

***Enterprise IT Service Management
Release and Deployment 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	6
2.3.1	Process Description	8
2.4	Key Concepts	9
2.4.1	Release Policy	9
2.4.2	Service Design Package	10
2.4.3	Release Design Options	11
2.4.4	Designing Release and Deployment Packages	11
2.4.5	Release and Deployment Models	11
2.4.6	Release and Deployment Plans	12
2.4.7	Communications Plan	12
2.5	Quality Control	12
2.5.1	Metrics, Measurements and Continual Process Improvement	12
2.5.2	Critical Success Factors with Key Performance Indicators	13
3.0	Governance	15
3.1	Roles and Responsibilities	15
3.1.1	Roles	16
3.1.2	Responsibilities	18
3.2	Policies	20
4.0	Sub-Processes	21
4.1	Plan and Prepare	21
4.2	Design Release	24
4.3	Build Release	27
4.4	Service Validation and Testing	30
4.5	Plan and Prepare for Deployment	34
4.6	Deploy and Verify	38
4.7	Early Life Support	41
4.8	Review and Close	44
	Appendix A – Acronyms	46
	Appendix B – Glossary	47
	Appendix C – Policies	50

List of Tables

Table	Title	Page
Table 1.	RDM Process Activity Descriptions	7
Table 2.	RDM Release Policy – Minimum Requirements	9
Table 3.	RDM Critical Success Factors with Key Performance Indicators	13



Table	Title	Page
Table 4.	RDM Defined Roles and Responsibilities	16
Table 5.	Responsibilities for Enterprise RDM	19
Table 6.	RDM Plan and Prepare Sub-Process Descriptions	22
Table 7.	RDM Design Release Sub-Process Descriptions	25
Table 8.	RDM Build Release Sub-Process Descriptions	28
Table 9.	RDM Service Validation and Testing Sub-Process Descriptions.....	31
Table 10.	RDM Plan and Prepare for Deployment Sub-Process Descriptions	35
Table 11.	RDM Deploy and Verify Sub-Process Descriptions	39
Table 12.	RDM Early Life Support Sub-Process Descriptions	42
Table 13.	RDM Review and Close Sub-Process Descriptions	45

List of Figures

Figure	Title	Page
Figure 1.	Process Design Pyramid	2
Figure 2.	RDM Relationship with other Initial Processes	4
Figure 3.	High-Level RDM Workflow.....	6
Figure 4.	RDM Roles	16
Figure 5.	RDM Plan and Prepare Sub-Process	22
Figure 6.	RDM Design Release Sub-Process.....	25
Figure 7.	RDM Build Release Sub-Process.....	28
Figure 8.	RDM Service Validation and Testing Sub-Process	31
Figure 9.	RDM Plan and Prepare for Deployment Sub-Process.....	35
Figure 10.	RDM Deploy and Verify Sub-Process.....	39
Figure 11.	RDM Early Life Support Sub-Process	42
Figure 12.	RDM Review and Close Sub-Process	45



Enterprise IT Service Management Release and Deployment 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 IT activities are executed in a uniform manner.

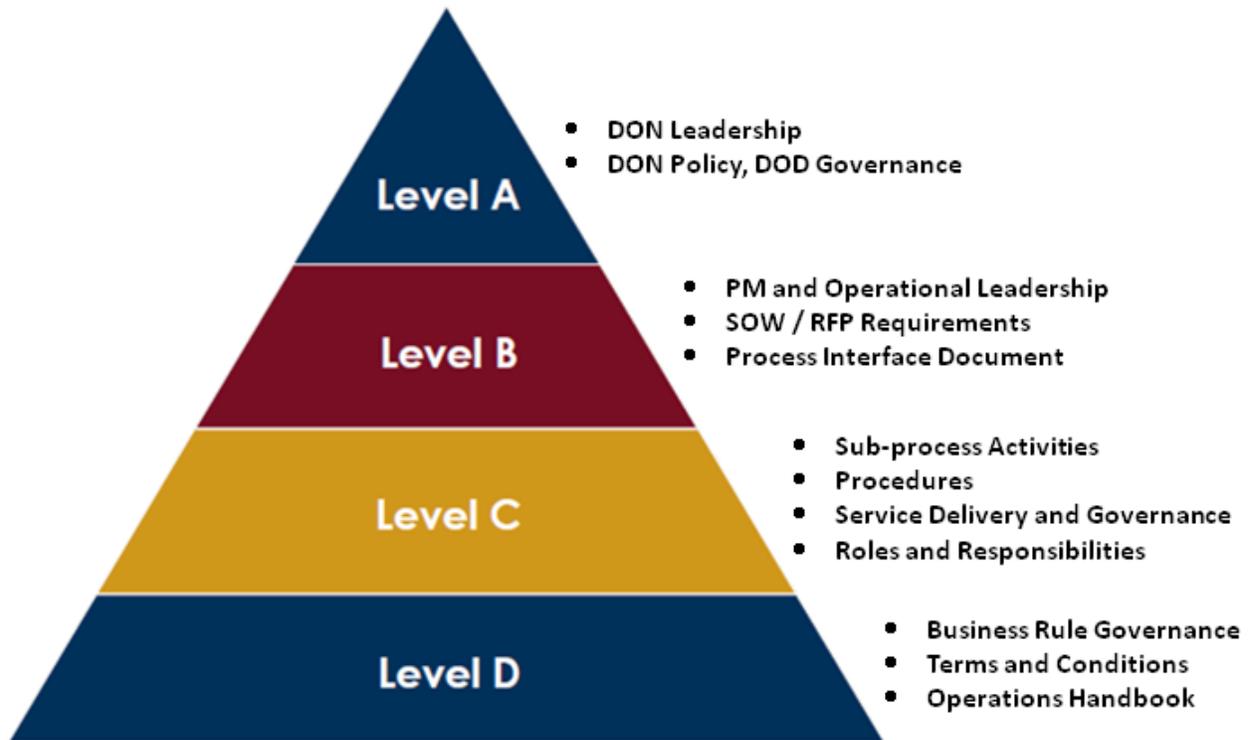
8 1.2 Scope

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

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

23 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
24
25
26





27

28

Figure 1. Process Design Pyramid

29 1.3 Document and Process Change Procedures

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

37



38 2.0 PROCESS OVERVIEW

39 2.1 Purpose, Goals, and Objectives

40 The primary purpose of Release and Deployment Management (RDM) is to ensure that releases
41 and deployments are thorough, supportable, and provide minimal impact to current operations.

42 The goal of RDM is to deliver releases into production, establish the effective use of the service
43 while providing value to the customer, and execute a transparent hand-off to service operations.

44 The RDM objective is to plan, schedule and control the movement of releases to both test and
45 live (i.e., production) environments. Additional objectives include:

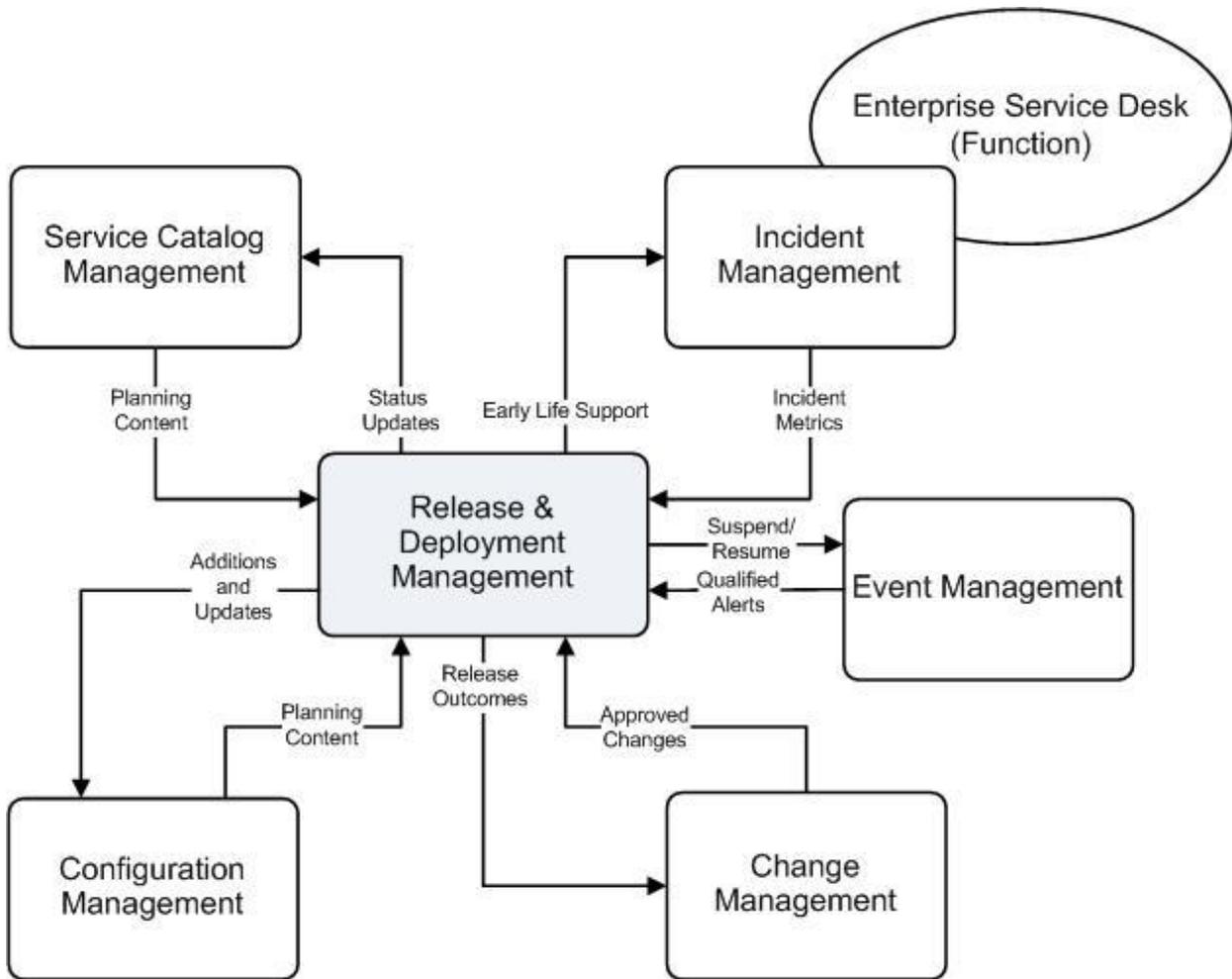
- 46 • Establishing a clear and comprehensive RDM plan that enables the customer and receiving
47 services to align their activities with the release plans
- 48 • Ensuring a release package can be built, installed, tested, and deployed successfully on time
- 49 • Validating that new or changed services contained in the release deliver the agreed service
50 requirements, utility and service levels
- 51 • Minimizing unpredicted impacts to production, service operations and organizations
- 52 • Ensuring customers and stakeholders accept and are satisfied with the release, and that
53 supporting documentation and training is appropriately pushed into production.

54 2.2 Relationships with other Initial Processes

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

62





63

64

Figure 2. RDM Relationship with other Initial Processes

65 The following list describes the RDM relationship (input or output) to other Initial Processes, as
66 depicted in Figure 2:

67 **Service Catalog Management**

68 — Planning Content: As the definitive source of record for services that are present in
69 the Configuration Management System (CMS), Service Catalog Management (SCM)
70 provides rapid, at-a-glance views into key service attributes to include availability
71 targets, maintenance windows, and change freeze periods.

72 — Status Updates: The Service Catalog's value is dependent on the accuracy of its
73 contents. As releases are deployed, status updates are received from Release and
74 Deployment Management and implemented in the Service Catalog (based on
75 approved RFCs).



76 Incident Management and the Service Desk

- 77 — Early Life Support: Early Life Support (ELS) is the additional expert service support
78 provided immediately after deployment to ensure service continuity and stakeholder
79 satisfaction. RDM proactively supports deployment activities in the ELS process step
80 by providing Incident Management an advanced level of training, documentation, and
81 high-touch support as the new service is introduced into production.
- 82 — Incident Metrics: Incident metrics associated with releases are critical to continual
83 process improvement.

84 Event Management

- 85 — Suspend/Resume: RDM notifies Event Management (EM) to suspend monitoring of
86 services or service components that will be interrupted or otherwise affected for the
87 duration of the deployment activity. This ensures that false incidents are not triggered.
88 RDM also notifies EM to resume monitoring once deployment activities have
89 completed.
- 90 — Qualified Alerts: EM notifies RDM about unusual events occurring after a release.

91 Change Management

- 92 — Authorized Changes: RDM will not deploy a release in the absence of a
93 corresponding and authorized Request for Change (RFC). Additionally, any
94 constraints associated with the authorization, such as the start and end time of the
95 release, are provided by this input.
- 96 — Release Outcomes: RDM “closes the loop” on authorized changes by informing the
97 Change Management (ChM) process with the outcome of the release. For example,
98 was the release successfully deployed within the approved window or did it extend
99 beyond this window? What was the outcome of post-implementation testing? Did the
100 release result in any incidents? This vital information enables ChM to determine how
101 best to position the RFC associated with this release.

102 Configuration Management

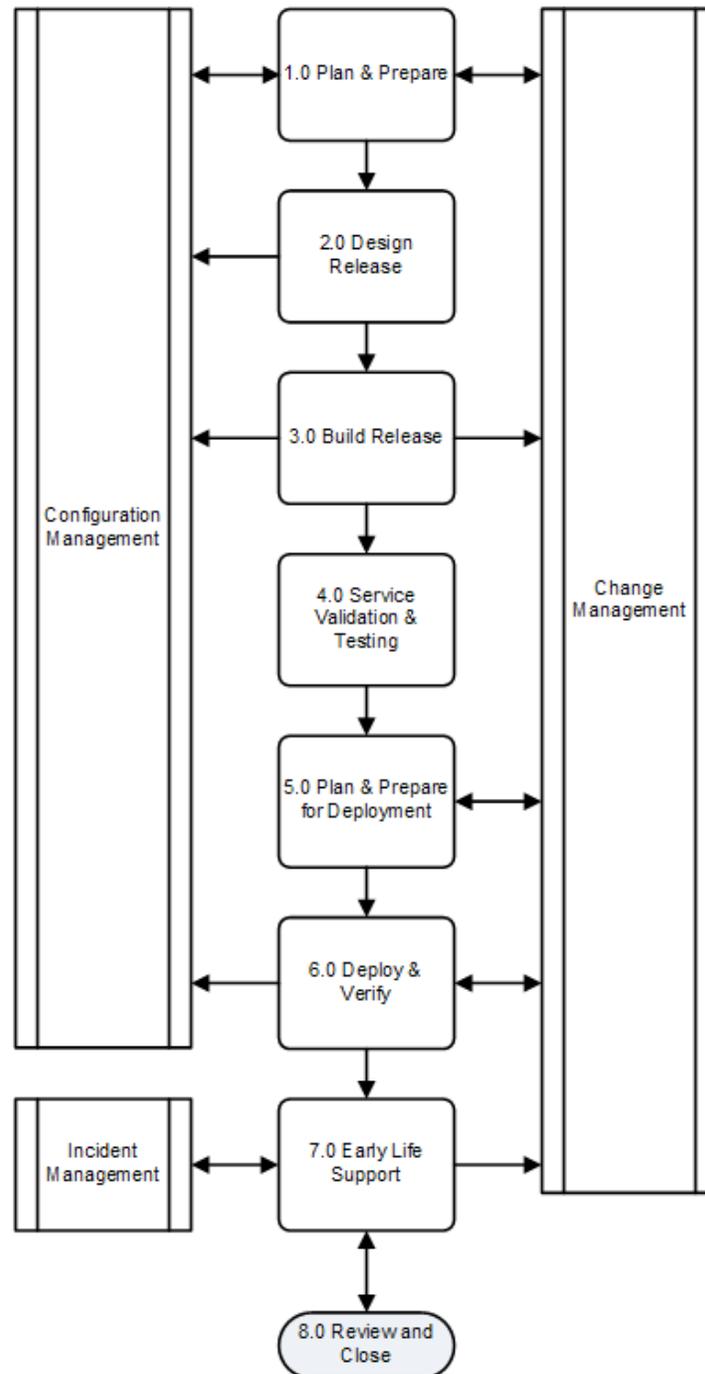
- 103 — Planning Content: The Configuration Management Database (CMDB) and supporting
104 processes provide invaluable information for the purposes of planning, preparing, and
105 designing a release. In the presence of an accurate CMDB, it is not necessary to
106 inventory the environment to predict work effort and manpower required to propagate
107 a large-scale enterprise release.
- 108 — Additions and Updates: The CMDB is updated as Configuration Items (CIs) are
109 introduced or updated to ensure it accurately reflects the as-deployed environment.

