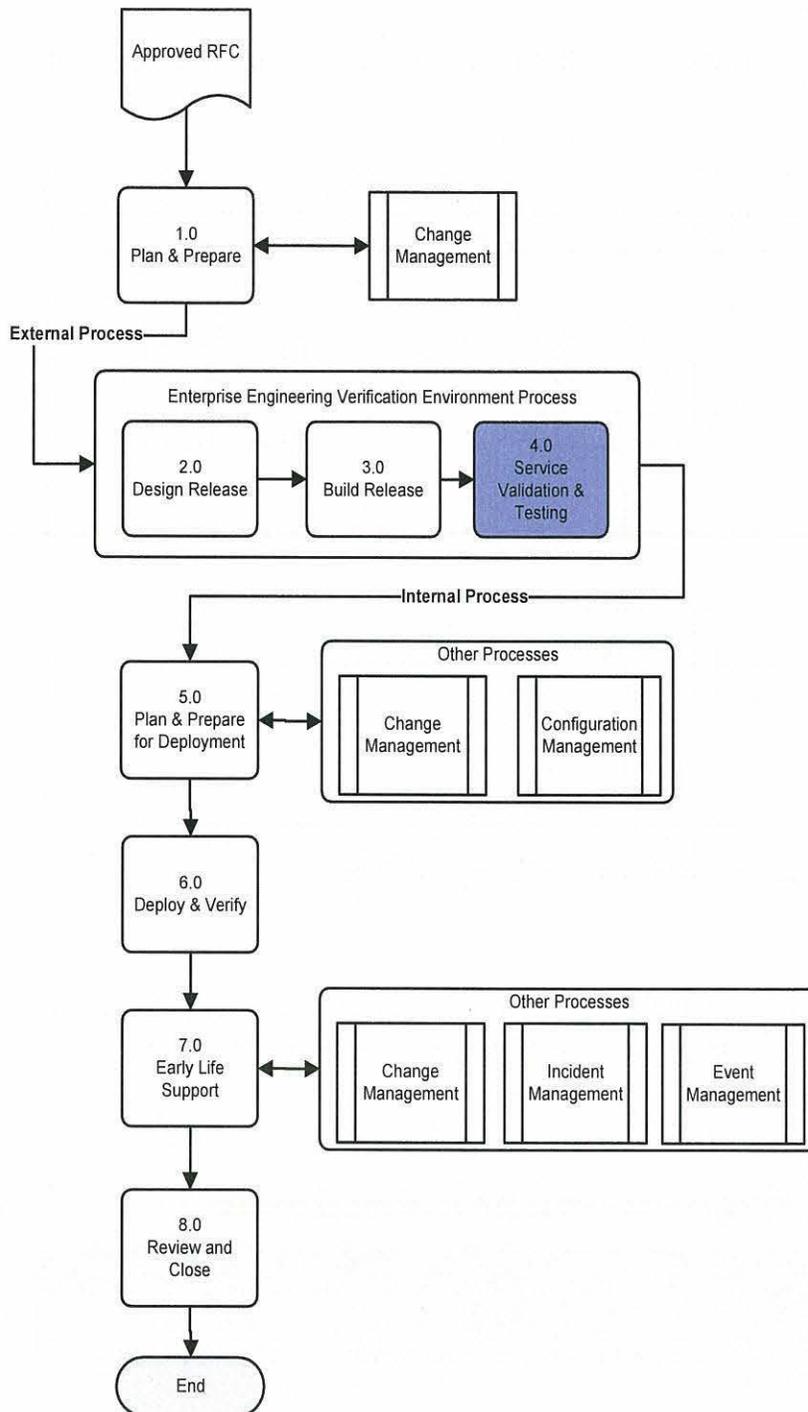


4.4 Service Validation and Testing



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.



All or some of the testing activities required are determined by the release plan and the implementation plan. These documents are validated, verified, and by the Service Test Managers and the Certification Test Managers.

