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

IN REPLY REFER TO:
2300/06A
CP

DEC 4 2013

From: Commandant of the Marine Corps

Subj: ENTERPRISE INFORMATION TECHNOLOGY SERVICE MANAGEMENT CONFIGURATION MANAGEMENT PROCESS GUIDE

Ref: (a) MCO 5271.1B

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

1. PURPOSE. The purpose of the Enterprise Information Technology Service Management (ITSM) Configuration Management Process Guide is to establish a documented and clear foundation for process implementation and execution across the Marine Corps Information Environment (MCIE). 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. 2300-06.

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: PCN 18623000600

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

Enterprise IT Service Management Configuration Management Process Guide

Release Date:
05 April 2013

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

Table of Contents

List of Tables

Table	Title	Page

List of Figures

Figure	Title	Page

Enterprise IT Service Management
Configuration Management Process Guide

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 Information Environment (MCIE). 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.

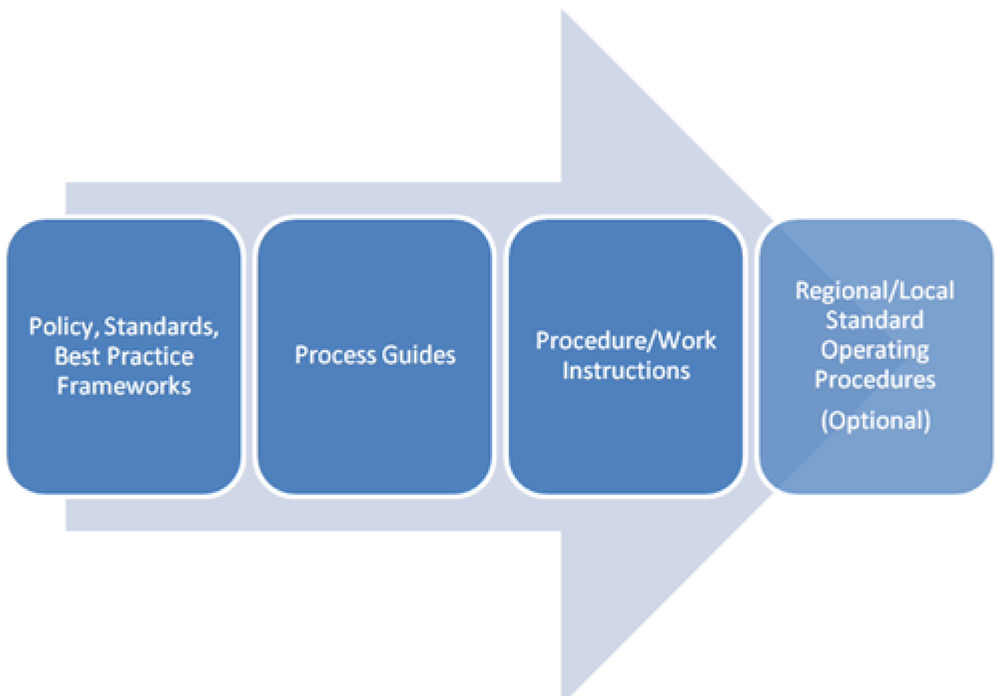


Figure 1. Process Document Continuum

1.2 Scope

The scope of this document covers all services provided in support of the MCIE 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 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. 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 5271.1C Information Resource Management (IRM) Standards and Guidelines Program.

2.0 PROCESS OVERVIEW

2.1 Purpose, Goals, and Objectives

The purpose of Configuration Management (CfM) is to ensure that the Configuration Items (CIs) required to deliver services are properly controlled, and that accurate and reliable information about those CIs is available when and where it is needed. This information includes details of how the CIs have been configured and the relationship between CIs.

The goal of CfM is to provide accurate information to ensure CI integrity and CI lifecycle management:

- Provide configuration management information to other ITSM processes to assist decision making.
- Minimize the number of quality and compliance issues caused by incorrect or inaccurate configurations.
- Define and control of components and infrastructure to maintain accurate information on planned and current state CIs.

The primary objectives of CfM are to:

- Ensure that CIs under the control of the IT organization are identified, controlled, and properly cared for throughout their lifecycle.
- Identify, control, record, report, audit, and verify services and other CIs, including version, baselines, and constituent components, their attributes, and relationships.
- Account for, manage, and protect the integrity of CIs through the service lifecycle by working with change management to ensure that only authorized components are used and only authorized changes are made.
- Ensure the integrity of CIs and configurations required to control the service by establishing and maintaining an accurate and complete Configuration Management System (CMS).
- Maintain accurate configuration information on the historical, planned, and current state of services and other CIs.
- Support efficient and effective service management processes by providing accurate configuration information to enable USMC to make decisions at the right time (e.g., authorize changes and releases).

This document does not cover USMC fixed asset accounting.

2.2 Relationships with Other Processes

IT Service Management processes are interrelated. The processes in Figure 2 are shown because of the strength of the relationships and dependencies between them. As the single repository of configuration data and information for IT service management, CfM supports, and interfaces with every other service management process and activity to some degree. Figure 2 depicts key relationships that exist between CfM and other processes. This figure is not all-encompassing and the relationships shown can be direct or indirect.

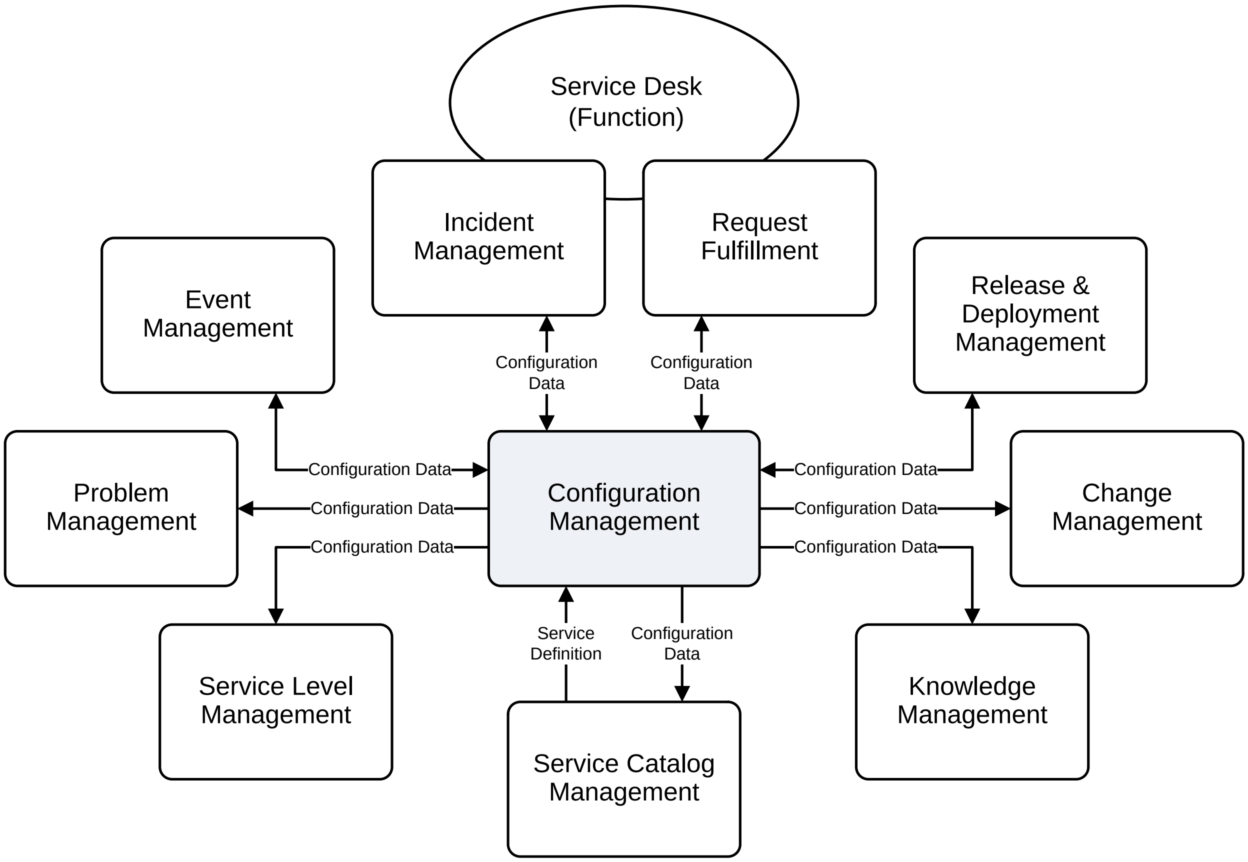


Figure 2. CfM Relationships with other Processes

The following list contains descriptions of the CfM relationships (inputs or outputs) depicted in Figure 2.

