

***Enterprise IT Service Management
Configuration Management
Process Guide***



***Release Date:
14 April 2011***

Table of Contents

Section	Title	Page
1.0	Introduction	1
1.1	Purpose	1
1.2	Scope	1
1.3	Document and Process Change Procedures	2
2.0	Process Overview	3
2.1	Purpose, Goals, and Objectives	3
2.2	Relationships with Other Initial Processes	3
2.3	High-Level Process Model	5
2.3.1	Process Description	8
2.4	Key Concepts	8
2.4.1	Asset	8
2.4.2	Asset Management	8
2.4.3	Attribute	9
2.4.4	Audit	9
2.4.5	Baseline	9
2.4.6	Change Advisory Board	9
2.4.7	Configuration Control	9
2.4.8	Configuration Identification	9
2.4.9	Configuration Item	9
2.4.10	Configuration Management Database	10
2.4.11	Configuration Management Plan	10
2.4.12	Configuration Management System	10
2.4.13	Definitive Hardware Store	10
2.4.14	Definitive Media Library	10
2.4.15	Labeling	10
2.4.16	Naming	11
2.4.17	Relationships	11
2.4.18	Service	11
2.4.19	Service Asset	11
2.4.20	Verification	11
2.4.21	CfM Policies	11
2.5	Quality Control	12
2.5.1	Metrics, Measurements, and Continual Service Improvement	12
2.5.2	Critical Success Factors with Key Performance Indicators	12
3.0	Governance	14
3.1	Roles and Responsibilities	14
3.1.1	Roles	15
3.1.2	Responsibilities	17
3.2	Policies	18
4.0	Sub-Processes	20
4.1	CfM Planning	20
4.2	Configuration Identification	23
4.3	Configuration Control	26
4.4	Status Accounting and Reporting	29
4.5	Verification and Audit	31
Appendix A – Acronyms		34
Appendix B – Glossary		35
Appendix C – Policies		38



List of Tables

Table	Title	Page
Table 1.	CfM Process Activity Descriptions	7
Table 2.	CfM Critical Success Factors with Key Performance Indicators	12
Table 3.	CfM Defined Roles and Responsibilities	15
Table 4.	Responsibilities for Enterprise CfM	17
Table 5.	CfM Planning Sub-Process Descriptions	21
Table 6.	CfM Configuration Identification Sub-Process Descriptions	24
Table 7.	CfM Configuration Control Sub-Process Descriptions	27
Table 8.	CfM Status Accounting and Reporting Sub-Process Descriptions	30
Table 9.	CfM Verification and Audit Sub-Process Descriptions	32

List of Figures

Figure	Title	Page
Figure 1.	Process Design Pyramid	2
Figure 2.	Sample CfM Relationship with other Initial Processes	4
Figure 3.	High-Level CfM Workflow	6
Figure 4.	CfM Roles	15
Figure 5.	CfM Planning Sub-Process.....	21
Figure 6.	CfM Configuration Identification Sub-Process	24
Figure 7.	CfM Configuration Control Sub-Process.....	27
Figure 8.	CfM Status Accounting and Reporting Sub-Process	30
Figure 9.	CfM Verification and Audit Sub-Process.....	32



Enterprise IT Service Management Configuration Management Process Guide

1 1.0 INTRODUCTION

2 1.1 Purpose

3 The purpose of this process guide is to establish a documented and clear foundation for process
4 implementation and execution across the United States Marine Corps (USMC) enterprise.
5 Process implementation and execution at lower levels (e.g., regional, local, and Programs of
6 Record) must align and adhere to directives and schema documented within this guide. The
7 active use of this guide ensures USMC Information Technology (IT) activities are executed in a
8 uniform manner.

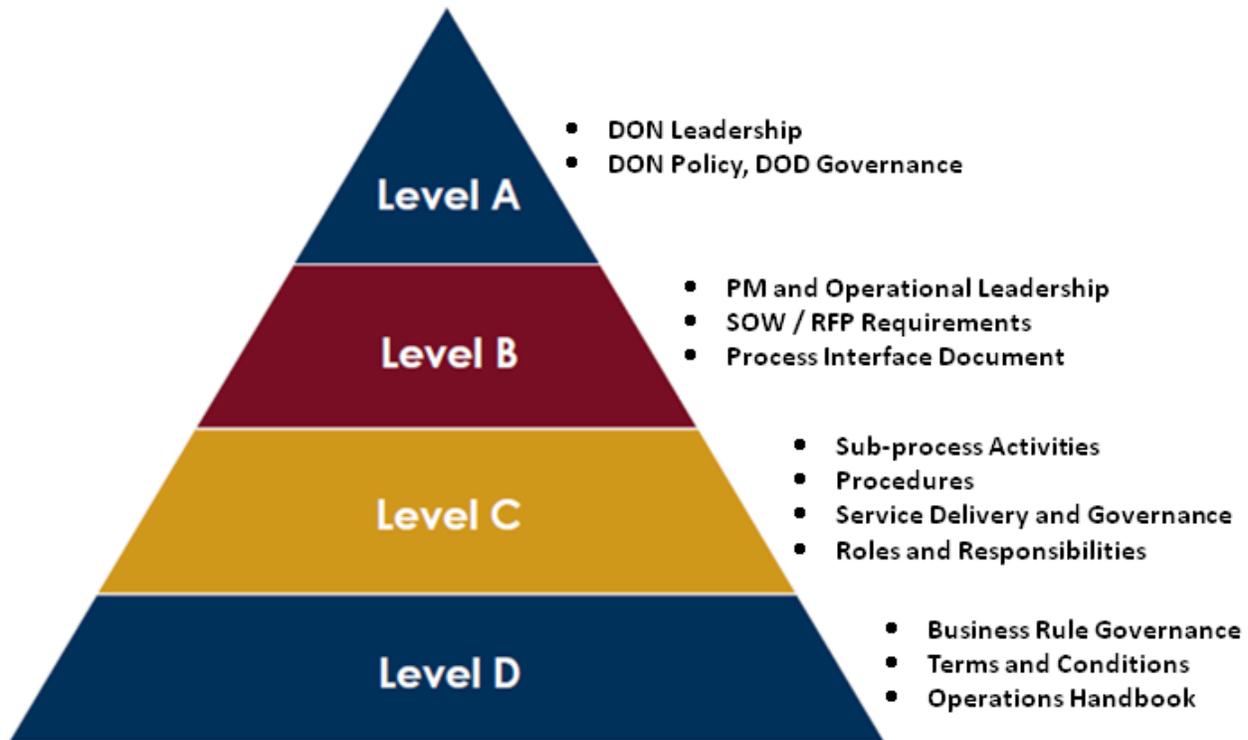
9 1.2 Scope

10 The scope of this document covers Marine Corps Enterprise IT Services (MCEITS) and garrison
11 Secret Internet Protocol Router Network (SIPRNet) related services owned by the USMC while
12 simultaneously providing a foundation for process implementation and execution across the
13 USMC enterprise. Information remains relevant for the global operations and defense of the
14 Marine Corps Enterprise Network (MCEN) as managed by Marine Corps Network Operations
15 and Security Center (MCNOSC) including all Regional Network Operations and Security
16 Centers (RNOSC) and Marine Air Ground Task Force Information Technology Support Center
17 (MITSC) assets and supported Marine Expeditionary Forces (MEF), Supporting Establishments
18 (SE) organizations, and Marine Corps Installation (MCI) commands.

19 This document uses the term “sub-process” to describe process layers that exist beneath the
20 parent process level. This sub-process layer is equivalent to process “Level C” as referenced in
21 the following diagram. Please note that procedures, also associated with Level C, are not
22 included within the scope of this document. The current Procedures and Work Instructions (PWI)
23 can be found at the following location:

24 https://ips.usmc.mil/sites/pg10docr/pm_ccr/E-ITSM/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2fsites%2fpg10docr%2fpm%5fccr%2fE%2dITSM%2fShared%20Documents%2fProcedure%20Work%20Instructions&FolderCTID=&View=%7b575B66E8%2dD286%2d4040%2d980A%2d12D8990F333E%7d
25
26
27





28

29

Figure 1. Process Design Pyramid

30 1.3 Document and Process Change Procedures

31 This document will be reviewed semi-annually for accuracy by the Process Owner with
 32 designated team members. Modifications to this document are ultimately governed by the USMC
 33 Enterprise Change Management (ChM) process. Please direct any questions or comments
 34 concerning this document to the USMC Enterprise Service Desk at 1-800-TBD,
 35 Support@usmc.smil.mil, Support@usmc.mil, or eitsm@usmc.mil. For detailed information on
 36 process change requests, refer to Section 2.3 of the *Enterprise IT Service Management Change*
 37 *Management Process Guide*.

38



39 2.0 PROCESS OVERVIEW

40 2.1 Purpose, Goals, and Objectives

41 The purpose and goal of Configuration Management (CfM) for MCEITS and garrison SIPRNet
42 services is to account for, manage, and protect the integrity of service assets and Configuration
43 Items (CIs) by recording their status and relationships, ensuring only authorized components are
44 used and ensuring only authorized changes are made.