Certification testing provides a recommendation to ChM for release approval or remediation of the release package.

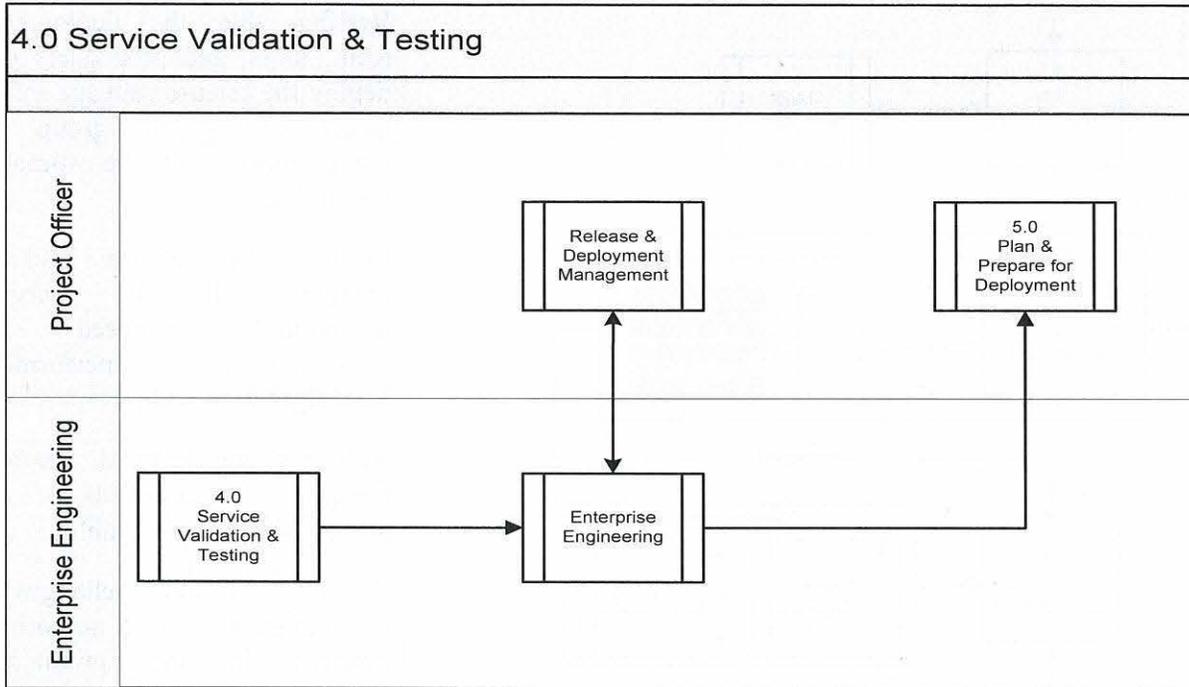


Figure 8. RDM Service Validation and Testing Sub-Process

Table 11 describes Service Validation and Testing process as a part of Enterprise Engineering steps as depicted in Figure 8. For more information, please review the Enterprise Engineering and Testing Process Guide.