Problem Management

— Configuration Data: Configuration data, present in the Configuration Management Database (CMDB), provides baseline information required to implement workarounds and to fix known errors.

Knowledge Management

— Configuration Data: Configuration data, present in the Configuration Management System (CMS), enables effective decision support and reduces the risks that arise from the lack of proper control of data.

Service Level Management

- Configuration Data: Configuration data, present in the CMDB, enables measured and reported achievement against one or more service level targets in the form of operational level agreements, underpinning contracts, and service level agreements.

Service Catalog Management

- 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 CfM and Service Catalog Management is required to ensure dependencies are effectively managed and service definitions stay in synch.

- Technical Service Content: The Technical Service Catalog is produced by Service Catalog Management directly from CMDB contents. This artifact details the technical or functional components that underpin IT services. As such, it exists as a report or as a filtered view of the CMDB.

Release and Deployment Management

- Planning Content: The CMS and supporting processes provide invaluable information for the purposes of planning, preparing, and designing 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.

Incident Management

- Configuration Data: Configuration data, present in the Configuration Management Database (CMDB), provides information to the Service Desk and the Incident Management process for the purposes of troubleshooting, diagnosis, and resolution of incidents. By knowing 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 disposition of CIs and associated services, systems, and applications.

Event Management

- Configuration Data: Configuration data, present in the CMDB, provides target and scope information necessary to architect and engineer service monitoring as well as establish correlation rules to help minimize redundant alerts.

Request Fulfillment

- Configuration Data: Configuration data, present in the CMDB, 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 ChM standard change process during the closure of a service request (record updates).

Change Management

- 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, CI data and history is updated both by Change Management (ChM) to CfM and vice versa. Configuration Management 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 CfM, keeping the CMDB current.

2.3 High-Level Process Model

The CfM process activities consist of five distinct sub-processes (i.e., (1) Management and Planning, (2) Configuration Identification, (3) Configuration Control, (4) Status Accounting and Reporting, and (5) Verification and Audit). The following activity model illustrated in Figure 3 is often used in environments, such as the USMC, where there are many partners and/or vendors:

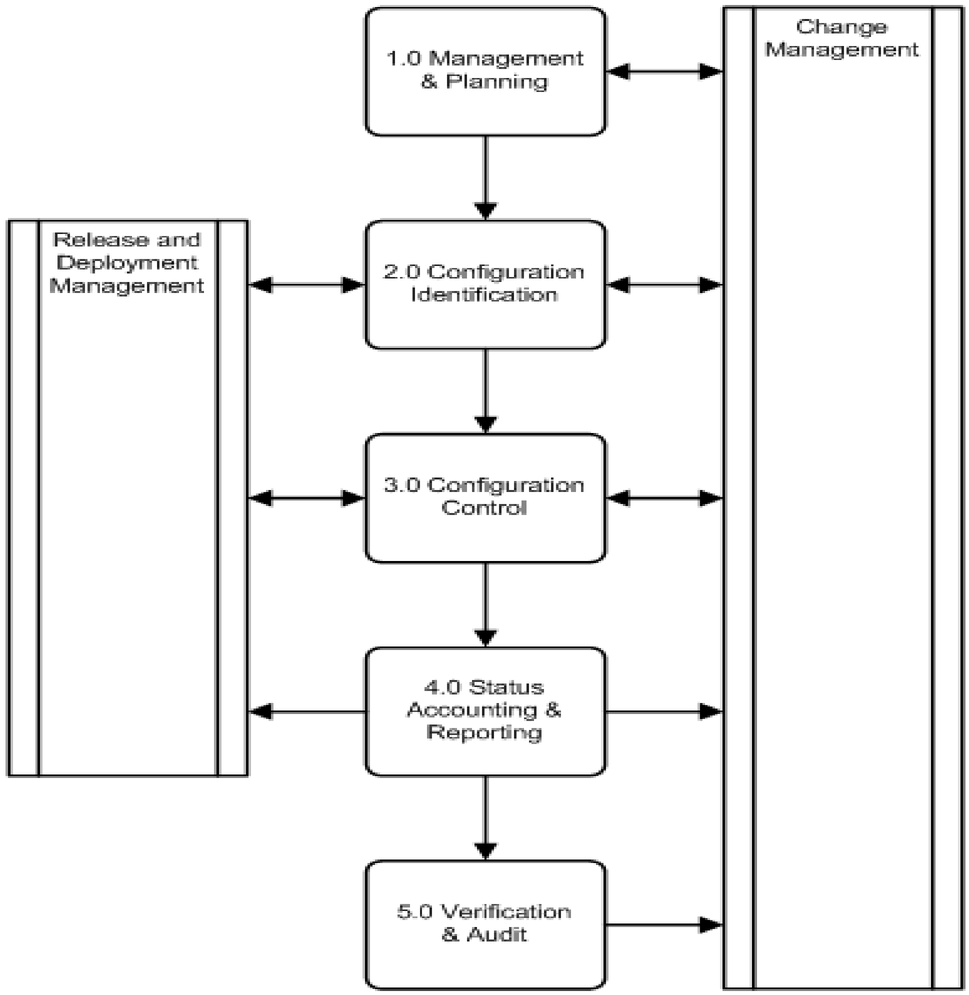


Figure 3. High-Level CfM Process Model

Table 2 contains descriptions of each sub-process. Each sub-process number is hyperlinked to its detailed description in Section 4.0, Sub-Processes.

Table 2. CfM Sub-Process Descriptions

Number	Sub-Process	Description
1.0	Management and Planning	Is the initial activity within the CfM 5 sub-processes. The activity sets the objectives and critical success factors to be achieved after delivery of the change, as well as specifying the organizational context and purpose (e.g., scope, requirements, applicable policies/standards,

Number	Sub-Process	Description
		organization, systems, tools, and interfaces with other processes and/or groups). The primary output of CfM management planning is the Configuration Management Plan (CMP), which specifies how configuration management will be implemented to include policies and procedures for a particular acquisition or program.
2.0	Configuration Identification	Defines how the classes and types of services assets and CIs are to be selected, grouped, classified, and defined including the appropriate characteristics (e.g., warranties for a service) to ensure they are manageable and traceable throughout their lifecycle. Define the roles and responsibility of the owner for a configuration item (CI) type at each stage of its lifecycle. CIs include hardware, software, services and documentation components of (and supporting) the USMC infrastructure. A key consideration of Configuration Identification is uniquely naming and labeling all CIs or service components of interest across the service and the relationship between them. Define and document criteria for selecting configuration items and the components that compose them. Policy dictates much of the framework for determining which CIs are developed and maintained (e.g., tracking Defense Information Systems Agency (DISA), Security Technical Implementation Guide (STIG), Certification & Accreditation (C&A), etc.). Select the configuration items and their components according to documented criteria. Assign unique identifier and specify the relevant attributes to configuration items. Specify when each configuration item is placed under control of configuration management. Identify the owner responsible for each configuration item.
3.0	Configuration Control	Ensure that there are adequate control mechanisms over CIs while maintaining a record of changes to CIs, versions, location and ownership. 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 features: (1) license control, (2) change management, (3) version control of software, hardware, image builds, and releases, (4) access control to facilities, storage areas, and CMS, (5) build control using CMS specifications, (6) promotion, migration of electronic data and information, (7) Establishing configuration baseline of CIs before performing a release in a manner that can be used for subsequent evaluation against actual deployment, (8) deployment and installation control, and (9) Maintaining the integrity of the definitive media library (DML).
4.0	Status Accounting and Reporting	Ensures that each CI will have one or more discrete states to progress through. Define the significance of each state. The following discrete states establish the a minimum lifecycle: (1) development or drat denoting that the CI is under development, (2) approved meaning that the CI may be used, and (3) withdrawn meaning that the CI has been taken/decommissioned from use. Define the method by which CIs move from one state to another. Typical activities include: (1) maintaining configuration records through the service lifecycle, (2) managing the recording, retrieval and consolidation of the current configuration status and the status of all preceding configuration to confirm information correctness, (3) making the status of items under CfM available throughout the lifecycle, (4) recording changes to the CIs from receipt to disposal, and (5) ensuring that changes to configuration baselines are properly documented.

