life cycle.

Successful completion of verification and audit activities results in a verified solution/CI(s) and a documentation set that may be confidently considered a Product Baseline. It also results in a validated activity to maintain the continuing consistency of solution to documentation.

The following workflow (Figure C-4-5) depicts the DML Verification & Audit activity:

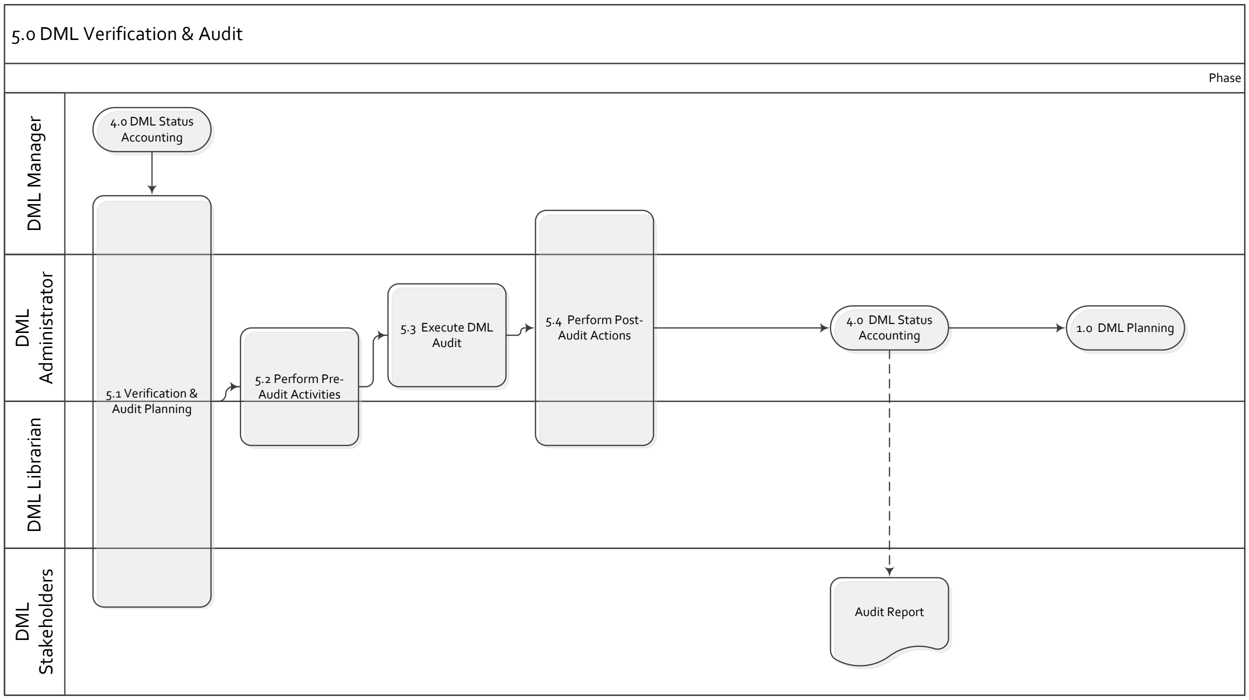

5.0 DML Verification & Audit
Phase
DML Manager
DML Administrator
DML Librarian
DML Stakeholders
4.0 DML Status Accounting
5.1 Verification & Audit Planning
5.2 Perform Pre-Audit Activities
5.3 Execute DML Audit
5.4 Perform Post-Audit Actions
4.0 DML Status Accounting
1.0 DML Planning
Audit Report

Figure C-4-5. DML Verification & Audit Activity

Table C-4-5 describes the DML Verification & Audit activity steps as depicted in Figure C-4-5.

Table C-4-5. DML Verification & Audit Activity Descriptions

5.0 DML Verification & Audit		
Number	**Activity**	**Description**
5.1	Verification & Audit Planning	Verification & Audit Planning involves four major activities: • Developing the Audit Plan for Stakeholder approval of audit scope, date/time, and resources, • Verifying the references used as the basis for the audit, such as the CMDB and DML repositories, are relevant and acceptable, and • Establishing a baseline reference point for the audit by assessing the current situation. Proceed to Step 5.2

5.0 DML Verification & Audit		
Number	**Activity**	**Description**
5.2	Perform Pre-Audit Activities	The activity of verifying the materials and resources are available and ready for the audit. Using the CMDB and DML repositories, data is obtained for the point-in-time of the audit. Physical print-outs and/or direct system access is used to verify the solutions, solution component CIs, and documentation are resident for review. Audit elements are verified with the Audit team with regards to: • Approved Schedule, • Approved Agenda, • Physical and Logical Audit aspects, • Approved Audit items (logical Certified solutions, logical solution CIs, electronic/physical documentation, physical media), • Facilities/Location of Audit (Physical vault, logical DML repositories, logical CMDB, logical IP Share), • Audit Rules of Conduct, and • Audit participants. Proceed to Step 5.3
5.3	Execute DML Audit	Activity of actual audit and comparison of the reference logical system records (CMDB) and/or baseline logical IP Share or physical documentation against the DML Certified solutions and component CIs. This includes Audit of the physical media controlled in the physical DML as well. The Audit follows the pre-Approved Audit Schedule to maintain consistency of time, resource management, and a defined and approved audit scope (items audited, if not all inclusive). The Audit Findings (discrepancies) are recorded and built into a final Audit Findings Report. Exceptions noted are documented. When determined the exceptions were due to activity violations, a risk impact analysis of the exceptions is included. Proceed to Step 5.4
5.4	Perform Post-Audit Actions	Activity in which diligent follow-up of the audit action items takes place. The Post-Audit activity consists of: • Recording the Audit Findings data, • Development of the POA&M for reconciliation between managed and discovered discrepancies, • Development of Recommendations, • Preparation of RFCs if updates to the CMDB are required, • Schedule for next or follow-up Audit, • Scheduling initiatives to remedy solutions/CIs with a significant level of risk of compliance related importance, and • Providing the above elements to DML Status Accounting (Output to Step 4.7) for DML Audit Reporting. Any updates to the CMDB should be performed through RFC submission to Change Management.

Appendix D – REFERENCES

In meeting and achieving this process guidance, the following directives and documentation should be referenced to ensure compliance and support for the implementation of the SACM process.

- ITIL® Service Strategy, Office of Government Commerce, TSO: 2011
- ITIL® Service Design, Office of Government Commerce, TSO: 2011
- ITIL® Service Transition, Office of Government Commerce, TSO: 2011
- ITIL® Service Operations, Office of Government Commerce, TSO: 2011
- ITIL® Continual Service Improvement, Office of Government Commerce, TSO: 2011
- Enterprise IT Service Management Change Management Process Guide
- D400.11939.01, NMCI Naming Standards
- MCO 5271.1C, Information Resource Management (IRM Standards and Guidelines Program)
- Federal Acquisition Regulations (FAR)
- Defense Federal Acquisition Regulation Supplement (DFARS)