Table 11. RDM Service Validation and Testing Sub-Process Descriptions

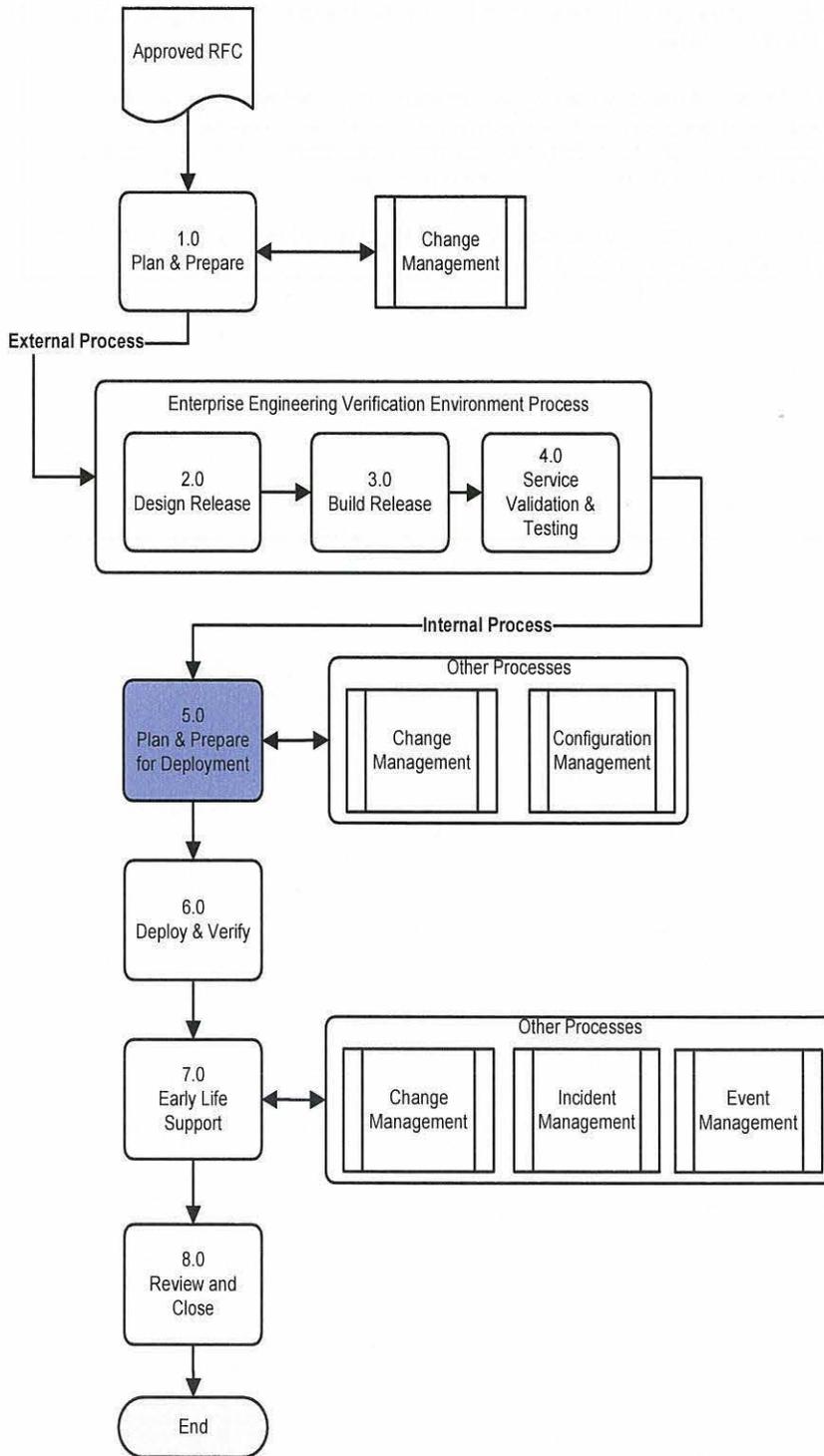
4.0 Service Validation & Testing		
Number	Process Activity	Description
4.0	Service Validation & Testing	<p>The test strategy defines the overall approach to organizing testing and allocating testing resources.</p> <p>The EEVE Team will build Test environments to the requirements specifications established to successfully test the build.</p> <p>The EEVE Team will execute the tests using standardized manual or automated</p>



4.0 Service Validation & Testing		
Number	Process Activity	Description
		<p>procedures. Testers record findings while testing. Tests are performed according to the test plans and cases.</p> <p>The EEVE Team will 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. These reports are reported to the Project Officer and to Change Management.</p> <p>RDM will assume the release has been validated and tested pulling from the DML in order to deploy into the environment.</p>



4.5 Plan and Prepare for Deployment



With recommendations from the Service Validation and Testing process presented to the MCEN Change Advisory Board (CAB) for review, the MCEN CAB approves the release to be deployed. MITSCs will participate in the MCEN CAB, as needed. 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.