Number	Sub-Process	Description
5.0	Verification and Audit	Ensure that change and release records have been properly authorized by change management and that implemented changes are as authorized. Ensure that before a major release or change, an audit of the specific configuration of the USMC's environment matches the CMS. The following activities include a series of reviews or audits: (1) ensure that there is conformity between the documented baselines and the actual USMC environment, (2) verify the physical existence of CIs in the organization or in the DML, (3) verify functional and operational characteristics of CIs and to check that the records in the CMS match the physical infrastructure, and (4) check that the release and configuration documentation is present before making the a release.

2.3.1 Process Description

CfM involves identifying the configuration of all items that make up a service or IT system such as software, hardware components, configuration data, and documentation, at a given starting point in time. Once CI relationships are defined, it proceeds with the systematic control of configuration changes and maintains the integrity and traceability of the configuration baseline throughout the lifecycle. CIs managed within the scope of CfM will follow asset and property management requirements as defined in Federal Acquisition Regulations (FAR), Defense Federal Acquisition Regulation Supplement (DFARS), DoD, DoN and USMC Directives.

This document does not cover USMC fixed asset accounting. For the purposes of this document, property and asset management are out of scope.

The scope of CfM includes all the hardware, software, licenses, warranties, business applications, business services, attributes, relationships, and documentation for IT services as defined in the IT Service Catalog. This data is identified, collected, verified, and stored in a Configuration Management System (CMS).

This process guide will assist personnel executing roles and activities within the CfM process. The process guide will be of interest to any individuals with a need to understand how the CfM process works within their IT organization.

2.4 Key Concepts

The following key concepts describe concepts unique to CfM:

2.4.1 Attribute

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

2.4.2 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.

2.4.3 Baseline

The baseline is a configuration that has been formally agreed and is managed through the change management process. A configuration baseline is used as a basis for future builds, releases, and changes. 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 procedures.

2.4.4 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.

2.4.5 Configuration Item

A configuration item (CI) is a service component that needs to be managed in order to deliver an IT service. 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. Also CIs may be grouped and managed together.

2.4.6 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 CIs to include relationships with other CIs.

2.4.7 Configuration Management Plan

The Configuration Management Plan (CMP) is a document defining how configuration management will be implemented (including policies and procedures) for a particular acquisition or program. (Source: MIL-HDBK061A)

2.4.8 Configuration Management System

The Configuration Management System (CMS) holds all the information for CIs within the designated scope. The CMS may consist of multiple CMDBs and interrelated systems. A set of tools, data, and information are used to support CfM. The CMS is part of an overall service knowledge management system and includes tools for collecting, storing, managing, updating, analyzing and presenting data about all configuration items and their relationships.

2.4.9 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.

2.4.10 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 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.

2.4.11 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.

2.4.12 Naming

Naming conventions should be 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.

2.4.13 Relationships

Relationships describe how the CIs work together to deliver the services. These relationships are held in the CMDB. The relationships between CIs are maintained so as to provide dependency information (e.g., CI is a part of another CI, CI is connected to another CI, CI uses another CI, and CI is installed on another).

2.4.14 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).

2.4.15 Verification

Verification, as in Configuration Verification, is a process that is common to configuration management, 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.

2.5 Continual Service 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.

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

2.5.1 Critical Success Factors with Key Performance Indicators

As with all processes, the performance of CfM should be monitored, reported on, and action taken to improve it. CfM is the central support process facilitating the exchange of information with other processes. However, CfM must be measured for its contribution to these other processes within the lifecycle and the overall KPIs that directly affect the USMC.

CSFs are defined as process-specific or service-specific goals that must be achieved if a process (or IT service) is to succeed. KPIs are the metrics used to measure service performance or progress toward stated goals.

The following CSFs and KPIs can be used to judge the efficiency and effectiveness of the process. 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.   Table 3 describes the metrics to be monitored, measured, and analyzed.

Table 3. CfM 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 CIs throughout the service lifecycle	1	Improved accuracy in budgets and charges for the assets utilized by each USMC organizations	Attracting and justifying funding for CfM 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 CfM
		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 CfM 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 CfM 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
		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

3.0 ROLES AND REPONSIBILITIES

Each 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. Process Managers report process deviations and recommended corrective action to the respective Process Owner. Authoritative process guide control is under the purview of the Process Owner.

Management (i.e., responsibility) of a process may be shared; generally, a single manager exists at the MCNOSC enterprise and at each MITSC. While the end goal is to have a single CfM Process Owner residing at the Enterprise Level, the USMC will initially use a shared process ownership framework. There will be a CfM Process Owner for the acquisition sector inclusive of all USMC IT Programs of Record (POR), as well as a CfM Process Owner for the Operational sector inclusive of all other USMC organizations at the enterprise, regional, and local levels. Multiple Configuration Managers exist at the regional (e.g., MITSC or RNOSC) and local levels. For certain processes, especially those within Service Design and Service Transition, managers also exist within MCSC and PORs. Some Service Operation processes (e.g., Event Management) will require managers at the RNOSC. There will be instances where roles are combined or a person is responsible for multiple roles. Factors such as AOR, size of user base, and size of the process support team dictate exactly which roles require a dedicated person(s) and the total number of persons performing each role. This process guide defines all *mandatory* roles.

3.1.1 Roles

The following abstract drawing (Figure 4) depicts process roles for the USMC, followed by a description of these roles (Table 4).

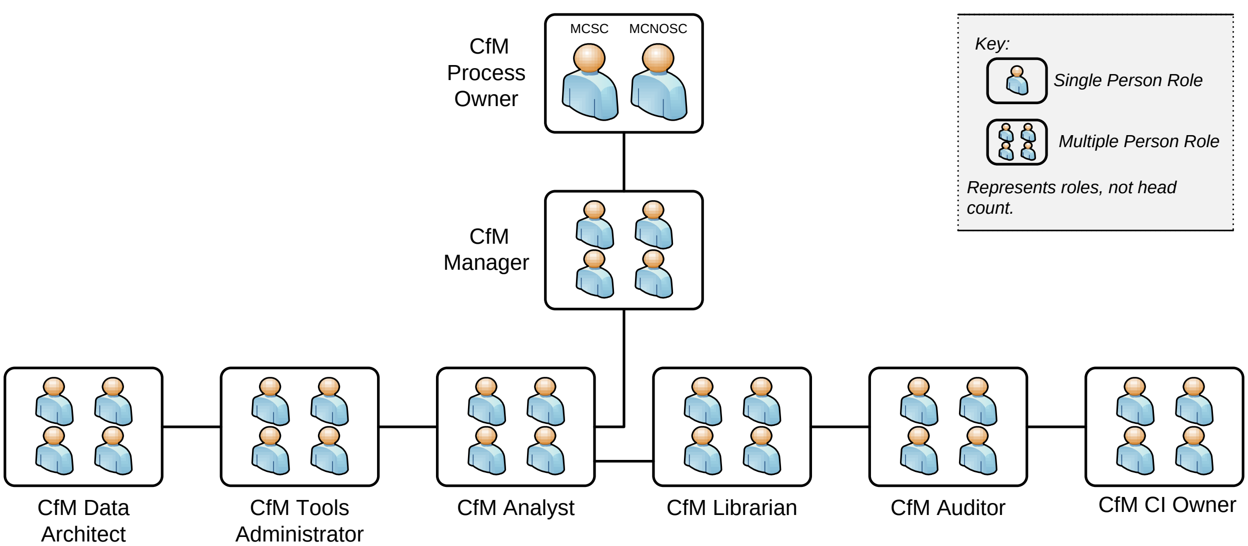


Figure 4. CfM Roles

Table 4. CfM Defined Roles and Responsibilities

Description	Overall Responsibility
Role #1 CfM 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. To these ends, 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 CfM process	• Ensures the Configuration Management process and working practices are effective and efficient • Ensures all stakeholders are sufficiently involved in the Configuration Management process • Decision maker on any proposed enhancements to the process • Ensures tight linkage between Configuration Management processes and other related processes • Adjudicates when new CI types are requested by CfM Managers
Role #2 CfM Manager	
The Configuration Manager is responsible for developing and implementing the specific CfM plans and processes for the infrastructure. The CfM Manager is the direct interface for CfM 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 Configuration Management Data Base (CMDB) data. There is a CfM Manager for each level of the environment.	• The overall point person responsible for all CfM activities and planning within the scope of the environment level for which responsibilities are defined • Ensures the CMDB is accurate and directly interfaces with Change Management to ensure the process is followed for CI changes • Defines reports to support the CfM process with respect to Status Accounting and Verification & Audit activities • Determines the need for new CI types when the situation arises and confers with the CfM Process Owner to gain concurrence
Role #3 CfM Analyst	
The CfM Analyst trains Asset and Configuration Management specialists and other staff in Asset and Configuration Management principles, processes, and procedures.	• Supports the creation of the Asset and Configuration Management processes and procedures to include CI registration procedures, access controls, and privileges • Ensures the correct roles and responsibilities are defined in the CfM plan/procedures • Proposes/concurs with the CfM 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 CfM 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