110



111 2.3 High-Level Process Model

112 The RDM process consists of eight distinct sub-processes and is highly integrated with the ChM
113 and Configuration Management (CfM) processes. The following workflow (Figure 3) depicts
114 these processes and sub-processes that collectively enable and underpin RDM. See Section 4.0
115 for complete descriptions of the sub-process activities.



116

117

Figure 3. High-Level RDM Workflow



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

120 **Table 1. RDM Process Activity Descriptions**

Number	Process Activity	Description
1.0	Plan and Prepare	<p>A release plan, high-level test plans and acceptance criteria are documented in the ChM Plan for the specified project and approved by ChM. RFC approvals are managed in ChM with input from RDM.</p> <p>The release plan is developed by the RD Manager. Approval requirements for the release plan will vary depending on the release size (Full, Package, or Delta), complexity, risk, and urgency.</p> <p>Each USMC base is responsible for their local plans. The motivating force is to complete Operational Directives (OpDirs). New and complex releases that involve acquisitions are supported by the Marine Corps Systems Command (MCSC).</p>
2.0	Design Release	<p>What needs to be built for the release and how it will be assembled and deployed is defined providing the overall testing approach for the Service Validation and Testing process through early build to final deployment. Necessary install scripts and mechanisms for testing and monitoring the install are designed at a high level. All Release documents are drafted in the design phase. Remediation procedures are developed for back-out if the deployment is unsuccessful.</p> <p>MCSC provides for the acquisition of IT and is involved with the full lifecycle.</p>
3.0	Build Release	<p>Procedures, tools, and checklists that come from the Design Release are utilized to provide repeatable practices and expected results. The deploying software capabilities are utilized.</p> <p>Baselines are recorded before and after the release package build to provide restore capability if needed in production.</p> <p>The proposed solution and test results are recorded and handed over to Service Operations for use in future releases.</p> <p>The USMC Program Manager for the Program of Record (POR) is responsible for the build release.</p>
4.0	Service Validation and Testing	<p>Service Validation and Testing performs a number of iterations throughout the Release and Deployment lifecycle:</p> <ul style="list-style-type: none"> • Verifies that the deployment team, tools, and procedures can deploy the release package into a target deployment group or environment within the estimated timeframe. • Ensures the release package contains all the service components required for deployment by initiating in a test environment and performing a configuration audit. • Validates the defined Service-Level Requirements for deploying into production are achievable and sustainable. • Ensures the proposed changes do not adversely affect authorized systems in the production environment. • Ensures authorized configurations and systems in the production environment do not have an adverse impact on the proposed application or change. • Tests the deployment team, tools, and procedures can install the release package into a target environment within the estimated timeframe. • Tests a deployment has completed successfully and that all service assets and configurations are in place as planned and meet their quality criteria. <p>The Systems Integration Environment (SIE) managed by MCSC, provides a test and integration function for systems, applications, or services destined for or residing in the Enterprise IT Center (EITCs).</p>
5.0	Plan and Prepare for Deployment	<p>With recommendations from the Service Validation and Testing process, the RD Manager presents to the ChM Change Advisory Board (CAB) the testing report for review. The ChM CAB approves the release to be deployed. Deployment resources are assigned. Readiness assessments are conducted. Risks are</p>



Number	Process Activity	Description
		identified and assessed in terms of potential disruption. Detailed implementation and backout plans are finalized and verified. When the detailed deployment plan is complete and readiness tests performed, the service is ready for deployment. The MCSC works with MCNOSC for implementation of the infrastructure.
6.0	Deploy and Verify	Deploying the release is the execution of the detailed deployment plan. A deployment can be installing of materials (hardware or software) and processes, the transfer of a service, the deployment of a new or changed service, the decommissioning or retirement of services, and/or the removal of assets. When complete, the RD Manager verifies the release with the stakeholders. Successful validation of the deployment triggers the launch of ELS. The MCSC works with MCNOSC during deployment of a new service or major upgrade.
7.0	Early Life Support	ELS is the additional expert service support provided immediately after deployment to ensure service continuity and stakeholder satisfaction. Resources from IT Operations introduce the new service capability and resources to operations in a controlled manner. Resource support scope is determined by the release content delivered. The MCNOSC service desk supports infrastructure releases. MCTSSA maintains a 24x7 helpdesk capable of providing support to deployed units managing tactical applications in the field.
8.0	Review and Close	The RD Manager conducts a review to ensure all RDM requirements for the RFC were met. The entrance and exit criteria for each stage of the process has been assessed and met. RDM updates the RFC in ChM and the RD Manager issues a close notification with the final review. All release participants and end users are notified of the final review results for the release.

121

122 2.3.1 Process Description

123 The purpose of RDM is to build, test, and deliver capabilities to provide services as specified in
124 Service Design to accomplish the stakeholder's requirements and deliver to Service Operations
125 the planned objectives with little or no impact to the customer.

126 Release Management is responsible for planning, building, testing, and controlling the release of
127 a new or changed service in test environments. In the pre-production environment, the integrity
128 of the new or changed service is tested and validated as a quality function before deploying into
129 the production environment.

130 Deployment Management is the process that follows Release Management by which a new or
131 changed service is moved to the live or production environment once testing is complete.

132 The scope of RDM, therefore, includes the processes, systems, and functions to package, build,
133 test and deliver a release into production, establishing the service specified in the Service Design
134 Package (SDP) before a hand-off to service operations.

135 The RDM process supports:

- 136 • Implementation planning, including the back-out plan of a release as well as required
137 resource plans
- 138 • Release preparation, including the distribution of hardware, software and support tools



- 139 • Preparation training, including the customer/user, operations, service desk and
140 implementation team for the release deployment
- 141 • Testing plans, supporting production testing, end user acceptance testing and back-out testing
142 procedures
- 143 • Controlled introduction testing (beta testing) after a cutover
- 144 • The RDM process adds value to the USMC by:
- 145 • Delivering change faster with minimum risk
- 146 • Assuring customers/end users can use the new or changed service as designed to support the
147 mission
- 148 • Improving consistency in implementation approach across the USMC environment
- 149 • Contributing to the auditing requirements for traceability

150 2.4 Key Concepts

151 The following is a description of concepts unique to RDM:

152 2.4.1 Release Policy

153 The Release policy defines the roles and responsibilities for the release part of RDM. The policy
154 covers release numbering, frequency, and the level of infrastructure that may be controlled by a
155 definable release. A policy may address all aspects of release for an organization, or the policy
156 can define the guidelines with additional supporting documentation for defining specifics for
157 each system or IT service.

158 Table 2 shows the minimum requirements for an RDM Release Policy.

159 **Table 2. RDM Release Policy – Minimum Requirements**

Item	Description
Release Unit	Describes the portion of the service or IT infrastructure to be released. The unit may vary in type or size of asset or CI, such as hardware or software. The size and impact of the release unit varies. Factors to be considered include ease and amount of change necessary; the amount of resources and time needed to build, test, distribute, and implement; the complexity of the interfaces affected by the release unit; and the storage available in the environment to perform the release activities of build, test, distribution, and going live. When building release units, the biggest factor to be considered is the potential impact to the user/customer. If the release unit can cause an outage to a critical system, the risk will need to be identified and planned for accordingly.
Release Identification	This is the unique release identification scheme and can be defined as: <ul style="list-style-type: none"> • Major release, billing system, v1, v2 • Minor release, billing system, v1, v2 • Emergency fix, billing system, v1, v2



Item	Description
Type of Release	<p>Full – A release that includes all components of the release unit. These components will be built, tested, distributed, and implemented together. This release is a completely new version of an application (e.g., Windows XP replaced by Vista). All components of the release unit are purchased/built, tested, and distributed together.</p> <p>Package – A combination of a delta release unit and/or full release to reduce the frequency of roll-outs or to build, test, and roll-out related releases which can influence each other. Individual changes (to software and/or hardware) may be grouped together into package releases in every instance where it is beneficial to do so without undue risk to the business. Each technical domain determines the specific requirements to identify those changes that can be safely grouped together.</p> <p>Delta – A delta, or partial, release is one that includes only CIs within the release unit that have actually changed or are new since the last full or delta release.</p>
Category of Release	<p>Major – Contains a large planned upgrade of an IT service with major new functionality.</p> <p>Minor – Contains a smaller update between major releases with small improvements or corrections.</p> <p>Emergency – Contains an urgent release, for example, a fault in the infrastructure that causes multiple or major incidents. An emergency fix cannot wait until the next major or minor release.</p>

160

161 2.4.2 Service Design Package

162 The Service Design Package (SDP) is regarded as the entirety of information required to
 163 effectively plan, deliver, and support an IT service. The SDP manages an IT service through all
 164 stages of its life cycle and interacts with Service Catalog Management, Service Portfolio
 165 Management, Life-Cycle Management, Financial Management, and Service Level Management.
 166 SDP encompasses all elements of the plan in the package from the concept in a development
 167 vacuum to production and retirement. Ideally, a mature SDP is available prior to entering the
 168 RDM process.

169 Major components of an SDP are:

- 170 • Overview – Provides the basic information like the name of the service and workflow
 171 approvals.
- 172 • Detailed Requirements – Specifies in more detail what conditions the new service and its
 173 underlying applications and infrastructure must fulfill, providing all information which is
 174 needed for building the new service.
- 175 • Technical and Organizational Implementation Blueprint – Details what must be done during
 176 Service Transition to meet the specified requirements.
- 177 • Planning Information – Sets an intended time frame for the service implementation and
 178 estimates the required resources. This information may be updated later by ChM or RDM.

179 The SDP will conform to ITILv3 standards. Initially the SDP will contain the following
 180 mandatory information:

- 181 • Unique identifier of the service
- 182 • Description of the service



- 183 • Service design plan
- 184 • Service transition plan
- 185 • Service operation and support plan
- 186 • Service improvement information

187 **2.4.3 Release Design Options**

188 There are several options for a release in the large and complex Marine Corps Wide (MCW)
189 environment. More than one approach is expected for transitioning from the current service to
190 the new or changed service. The most commonly used options are described below:

191 *Big Bang vs. Phased Option* – Big Bang – a new or changed service is deployed to all user areas
192 in one operation (introducing an application). Or, phased approach – the service is deployed in
193 phases, and the deployment is incrementally repeated until the service is fully deployed (by unit,
194 or base).

195 *Push–Pull* – The push approach is executed when a service is deployed from the center (a
196 headquarters organization), followed by deployment to target locations. The push approach is
197 used for updating service components. A pull approach is employed for software releases where
198 software is made available at a central location and users can access the location to pull down the
199 software at their convenience (i.e., software version upgrades). Pull is optimal when the software
200 is restricted by licensing to a select group of users.

201 *Automated vs. Manual* – The deployment choice of automation or manual is determined in
202 release planning. When a release can be automated, the benefit of repeatable and consistent
203 actions, along with the efficient use of release resources is realized. Automated deployment
204 requires extensive testing to avoid unnecessary problems but completes quicker and more
205 efficiently since it does not require as many resources as a manual deployment. Manual
206 deployments require closer monitoring, but sometimes are unavoidable.

207 **2.4.4 Designing Release and Deployment Packages**

208 The scope and content of each release package is defined within the Release Plan for that release.
209 The release and deployment team must understand the relevant architecture to plan, package,
210 build and test a release. This knowledge helps to prioritize the release and deployment activities
211 and manage dependencies. The dependencies can be identified by viewing service architectural
212 elements in the Technical Service Catalog. The dependencies are built and tested by Service
213 Validation and Testing. Coordination with the Program of Record (POR) team occurs during the
214 design phase.

215 **2.4.5 Release and Deployment Models**

216 Service Design selects the most suitable release and deployment model including the approach,
217 mechanisms, processes, procedures and resources required to build and deploy the release on
218 time and within budget. Elements of the release and deployment models include: the release
219 structure for building a package and target environments, the exit and entry criteria for each



220 stage, the controlled environments for building and testing each release level, the roles and
221 responsibilities for each Configuration Item (CI), the release promotion and configuration
222 baseline, the release and deployment schedules, support activities for documenting and tracking
223 the release activities, and the hand-off activities and responsibilities.

224 **2.4.6 Release and Deployment Plans**

225 Release and deployment plans must be reviewed by all stakeholders. They include:

- 226 • Scope and content of release
- 227 • Risk assessment of the release
- 228 • Organizations and stakeholders affected
- 229 • Stakeholders that approve the release
- 230 • Teams responsible for the release
- 231 • Approach for working with the stakeholders and the deployment groups to develop the
232 delivery and deployment strategy, resources and amount of change that can be supported.
- 233 • Communication Plan

234 The release plan identifies the modifications or updates to the catalog along with the release
235 objectives in relation to the mission's goals. Release components and specific deliverables must
236 be captured in detail in the plan. A release plan is developed with consensus of all stakeholders.

237 **2.4.7 Communications Plan**

238 The communication plan is a component of the Release and Deployment Plan and is required for
239 certain types of releases. The goal of the communications plan is to continuously inform all
240 stakeholders at critical gates of relevant issues at each stage of the release. Additionally, Service
241 Management processes not directly involved in the release could be affected by the release and
242 need to be kept informed, and at times consulted about the Release.