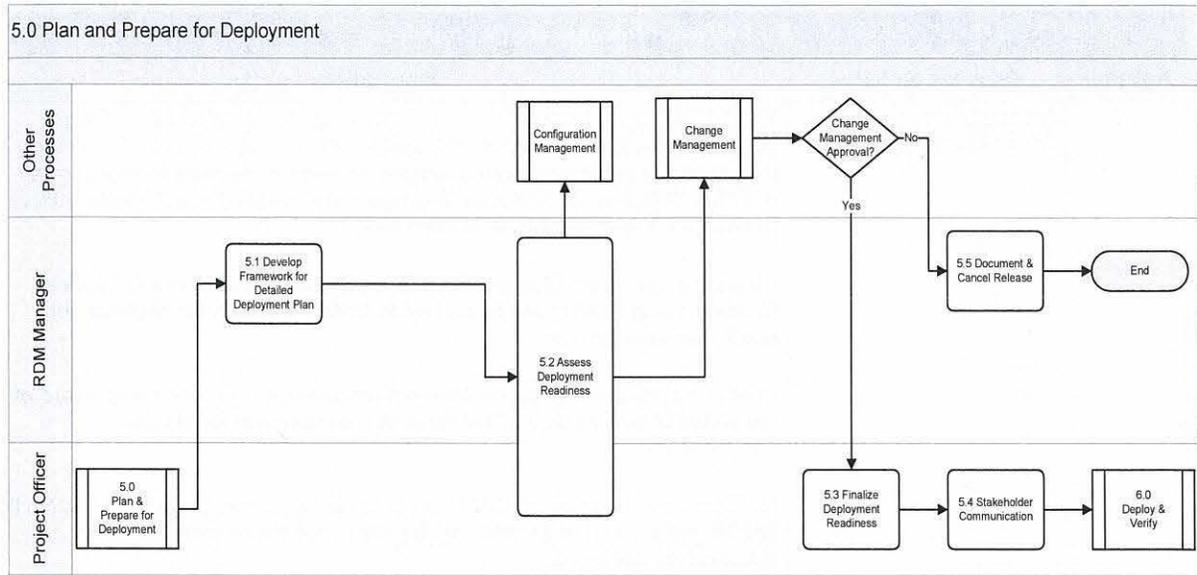


Figure 9. RDM Plan and Prepare for Deployment Sub-Process

Table 12 describes the Plan and Prepare for Deployment sub-process steps as depicted in Figure 9.