45 The primary objective of the CfM process is to enable other IT Service Management (ITSM)
46 processes to access valuable historical, planned, and current state information to support:

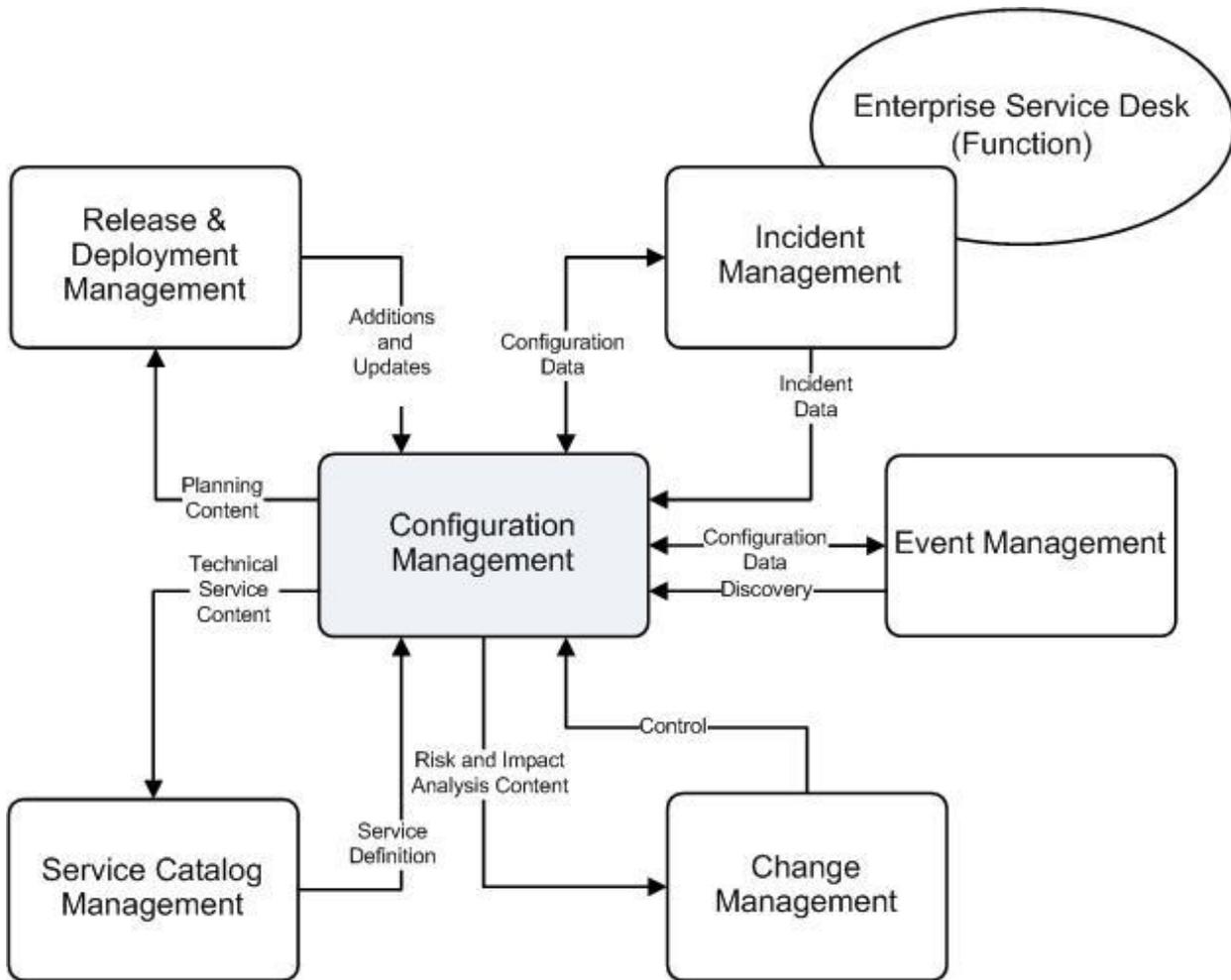
- 47 • Accurate identification of CIs
- 48 • Control of service and infrastructure components
- 49 • Impact assessment of incidents and problems
- 50 • Impact assessment of proposed changes
- 51 • Identification and assessment of incident and problem resolutions
- 52 • Planning and designing new or changed services
- 53 • Planning technology refresh and software upgrades
- 54 • Planning release and deployment packages
- 55 • Optimizing CI utilization and costs (e.g., data center and service consolidation, reduction
56 of configuration variations, and re-use of assets)

57 This document does not cover USMC fixed asset accounting. For information on Asset
58 Management refer to section 2.4.2.

59 2.2 Relationships with Other Initial Processes

60 All IT Service Management processes are interrelated. The six (6) Initial Processes in Figure 2
61 were selected due to the strength of the relationships and dependencies between them and the
62 degree to which they underpin USMC near-term objectives. While any one of the Initial
63 Processes can operate in the presence of an immature process, the efficiency and effectiveness of
64 each is greatly enhanced by the maturity and integration of all Initial Processes. Figure 2 depicts
65 key relationships that exist between CfM and the other Initial Processes. This figure is not all-
66 encompassing and the relationships shown can be direct or indirect.





67

68

Figure 2. Sample CfM Relationship with other Initial Processes

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

71

- Service Catalog Management

72

- Service Definition: The Service Catalog is the definitive source of record for services that are present in the Configuration Management System (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.

73

74

75

76

77

- 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.

78

79

80

81

- Release and Deployment Management



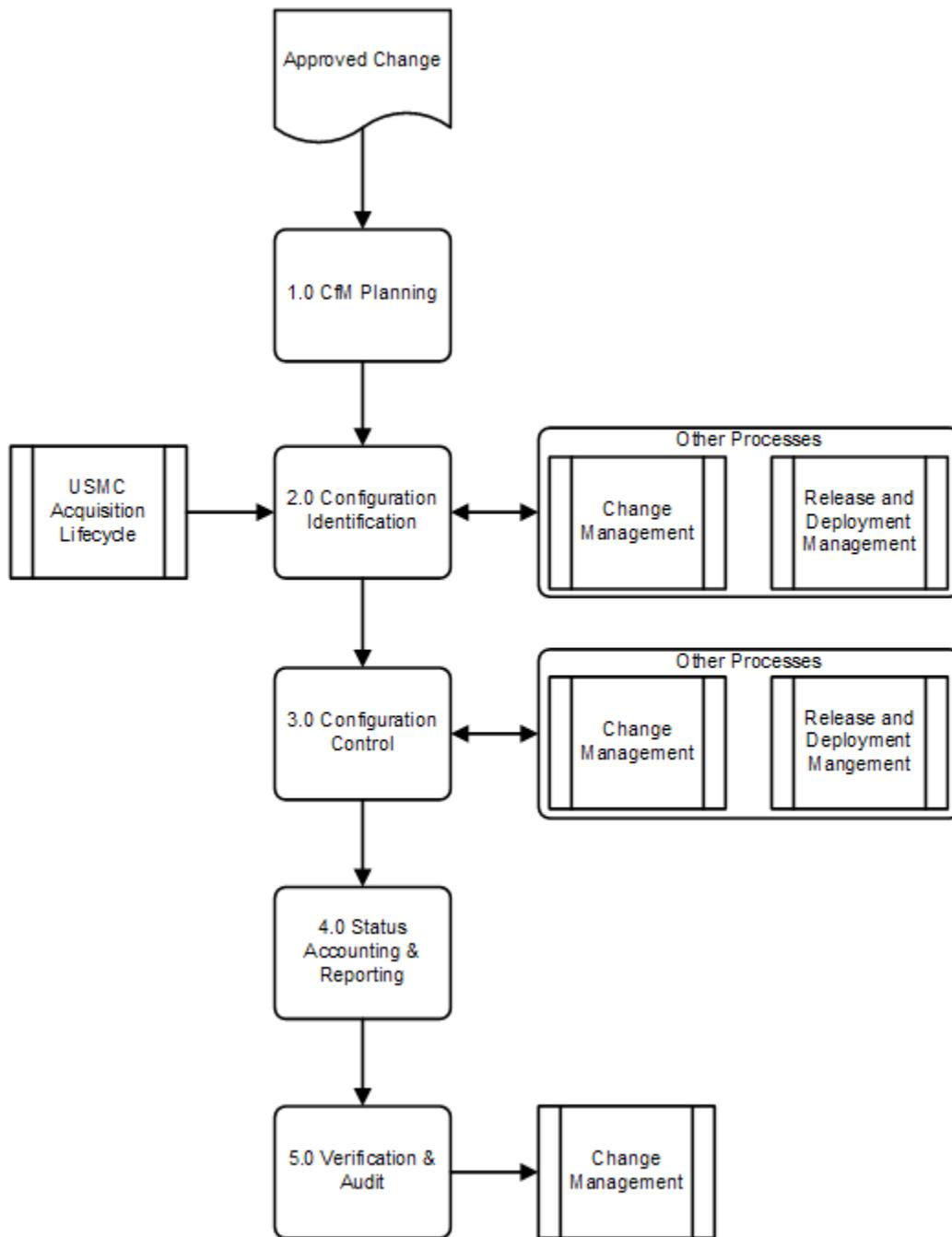
- 82 — Planning Content: The CMS and supporting processes provide invaluable information
83 for the purposes of planning, preparing, and designing a release. For example, in the
84 presence of an accurate CMS, the environment does not need to be inventoried to
85 predict work effort and manpower required to propagate a large-scale enterprise
86 release.
- 87 — Additions and Updates: The CMS is updated as CIs are introduced or updated to
88 ensure it accurately reflects the as-deployed environment.
- 89 • Incident Management
- 90 — Configuration Data: Configuration data, present in the Configuration Management
91 Database (CMDB), provides information to the Service Desk and the Incident
92 Management process for the purposes of troubleshooting, diagnosis, and resolution of
93 incidents. By knowing the extent to which CIs are affected, incidents can be assessed
94 for impact and prioritized accordingly.
- 95 — Incident Data: Incidents are linked to CIs in the CMDB. This provides the Service
96 Desk and other interested parties information regarding the disposition of CIs and
97 associated services, systems, and applications.
- 98 • Event Management
- 99 — Configuration Data: Configuration data, present in the Configuration Management
100 Database (CMDB), provides target and scope information necessary to architect and
101 engineer service monitoring as well as establish correlation rules to help minimize
102 redundant alerts.
- 103 — Discovery: The CMDB leverages discovery information from Event Management for
104 audits and reconciliation activities.
- 105 • Change Management
- 106 — Risk and Impact Analysis Content: The CMS depicts relationships between services
107 and CIs, enabling risk and impact analysis for the purposes of Request for Change
108 (RFC) evaluation.
- 109 — Control: To keep information current, CI data and history is updated both by Change
110 Management (ChM) to CfM and vice versa. Configuration Management provides the
111 infrastructure data required to assess customer impact of an IT infrastructure
112 component failure and aids identification of the CI owners and associated user(s).
113 Status of changes, especially completion, is an input to CfM, keeping the CMDB
114 current.