Description	Overall Responsibility
	• Builds system baselines for promotion and release • Maintains project status information and status accounting records and reports • Assists CfM Manager in report definition when necessary • Supports Change Owners in Configuration Identification process and in support of Configuration Control activities
Role #4 CfM Data Architect	
The CfM Data Architect is primarily responsible for Configuration Identification. The CfM Data Architect consults regularly with the CfM Configuration Analyst and the CfM Librarian during the CfM 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 CfM (including requests for changes, deviations from specifications, etc.) and ensures that relevant technical strategies, policies, standards and practices are applied correctly
Role #5 CfM Librarian	
The CfM Librarian is the custodian and guardian of all master copies of software, assets and documentation CIs registered within CfM.	• Control the receipt, identification, storage, and withdrawal of all support CIs • Provide information on the status of CIs • Number, record, store, and distribute Asset and Configuration Management issues • Assist CfM Analyst in Configuration Identification activities
Role #6 CfM Configuration Auditor	
The CfM Configuration Auditor is responsible for planning and executing audits of configuration data and validating CMS/CMDB accuracy. The CfM Configuration Auditor is responsible for assessing and analyzing requests for verification and audits. The CfM Configuration Auditor consults regularly with the CfM Configuration Analyst and occasionally with the CfM Librarian, and the CI Owner when performing CfM verifications and audits.	• Assesses and analyzes requests for CfM 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

Description	Overall Responsibility
	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
Role #7 CfM CI Owner	
The CfM CI Owner is responsible to all stakeholders for the CIs to which it's assigned. A CI Owner is designated by the CfM Manager to manage one or more classes of CIs and assist the CfM 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.	• Works with configuration items (CIs) assigned to maintain • Updates and deletes assigned CIs • Registers new CIs upon approval • Transfers ownership of a CI • Generates and view reports of the CIs assigned • Under the direction of the CfM 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
Role #8 CfM Tools Administrator	
The CfM 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 Asset and Configuration Management environments in terms of databases and software libraries, workflows, and report generation.	• Monitors the performance and capacity of existing Asset and Configuration Management systems • Recommends improvement opportunities • Undertakes standard housekeeping and fine tuning within the Change Control process • Supports requests for tool changes necessitated from Reporting and Audit / Reconciliation efforts

3.1.2 Responsibilities

Processes may span organizational boundaries; therefore, procedures and work instructions within the process need to be mapped to roles within the process. These roles are then mapped to job functions, IT staff, and departments. The process owner is accountable for ensuring process interaction by implementing systems that allow smooth process 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 5 displays the organizational-level RASCI model for CfM. Table 6 displays the RASCI model for CfM by process roles.

- **R**esponsible – Completes the process or activity; responsible for action/implementation. The degree of responsibility is determined by the individual with the 'A'.
- **A**ccountable – Approves or disapproves the process or activity. Individual who is ultimately answerable for the task or a decision regarding the task.
- **C**onsulted – Gives needed input about the process or 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 process or 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 a one-way communication.

Table 5 establishes responsibilities for high-level process activities by organization. Table 6 shows process responsibilities by role.

Table 5. Responsibilities for Enterprise CfMCfM Sub-Process	**MCNOSC**	**HQMC (C4)**	**MCSC**	**MCCDC**	**RNOSC**	**MITSC**	**Application or Service Owner**	**Tenant/Supported Command**
Management and Planning	AR	I	AR	C		C	C	S
Configuration Identification	AR	I	AR	C		S	C	S
Configuration Control	AR	I	AR	C		S	S	S
Status Accounting and Reporting	AR	I	AR	C	I	S	S	S
Verification and Audit	AR	I	AR	C	I	S	C	S

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

Note: Any organization 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: More than one organization can be accountable for each sub-process due to the shared process ownership.

Table 6. Process Responsibilities by Role

CfM Sub-Process	Process Owner	Process Manager	Configuration Analyst	Data Architect	Librarian	Configuration Auditor	CI Owner	Tools Administrator
Management and Planning	AR	R	S	S	S	S	C	C
Configuration Identification	A	R	S	R	S	C	C	S
Configuration Control	A	R	R	C	S		S	
Status Accounting and Reporting	A	R	R	S	S		S	C
Verification and Audit	A	R	S	S	C	R	C	S

Legend:

Responsible (R) – Completes the process or activity

Accountable (A) – Authority to approve or disapprove the process or activity

Support (S) – Assists in execution of process or 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.

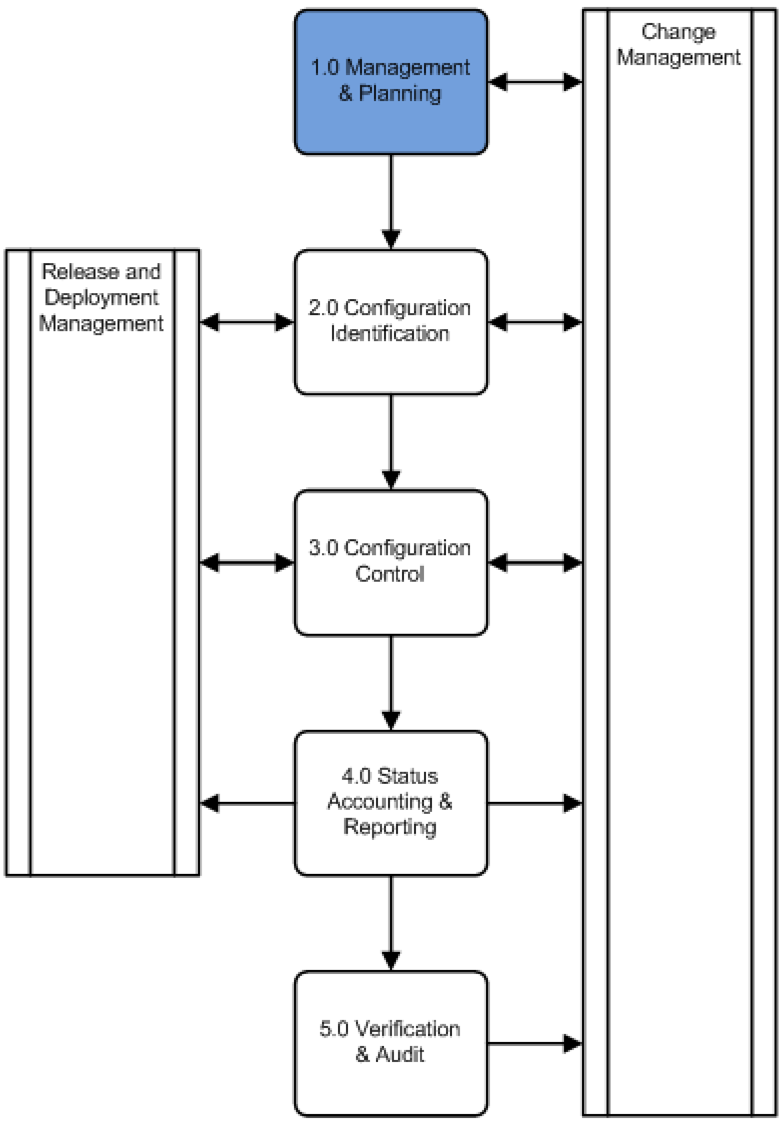
Note: Only one role can be accountable for each sub-process.

4.0 SUB-PROCESSES

The USMC CfM process consists of five sub-processes. As depicted, the CfM process is responsible for identifying, controlling, recording, tracking, reporting, auditing, and verifying information about CIs required to deliver an IT Service (including their relationships).