Table 12. RDM Plan and Prepare for Deployment Sub-Process Descriptions

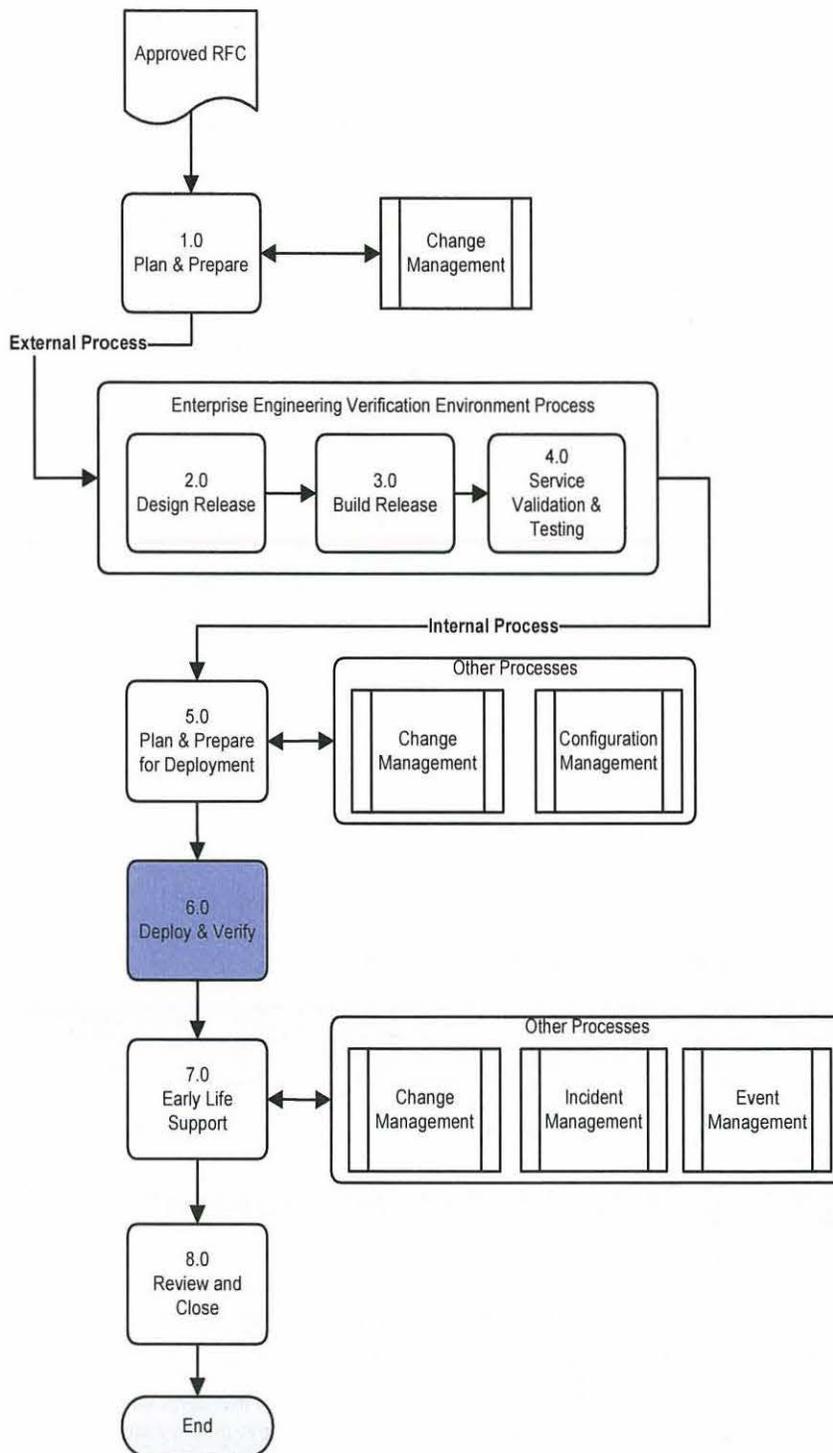
5.0 Plan and Prepare for Deployment		
Number	Process Activity	Description
5.1	Develop Framework for Detailed Deployment Plan	<p>The RDM Manager and RDM Coordinator will utilize the Implementation Plan (associated with the Release Plan) and perform a quality check on the release package. The RDM Manager will assess and validate the corresponding questions below:</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 RDM Manager will determine if staging the environment is required. If so, the RDM 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	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>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> <p>Notification will be sent to CfM in order to update corresponding CIs within the CMDB. Note: Final notification will be sent once the release has been successfully deployed.</p>
5.3	Finalize Deployment Readiness	<p>A deployment approval is received from ChM.</p> <p>The RDM Manager and Deployment Manager verify detailed deployment plans and finalizes deployment readiness tests. The release deployment is promoted to Deploy and Verify.</p>
5.4	Stakeholder Communication	<p>The RDM Manager and RDM Coordinator issue a formal notification to all stakeholders consulted in building the deployment plan.</p>
5.5	Document and Cancel Release	<p>If ChM rejects the deployment based on the testing results, the deployment recommendation and deployment readiness assessment, the RDM Manager documents the rejection and cancels the release record.</p>



4.6 Deploy and Verify



- Learning material has been made available to stakeholders
- Users are prepared to operate the new or changed service

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 RDM Manager verifies the release with the stakeholders, which can include:

- Service assets and capabilities are in place
- Documentation updates are completed



- Measurements and reporting systems are established
- Successful validation of the deployment triggers the launch of Early Life Support (ELS).