115 2.3 High-Level Process Model

116 The CfM process consists of five distinct sub-processes and is integrated with the Change
117 Management processes. The following workflow (Figure 3) depicts these processes and sub-



118 processes that collectively enable and underpin CfM. See Section 4.0 for complete descriptions
119 of the sub-process activities.



120

121

Figure 3. High-Level CfM Workflow

122 Table 1 contains descriptions of each sub-process. Each sub-process number is hyperlinked to its
123 detailed description in Section 4.0, Sub-Processes.



Table 1. CfM Process Activity Descriptions

Number	Process Activity	Description
1.0	CfM Planning	<p>Planning is the initial activity within the CfM process. It sets the objectives and critical success factors to be achieved through CfM, as well as specifying the organizational context for CfM activities, and identifying policies and relationships to other processes.</p> <p>The primary output of CfM planning is the Configuration Management Plan (CMP), which specifies how configuration management will be implemented (including policies and procedures) for a particular acquisition or program.</p>
2.0	Configuration Identification	<p>Defines how the classes and types of services, assets and CIs are to be selected, grouped, classified, and defined, including the appropriate attributes to be captured.</p> <p>CIs include hardware, software, services and documentation components of (and supporting) the USMC infrastructure.</p> <p>A key consideration of Configuration Identification is the unique and consistent naming and labeling of all assets or service components.</p> <p>The initial identification or recording of assets originates during the acquisition process at the time of procurement. Responsibility for carrying out configuration identification activities runs across many levels of the USMC. However, the process owner is ultimately accountable for configuration identification of all IT assets.</p> <p>Policy dictates much of the framework for determining which assets and configurations are developed and maintained. For example, tracking Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) compliance is required for Certification & Accreditation (C&A) approvals and audits.</p> <p>When CIs are identified through auto-discovery activities, a reconciliation step is 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.</p> <p>All updates to the CMDB must be processed through Change Management.</p>
3.0	Configuration Control	<p>Activities which ensure that no CI is added, modified, replaced, or removed without appropriate controlling documentation or procedure being followed.</p> <p>Configuration Control uses the Change Management Process to request and approve configuration changes throughout an asset's lifecycle. Updates to the CMDB after changes are released provide current CI status and configuration.</p> <p>Procedures must be in place to cover license, change, version, access, build, release, deployment, installation and DML integrity control.</p>
4.0	Status Accounting and Reporting	<p>Configuration data and documentation is recorded within the CMS as each asset or CI progresses through its lifecycle. Recording provides the status of the configuration of a service and its environment as the configuration evolves through the service lifecycle.</p> <p>The way CIs progress through each state is proscribed through procedure and controlled through Change Management.</p>
5.0	Verification and Audit	<p>Reviewing the fielded systems to the documented baseline ensures conformity. Any discrepancies uncovered have root cause analysis performed as a part of the audit to ensure accuracy in the future. Audits are performed before deploying a major release or change. Other audits are performed at planned or random intervals as needed. Audit intervals and staff involvement is proscribed within the CMP.</p> <p>A key component of verification and audit activities is reconciliation between managed and discovered inventories and configurations.</p>



Number	Process Activity	Description
		Any updates to the CMDB are performed through Change Management.

125

126 2.3.1 Process Description

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

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

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

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

144 2.4 Key Concepts

145 The following key concepts describe concepts unique to CfM:

146 2.4.1 Asset

147 An asset is a distinguishable entity that provides a service or capability. Assets are people,
 148 physical entities, logical entities such as processes and knowledge, applications or information
 149 located either within or outside the United States and owned or operated by domestic, foreign,
 150 public, or private sector organizations. Assets are both physical and logical components used
 151 when composing a service that will be governed and eventually offered for consumption by an
 152 end user.

153 2.4.2 Asset Management

154 Asset Management is the process responsible for tracking and reporting the listing of items used
 155 as part of a service throughout its entire lifecycle. This includes the financial and ownership
 156 characteristics of the items throughout their lifecycle. An Asset Management process will be
 157 developed to work closely with CfM.



158 **2.4.3 Attribute**

159 Attribute describes the characteristics of a CI which are valuable to record and which will
160 support CfM and the ITSM processes they support. Attributes are identified to the level of
161 functional detail description needed, including characteristics such as manufacturer, model, serial
162 number, or cost.

163 **2.4.4 Audit**

164 An Audit ensures there is conformity between the documented baselines (e.g., agreements,
165 interface control documents) and the actual business environment to which they refer. It verifies
166 the physical existence of CIs in the organization or in the DML and spares stores, the functional
167 and operational characteristics of CIs, and it confirms records in the CMS match the physical
168 infrastructure.

169 **2.4.5 Baseline**

170 Configuration baselines define a formal milestone or point of departure for a system or CI.
171 Baselines establish a configuration definition from which configuration changes will be tracked
172 and documented. Industry best practices normally identify three baselines for the validation and
173 acquisition of systems: the Functional, Allocated and Product Baselines. The baselines are
174 documented by approved configuration identification (documentation), which is the basis for
175 controlling changes to CI requirements.

176 **2.4.6 Change Advisory Board**

177 A Change Advisory Board is a group of people that advises the Change Manager in the
178 assessment, prioritization, and scheduling of changes. This board is made up of representatives
179 from all areas within the IT service provider and representatives from the business and third
180 parties such as suppliers. Specific membership varies by organization.

181 **2.4.7 Configuration Control**

182 Configuration Control is a set of processes and approval stages required to change a CI attribute.
183 Configuration control is the oversight to ensure that a CI is changed through the Change
184 Management process.

185 **2.4.8 Configuration Identification**

186 Configuration Identification is the selection, identification, and labeling of the configuration
187 structures and CIs including their respective technical owner and the relationships between them.
188 CIs become the manageable unit that is planned for release into a configuration controlled
189 environment. The CIs consist of hardware, software, services, and documentation.

190 **2.4.9 Configuration Item**

191 A CI is any component that needs to be managed in order to deliver an IT service. Information
192 about each CI is recorded in a configuration record within the Configuration Management



193 System and is maintained throughout its lifecycle by Configuration Management. CIs are under
194 the control of Change Management. CIs include IT services, hardware, software, buildings,
195 people and formal documentation such as process documentation and Service-Level Agreements
196 (SLAs).

197 **2.4.10 Configuration Management Database**

198 The Configuration Management Database (CMDB) is a large central logical repository used to
199 store configuration records throughout their lifecycle and makes that information accessible to
200 other service processes. The CMDB may consist of a federated relationship of databases linked
201 to a central repository.

202 **2.4.11 Configuration Management Plan**

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

206 **2.4.12 Configuration Management System**

207 The Configuration Management System (CMS) holds all the information for CIs within the
208 designated scope. The CMS may consist of multiple CMDBs and interrelated systems.

209 **2.4.13 Definitive Hardware Store**

210 The Definitive Hardware Store (DHS) is a secure area set aside for the storage of definitive
211 hardware spares maintained at the current operational level of the corresponding CI in the live
212 environment. Only authorized hardware is accepted into the DHS via the Change and Release
213 processes.

214 **2.4.14 Definitive Media Library**

215 The Definitive Media Library (DML) is the secure library into which definitive authorized
216 versions of all software CIs are stored and protected. The DML is both a physical and electronic
217 media storage repository where master copies of software versions are stored, including specific
218 applications and patches. Only authorized software is accepted into the DML and it is strictly
219 controlled by Change and Release Management. The DML is a common base for the Release and
220 Deployment Management and Configuration Management processes.

221 **2.4.15 Labeling**

222 Physical device CIs are labeled with their assigned unique name so that they can be easily
223 identified. Items need to be distinguished by unique, durable identification (e.g., labels or
224 markings that follow relevant standards where appropriate). Physical, non-removable asset tags
225 (labels) should be attached to all hardware CIs; cables/lines should be clearly labeled at each end
226 and at all inspection points.



227 2.4.16 Naming

228 All devices under configuration management require a unique name to identify them. Names are
229 created and assigned at the local level using the existing enterprise unique convention. Devices
230 may not share names; unique names are used to establish relationships between and as
231 components of system.