4.1 Management & Planning

Configuration management and planning is the initial activity within the CfM five sub-processes. The output of management and planning is the Configuration Management Plan (CMP), which specifies how configuration management will be implemented. The content of a CMP includes:



- *Scope* – defining the strategy, polices, and convention for controlling CIs. Policy dictates much of the framework for determining which configurations are developed and maintained (e.g., tracking Defense Information Systems Agency (DISA), Security Technical Implementation Guide (STIG), Certification & Accreditation (C&A), etc.).
- *Requirements* – understanding overall requirements for CfM and CMS.
- *Applicable policies and standards* – approved procedures for making changes to the CMS, license and version numbering control, naming conventions, CI status codes, and CI attributes. Criteria for selecting configuration items and their components.
- *Control authority* – establish authority and procedures for creating baselines.
- *Systems and tools* – integration of CMDBs with the CMS; designing championing and overseeing implementation of the CMS.

The following workflow (Figure 5) depicts the CfM Management Planning sub-process:

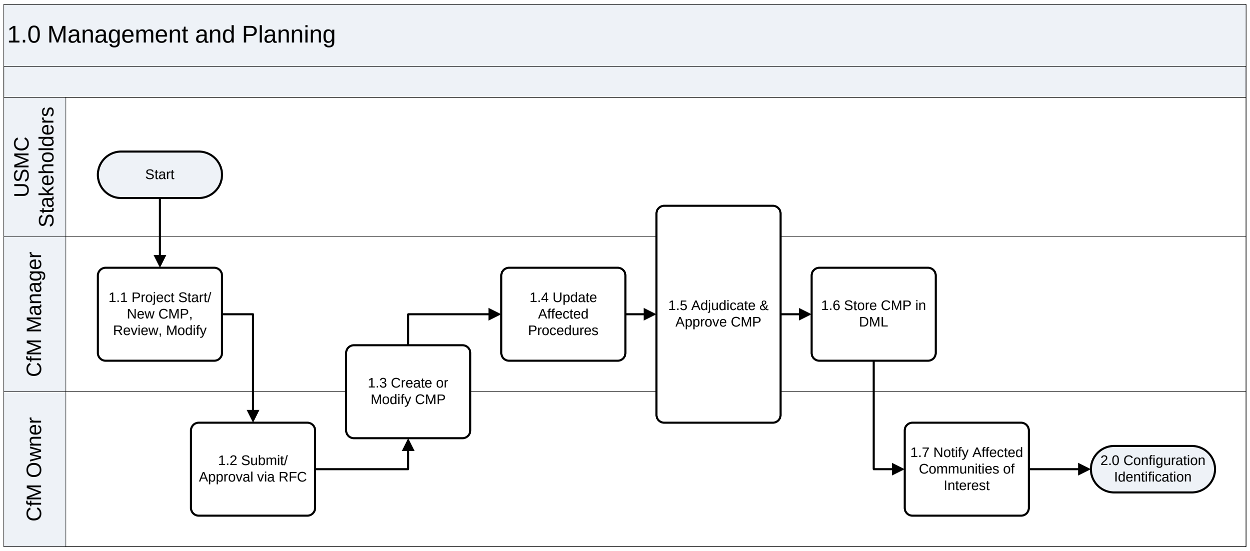


Figure 5. Management and Planning Sub-Process

Table 7 describes the Management and Planning sub-process steps as depicted in Figure 5.

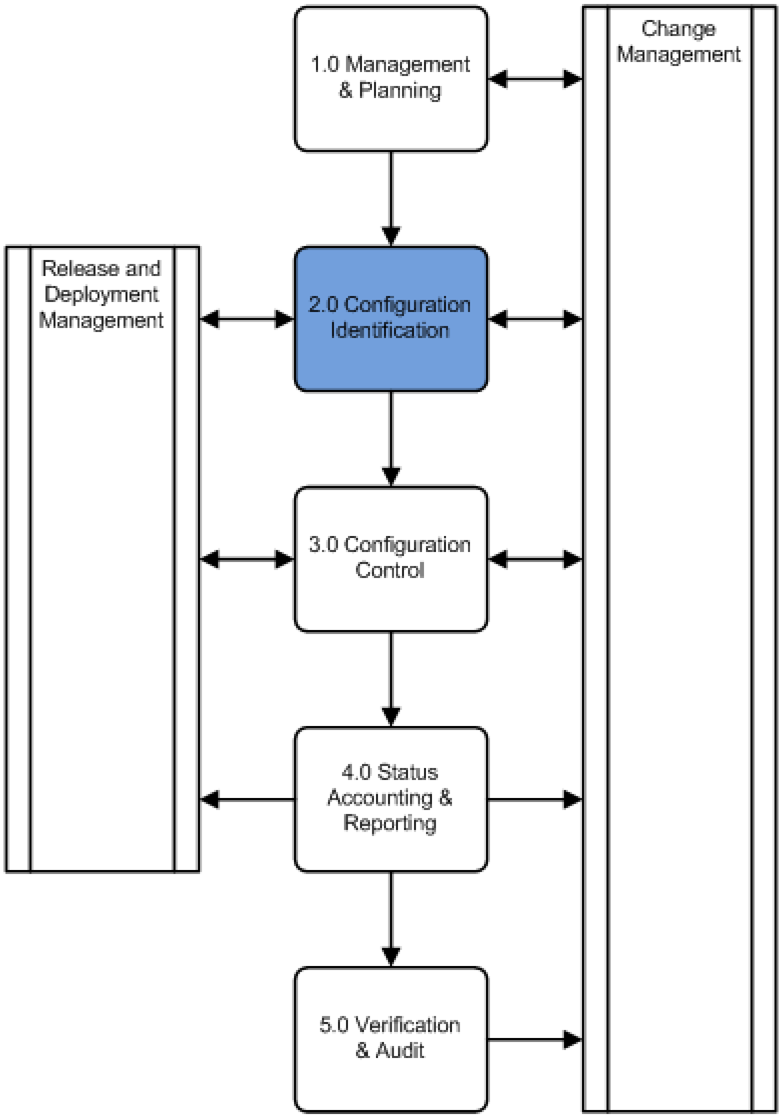
Table 7. Management and Planning Sub-Process Descriptions

1.0 Management and Planning		
Number	**Sub-Process**	**Description**
1.1	Project Start	The Management and Planning sub-process begins with the initiation of projects and programs which require creation or revisions to a CMP, and periodic CMP reviews. The scope and level of CfM oversight is driven by contractual terms, organizational policies and structure, industry standards, and technical specifications invoked for a project or program. USMC projects and programs, to include Programs of Record such as MCEITS, that require CfM Management and Planning activities.
1.2	Submit and receive approval via RFC	All changes are managed by the USMC Enterprise Change Management (ChM). CfM Process Owners submit an RFC for the proposed changes. Once approval is received, the revision may proceed.
1.3	Create or Modify CMP	CMPs are created and maintained under the oversight of the CfM process owners.
1.4	Update Affected Procedures	Update affected procedures (e.g. PWI, training, etc.) to reflect the revisions made to the CMP.
1.5	Adjudicate and Approve CMP	Modifications will be captured via Comment Resolution Matrix (CRM) and those comments/recommendations will be adjudicated with the appropriate stakeholders, e.g. HQMC/C4, MCSC, and MCNOSC. Finalize RFC with ChM.
1.6	Store CMP in DML	Once approved, the CMP is stored in the DML as a documentation CI.

1.0 Management and Planning		
Number	**Sub-Process**	**Description**
1.7	Notify Affected Communities of Interest	Notify the affected communities of interest of the new of updated CMP.

4.2 Configuration Identification

Configuration identification defines how the classes and types of CIs are to be selected, grouped, classified, and defined including the appropriate characteristics (e.g., warranties for a service) to ensure they are manageable and traceable throughout their lifecycle.



A key consideration of Configuration Identification is uniquely naming and labeling all service components of interest across the service and the relationship between them.

CIs include hardware, software, services and documentation components of (and supporting) the USMC infrastructure.

Define the roles and responsibility of CI owners at each stage of CI lifecycles.

Select the configuration items and their components according to documented criteria. Assign unique identifier and specify the relevant attributes to configuration items. Specify when each configuration item is placed under control of configuration management.

Identify the owner responsible for each configuration item.

The following workflow (Figure 6) depicts the Configuration Identification sub-process.