243 **2.5 Quality Control**

244 **2.5.1 Metrics, Measurements and Continual Process Improvement**

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



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

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

259 2.5.2 Critical Success Factors with Key Performance Indicators

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

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

266 Table 3 describes the metrics that will be monitored, measured, and analyzed:

267 **Table 3. RDM Critical Success Factors with Key Performance Indicators**

CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Benefits
1	Releases are implemented efficiently and effectively	1	% of release success rate Calculation: 1 minus (the number of failed releases divided by the total number of releases implemented)	Minimal risk and service disruption. A release package can be built, installed, tested, and deployed efficiently, successfully, and on schedule.
2	Releases are of high quality	2	Release Incident Rate Calculation: The number of releases resulting in Incidents divided by the total number of releases implemented	Satisfied stakeholders and end users. Production services are protected from adverse impacts of change. There is minimal unpredicted impact on production services, operations, and support organizations.
		3	Service Validation and Testing shows % of releases that do not result in a defect Calculation: Releases with no linked defects over all releases.	
		4	Average number of known errors per release. Calculation: The number of known errors by category by release over time	
3	Production services are protected from adverse impacts of change	5	% of Approved releases that do not result in an incident Calculate: Releases with no linked incidents over all releases	Minimal unpredicted impact on production services, operations, and support organization.



CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Benefits
4	Releases implemented in a timely manner	6	% of releases implemented in the approved release implementation window Calculation: Release work orders marked "complete" within the approved implementation window	A higher percentage of on-time release deployments delivers a greater percentage of expected functional performance on time and ensures resources required to support the release are used effectively and efficiently.

268



269 3.0 GOVERNANCE

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

- 272 • Who makes directing, controlling, and executing decisions
- 273 • How the decisions are made
- 274 • What information is required to make the decisions
- 275 • What decision making mechanisms should be required
- 276 • How exceptions are handled
- 277 • How the governance results should be reviewed and improved

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

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

286 3.1 Roles and Responsibilities

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

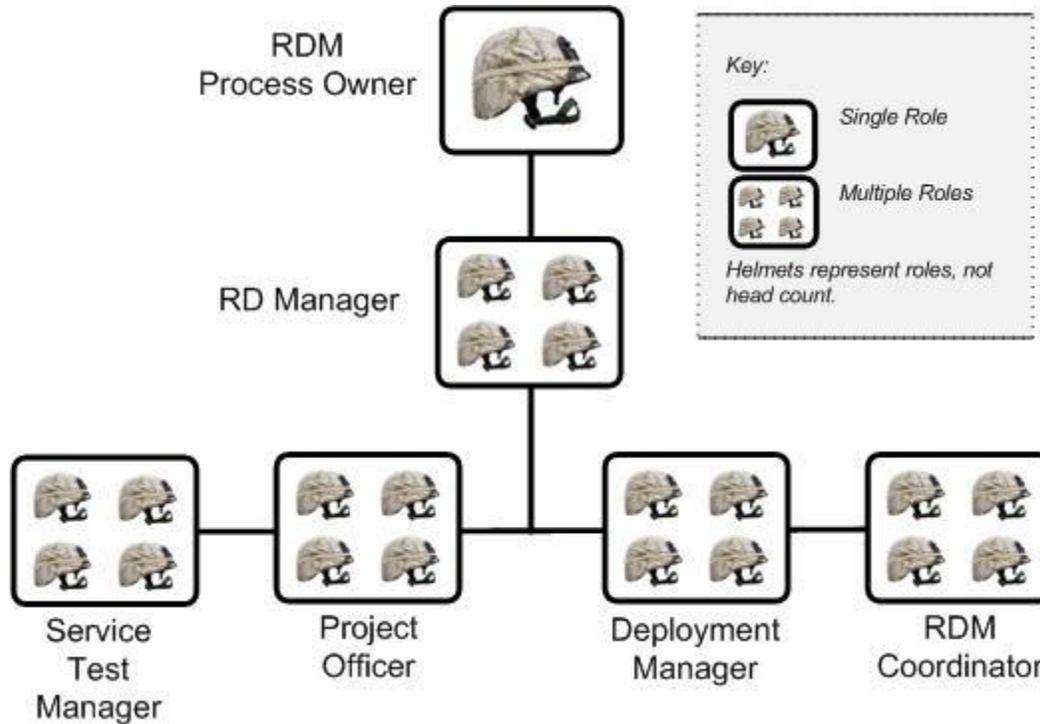
291 While the end goal is to have a single RDM Process Owner residing at the Enterprise Level, the
292 USMC will initially use a shared process ownership framework. There will be a RDM Process
293 Owner for the Acquisition sector inclusive of all USMC IT Programs of Record, as well as a
294 RDM Process Owner for the Operational sector inclusive of all other USMC organizations at the
295 enterprise, regional, and local levels.

296 Management (i.e., responsibility) of a process may also be shared; generally, a single manager
297 exists at the MCNOSC enterprise and at each MITSC. However, as with many other processes
298 within Service Design and Service Transition, RD managers also exist within
299 MARCORSYSCOM and Programs of Record. Process roles do not equate to billets; there will
300 be instances where roles are combined or a person is responsible for multiple roles. Factors such
301 as Area of Responsibility (AOR), size of user base, and size of the process support team dictate
302 exactly which roles require a dedicated person(s) and the total number of persons performing
303 each role. This process guide defines all *mandatory* roles.



304 **3.1.1 Roles**

305 The abstract drawing shown in Figure 4 depicts the mandatory process roles for USMC,
306 followed by a description of these roles in Table 3.



307
308

Figure 4. RDM Roles

309

Table 4. RDM Defined Roles and Responsibilities

Description	Overall Responsibilities
Role #1 RDM 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</p>	<ul style="list-style-type: none"> Identifies and manages the process CSFs Defines and communicates process purpose, goals, policies and procedures, responsibilities, and accountabilities Facilitates the process to produce user satisfaction Approves measurements, targets, and reporting to improve the efficiency and effectiveness of the process Reports on and communicates process performance Decision maker on any proposed enhancements to the process Consults with release and deployment managers



Description	Overall Responsibilities
results of the RDM process.	
Role #2 RD Manager	
<p>Responsible for the detailed tasks of running an effective release and deployment process. This includes a plan, design, build, configuration, and test of the hardware and software involved in the package on the release side.</p> <p>The RD Manager decides what resources are needed, especially with a full or major release which may require the Deployment Manager and the Project of Record Officer.</p> <p>The RD Manager communicates regularly with the other RD managers, coordinators, the RDM Process Owner, and other process managers as needed.</p>	<ul style="list-style-type: none"> • Manages all aspects of the end-to-end release process • Represents RDM on the CAB • Updates CfM and ChM through notifications • Ensures coordination of build and test environment with the release teams • Ensures teams follow the organization's established policies and procedures • Provides management reports on release progress, service release and deployment policy and planning • Deals with the release package design, build, and configuration • Oversees creation of the release package • Facilitates release package acceptance, including the authorized sign-off • Deals with service roll-out planning, including the method of deployment • Ensures release package testing meets pre-defined Acceptance Criteria • Signs off the release package for implementation • Deals with release communication, preparation, and training • Audits hardware and software before and after the implementation of release package changes • Handles the storage and traceability/audit ability of controlled software in both centralized and distributed systems • Assigns, categorizes, and prioritizes release requests • Updates the request status • Maintains a listing of the master release schedule • Collects and maintains process metrics data • Facilitates resource commitment and allocation • Resolves escalated process issues with documented corrective actions • Escalates unresolved exceptions to management as required • Conducts post-implementation review meetings • Identifies problems and improvements to the process owner • Reviews and maintains RDM process documentation • Monitors the effectiveness of the process and generates improvement plans • Communicates release and deployment plans, release and deployment status, issues with time-stamped recovery actions, project performance, testing results, stakeholder acceptance and status, and notification on any activities related to the RDM process
Role #3 Service Test Manager	
<p>Oversees the tests as set out in the testing plans and/or service package.</p> <p>The service test manager may vary by release test type required and there may be more than one test manager depending on the size of the release and the number of times Service Validation and Testing occurs.</p>	<ul style="list-style-type: none"> • Defines the test strategy • Designs and plans tests conducted, test scripts, test data, setting parameters to ensure appropriate coverage/control • Allocates and oversees test resources • Provides management reports on test progress outcomes • Rates the issues and risks assessed • Manages the team conducting the tests • Records, analyzes, and diagnoses test results, including problems generated and findings on retested problems



Description	Overall Responsibilities
	<ul style="list-style-type: none"> • Manages test environment requirements • Verifies tests conducted by release and deployment • Administers test assets and components • Validates SLR metrics • Validates performance level requirements • Ensures production environment is not affected by the release
Role #4 Project Officer (POR)	
<p>Large projects have full releases and for releases coming from a program of record, a Project Officer is required to support the deployment activities. The Project Officer ties the release into the overall project goals.</p>	<ul style="list-style-type: none"> • Includes plans for the deployment of solutions in the overall project plan • Manages the deployment of the solution on a day-to-day basis • Utilizes relevant standards, procedures, and components as used within the organization • Maintains and communicates status reporting as specified by the project plan • Becomes liaison between RDM process and the POR
Role #5 Deployment Manager	
<p>Responsible for the deployment and verification of new or changed components in the production environment.</p> <p>This resource is an existing specialist coming from the project staff and is determined by the release content. The Deployment Manager adheres to the release schedule and provides appropriate updates to the RD Manager and Project Officer.</p>	<ul style="list-style-type: none"> • Executes the implementation according to plan • Monitors the plan for success or failure • Manages the installation – defines the duration, coordinates the geographic requirements, and manages the vendor involvement • Documents the results of the installation • Opens incident/problem management tickets as needed • Verifies the success of the installation or opens RFCs to improve the release or initiates the back-out plan if required • Assesses current infrastructure performance and capacity • Integrates automation tools as required with other environments • Validates infrastructure modifications • Assesses prioritized release requests for technical content and impacts • Supports the design, build, and test sub-processes • Ensures all management processes are followed • Develops project plans for the deployment of solutions • Ensures suitable environment exists at designated locations • Performs RFC assessment and reviews the Change Schedule (CS)
Role #6 RDM Coordinator	
<p>Supports the RDM Manager.</p> <p>Manages records, tracks action items, and provides process-related reports.</p> <p>Ensures quality control of the entire RDM process throughout the lifecycle of a service package.</p>	<ul style="list-style-type: none"> • Coordinates projects and programs • Integrates the deployment management activities with the associated development teams • Ensures all projects achieve project hand-off and acceptance criteria • Develop and implement adhering to process standards • Conducts and coordinates post-implementation reviews of all major projects and major deployments

310

311 **3.1.2 Responsibilities**

312 Processes may span departmental boundaries; therefore, procedures and work instructions within
 313 the process need to be mapped to roles within the process. These roles are then mapped to job
 314 functions, IT staff, and departments. The Process Owner is accountable for ensuring process
 315 interaction by implementing systems that allow smooth process flow.



316 The Responsible, Accountable, Consulted, Informed, Participant (RACI-P) model is a method
317 for assigning the type or degree of responsibility that roles (or individuals) have for specific
318 tasks. Table 5 displays the department-level RACI-P model for RDM.

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

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

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

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

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

328 Table 5 establishes responsibilities for high-level process activities by organization.

329 **Table 5. Responsibilities for Enterprise RDM**

RDM Process Activities	MCNOSC	HQMC (C4)	MCSC	MCCDC	RNOSC	MITSC	Application Owner	Tenant/Supported Command
Plan and Prepare	P	I	RA		P	CP	RC	
Design Release	P		RA		I		RC	
Build Release	P		RA				RC	
Service Validation and Testing	P		RA		I	P	RC	I
Plan and Prepare for Deployment	RA	I	P		CP	CP	RC	I
Deploy & Verify	RA	I	P		CP	P	RC	I
Early Life Support	RA	I	P		P	P	RC	I
Review and Close	RA	I	P		P	P	RC	I

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

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.

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



330

331 **3.2 Policies**

332 This process requires the following policies for success:

333

334

1. Roles established

335

336

337

Although the number of people involved will vary based on the size of the location and number of CIs, RDM will have a process owner who acts as adjudicator, a process manager, and other key roles.

338

2. The following requires C4 policies published:

339

340

341

342

343

- a. Audit intervals
- b. Funding
- c. Span of authority (ex. CAB structure)
- d. Release definitions (ex. enterprise, regional, local)
- e. Sponsorship and engagement

344

3. Awareness Campaign

345

346

347

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

348

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

349

350

351

352

353

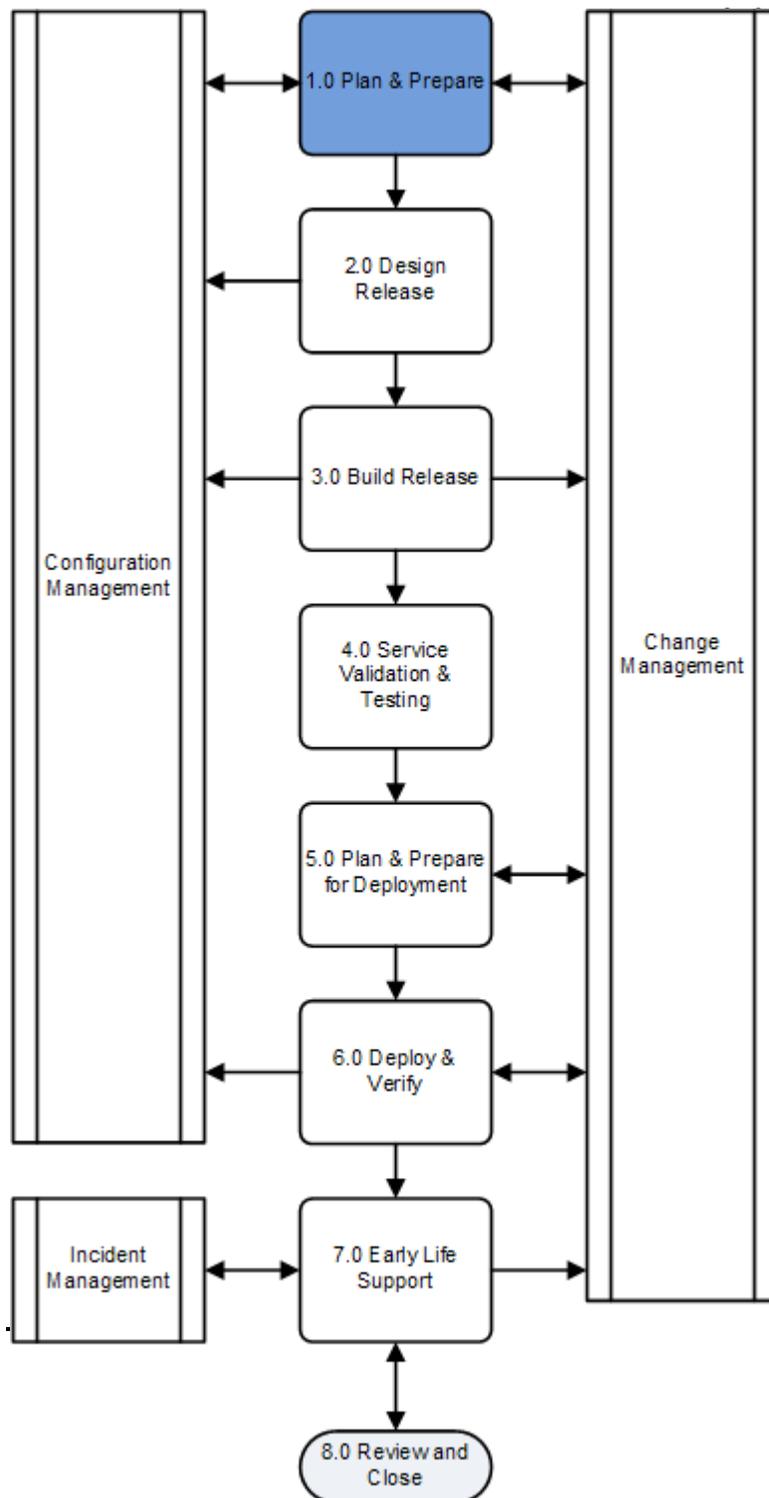
354

- a. FCAPS standard is followed, providing control for daily operations and systems administrative support interacting with DISA and at the RNOSCs
- b. DIACAP requirements for releases that affect the security posture of the network are followed
- c. DoD compliance including Common Criteria Certification



355 **4.0 SUB-PROCESSES**

356 The RDM process for USMC consists of eight (8) sub-processes. While each release will follow
 357 each sub-process on some level, not every activity within each sub-process is utilized for every
 358 USMC organization or type of release. For example, under normal circumstances, minor releases
 359 unique to a particular MITSC will not utilize every phase or type of testing associated with
 360 Service Validation and Testing. Therefore, to understand RDM in its entirety, examination at the
 361 sub-process level is required.