232 2.4.17 Relationships

233 Relationships refer to the connection, tier, or type of binding or membership that one CI has to
234 another. Relationships can be top-down, bottom-up, or horizontal. They can be categorized as
235 hardware-to-hardware, hardware-to-software, hardware/software to business application, and
236 hardware/software to service.

237 2.4.18 Service

238 A service is a means of delivering value to customers by facilitating outcomes customers want to
239 achieve without the ownership of specific costs and risks. Services facilitate outcomes by
240 enhancing the performance of associated tasks and reducing the effect of constraints. Examples
241 of services are email, provisioning, and financial management.

242 2.4.19 Service Asset

243 A Service Asset is any capability or resource of a service provider.

244 2.4.20 Verification

245 Verification, as in Configuration Verification, is a process that is common to configuration
246 management, systems engineering, design engineering, manufacturing, and quality assurance. It
247 is the means by which a contractor verifies his design solution. The functional aspect of
248 configuration verification encompasses all of the test and demonstrations performed to meet the
249 quality assurance sections of the applicable performance specifications. (Source: HNDBK-61A)

250 2.4.21 CfM Policies

251 Emerging CfM policies leverage existing directives and guidance to ensure adherence to DoD
252 and other regulatory standards. Documents include, but are not limited to, the following:

DoDI 8115.02	Information Technology Management Implementation
DoD 4160.21-M	Defense Material Disposition Manual
SECNAVINST 7320.10A	DON Personal Property Policies and Procedures
MCO P4000.57	Marine Corps Total Life Cycle Management
MCO 4100.51B	Automatic Identification Technology (AIT)
MCO 4500.11E	Instructions for the Disposition/Utilization of Excess Personal Property
MCO P5233.1	Automatic Data Processing Management Standards Manual

253



254 **2.5 Quality Control**255 **2.5.1 Metrics, Measurements, and Continual Service Improvement**

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

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

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

270 **2.5.2 Critical Success Factors with Key Performance Indicators**

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

274 The following CSFs and KPIs can be used to judge the efficiency and effectiveness of the
 275 process. Results of the analysis provide input to improvement programs (i.e., continual service
 276 improvement).

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

278 **Table 2. CfM Critical Success Factors with Key Performance Indicators**

CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Benefits
1	Identified Services, CIs and key attributes are captured in the CMDB and are complete	1	Percentage of CI discrepancies per sample audit The CMDB is audited on a scheduled basis. The volume of discrepancies is captured and trended over time. Calculation: Total errors detected / total number of CIs audited * 100	An accurate CMDB provides foundation for improved Incident, Change and Release Management processes.



		2	Percent of CIs in the CMDB with all key attributes defined Calculation: Number of CIs with missing key attributes as percent of all CIs Note: Key attributes will be defined as part of the Configuration Management Planning activity.	Effectiveness of the CMDB will only be realized when the information is complete and consistently entered.
2	Production services are protected from the adverse impacts of changes or failure to make needed changes	3	Errors detected in CMDB The CMDB is audited on a scheduled basis. Errors are recorded as: Calculations: <ul style="list-style-type: none"> Count of CIs identified during audit which were not in the CMDB Count of CIs in the CMDB which could not be found during the audit Note: The volume of discrepancies is captured and trended over time.	Accurate data in the CMDB provides improved ability to assess risk of changes, to correctly apply changes, and to mitigate risk of failure to make needed changes.

279
280

281 3.0 GOVERNANCE

282 Governance deals with the authority and accountability for directing, controlling, and executing
283 IT services. IT governance involves creating the governing principles. This includes:

- 284 • Who makes directing, controlling, and executing decisions
- 285 • How the decisions are made
- 286 • What information is required to make the decisions
- 287 • What decision making mechanisms should be required
- 288 • How exceptions are handled
- 289 • How the governance results should be reviewed and improved

290 Enterprises have always strived for effective administration, direction, and control. However,
291 there is an increased focus on IT governance because of federal regulations related to privacy,
292 antiterrorism, security, and other factors.

293 IT governance encompasses the organizational structures and IT management processes used to
294 sustain and extend strategies and objectives. Clearly defining roles and responsibilities within
295 each process is a critical activity of IT governance for the USMC. By introducing controlled
296 governance, the level of transparency and accountability within IT operations is improved,
297 thereby reducing risks while linking IT goals with USMC mission accomplishment.

298 3.1 Roles and Responsibilities

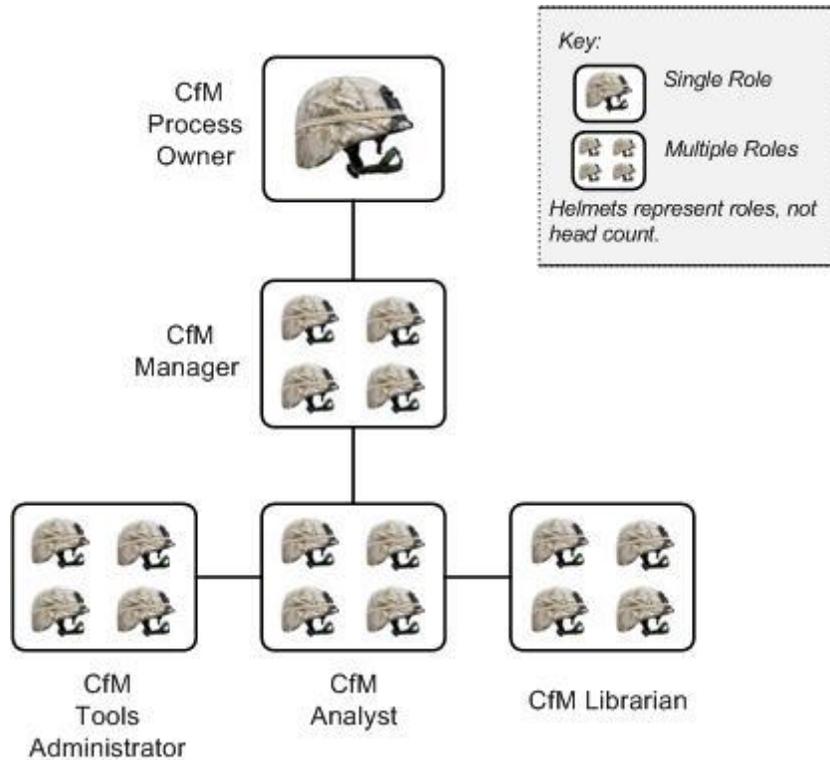
299 Each process has roles and responsibilities associated with design, development, execution, and
300 management of the process. A role within a process is defined as a set of responsibilities. Process
301 Managers report process deviations and recommended corrective action to the respective Process
302 Owner. Authoritative process guide control is under the purview of the Process Owner.

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



316 **3.1.1 Roles**

317 The following abstract drawing (Figure 4) depicts process roles for the USMC, followed by a
318 description of these roles (Table 3).



319

320

Figure 4. CfM Roles

321

Table 3. CfM Defined Roles and Responsibilities

Description	Overall Responsibility
Role #1 CfM Process Owner	
<p>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.</p> <p>May delegate specific responsibilities to another individual within their span of control, but remains ultimately accountable for the results of the CfM process</p>	<ul style="list-style-type: none"> • 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



Description	Overall Responsibility
Role #2 CfM Manager	
<p>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.</p>	<ul style="list-style-type: none"> • 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 Tools Administrator	
<p>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.</p>	<ul style="list-style-type: none"> • 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
Role #4 CfM Analyst	
<p>The CfM Analyst trains Asset and Configuration Management specialists and other staff in Asset and Configuration Management principles, processes, and procedures.</p>	<ul style="list-style-type: none"> • 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 • 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



Description	Overall Responsibility
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.	<ul style="list-style-type: none"> 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

322

323 **3.1.2 Responsibilities**

324 Processes may span departmental boundaries; therefore, procedures and work instructions within
325 the process need to be mapped to roles within the process. These roles are then mapped to job
326 functions, IT staff, and departments. The process owner is accountable for ensuring process
327 interaction by implementing systems that allow smooth process flow.

328 The Responsible, Accountable, Consulted, Informed, Participant (RACI-P) model is a method
329 for assigning the type or degree of responsibility that roles (or individuals) have for specific
330 tasks. Table 4 displays the department-level RACI-P model for CfM.

331 **Responsible** – Completes the process or activity; responsible for action/implementation. The
332 degree of responsibility is determined by the individual with the ‘A’.

333 • **Accountable** – Approves or disapproves the process or activity. Individual who is
334 ultimately answerable for the task or a decision regarding the task.

335 • **Consulted** – Gives needed input about the process or activity. Prior to final decision or
336 action, these subject matter experts or stakeholders are consulted.

337 • **Informed** – Needs to be informed after a decision or action is taken. May be required to
338 take action as a result of the outcome. This is a one-way communication.

339 • **Participant** – Assists ‘R’ in the execution of the process and/or activity.