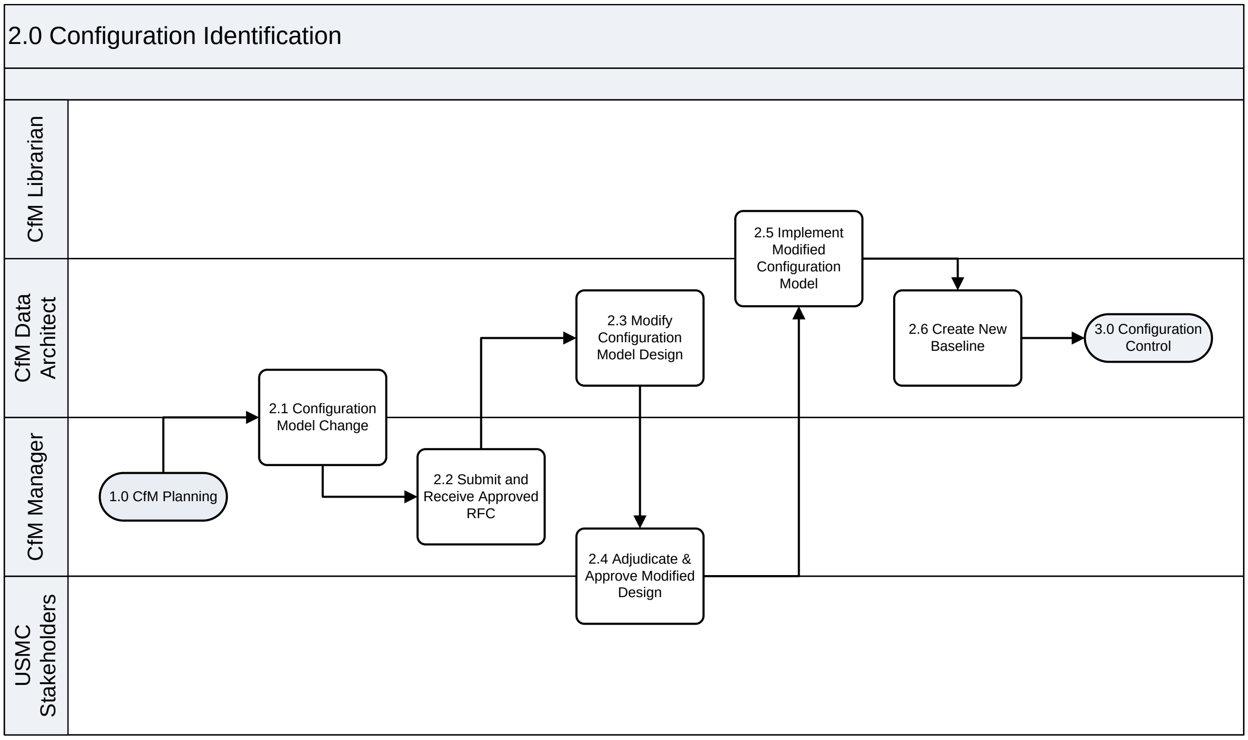


Figure 6. Configuration Identification Sub-Process

Table 8 describes the Configuration Identification sub-process steps as depicted in Figure 6.

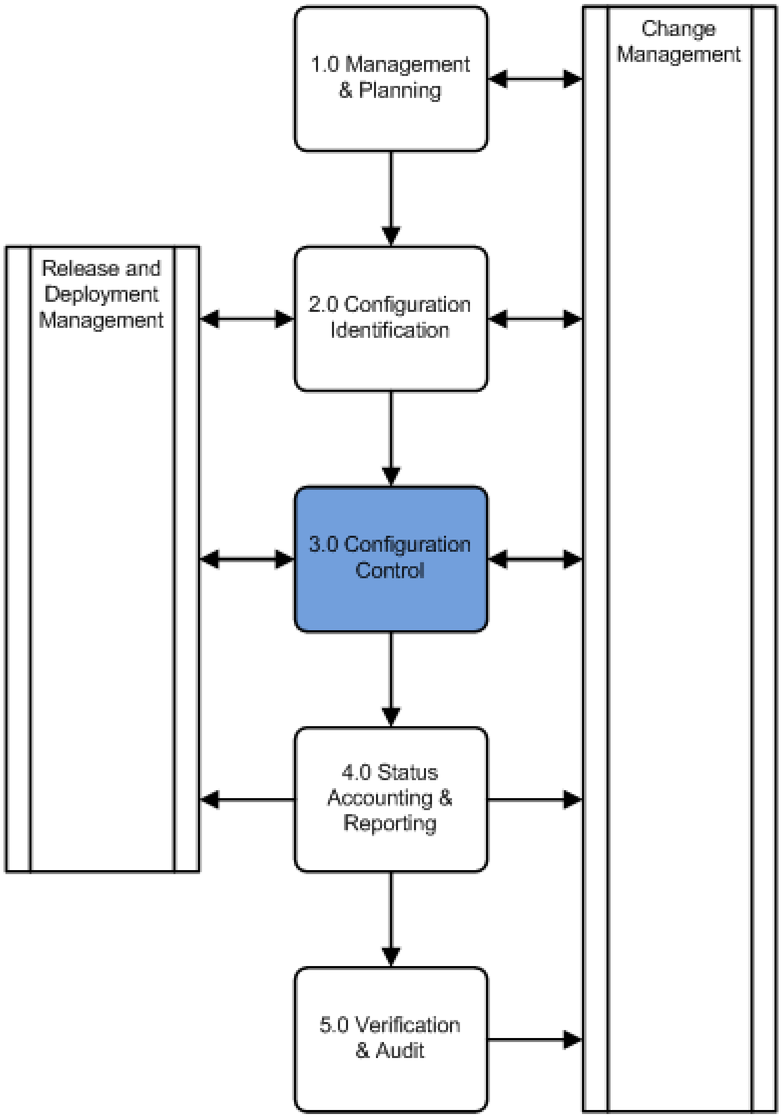
Table 8. Configuration Identification Sub-Process Descriptions

2.0 Configuration Identification		
Number	**Sub-Process**	**Description**
2.1	Change needed to the Configuration Model	Triggered by Acquisition, ChM, RDM, Configuration Verification and Audit, or Discovery Tools, an update to a CI type, relationship, attribute, or naming convention is required. When CIs are identified through auto-discovery activities, a reconciliation step should be performed to reconcile any discrepancies between the CMDB managed under Change Control and what is discovered. Reconciliation is performed using agreed-upon policies and procedures to deal with different types of discrepancies.
2.2	Submit and receive approval via RFC	All changes are managed by the USMC Enterprise Change Management (ChM). CfM Process Owners submit an RFC for the proposed changes. Once approval is received, the revision may proceed.
2.3	Modify Configuration Model Design	When a new type of CI is identified for inclusion within the CMS, a number of steps follow as applicable: • Creating specific naming conventions for the CI type • Creating specific labeling conventions • Defining attributes for the CI type • Defining lifecycle states for the CI type and the transitions between

2.0 Configuration Identification		
Number	**Sub-Process**	**Description**
		states • Defining documentation for the CI type • Defining relationships to other CI types • Identification of CI Owners Changing the configuration model can have an effect on existing reports and may involve modifications to the ITSM tool(s) workflow or schema.
2.4	Adjudicate and Approve Modified Design	Adjudicate and approve configuration model modifications with the appropriate stakeholders, e.g. HQMC/C4, MCSC, and MCNOSC. Finalize RFC with ChM.
2.5	Implement the Modified Configuration Model	Implement the approved configuration model in the CMS.
2.6	Create New Baseline	Create a new configuration model baseline upon which future changes are based.

4.3 Configuration Control

Configuration control ensures that there are adequate control mechanisms over CIs while maintaining a record of changes to CIs, versions, location and ownership. The 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 features:



- 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 performing a release in a manner that can be used for subsequent evaluation against actual deployment.
- Promotion and/or migration of electronic data and information, maintaining the integrity of the definitive media library DML and CMS within the overarching SKMS.