**4.1 Plan and Prepare**

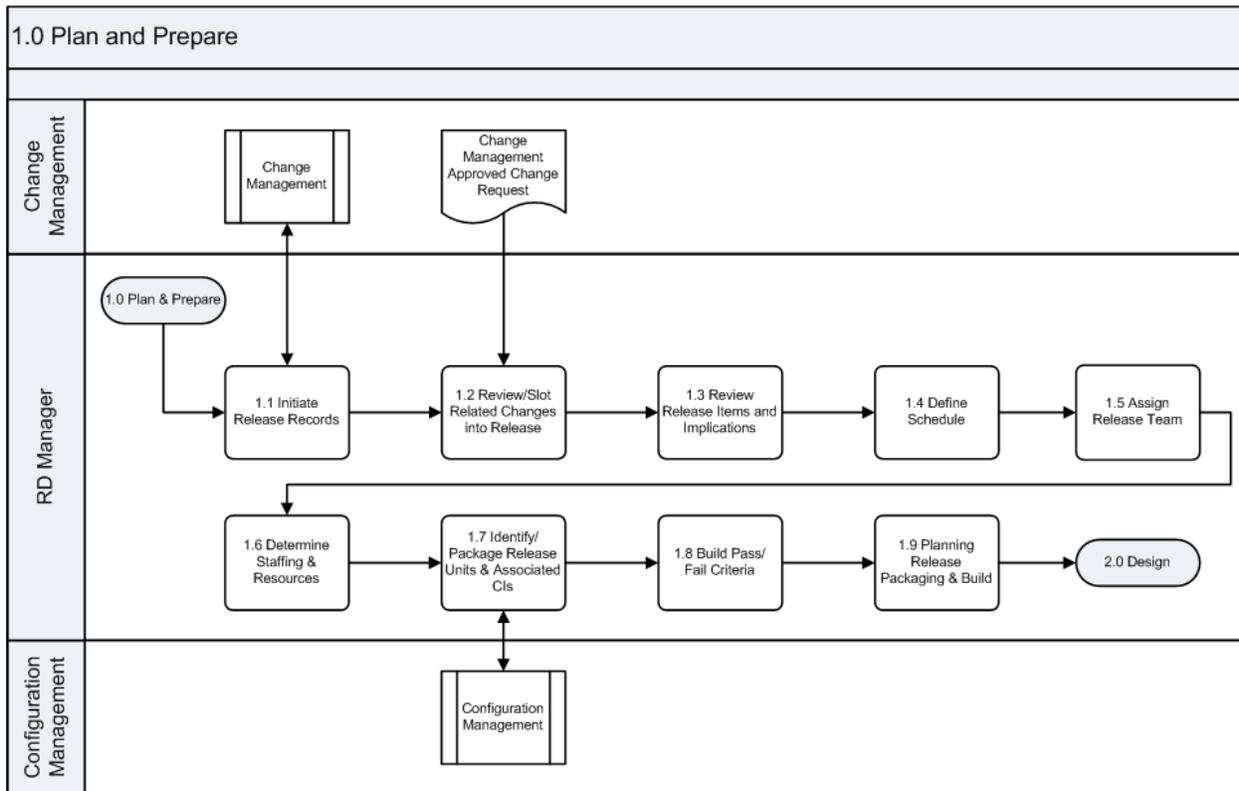
This first sub-process determines the strategy for how each release is defined and brought into existence in a state ready for deployment. It includes understanding the components of the release (from one or more Service Packages) and considering the impact of the one or more authorized RFCs which relate to the release contents in order to create the overall plan for the release.

The planning covers building, testing, and verifying the release (including the possible need for pilot deployments), as well as establishing a model for how the finalized release should be deployed.

All plans and acceptance criteria are documented in the ChM Plan for the specified project and approved by ChM. RFC approvals are managed in ChM with input from RDM.

The release plan is developed by the RD Manager. Approval requirements for the release plan will vary depending on the

394 release size (Full, Package or Delta), complexity, risk, and urgency.



395

396 **Figure 5. RDM Plan and Prepare Sub-Process**

397 Table 6 describes the Plan and Prepare sub-process steps as depicted in Figure 5.

398 **Table 6. RDM Plan and Prepare Sub-Process Descriptions**

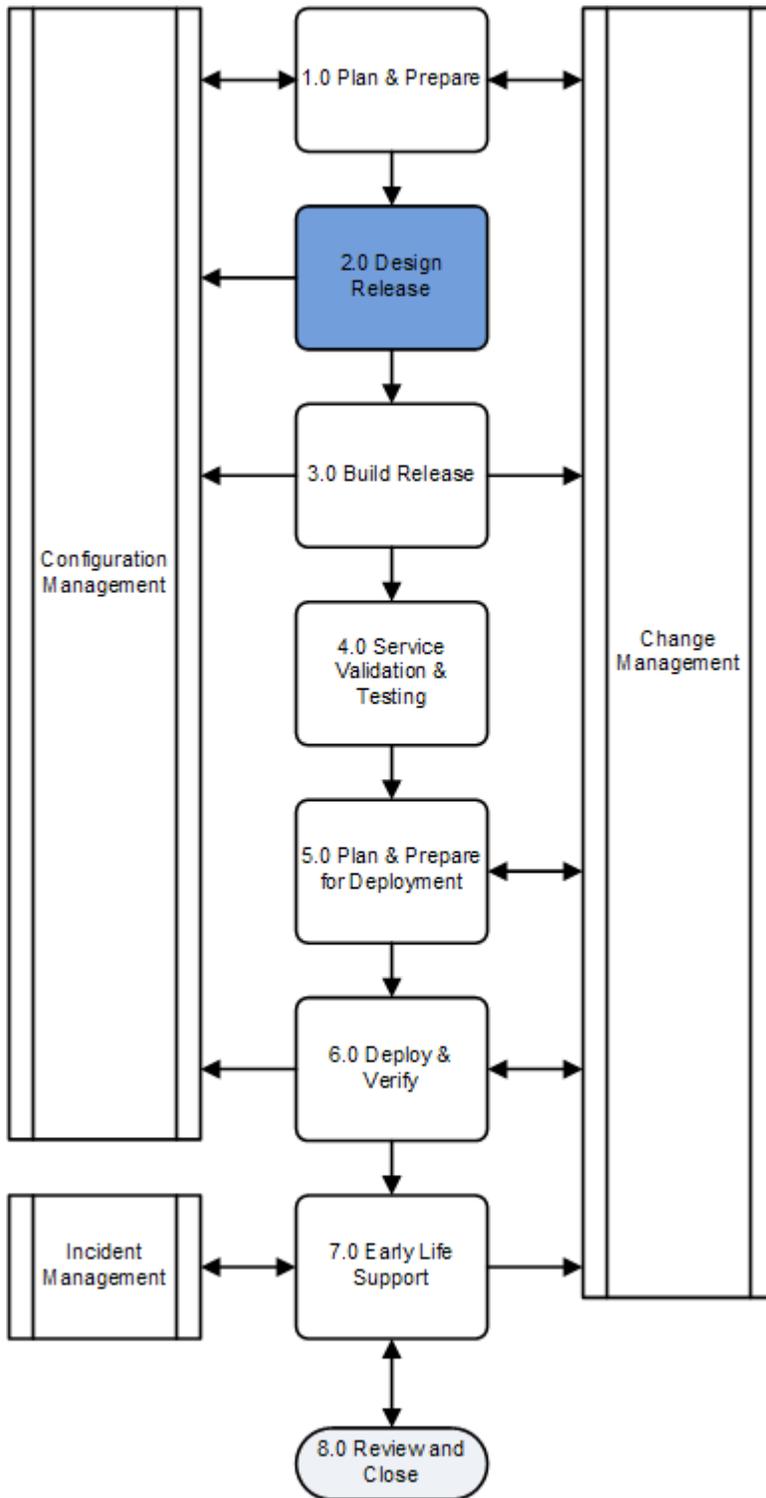
1.0 Plan and Prepare		
Number	Process Activity	Description
1.1	Initiate Release Records	Collaborate with ChM to create the initial release structures based on Release Category (Major, Minor, or Emergency), Release Type (Full, Delta, or Package) and maturity of scheduling. The release policy defines the release type and category.
1.2	Review/Slot Related Changes into Release	The change request is reviewed as related to the release as well as recent change requests. The RD Manager determines if there are similar change requests that can be supported in the same release, preventing replication in multiple releases.
1.3	Review Release Items and Implications	The items to be included in the release package are reviewed. The items in the release package are assessed to determine whether they can be supported within a single deployment or require multiple deployments. Items are also assessed to identify the implications of supporting the release to other processes, services and teams that could be affected by the release. With the assessment complete, the RD Manager documents the release package proposal.



1.0 Plan and Prepare		
Number	Process Activity	Description
1.4	Define Schedule	Schedule planning and definition is conducted. The RD Manager allows sufficient time within the release schedule to support rework and back-out plans, if required. For PORs, the RD Manager coordinates the schedule with the POR schedule contact.
1.5	Assign Release Team	Assessing the release scope and content, the RD Manager assigns a team, works with impacted stakeholders to develop a strategy, secures the resources, determines if there is sufficient capacity to absorb the change, and scales the release plan to the release size. Resources are assigned based on the release type and category. If the release is a full release, organizations, such as SIE, may be involved for testing support. If the release is a delta release, regional organizations, such the MITSCs impacted, may be the only organizations required to support testing. The RD Manager determines and engages the appropriate resources (Deployment Manager, Service Test Managers, Application Owners, Service Owners, etc.) needed to support the release.
1.6	Determining Staffing and Resources	The RD Manager determines the staffing and resources required for the release. The RD Manager negotiates resource availability with support teams and test partners. Resource trade-offs and risks to the testing and deployment schedules are documented in the issues list. The Deployment Manager, Service Test Managers, Application Owners, and Service Owners, as appropriate, are involved in these negotiations.
1.7	Identify/Package Release Unit and Associated CIs	The release units and associated CIs to be included in the release package are identified. Working with ChM and CfM, the RD Manager identifies and analyzes all new and changed CIs for inclusion in the release.
1.8	Build Pass /Fail Criteria	Release pass/fail criteria is built sufficient for operability standards in Service Operations. Pass/fail criteria is specific to the release. Pass/fail criteria is developed for each gate in the release and negotiated with the stakeholders. Pass/fail criteria encompasses each approval point through the release and deployment stages, starting with release planning through testing, up to and including user acceptance. When the pass/fail criteria negotiations are complete, the final acceptance criteria negotiated is communicated to all stakeholders by the RD Manager.
1.9	Planning Release Packaging and Build	In planning the release packaging and build, the RD Manager: <ul style="list-style-type: none"> • Develops mechanisms, plans, and procedures to verify exit and entry criteria • Manages stakeholder communications • Trains people and transfers knowledge • Establishes services and service assets • Negotiates schedules • Develops service management capabilities and resources, assesses readiness of target deployment groups • Defines and negotiates exit criteria <p>To implement the release packaging process, the RD Manager needs sufficient information and capabilities required to build, copy, promote, distribute, audit, install, and activate procedures, and to purchase software licenses and Intellectual Property Rights (IPRs).</p> <p>The RD Manager is expected to have the expertise in new, change, retirement, disposal procedures, and building exit criteria templates to support the release requirements.</p> <p>The finished product is the planned Release Package.</p>



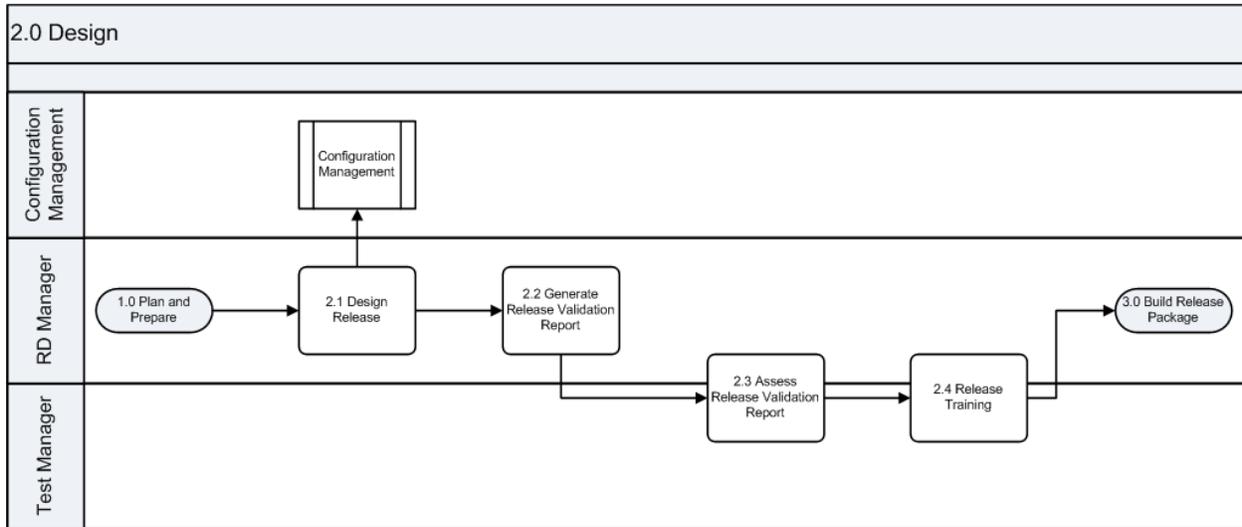
401 **4.2 Design Release**



This activity determines what needs to be built for the release and how it will be assembled and deployed. During this sub-process, the release build, installation, and roll-back scripts are designed at a high level. In addition, software and hardware components are obtained for the build activity and the test environment is put in place.

The test strategy is defined providing the overall testing approach for the Service Validation and Testing process. Draft remediation procedures are developed as backup if the deployment is unsuccessful.





422

423

Figure 6. RDM Design Release Sub-Process

424 Table 7 describes the Design Release sub-process steps as depicted in Figure 6. Note: This is
 425 the first of many times that RDM sub-processes interface with Service & Validation Testing
 426 (SV&T) sub-process. Entrance and exit to and from SV&T occurs at the same point.