340 Table 4 establishes responsibilities for high-level process activities by organization.

341

Table 4. Responsibilities for Enterprise CfM

CfM Process Activities	MCNOSC	HQMC (C4)	MCSC	MCCDC	RNOSC	MITSC	Application or Service Owner	Tenant/Supported Command
CfM Planning	R	I	AP	C		C	C	P
Configuration Identification	R	I	AP	C		P	I	P
Configuration Control	R	I	AP	C		P	I	P



CfM Process Activities	MCNOSC	HQMC (C4)	MCSC	MCCDC	RNOSC	MITSC	Application or Service Owner	Tenant/Supported Command
Status Accounting and Reporting	R	I	AP	C	I	P	I	P
Audits and Verification	R	I	AP	C	I	P	I	P
<p><i>Legend:</i></p> <p><i>Responsible (R) – Completes the process or activity</i></p> <p><i>Accountable (A) – Authority to approve or disapprove the process or activity</i></p> <p><i>Consulted (C) – Experts who provide input</i></p> <p><i>Informed (I) – Notified of activities</i></p> <p><i>Participant (P) – Assists in execution of process or activity</i></p> <p><i>Note: Any department that is designated as Responsible, Accountable, Consulted, or Participant is not additionally designated as Informed because being designated as Responsible, Accountable, Consulted, or Participant 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.</i></p> <p><i>Note: Only one department can be accountable for each process activity.</i></p>								

342

343 **3.2 Policies**

344 This process requires the following policies for success:

345

346

1. Roles Established

347

348

349

Although the number of people involved will vary based on the size and complexity of the environment under the CfM scope, CfM will have a Process Owner who acts as adjudicator, a process manager, and other key roles.

350

2. C4 Guidance

351

352

Certain assumptions are made regarding this process. The following is C4 implementation guidance:

353

a. Audit intervals

354

b. Funding

355

c. Span of authority (ex. CAB structure)

356

d. Release definitions (ex. enterprise, regional, local)

357

e. Sponsorship and engagement

358

3. Awareness Campaign



359 A comprehensive awareness campaign is planned and carried out as part of process
360 implementation to ensure proper communication to users, stakeholders, and support
361 personnel.

362 4. Compliance with Governance requirements (see Appendix C for more information):

363 a. DIACAP: This process and supporting activities conform to DIACAP security
364 requirements.

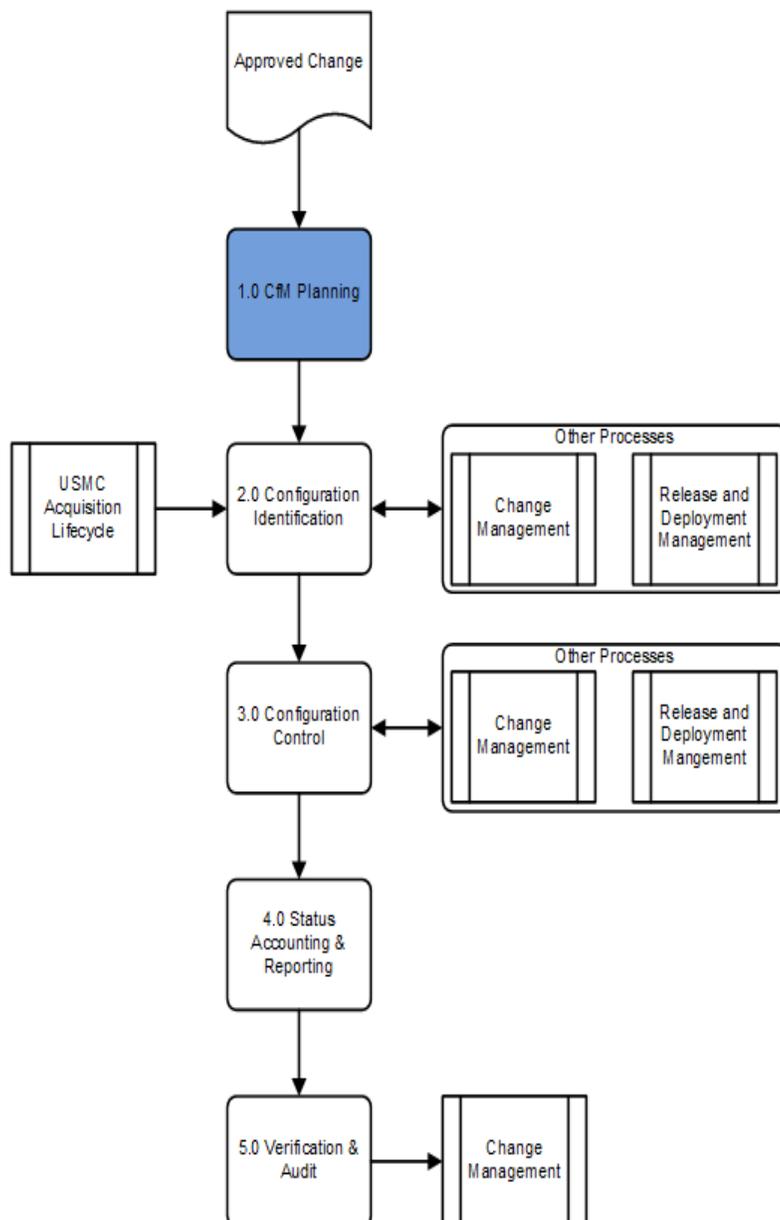
365 b. DoD compliance including Common Criteria Certification

366



367 **4.0 SUB-PROCESSES**

368 The USMC CfM process consists of five sub-processes. As depicted, the CfM process is
 369 responsible for identifying, controlling, recording, tracking, reporting, auditing and verifying the
 370 value and ownership of service assets throughout their lifecycles and for maintaining information
 371 about CIs required to deliver an IT Service (including their relationships).

372 **4.1 CfM Planning**

CfM Planning is required when the program is not ongoing or a new CI not defined or planned for is identified. This includes consulting with service design prior to the introduction of a new CI type. The CfM Planning activity consists of defining and articulating the strategy, policy, and scope of the CfM program.

The end product of the CfM Planning activity is the Configuration Management Plan, associated procedures and work instructions. The CfM Plan and procedures are developed by the CfM Manager at each level of oversight and control.

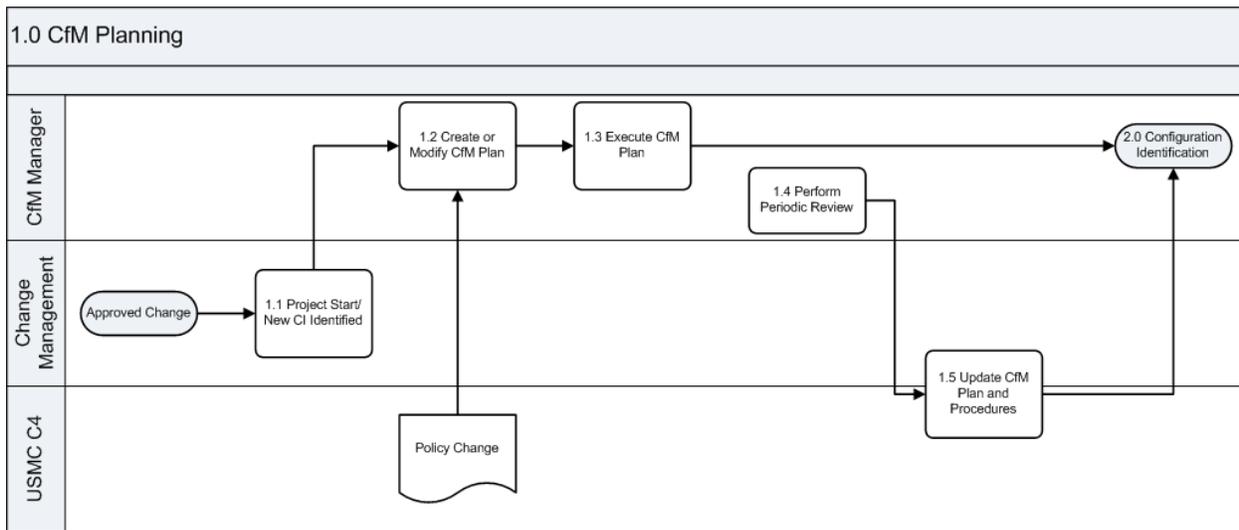
CfM Planning sets and documents:

- The objectives and key success factors of what should be achieved through CfM
- The organizational context within which CfM activities are to be implemented
- The interfaces and relationships to the Change Management and Release Management processes
- The location of the approved storage areas and libraries for hardware, software, and documentation

402



403 The following workflow (Figure 5) depicts the CfM Planning sub-process.



404

405

Figure 5. CfM Planning Sub-Process

406 Table 5 describes the CfM Planning sub-process steps as depicted in Figure 5.

407

Table 5. CfM Planning Sub-Process Descriptions

1.0 CfM Planning		
Number	Process Activity	Description
1.1	Project Start/New CI Identified	The CfM Planning Process begins with the initiation of projects and programs which introduce new CIs to the USMC infrastructure. The scope and level of configuration management oversight is driven by the terms within the contract, organizational/industry policies and standards and technical specifications invoked for the project. USMC projects and programs, to include Programs of Record such as MCEITS, are significant sources of new CIs requiring measured CfM planning activities.
1.2	Create or Modify CfM Plan	A CfM Plan (normally referred to as the Configuration Management Plan or CMP) is created based on many factors including: the contract, business drivers, funding, regulations, C4 and Command guidance, technical requirements, standards and applicable laws for the configuration of assets. Once created, the CMP is impounded in the DML as a documentation CI. The nomination of a USMC CfM Process Owner and the preparation of this process guide are examples of CfM planning activities. All USMC CMPs for any MCI or specific project are outputs of this activity.
1.3	Execute CfM Plan	As a project or program proceeds through its lifecycle, the CfM Plan is executed. Milestones trigger planned actions and reviews of the CfM Plan and associated procedures. CfM Managers at each level of oversight are responsible for the execution and review of these plans.