The following workflow (Figure 7) depicts the Configuration Control sub-process:

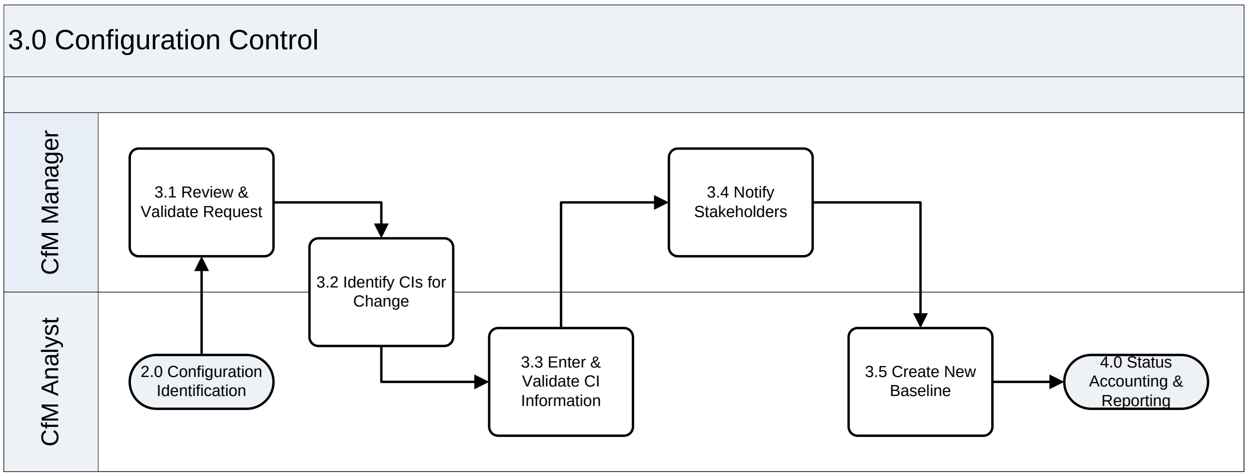


Figure 7. Configuration Control Sub-Process

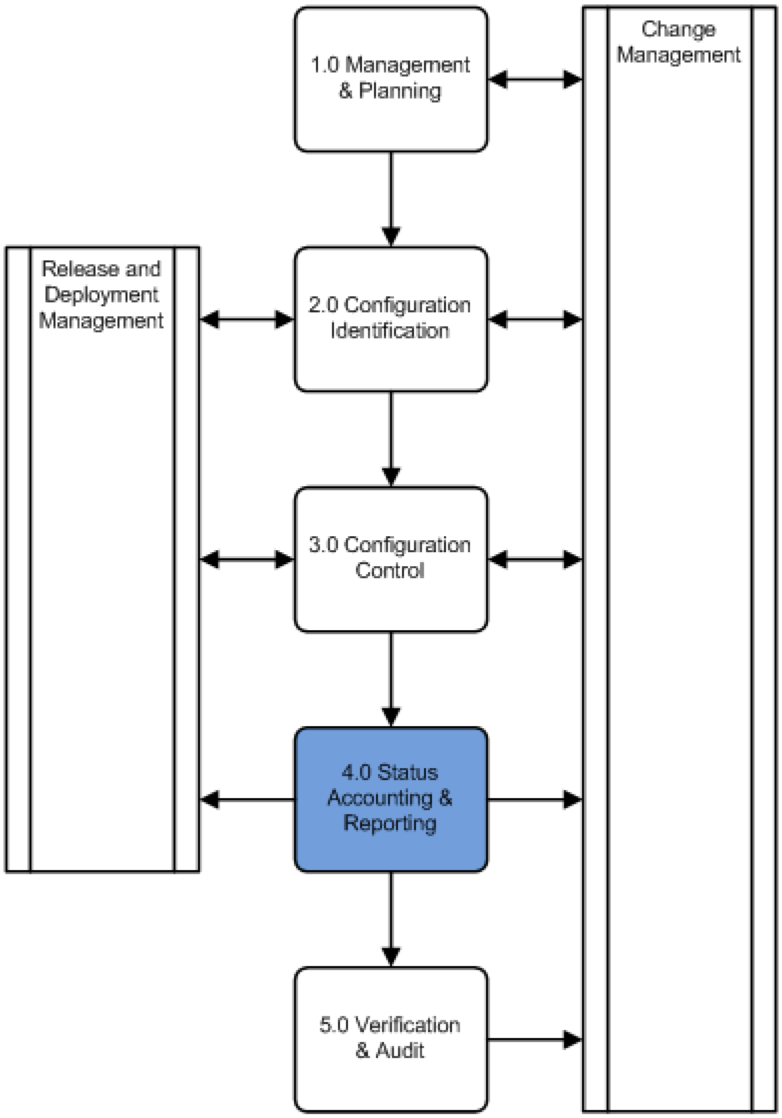
Table 9 describes the Configuration Control sub-process steps as depicted in Figure 7.

Table 9. Configuration Control Sub-Process Descriptions

3.0 Configuration Control		
Number	**Sub-Process**	**Description**
3.1	Review & Validate Request	RFCs processed through ChM may require configuration information. ChM passes information to and receives information from CfM throughout the change process. CfM reviews information about CIs that need to be added or updated. Determine that the RFC contains all of the configuration information necessary to go forward. Review and validate that changes are within scope of the CMP and the configuration model. If not within scope, determine that the change is appropriate, has the correct authorization, and has sufficient justification. If it does, the change cannot proceed until the CMP and/or configuration model has been updated to accommodate the needs of the change.
3.2	Identify CIs for Change	Determine the affected CIs to be added, updated, or retired. Where appropriate the necessary records are created to support the change.
3.3	Enter & Validate CI information	Update configuration records as necessary (Change to CI status, relationships, and attributes). Validate automated updates coming from auto-discovery tools and other data sources.
3.4	Notify Stakeholders	Contact appropriate stakeholders including CI Owners to notify them of the configuration change and have them validate the updated information in the CMS.
3.5	Create New Baseline	As specified in the CMP, a new baseline of all affected CIs involved in release of the new or modified service may be needed as a consequence of the change/release.

4.4 Status Accounting and Reporting

There are two types of reports: reports accounting for the lifecycle status of CIs as defined by CI type, and other CfM reports in support of services throughout the service lifecycle. Different CI types have different lifecycle statuses according to the nature of the type. Some CI types have many lifecycle states, others have just a few. The following discrete states provide a high level guideline:



- Development or draft denoting that the CI is under development,
- Approved meaning that the CI may be used, and
- Withdrawn meaning that the CI has been taken/decommissioned from use.

Typical activities 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 CfM available throughout the lifecycle,
- Recording changes to the CIs from receipt to disposal.

The following workflow (Figure 8) depicts the Status Accounting and Reporting sub-process:

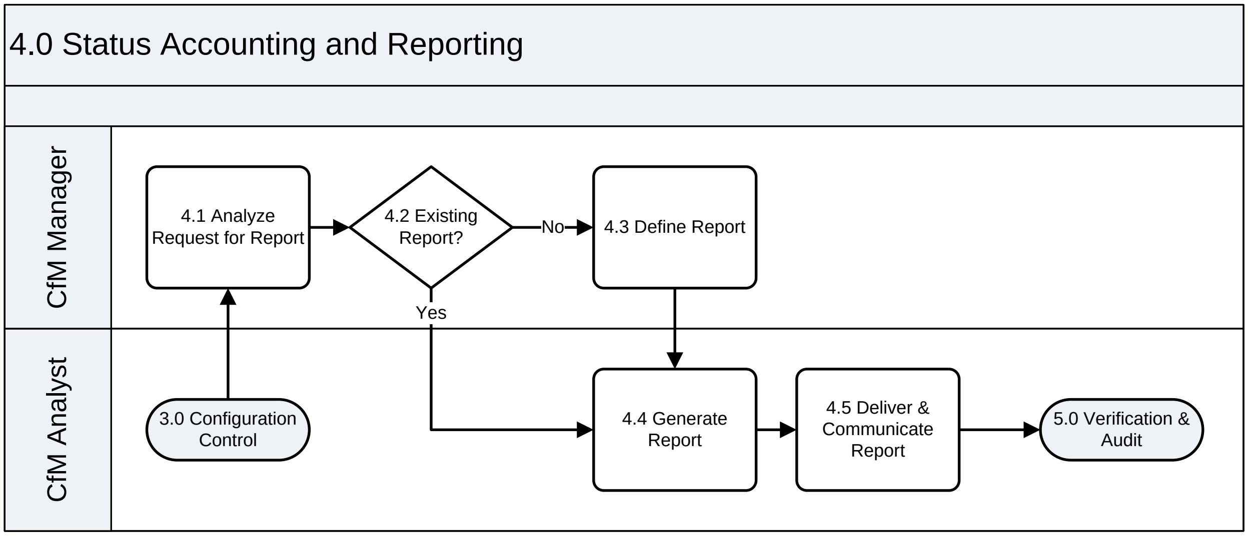


Figure 8. Status Accounting and Reporting Sub-Process

Table 10 describes the Status Accounting and Reporting sub-process steps as depicted in Figure 8.