427

Table 7. RDM Design Release Sub-Process Descriptions

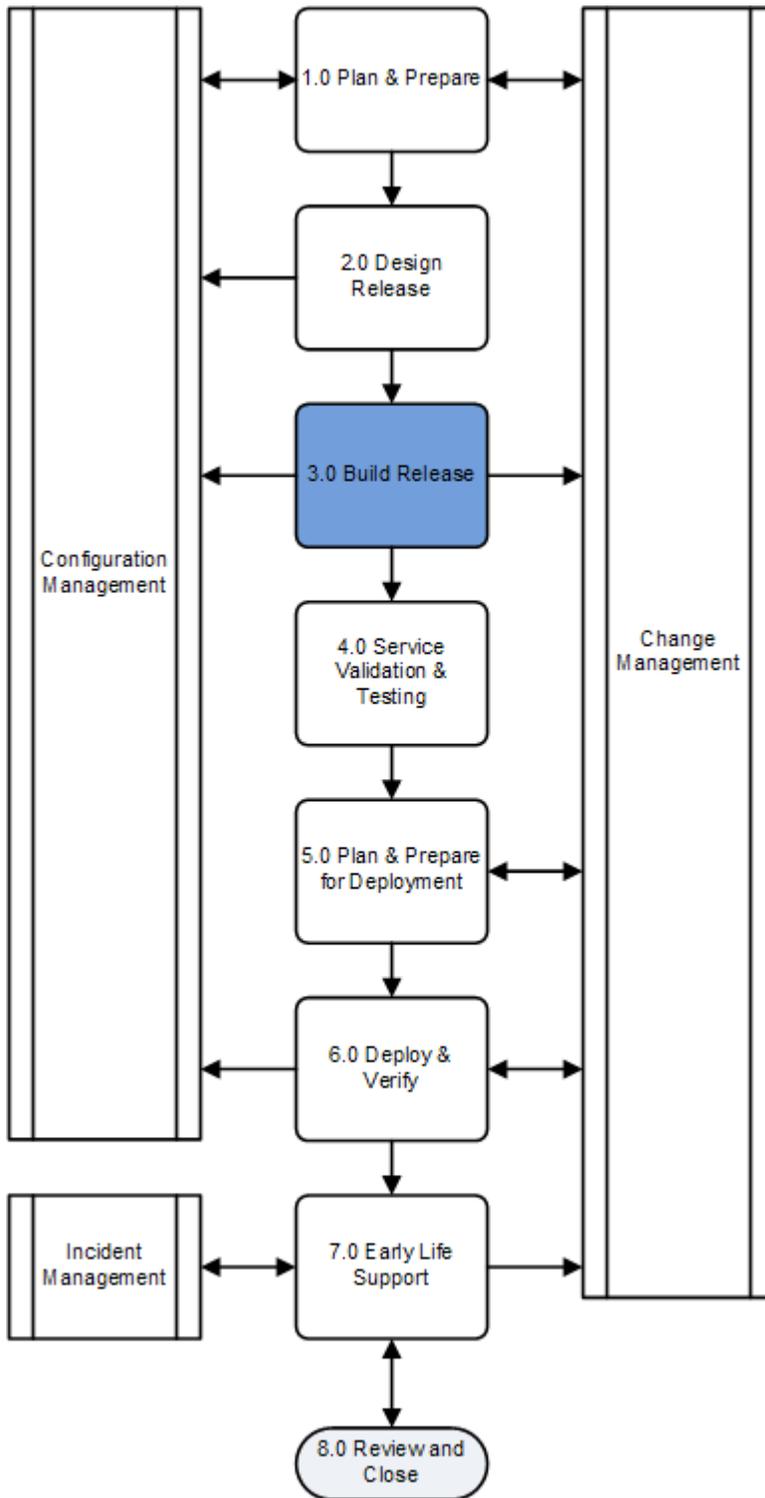
2.0 Design Release		
Number	Process Activity	Description
2.1	Design Release	<p>Service Design defines the approach for transitioning from a current service to a new or changed service or service offering.</p> <p>The SDP defines the service and the service solution design components to be transitioned to deliver the required service package(s) or service level package(s). Release options are considered and selected dependant on resource impacts and expected outcomes.</p> <p>When designing the release package, the release team must account for the changes from the current architectural baseline to targeted baseline architecture post-release using CfM.</p> <p>A release package can be a single release unit or a structured set of release units. Release packages should be designed with the ability to remove a release unit if un-resolvable issues surface in testing.</p> <p>The release team must design and schedule build and test plan activities. Resources and resource responsibilities are assigned. Exit and entrance criteria are used in designing release activities.</p> <p>Verify all release documents have been drafted.</p> <p>When all the release design activities are complete, the RD Manager has a test strategy defining the overall release approach.</p>



2.0 Design Release		
Number	Process Activity	Description
2.2	Generate Release Validation Report	The release design is validated against the SDP requirements of the new or changed service. A validation report is generated verifying the design with the SDPs supported in the release. All issues and risks are identified in the validation process. Issues are prioritized.
2.3	Assess Release Validation Report	The validation report must be evaluated to assess the impact of identified deviations and risks. Step 2.3 interacts with SV&T to access the validation report.. In conducting the evaluation, the RD Manager assesses if the release contents need to be modified.
2.4	Release Training	Training of the build, test, and deployment team members will be required. A release training plan must be developed with: <ul style="list-style-type: none"> • Training requirements related to release activities • Build, test, and deployment team members identified • A training schedule documented and distributed. The RD Manager ensures the training plans are complete for operations, service desk, and implementation team. The RD Manager confers with the Service and/or Application owners to ensure the user training plan and schedules are complete.

428



429 **4.3 Build Release**

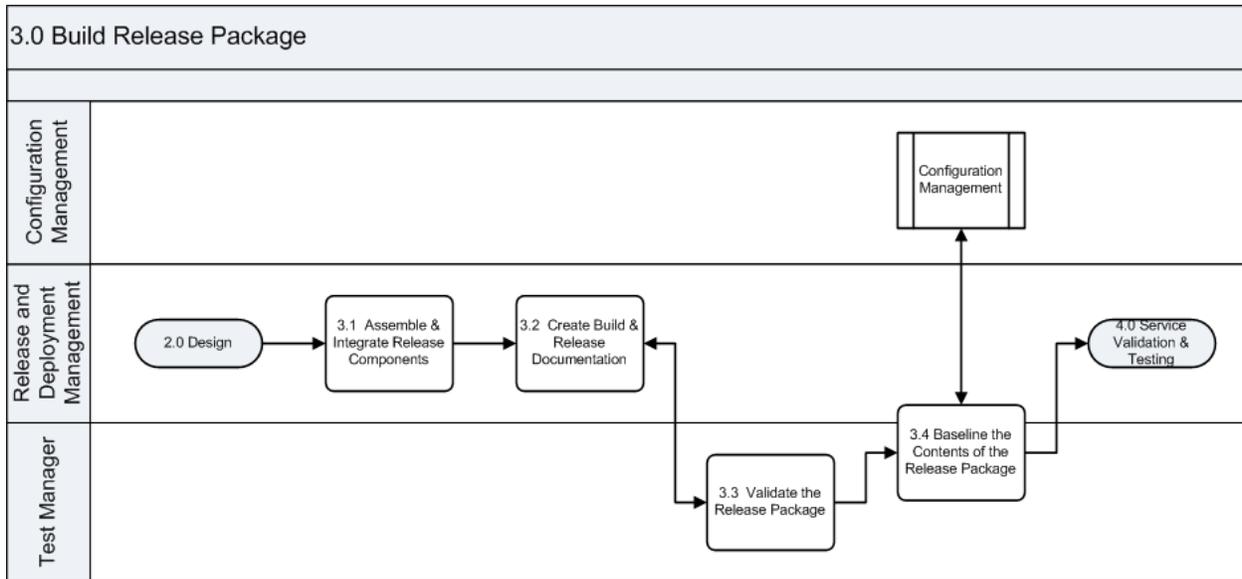
In building the release package, build management procedures, tools, and checklists are utilized to provide repeatable practices and expected results.

Baselines are recorded before and after the release package build to provide restore capability if needed in production.

The proposed solution and test results are recorded and handed over to Service Operations for use in future releases.

After the release has been designed, this activity builds the scripts and other aspects needed to assemble and to deploy the release. This includes:

- Creating the build environment
- Creating build, install, and roll-back scripts
- Placing software in the Definitive Media Library (DML)
- Creating support, training, and deployment documentation
- Notifying CfM to update the CMDB with information about the release package



463

464

Figure 7. RDM Build Release Sub-Process

465

Table 8 describes the Build and Release Package sub-process steps as depicted in Figure 7.

466

Table 8. RDM Build Release Sub-Process Descriptions

3.0 Build Release		
Number	Process Activity	Description
3.1	Assemble and Integrate Release Components	In building the release, the deployment team initially assembles and integrates the release components. The RD Manager uses deployment team resources to develop management procedures, methodologies, tools, and checklists when building the release package. The use of tools ensures the release package is built with a standard, controllable, and reproducible approach complying with the original SDP. A release package changes as modifications to the release occurs as a result of the testing results.
3.2	Create Build and Release Documentation	Documentation is created by the deployment team detailing build and release requirements. The documentation can include: <ul style="list-style-type: none"> • Build, installation and test plans, procedures, and scripts • Guidelines for monitoring and checking the quality of the release with direction for recognizing and managing problems • Processes (automated or manual) required to distribute, deploy, and install the release in the target environment • Procedures to back out release units or remediate a change if the release fails • Procedures for tracking and managing software licenses



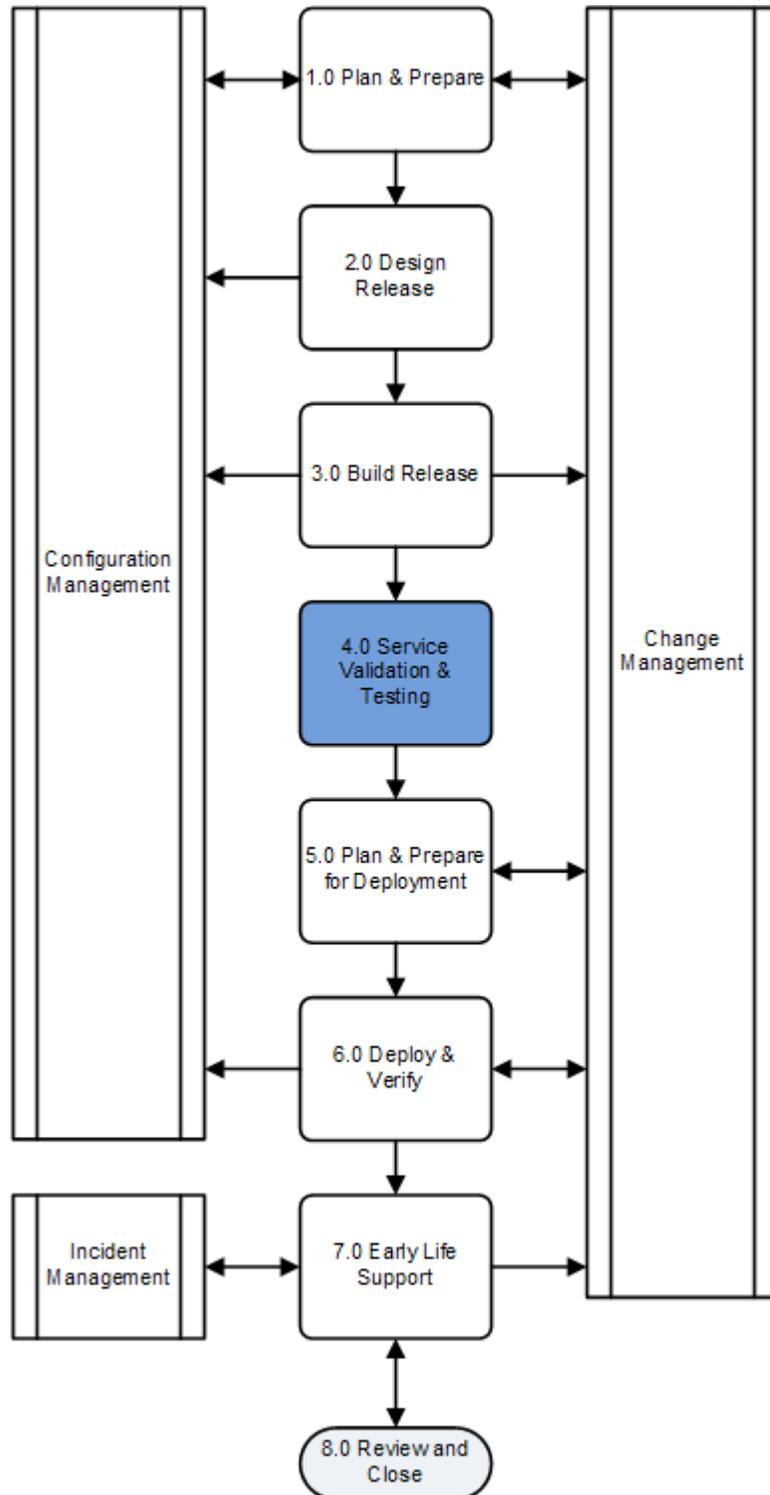
3.0 Build Release		
Number	Process Activity	Description
3.3	Validate the Release Package	<p>The Test Manager validates that the release package is complete. This step includes validating the components are present and documented.</p> <p>The package validation occurs throughout the release lifecycle with the validation activities occurring at least three times before deployment. The package validations occur for:</p> <ul style="list-style-type: none"> • Individual components • Assembled components • The release package
3.4	Baseline the Contents of the Release Package	<p>Once the initial release package is complete, a document is generated baselining the contents.</p> <p>As testing occurs, the release content within the release package will change. Each subsequent build is baselined and the baseline document is forwarded to CfM for inclusion in the CMDB.</p> <p>The documentation of the updated view enables back-out activities to previous views, if warranted.</p> <p>The RD Manager notifies ChM the release package is defined and delivered to Service Validation and Testing.</p>

467

468



469 **4.4 Service Validation and Testing**



Service Validation and Testing (SV&T) performs a number of iterations throughout the Release and Deployment lifecycle:

Verifies that the deployment team, tools, and procedures can deploy the release package into a target deployment group or environment within the estimated timeframe.

Ensures the release package contains all the service components required for deployment (e.g., by performing a configuration audit).

Validates the defined Service-Level Requirements are achievable and sustainable.

Ensures the proposed changes do not adversely affect authorized systems in the production environment. Ensures authorized configurations and systems in the production environment do not have an adverse impact on the proposed application or change.

Tests the deployment team, tools, and procedures to ensure they can install the release package into a target environment within the estimated timeframe.

Tests to ensure a deployment has completed successfully and that all service assets and configurations are in place as planned and meet their quality criteria.