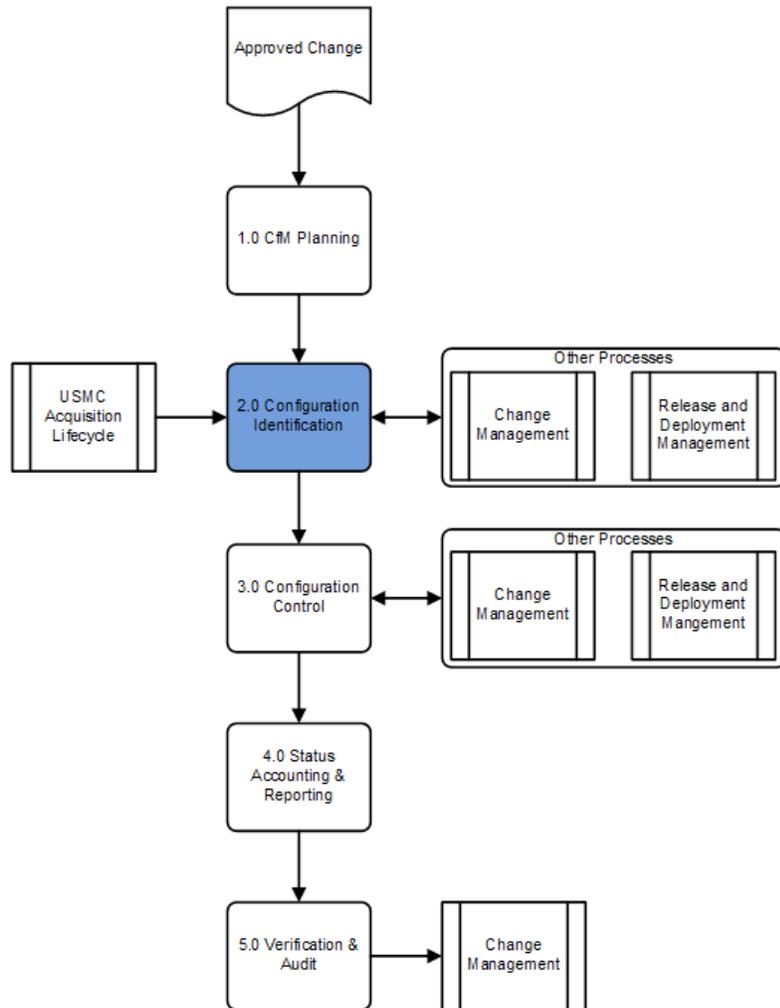
1.0 CfM Planning		
Number	Process Activity	Description
1.4	Perform Periodic Review	All Configuration Management planning documents are reviewed periodically. After the review of the documents and the current project situation, the CfM Plan may or may not be revised.
1.5	Update CfM Plan and Procedures	The CfM Plan and affected procedures are updated to reflect the decisions made during the project lifecycle. All iterations of the CfM Plan are checked in and out of the Documentation Library. Updates to the CfM Plan, while the responsibility of the CfM Manager, are under Change Control.

408

409



410 **4.2 Configuration Identification**

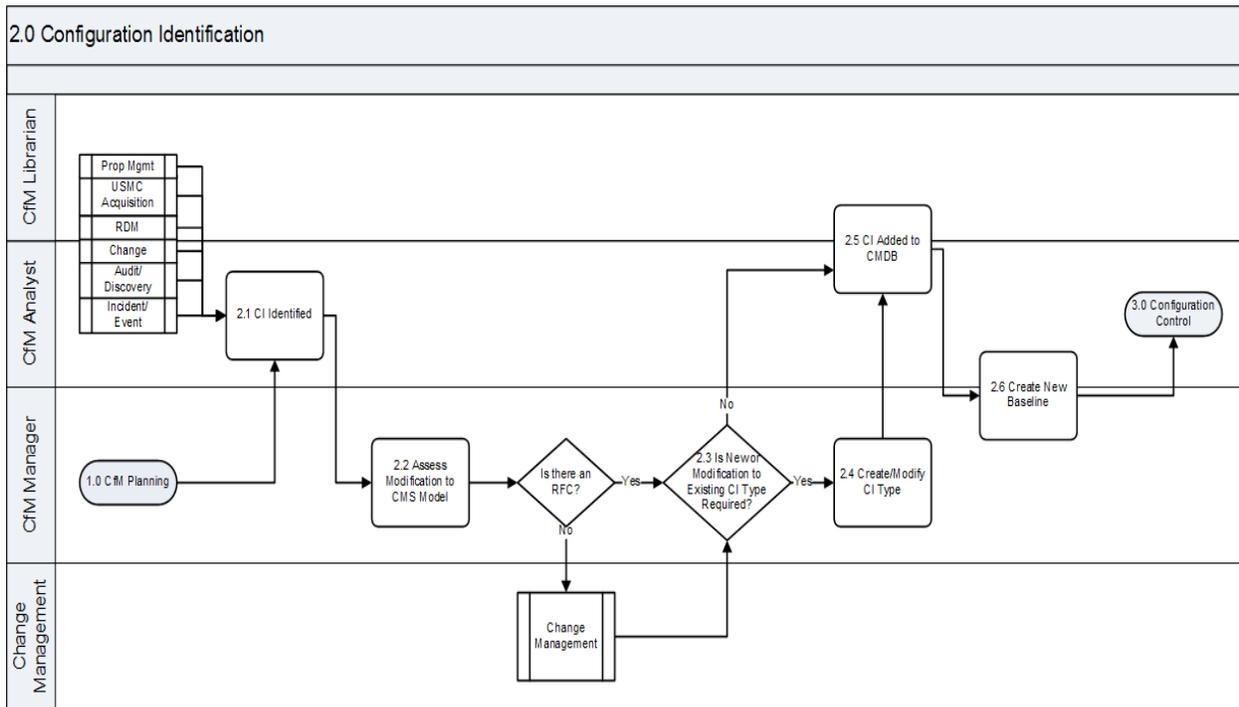


Configuration Identification is the selection, identification, and labeling of the services, configuration structures and CIs, including a CI's respective technical owner and relationships. CIs become the manageable unit planned for release into a configuration controlled environment. CIs consist of hardware, software, services, and documentation.

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



427



428

429

Figure 6. CfM Configuration Identification Sub-Process

430

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

431

Table 6. CfM Configuration Identification Sub-Process Descriptions

2.0 Configuration Identification		
Number	Process Activity	Description
2.1	CI Identified	<p>Triggered by a new CI from the Acquisition, Change, Release, or Audit/Discovery Tools process, a new CI is detected or created.</p> <ul style="list-style-type: none"> • During the initial population of a CMDB within the Configuration Management System (CMS), this discovery can be manual, automated, or both. • 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. All updates to the CMDB are handled through Change Management.
2.2	Assess Modification to CMS Model	<p>When a new type of CI is identified for inclusion within the CMS, a number of steps follow as applicable:</p> <ul style="list-style-type: none"> • Creating specific naming conventions for the CI type • Creating specific labeling conventions • Defining attributes for the CI type

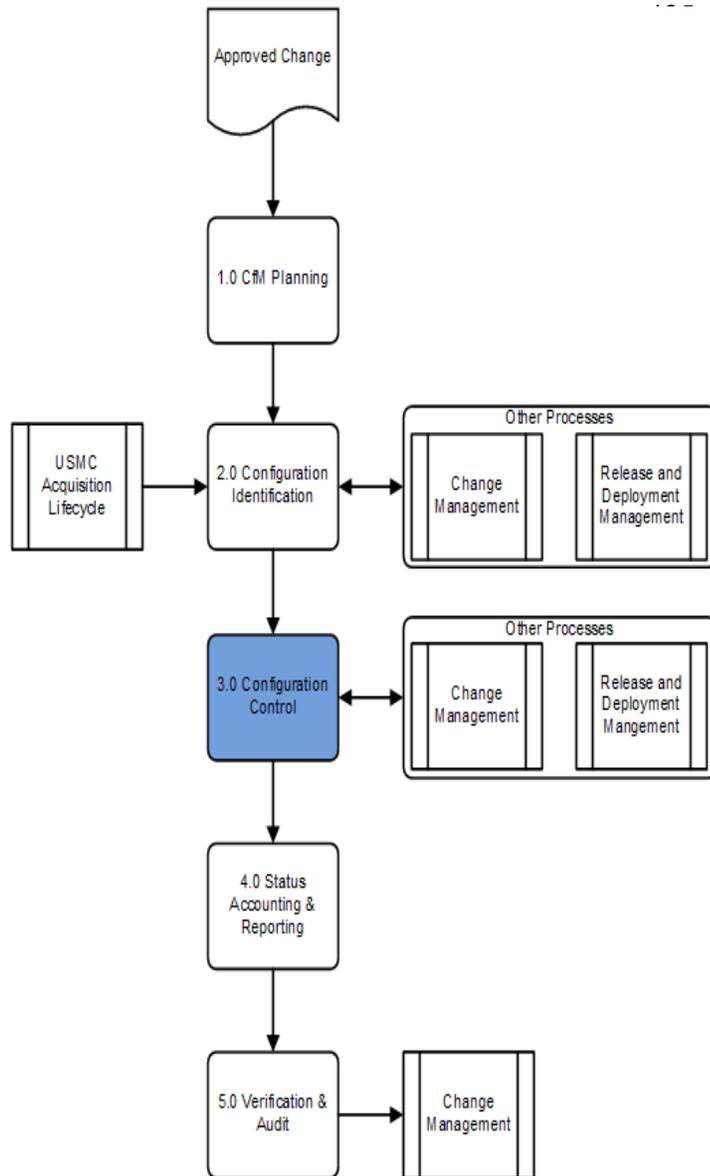


2.0 Configuration Identification		
Number	Process Activity	Description
		<ul style="list-style-type: none"> Defining documentation for the CI type Defining relationships to other CI types Adding a CI type can have an effect on existing reports and may involve modifications to the ITSM tool(s) workflow or schema. Review by the CfM Manager and Process Owner is required.
2.3	Is New or Modification to Existing CI Type Required?	Determine whether new CI requires creation of a new CI type or if it matches an existing CI type.
2.4	Create / Modify CI Type	The CI Type is created or modified to support the new variety of CIs added to the CMDB.
2.5	CI added to CMDB	CIs are added to the CMDB as a consequence of an automated function, import from another source, or manual data entry. Where manual update is necessary, the administration is completed by the CfM Librarian or Analyst.
2.6	Create New Baseline	When CIs (and CI types) are introduced to the CMDB, the initial state constitutes a baseline from which future changes are made. For the new CI type, the appropriate section(s) of the corresponding POR or Project Configuration Management Plan must be updated and submitted through Change Control.