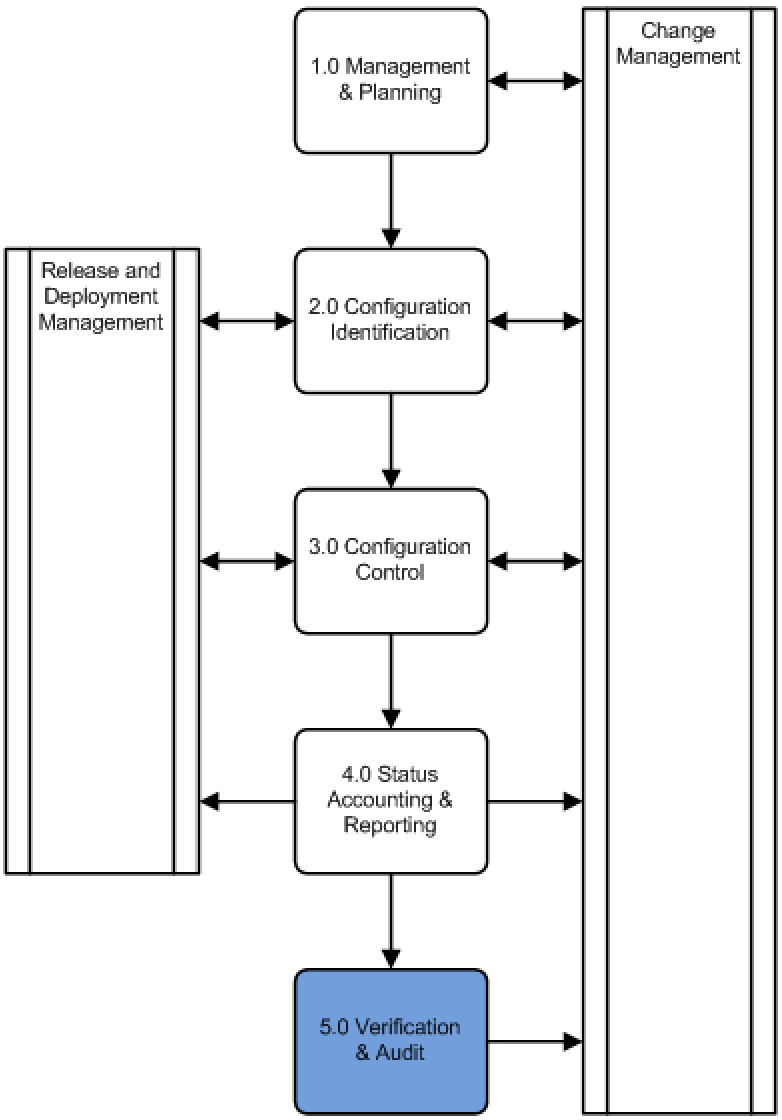
Table 10. Status Accounting and Reporting Sub-Process Descriptions

4.0 Status Accounting and Reporting		
Number	**Sub-Process**	**Description**
4.1	Analyze Request for Report	Requests for reports are analyzed to determine what information is to be retrieved, the format, and the availability of information requested, etc.
4.2	Existing Report?	It is determined whether a predefined report already exists within the reporting system.
4.3	Define Report	The CfM Manager works with the requestor to define the contents and the format of the report, determines the frequency of the report and whether the report should be added to the predefined list of reports or is a one-time generated report. The CfM Manager also specifies the attributes and the data values from the CMDB used to generate the report.
4.4	Generate Report	The CfM Analyst receives and processes requests for standard reports. The CI and CMS information is made available to any authorized requestor. The CI and CMS information can: • Range from detailed attributes and relationships to summarized information • Encompass an individual CI or a collection of CIs • Be unformatted, raw data, or pre-determined reports Report generation can be the result of a planned schedule or in response to an individual request.

4.0 Status Accounting and Reporting		
Number	**Sub-Process**	**Description**
4.5	Deliver and Communicate Report	The CfM Analyst moves the generated report to a designated website or distributed via email. Report contents are communicated as appropriate.

4.5 Verification and Audit

The Verification and Audit Ensures that change and release records have been properly authorized by change management and that implemented changes are as authorized. Ensure that before a major release or change, an audit of the specific configuration of the USMC's environment matches the CMS. The following activities include a series of reviews or audits:



- Ensure that there is 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, and
- Check that the release and configuration documentation is present before making the release.

The following workflow (Figure 9) depicts the Verification and Audit sub-process:

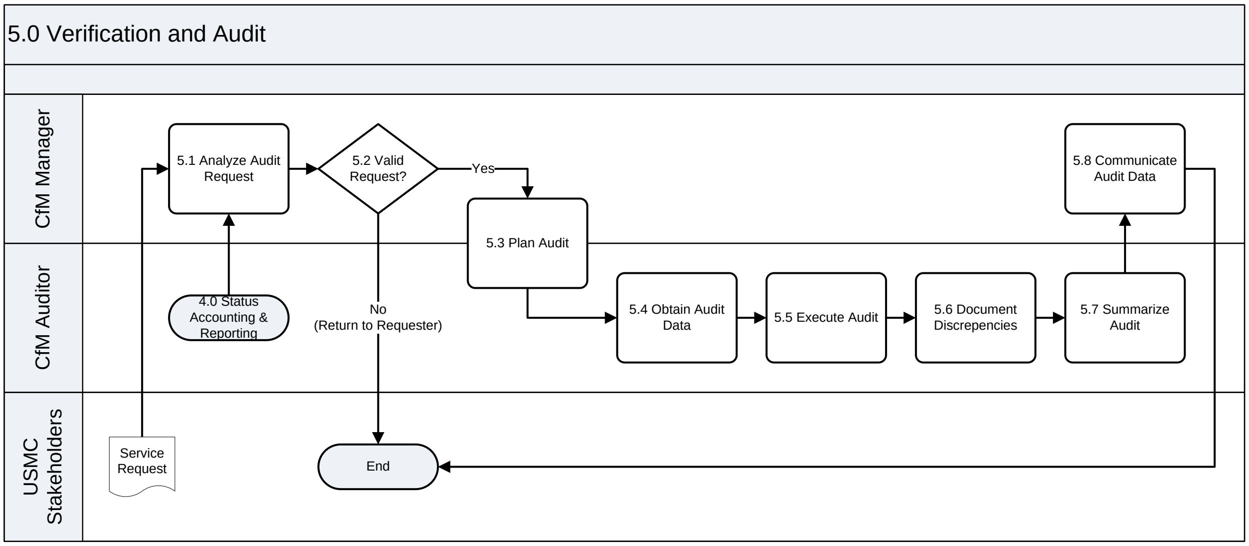


Figure 9. Verification and Audit Sub-Process

Table 11 describes the Verification and Audit sub-process steps as depicted in Figure 9.

Table 11. Verification and Audit Sub-Process Descriptions

5.0 Verification and Audit		
Number	**Sub-Process**	**Description**
5.1	Analyze Audit Request	The requirements are reviewed and validated regarding the need for the audit. Configuration audits occur: • Shortly after changes to the CMS • Before and 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 CMP, annually at a minimum • At random intervals. • In response to the detection of any unauthorized CIs
5.2	Valid Request?	It is determined whether a request is valid based on pre-determined criteria. If the request is not justified, the request is returned to the requestor following existing audit guidelines.

5.0 Verification and Audit		
Number	**Sub-Process**	**Description**
5.3	Plan Audit	Planning for an audit involves four major activities: • Verifying the reference model used as a basis for the audit, such as reconciliation tools, is relevant and acceptable • Establishing a baseline reference point by assessing the current situation • Preparing a detailed report for the difference between the reference model and the current situation in the form of a gaps analysis supported by a risk analysis and plan of action • Scheduling a program of initiatives to remedy CIs with a significant level of risk of compliance related importance **Note:** These activities are performed for both Scheduled Audits as defined in the CfM Plan and those audits performed ad-hoc in support of other service management efforts.
5.4	Obtain Audit Data	Using the CMDB and system libraries, data is obtained for the point-in-time of the audit.
5.5	Execute Audit	The physical data is compared to documented data using the audit procedure. Before making a conclusion, it is ensured that any anomalies are addressed.
5.6	Document Discrepancies	An audit report is generated documenting the discrepancies uncovered in the structure and content of the system audited. A key component of the verification and audit activities is the reconciliation between the managed and discovered inventories and configurations. Any updates to the CMDB should be performed through Change Management.
5.7	Summarize Audit	Exceptions noted are documented. It is determined if the exceptions were due to process activity violations. A risk impact analysis of the exceptions is included. Also documented and communicated is the remediation required to meet the baseline requirements of the reference model. The recommended course(s) of action are prioritized.
5.8	Communicate Audit Data	The audit data is communicated to stakeholders, along with a recommended course of action. If updates to the CMDB are required, RFCs are prepared.

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 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 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 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 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.