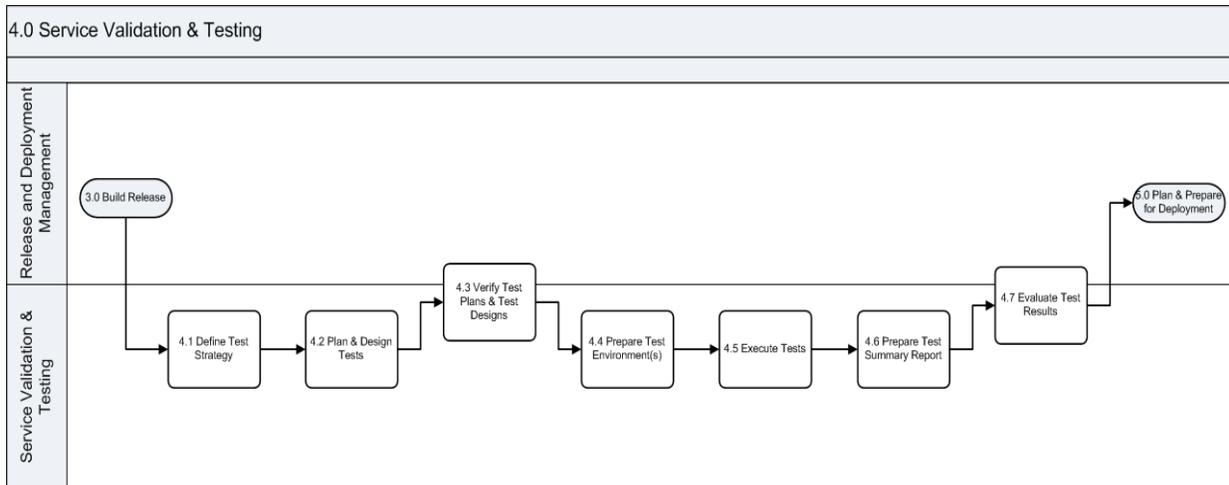
507 Testing activity support is

508 negotiated during Plan and Prepare (1.0) by the RD Manager and approved by the Change



509 Manager. All or some of the testing activities required are determined by the release plan and
510 supported by the Service Test Managers.

511 SV&T provides a recommendation to ChM for release approval or remediation.



512

513 **Figure 8. RDM Service Validation and Testing Sub-Process**

514 Table 9 describes Service Validation and Testing sub-process steps as depicted in Figure 8.

515 **Table 9. RDM Service Validation and Testing Sub-Process Descriptions**

4.0 Service Validation & Testing		
Number	Process Activity	Description
4.1	Define Test Strategy	<p>The test strategy defines the overall approach to organizing testing and allocating testing resources. The test strategy includes:</p> <ul style="list-style-type: none"> • The purpose, goals, and objectives of testing • Scope • Key considerations, to include critical elements where mission priorities and risk assessment suggest testing should concentrate • The high-level test approach, to include identification of any known test models • Timing <p>Recommendations from the deployment team provide input to the release team test parameters at a high level to ensure Quality Assurance (QA) outcomes and minimize test issues.</p> <p>The following tasks take place in 4.1 Define Test Strategy:</p> <ul style="list-style-type: none"> • The test team reviews the Service Design Package (SDP) to become familiar with service additions or changes incorporated into the release and any test strategy delineated in the SDP. • Create test plan. • Develop test strategy. • Develop the necessary requirements for testing. This includes the entrance and exit criteria that define a successful test. • Develop initial test schedule. • Obtain test strategy approval.
4.2	Plan and Design Tests	<p>While the testing process is shown schematically, test activities are not required to be executed sequentially. Test activities may take place in parallel with test execution</p>



4.0 Service Validation & Testing		
Number	Process Activity	Description
		<p>beginning before test design is complete.</p> <p>Test planning and design starts early in the service lifecycle. These activities include:</p> <ul style="list-style-type: none"> • Resource needs • Hardware, networking, staff numbers, and skills • User/customer resources required • Support service requirements, such as security, access, and communications • Schedules for significant milestones, hand-offs and delivery dates • Location and time of delivery • Financial requirements <p>Specific tasks that occur in test plan and design are:</p> <ul style="list-style-type: none"> • Determine the test scenarios to execute from the testing strategy. The scenarios are grouped or high level test approaches of like testing that sometimes generate multiple test cases. • Development of detailed test cases for each scenario. These test cases require step by step instructions, expected results, pass/fail criteria and other pertinent information. • For each release, a comprehensive load and performance plan is required. This includes necessary volume, stress, soak and performance testing determined necessary. • Finalize the test schedule prior to execution to include test case level detail.
4.3	Verify Test Plans and Test Designs	<p>Verification of plans and designs ensures:</p> <ul style="list-style-type: none"> • The test model delivers adequate and appropriate test coverage based on the risk of the service to be delivered or upgraded • All interfaces and integrations are tested • The test cases are accurate and complete • Conduct Test Readiness Review with stakeholders prior to execution.
4.4	Prepare Test Environments	<p>Test environments are built to the requirements specifications established to successfully test the build. Additional tasks are required to prepare the test environment to support test execution:</p> <ul style="list-style-type: none"> • Baseline the test environment to ensure the capability to restore if needed. Ensure Configuration Management is informed of each baseline. • Verify the environments are built to the specifications designed and required. • Deploy the release to the test environment. • Validate the deployment has completed successfully.
4.5	Execute Tests	<p>Executes the tests using standardized manual or automated procedures. Testers record findings while testing. Tests are performed according to the test plans and cases.</p> <ul style="list-style-type: none"> • Test defects are recorded, evaluated, remediated or escalated. • Issues must be resolved or documented as known errors by the same tester. • On a regular pre-defined interval prepare status reports on the testing progress.
4.6	Prepare Test Summary Report	<p>Develop the testing summary document based on results discovered during test execution. The actual test results are compared to the expected test results and recorded in the summary document.</p> <ul style="list-style-type: none"> • Forward completed summary documentation to the Release Manager. • Develop any action plans necessary to remediate unresolved defects. • Promote the release to deployment.
4.7	Evaluate Test Results	<p>The actual test results are compared to the expected test results. Results may be interpreted as pass/fail or risk to the Marines or service providers. Any change in value of what is being delivered or a higher cost than intended must be identified.</p> <p>A report is generated summarizing test metrics and results stating whether the baseline was met, or the service meets or exceeds expectations, or if the service</p>



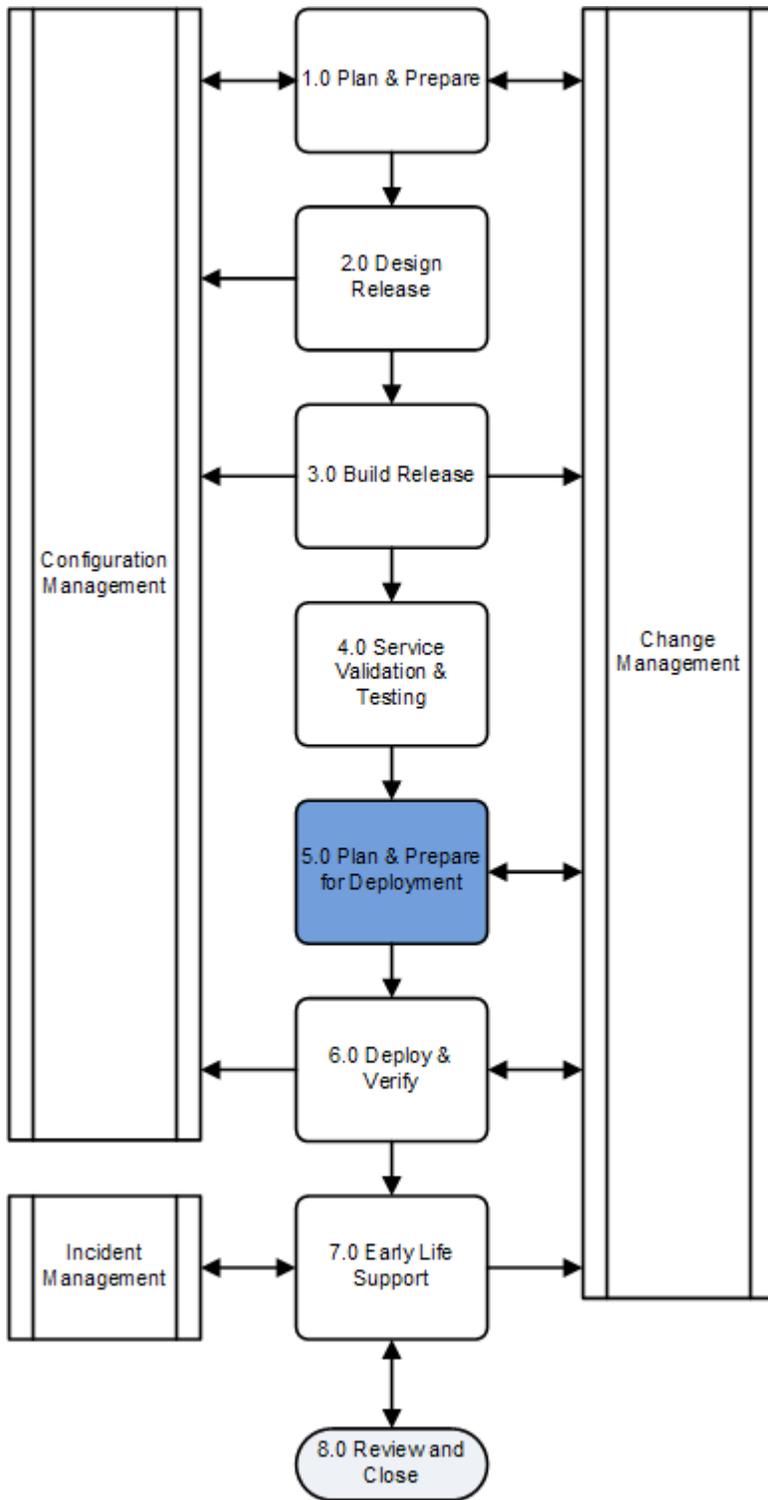
4.0 Service Validation & Testing		
Number	Process Activity	Description
		delivered enables the users to deliver as intended. The RD Manager assesses the test results and prepares a deployment recommendation.

516
517



518 4.5 Plan and Prepare for Deployment

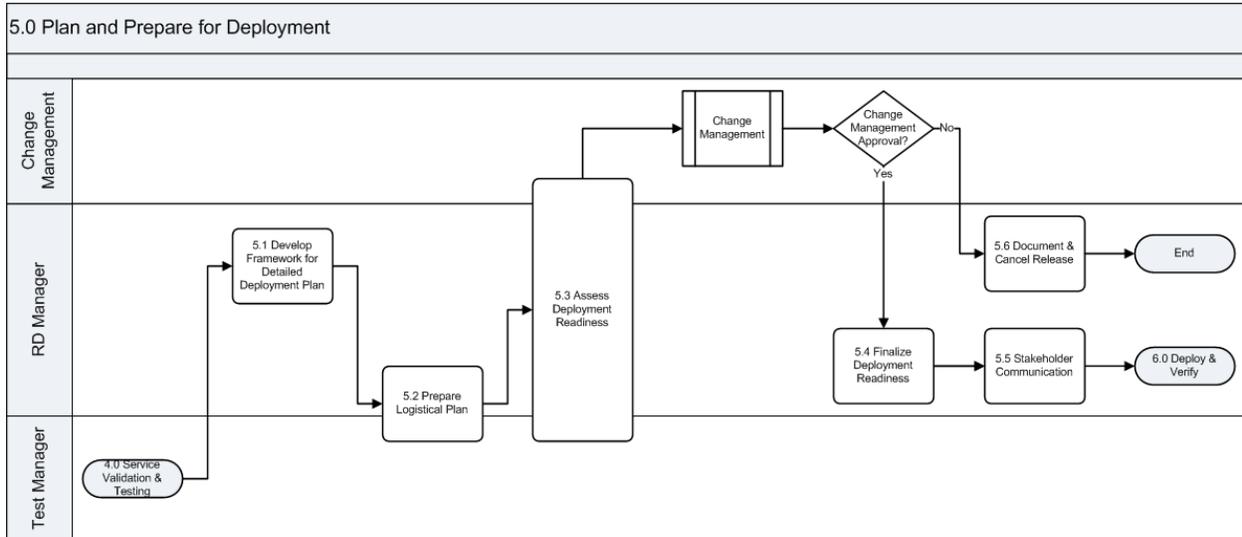
519



With recommendations from the Service Validation and Testing process presented to the ChM Change Advisory Board (CAB) for review, the ChM CAB approves the release to be deployed. Deployment resources are assigned. Readiness assessments are conducted. Risks are identified and assessed in terms of potential disruption. Detailed implementation plans are developed and verified.

When the detailed deployment plan is complete and readiness tests have been performed, the service is ready for deployment.





538

539

Figure 9. RDM Plan and Prepare for Deployment Sub-Process

540 Table 10 describes the Plan and Prepare for Deployment sub-process steps as depicted in Figure
541 9.

542

Table 10. RDM Plan and Prepare for Deployment Sub-Process Descriptions

5.0 Plan and Prepare for Deployment		
Number	Process Activity	Description
5.1	Develop Framework for Detailed Deployment Plan	<p>The RD Manager responsible for the release deployment assesses the release requirements gathered earlier in the release process by validating the following information:</p> <ul style="list-style-type: none"> • What needs to be deployed? • Who are the users? • Where are the users located? • Are there location dependencies? • Who needs to be prepared in advance of the deployment? • Date the deployment must be completed by. • Why is the deployment happening? • What are the CSIs and exit criteria? • What is the current capability of the service provider? <p>The answers to the questions provide the framework for the logistical details required in the final deployment plan. In this framework, the RD Manager will determine if staging the environment is required. If so, the RD Manager will provide staging environment requirements as part of the logistics plan developed in the next sub-process step.</p> <p>Verify detailed implementation and backout plans are finalized.</p>