432

433



434 **4.3 Configuration Control**

400

The objective of Configuration Control is to ensure that only authorized and identified CIs are installed in the infrastructure, and recorded and tracked in the CMDB. When a change is processed to a CI in the Change Management System, the change moves through a series of required process steps defined by the Change Management System. Procedural and technical controls ensure unauthorized change is virtually impossible. Licenses and maintenance support contracts are managed and updated as CIs. They can be added, updated, or deleted. All actions that drive Configuration Control are executed through the Change Management System. The Configuration Manager interacts in the Change Management process throughout the lifecycle of a change managing CI additions, modifications, and retirement requirements.

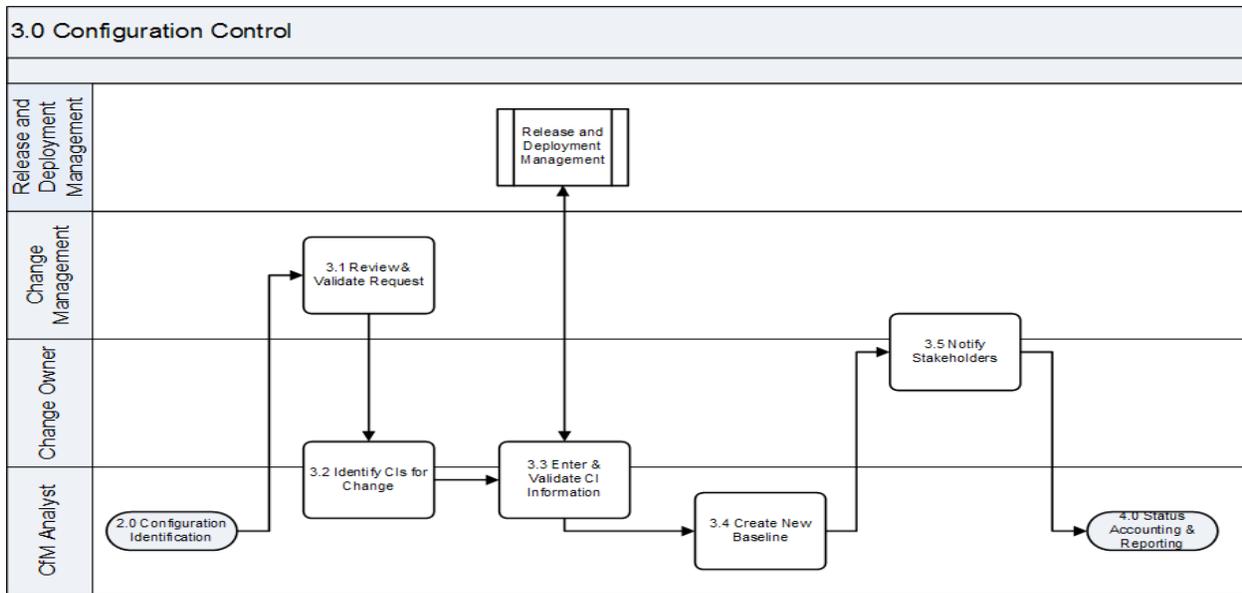
Changes to CIs are made via approved and released RFCs.

The Configuration Control activity updates the status of CIs as they progress from delivery to live use, decommissioning, and removal. Changes to attributes of CIs are recorded and related to the RFC that authorized the change.

467 Information Assurance (IA) activities around approval (in Configuration Control) and scanning
 468 for compliance (in Verification and Audit) do not appear within this document, but will appear at
 469 the next level down of the process workflow detail (level D of Figure 1. Process Design
 470 Pyramid).

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





472

473

474

Figure 7. CfM Configuration Control Sub-Process

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

476

Table 7. CfM Configuration Control Sub-Process Descriptions

3.0 Configuration Control		
Number	Process Activity	Description
3.1	Review & Validate Request	Analyze, define, formalize, negotiate, validate, and agree service requirements as they relate to the prevailing service request. RFCs are processed through Change Management (ChM), requiring configuration information. The ChM process passes information to and receives information from CfM throughout the change process.
3.2	Identify CIs for Change	CIs associated with the change are identified. Where appropriate, they are created to support the RFC. As part of the RFC preparation process, CIs are associated to/with the change.
3.3	Enter & Validate CI information	The ChM process results in approved or rejected changes. Ultimately, changes are successfully implemented, cancelled, or fail and are rolled back. After an approved change is released to the production environment, Release Management notifies ChM of the CIs updated within the CMDB (whether it is a change in CI status or an attribute change).



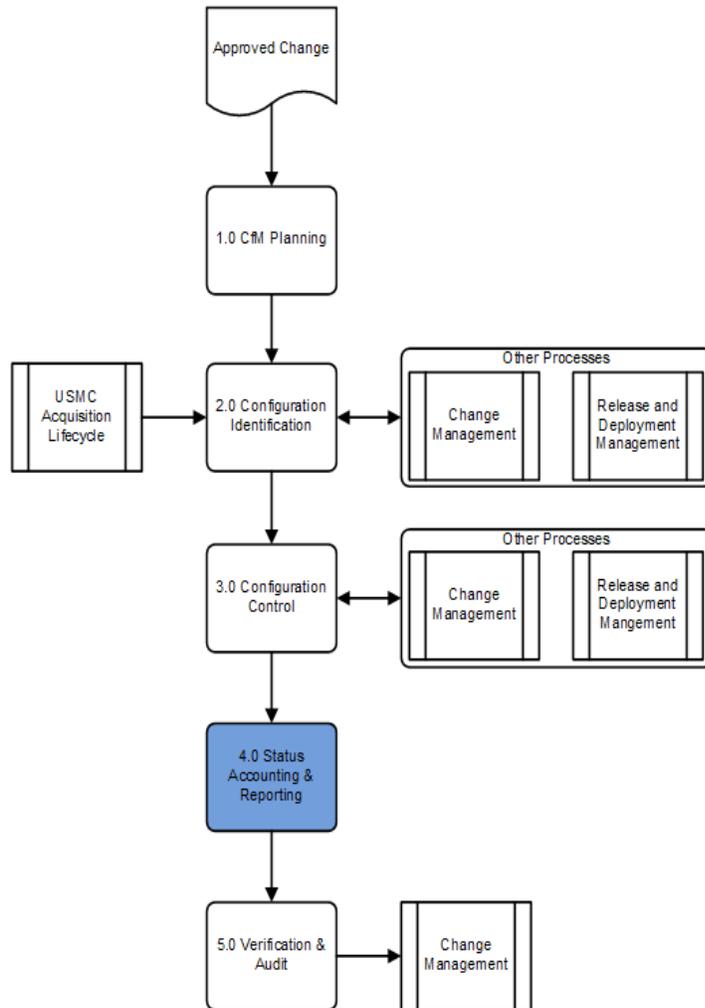
3.0 Configuration Control		
Number	Process Activity	Description
3.4	Create New Baseline	As specified in the CMP, a new baseline may be needed as a consequence of the change/release. CfM creates a baseline of all affected CIs involved in release of the new or modified service. Updates will reflect moves, repairs, installations, as well as system retirements.
3.5	Notify Stakeholders	Notification is a key activity within the ChM and CfM processes. Upon notification of delivery of services by the release manager, stakeholders are notified. Configuration update validation notification arrives from the ChM process during RFC review and close process. MCSC is notified of a new CI in the CMDB from acquisition and updates to status are provided throughout the asset life cycle.