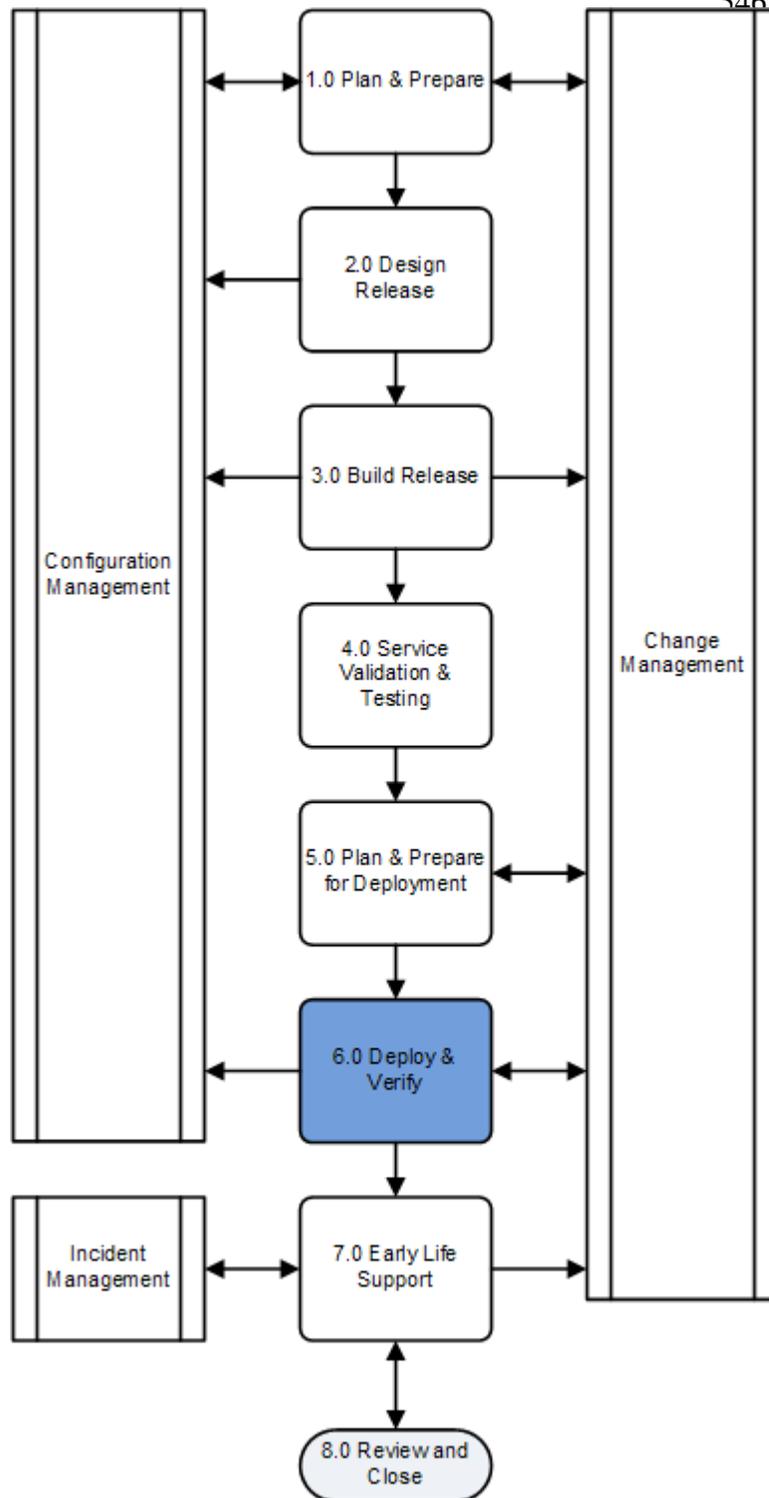
5.0 Plan and Prepare for Deployment		
Number	Process Activity	Description
5.2	Prepare Logistical Plan	<p>Using the framework, the RD Manager gathers the logistics required to build the detailed deployment plan. Some but not all of the information required covers the following areas:</p> <ul style="list-style-type: none"> • The release units and service components to be delivered • The lead times required with impacts if delayed • The status plan for tracking deliveries and confirmations • The resource requirements and availability • If staging environments are required, detailed requirements • Detailed international, national and regional considerations and impacts. • Supplementary plans for the retirement, decommission and/or disposal of units and service components out of scope as a result of the deployment. These plans can include software and licenses, hardware, support contracts, and any accommodations no longer needed. • Implementation and retirement plans for any interim service and equipment requirements required to run in parallel during the deployment transition.
5.3	Assess Deployment Team Readiness	<p>The RD manager confirms the entry criteria for planning and preparing a deployment with the stakeholders, customers, and service provider teams. Readiness assessments are conducted as early in the release process as possible. Release readiness assessments are revisited at scheduled intervals to ensure the readiness level is maintained.</p> <p>The readiness assessment identifies:</p> <ul style="list-style-type: none"> • Issues and risks that might occur when delivering the new service, such as, gaps in training and skills, the need for dedicated resources or supplier support, and any late changes in requirements • Gaps that need to be resolved <p>The readiness assessments includes:</p> <ul style="list-style-type: none"> • Impacts requiring financial support and assets • Impacts to procedures and regulatory requirements • Impacts to current capabilities of users to use and gain value from the change in service • Impacts to current services, capabilities, and resources in use • Organizational readiness • Impacts to applications, information, and data • Impacts to infrastructure and facilities <p>The readiness assessments confirms:</p> <ul style="list-style-type: none"> • Risk mitigation plans are in place • Transition, upgrade, disposal, and retirement plans are in place • Logistics and delivery planning is complete • Training and communications is complete • Service Operations is mobilized to support the delivery • Users are ready to use the service <p>All testing results and the deployment recommendation from 4.0 Service Validation and Testing are forwarded to ChM along with the deployment readiness assessment.</p> <p>ChM is a participant in the deployment readiness assessment and aware of the status at every stage. ChM has the final approval for release deployments.</p>
5.4	Finalize Deployment Readiness	<p>A deployment approval is received from ChM.</p> <p>The RD Manager verifies detailed deployment plans and finalizes deployment readiness tests. The release deployment is promoted to Deploy and Verify.</p>



5.0 Plan and Prepare for Deployment		
Number	Process Activity	Description
5.5	Stakeholder Communication	The RD Manager issues a formal notification to all stakeholders consulted in building the deployment plan.
5.6	Document and Cancel Release	If ChM rejects the deployment based on the testing results, the deployment recommendation and deployment readiness assessment, the RD Manager documents the rejection and cancels the release record.

543
544



545 **4.6 Deploy and Verify**

546

Deploying the release is the implementation of the detailed deployment plan. A deployment can be the deployment of materials (hardware or software) and processes, the transfer of a service, the deployment of a new or changed service, the decommissioning or retirement of services, and or the removal of assets.

This activity performs the physical, technical, and other tasks (such as delivering training and registering users) which move the capabilities deployed into production. This includes distribution and installation of hardware and software, and ensuring appropriate data is provided for asset and configuration updates

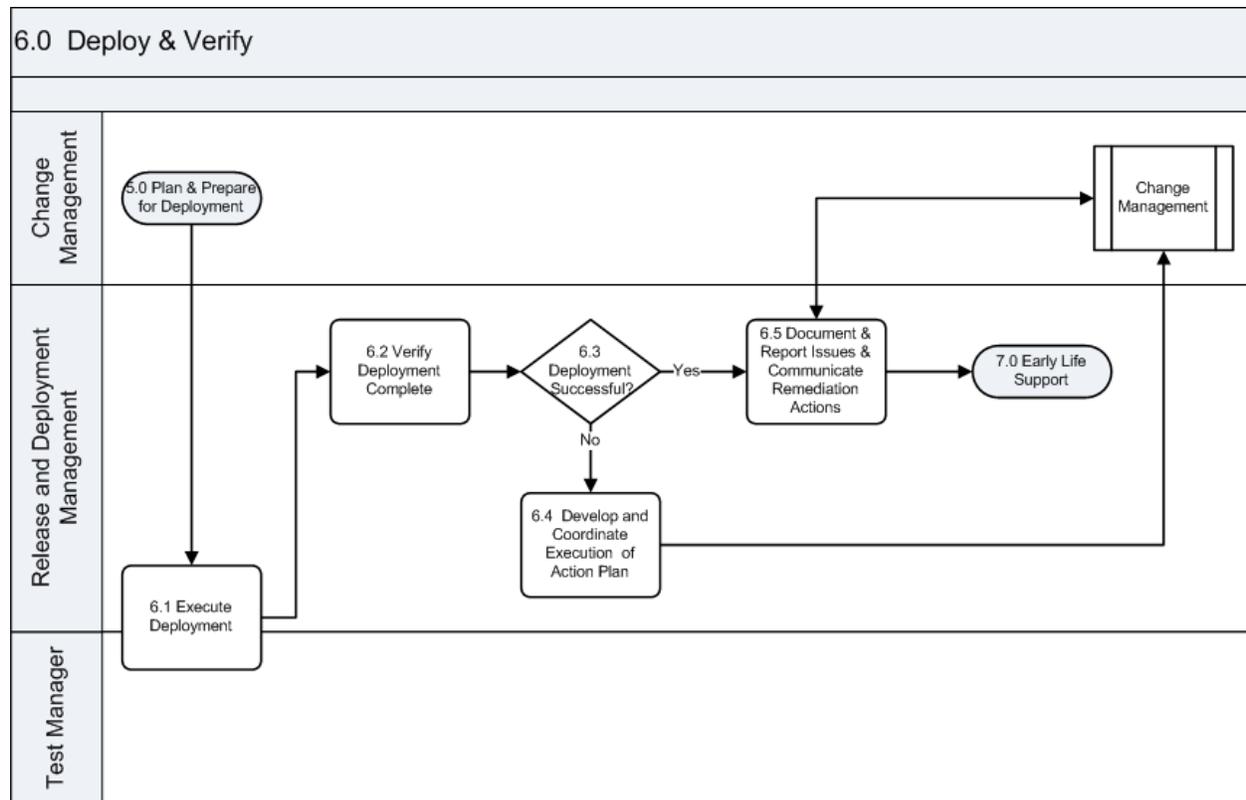
When the deployment is complete, the integrity of the solution is verified with stakeholders validating the capability of using or operating the service. The RD Manager verifies the release with the stakeholders, which can include:

- Service assets and capabilities are in place
- Documentation updates are completed
- Learning material has been made available to stakeholders
- Users are prepared to operate the new or changed service

585 • Measurements and reporting systems are established

586 • Successful validation of the deployment triggers the launch of Early Life Support (ELS).





587

588

Figure 10. RDM Deploy and Verify Sub-Process

589

Table 11 describes the Deploy and Verify sub-process steps as depicted in Figure 10.

590

Table 11. RDM Deploy and Verify Sub-Process Descriptions

6.0 Deploy & Verify		
Number	Process Activity	Description
6.1	Execute Deployment	<p>If a service, the Deployment Manager will deploy the service release package conducting the following activities:</p> <ul style="list-style-type: none"> Distribute and deliver service and service components at the correct time and location Build, configure, and install the service and service components with the converted or new data and information Test the system and services according to the installation and acceptance tests, producing results reports Record any incidents, issues, or deviations from the plans Correct any deviations that exceed design limitations and constraints <p>If the new or changed processes, systems and tools deployment is supported by the service provider teams responsible for Service Management activities, the Deployment Manager will:</p> <ul style="list-style-type: none"> Ensure everyone is trained and confident to operate, manage, and maintain the service as defined in the deployment Remove or archive redundant services and assets processes, procedures, and tools <p>If decommissioning or retiring a service or service assets, the Deployment Manager</p>

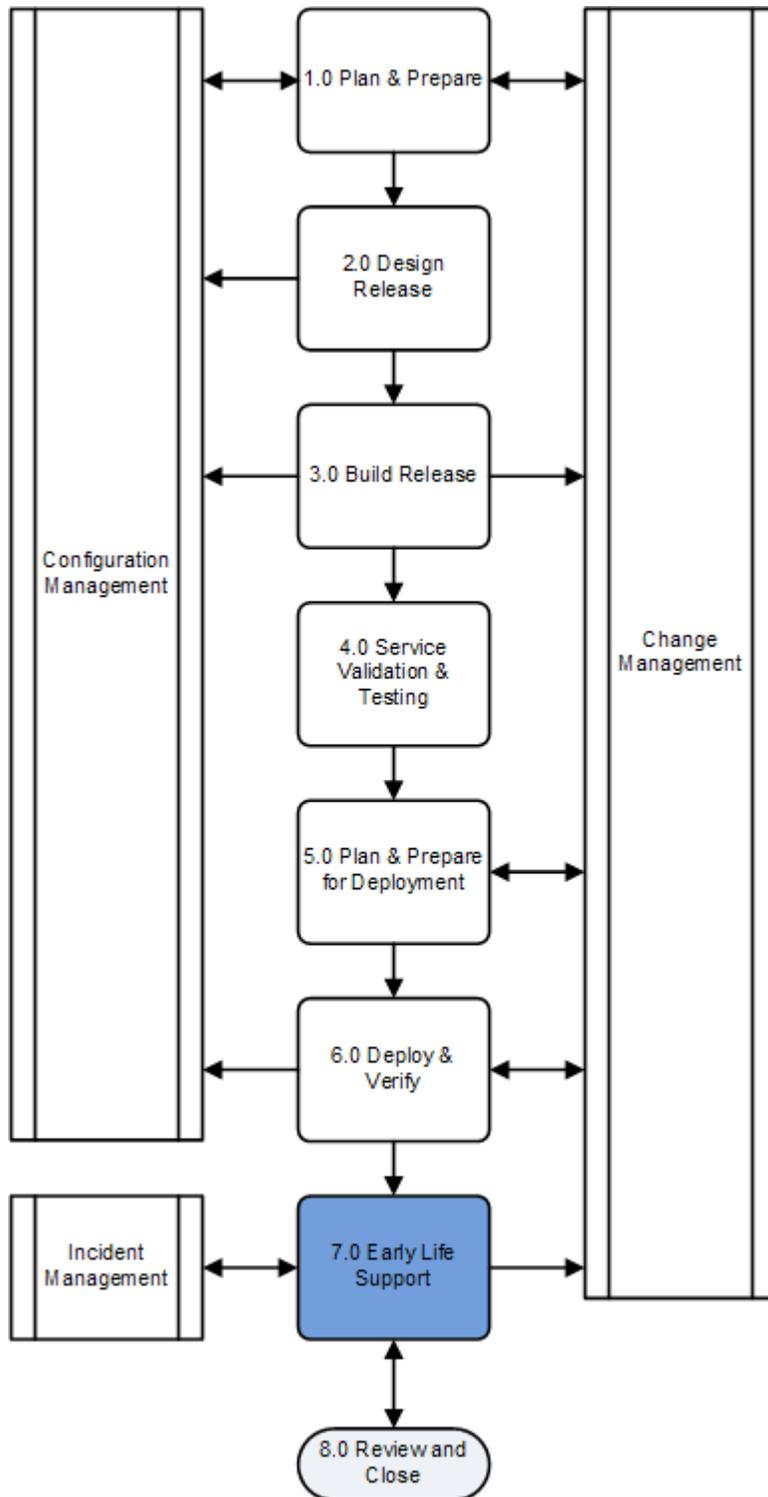


6.0 Deploy & Verify		
Number	Process Activity	Description
		<p>will deploy the release package conducting the following activities:</p> <ul style="list-style-type: none"> • Remove deployed copies of software and data from retired hardware • Identify licenses and other assets which can be redeployed • Dispose of equipment in compliance with procedures • Move assets that can be redeployed to secured storage • Maintain records of decommissioned or retired services <p>Management of redundant assets associated with a retired service will be detailed in the deployment plan. Management activities will include:</p> <ul style="list-style-type: none"> • Saving licensing fees, eliminating unnecessary capacity usage and preventing accidental use • Deleting or archiving redundant data as related to prior services • Assessing support contracts for renegotiation • Assessing service desk workload where appropriate • Archiving records affected by the retirement within the knowledge base
6.2	Verify Deployment Complete	<p>Validations will be executed by the deployment team to specifically verify:</p> <ul style="list-style-type: none"> • The service, service assets and service capabilities and resources are in place with audits performed on the deployed baseline against the planned baseline • Updates to documentation and information is completed • Communication, orientations, and training materials are ready to distribute to stakeholders and Service Operations • All roles and responsibilities are assigned to individuals and organizations • Users are trained and prepared to operate and use the new or changed service or service capability under all conditions • Users have access to information to use, operate, and support the service • A measurement and reporting system is established to measure the performance of the service • Remediation is in place with known work-arounds
6.3	Deployment Successful?	<p>ELS entrance criteria met?</p> <p>If yes go to step 6.5, Document and Report Issues and Remediation Actions.</p> <p>If no, go to step 6.4, Develop and Coordinate Execution of Action Plan.</p>
6.4	Develop and Coordinate Execution of Action Plan	<p>The deployment is not successful. The Deployment Manager may recommend up to and including the implementation of the back-out plan. The Deployment Manager will coordinate the execution of the action plan with the deployment team.</p> <p>The Deployment Manager notifies ChM of the execution of the action plan.</p>
6.5	Document and Report Issues and Remediation Actions	<p>The deployment team will document the results from each deployment step and develop remediation activities, as required. If at any time a remediation becomes significant without a work-around, back-out plans must be considered as alternative solutions.</p> <p>The risks and impacts of the current production state are assessed and documented.</p> <p>The final deployment results and remediation activities are communicated with a production ready recommendation to stakeholders in compliance with the User Acceptance Criteria.</p> <p>The deployment is promoted to Early Life Support.</p>

591
592

593 **4.7 Early Life Support**

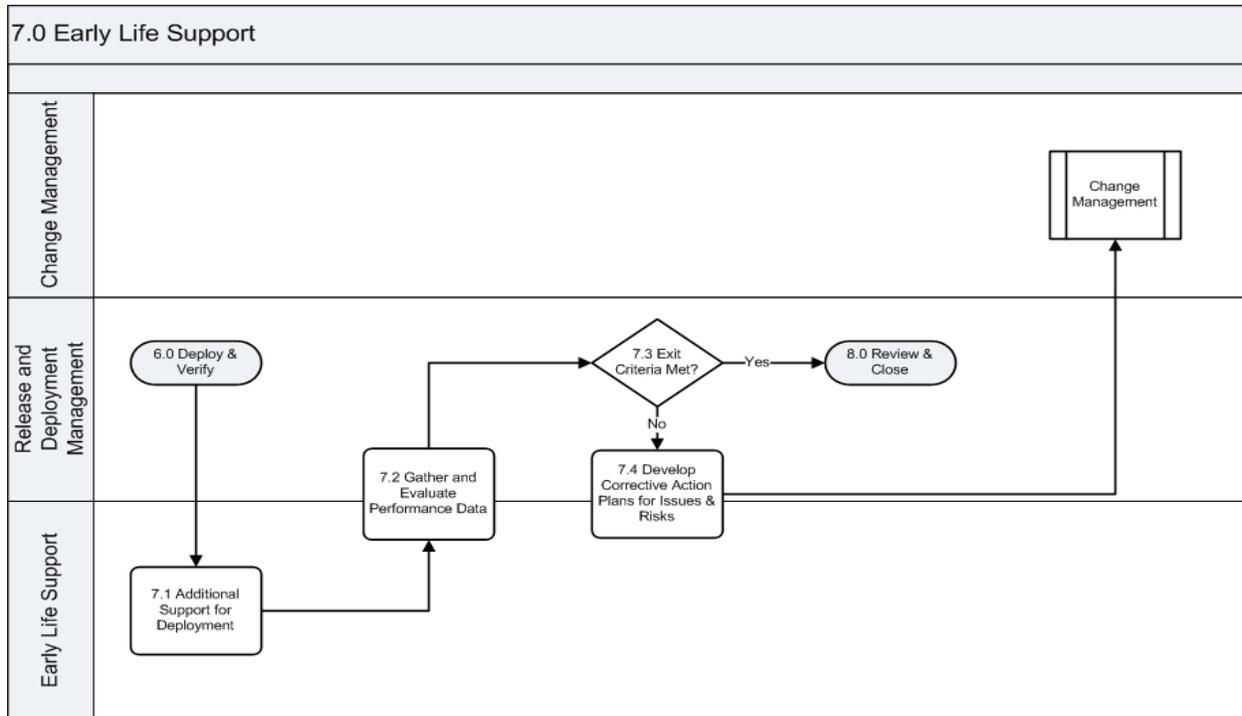
594



ELS is the additional expert service support provided immediately after the deployment to ensure service continuity and stakeholder satisfaction. Resources from IT Operations introduce the new service capability and resources to operations in a controlled manner. Resource support scope is determined by the release content delivered.

In Service Design, the stakeholders have agreed to the entry and exit criteria for ELS, but it may be necessary to renegotiate the performance targets and exit criteria early in the ELS stage as performance results are generated in the production environment. The RD Manager negotiates with the stakeholders for release approval. Release approval may include known errors with interim work-arounds or back-out plans are invoked if a satisfactory release is not possible.





624

625

Figure 11. RDM Early Life Support Sub-Process

626

Table 12 describes the Early Life Support sub-process steps as depicted in Figure 11.

627

Table 12. RDM Early Life Support Sub-Process Descriptions

7.0 Early Life Support		
Number	Process Activity	Description
7.1	Additional Support for Deployment	As the transition is initiated, the deployment team alerts users where issues may surface and provide direction for roles and responsibilities, funding requirements, raising incidents and change requests, escalation procedures, complaint procedures using tools and aids, and software licensing rules. The exit criteria and performance targets are finalized with the stakeholders. The transition of the new or changed service to Service Operations is initiated in a controlled manner.

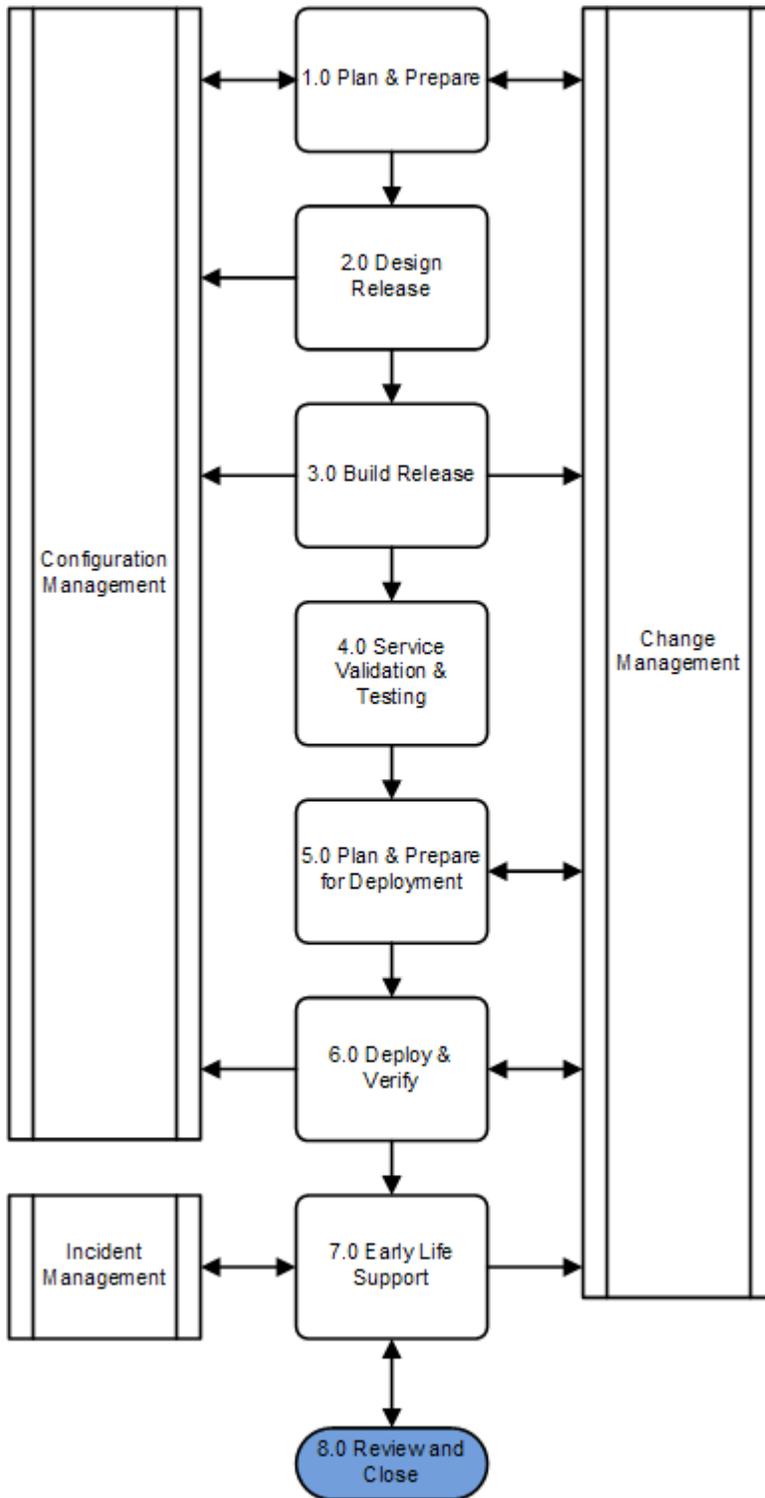


7.0 Early Life Support		
Number	Process Activity	Description
7.2	Gather and Evaluate Performance Data	<p>Performance data (number of incidents and problems by type) is collected as soon as possible after the transition begins. Results are analyzed. Improvements are implemented. If appropriate, performance data between different deployment groups is compared.</p> <ul style="list-style-type: none"> The documentation and knowledge base is updated with known errors, work-arounds and frequently asked questions. At agreed milestones, the service performance achieved is documented and communicated. The transitioned service is consistently monitored from ELS initiation against the ELS exit criterion throughout ELS until the exit criterion is met. Using the performance data with the known errors and work-arounds, the service stability is assessed. If more than one work group is participating in the deployment, variations in performance between different groups should be analyzed with improvements implemented across deployment groups.
7.3	Exit Criteria Met?	<p>ELS exit criteria is met when:</p> <ul style="list-style-type: none"> Users can use the service Service owners and process owners can manage and operate the service in compliance with the service model, performance standards, and processes Service delivery is managed across service provider interfaces Consistent progress is made at each ELS milestone Service levels and service performance standards are consistently achieved SLAs are finalized and signed Unexpected variations in performance of service can be monitored, reported, and managed Training and knowledge transfer activities are complete The service release, SLAs, and any contractual deliverables are signed-off Approval from the Application / Service owner(s) is secured. <p>The release is promoted to Review and Close.</p>
7.4	Develop Corrective Action Plans for Issues and Risks	<p>If exit criterion is not met, corrective action plans are developed and implemented and forwarded to Change Management for review and disposition.</p> <p>An assessment is made to determine if issues uncovered in ELS should be passed to CSI. The following categories are reviewed as potential sources of issues:</p> <ul style="list-style-type: none"> Feedback on deployment model and plan Errors in procedures Perceptions of where things could go wrong, or where intervention might be required Incorrect data in relevant records Incidents or problems caused by deployment Problems with updating records

628

629

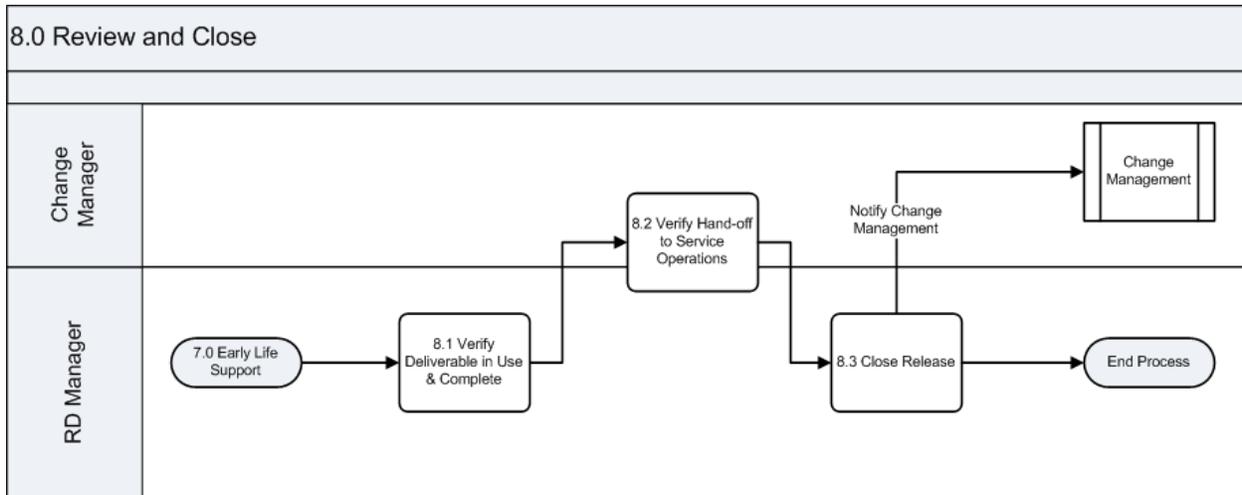


630 **4.8 Review and Close**

The RD Manager conducts a review to ensure appropriate and thorough knowledge transfer, training, and documentation is delivered to the stakeholders and end users. All fixes and changes are complete and have been presented to the customer for risk acceptance. All problems and known errors are identified and documented with known work-arounds. The entrance and exit criteria for each stage of the process has been assessed and met.

The RD Manager reviews the tasks completed during deployments and determines that all objectives of the deployment plan were met. A management plan is established for outstanding risks, issues, incidents, and known errors before the deployment is closed.

The RD Manager issues a close notification as the last step in the review. All release participants and end users are notified of the final review results for the release.



662

663

Figure 12. RDM Review and Close Sub-Process

664

Table 13 describes the Review and Close sub-process steps as depicted in Figure 12.

665

Table 13. RDM Review and Close Sub-Process Descriptions

8.0 Review and Close		
Number	Process Activity	Description
8.1	Verify Deliverable in Use and Complete	<p>A deployment review is conducted, assessing the deliverable:</p> <ul style="list-style-type: none"> • The customer, user, and service provider experience, feedback, and satisfaction. (Surveys) • Identifying any exit criteria not met • Verifying actions, critical fixes, and changes are complete • Reviewing open changes. Ensuring the open changes are acceptable as part of the hand-off process • Reviewing the performance targets and achievements • Ensuring there are no capability, resource, capacity, or open performance gaps or issues • Verifying all problems, known errors, and work-arounds are documented and accepted by customer and suppliers • Addressing the identified risks or negotiating the movement of the risks to the Service Transition Risk Log • Verifying redundant assets have been removed • Verifying the service is ready for transition from ELS to Service Operations.
8.2	Verify Hand-off to Service Operations	Coordinate the transition of deployment group support to Service Operations with ChM.
8.3	Close Release	The release is closed and ChM is notified that the release has been transitioned to Service Operations.



666

Appendix A – ACRONYMS

667

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

668

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.



671
672

Appendix C – POLICIES

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

675 [https://ehqmc.usmc.mil/org/c4/projects/CP/eitsm/Shared%20Documents/E-](https://ehqmc.usmc.mil/org/c4/projects/CP/eitsm/Shared%20Documents/E-ITSM_TO_13_Government_Policies.doc)
676 [ITSM_TO_13_Government_Policies.doc](https://ehqmc.usmc.mil/org/c4/projects/CP/eitsm/Shared%20Documents/E-ITSM_TO_13_Government_Policies.doc)
677