477

478



479 **4.4 Status Accounting and Reporting**

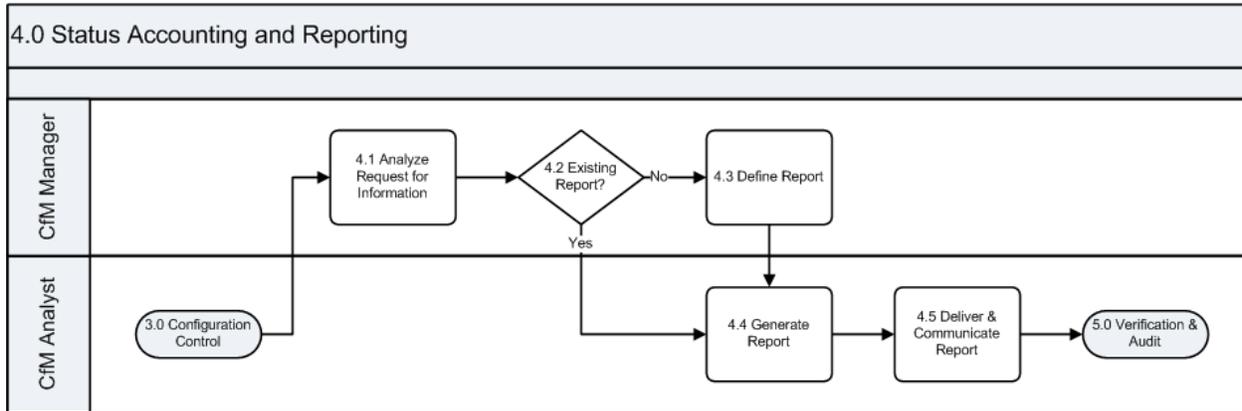


The Configuration Status Accounting and Reporting sub-process ensures all configuration data and documentation is recorded as each asset or CI progresses through its lifecycle. It provides the status of the configuration of a service and its environment as the configuration evolves through the service lifecycle.

Status Accounting and Reporting provides the current and historical data concerned with each CI that enables tracking of changes to CIs and their records (i.e., tracking the status as a CI changes from one state to another: procured, deployed, operational, and decommissioned).

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





501

502

503

Figure 8. CfM Status Accounting and Reporting Sub-Process

504

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

505

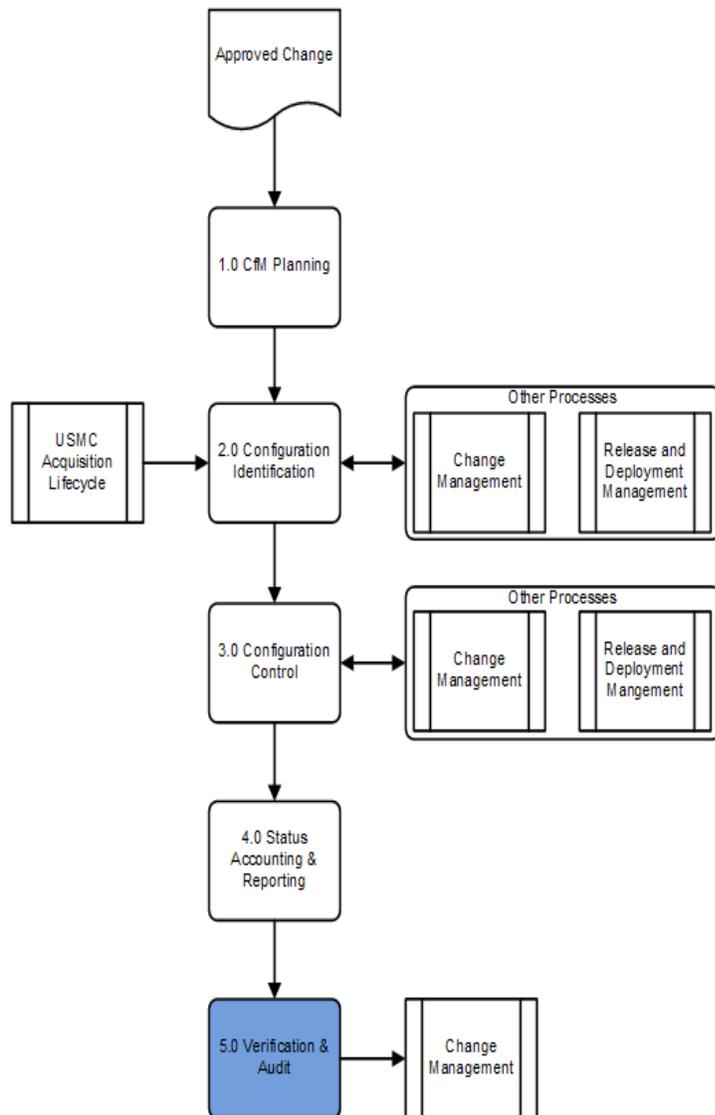
Table 8. CfM Status Accounting and Reporting Sub-Process Descriptions

4.0 Status Accounting and Reporting		
Number	Process Activity	Description
4.1	Analyze Request for Information	The Request for Information is 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: <ul style="list-style-type: none"> • 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.
4.5	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.

506

507



508 **4.5 Verification and Audit**

The Verification and Audit sub-process performs the inspection between the recorded data in the CMDB and the actual physical condition of the assets in the field. Verification is the process of comparing a work product with its parent specification or a standard for the purpose of detecting errors. Verification answers the question “Was the product built correctly?” Configuration audits provide the framework and the detailed requirements necessary to verify the development effort has successfully achieved all of the requirements specified in the configuration baselines.

This sub-process ensures conformity between documented baselines and the actual business environment to which they refer. The requirements necessary to implement the release are defined in this step. This responsibility is owned by the CfM Manager.

The CfM team participates in program and design reviews and conducts baseline audits in accordance with a defined audit procedure. Baseline audits are conducted on server hardware, software and network

539 components on an annual basis with more frequent audits based on the change and release
540 activity of the environment. Specific milestone requirements for conducting specifically defined
541 audits are supported.

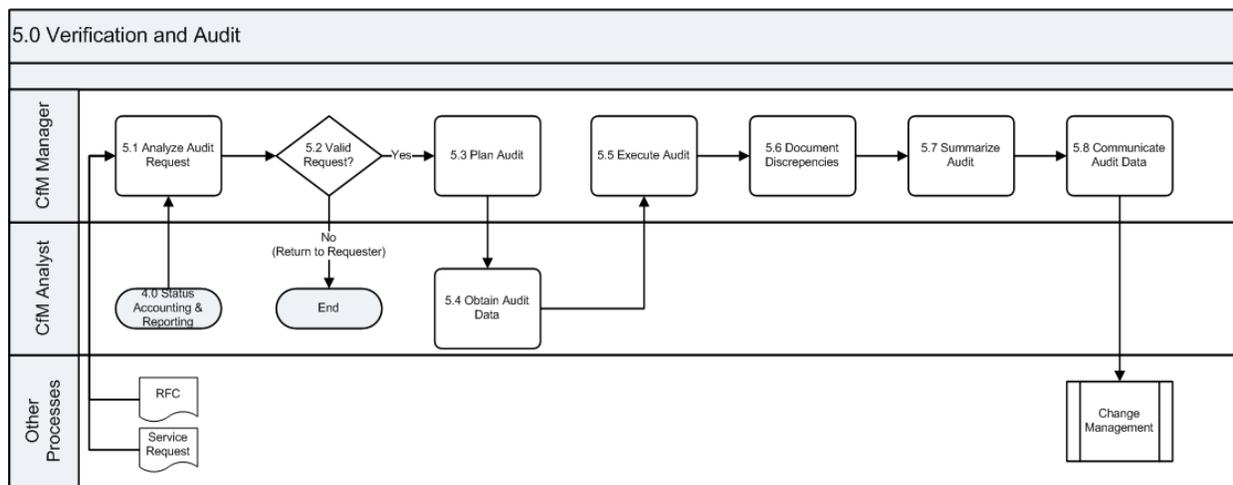
542 These audits help ensure:

- 543 • Changes to CIs are properly documented in the CMDB and all supporting documentation
- 544 • All CIs identified for specified baselines are present, and no extraneous CIs exist in the
545 baseline
- 546 • CIs are acquired into the product baseline according to the documented standards and
547 procedures



- 548 • No unlicensed or unapproved software is installed or in use in the environment
- 549 infrastructure
- 550 • Conformity between the documented baselines (e.g., agreements, interface control
- 551 documents) and the actual business environment to which they refer
- 552 • Verification of the physical existence of CIs in the organization or in the DML and spares
- 553 stores, the functional and operational characteristics of CIs and ensure the records in the
- 554 CMS match the physical infrastructure
- 555 • The release and configuration documentation is present before making a release

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



557

558

Figure 9. CfM Verification and Audit Sub-Process

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

560

Table 9. CfM Verification and Audit Sub-Process Descriptions

5.0 Verification and Audit		
Number	Process Activity	Description
5.1	Analyze Audit Request	<p>The requirements are reviewed and validated regarding the need for the audit. Configuration audits occur:</p> <ul style="list-style-type: none"> • 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



5.0 Verification and Audit		
Number	Process Activity	Description
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.
5.3	Plan Audit	<p>Planning for an audit involves four major activities:</p> <ul style="list-style-type: none"> • 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 <p>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.</p>
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	<p>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.</p> <p>Also documented and communicated is the remediation required to meet the baseline requirements of the reference model.</p> <p>The recommended course(s) of action are prioritized.</p>
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.



562

Appendix A – ACRONYMS

563

The official list of E-ITSM acronyms can be found through the link referenced below:

564

https://ips.usmc.mil/sites/pg10docr/pm_ccr/E-ITSM/Shared%20Documents/Forms/AllItems.aspx



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 <i>normal</i> 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 specifies 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.



567

Appendix C – POLICIES

568 References to industry governing policies and laws can be found through the link referenced
569 below:

570 https://ehqmc.usmc.mil/org/c4/projects/CP/eitsm/Shared%20Documents/E-ITSM_TO_13_Gover
571 [nment_Policies.doc](https://ehqmc.usmc.mil/org/c4/projects/CP/eitsm/Shared%20Documents/E-ITSM_TO_13_Gover)