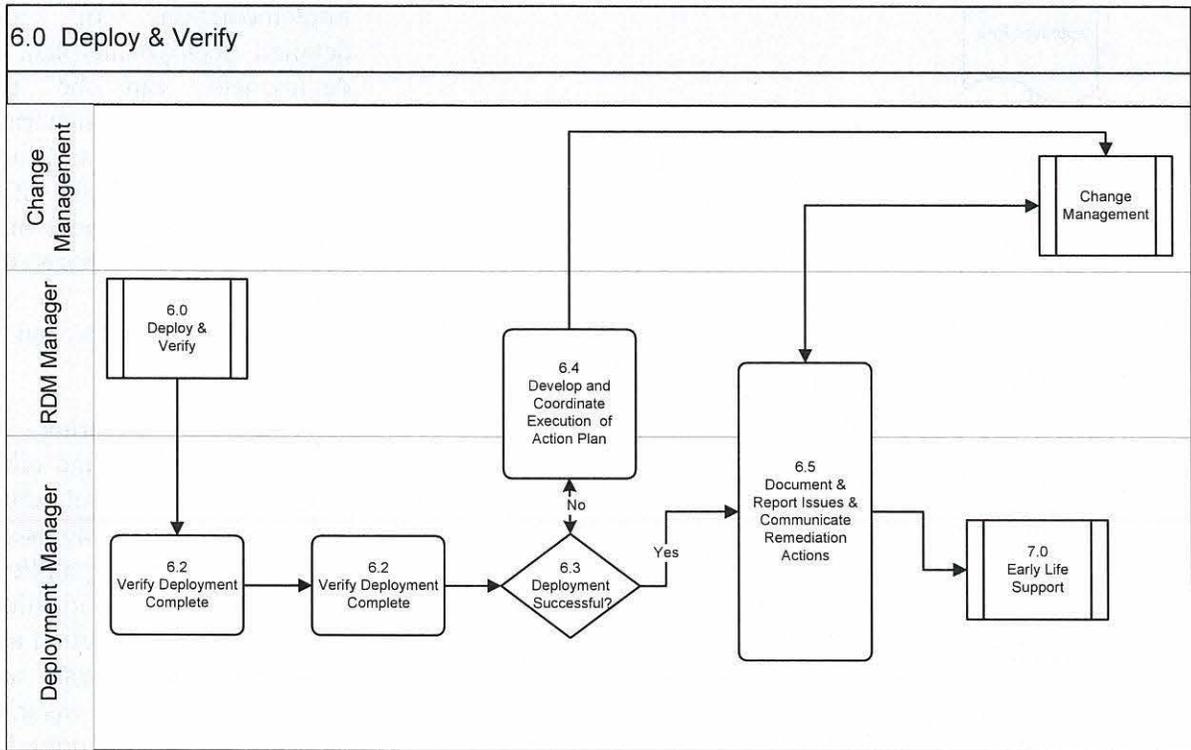


Figure 10. RDM Deploy and Verify Sub-Process

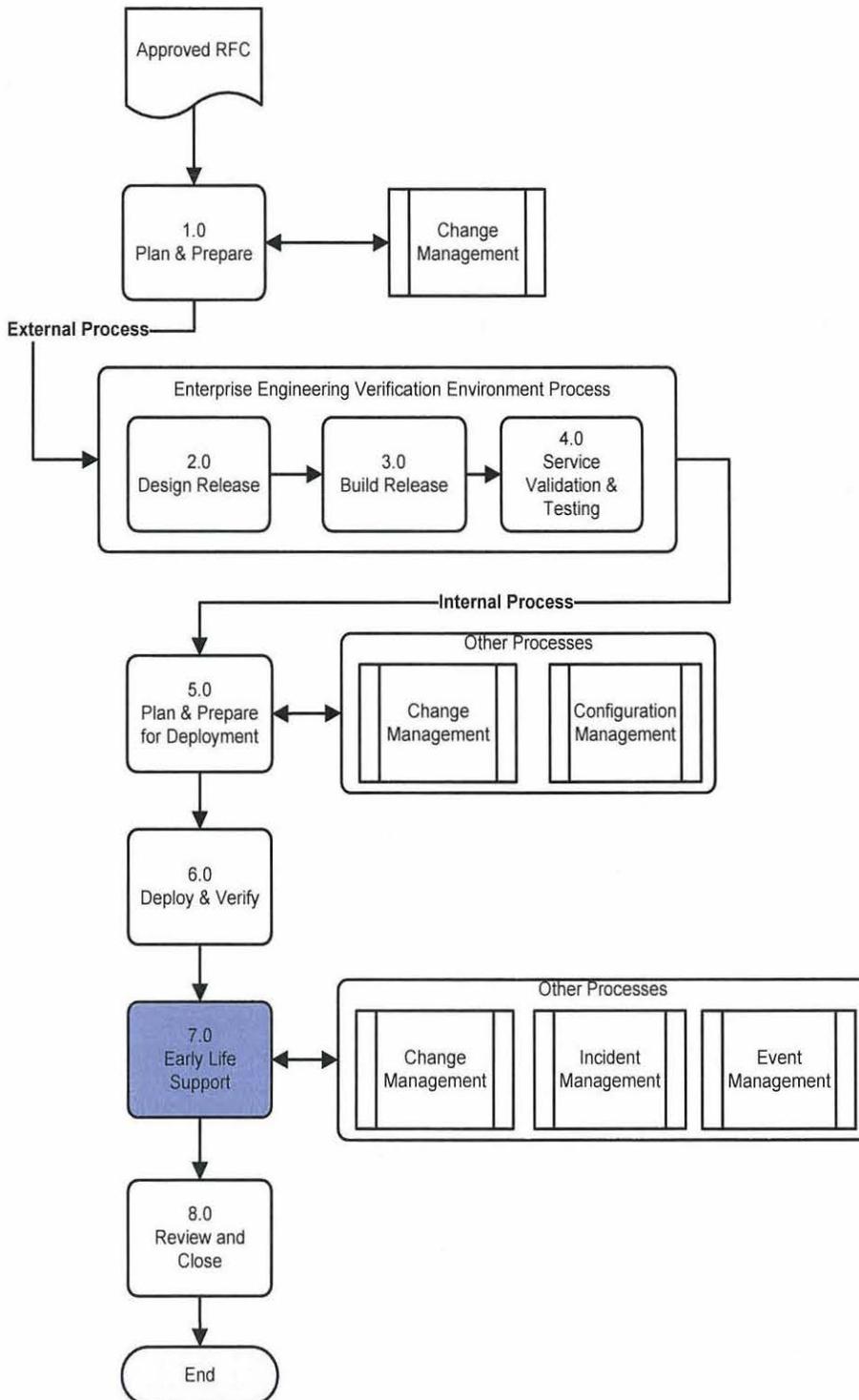
Table 13 describes the Deploy and Verify sub-process steps as depicted in Figure 10.

Table 13. RDM Deploy and Verify Sub-Process Descriptions

6.0 Deploy & Verify		
Number	Process Activity	Description
6.1	Execute Deployment	When adding a service, decommissioning, retiring a service or service asset, the Deployment Manager will deploy the service release package in accordance with the established PWIs.
6.2	Verify Deployment Complete	Validations will be executed by the deployment team in accordance with established PWIs.
6.3	Deployment Successful?	ELS entrance criteria met? If yes go to step 6.5, Document and Report Issues and Remediation Actions. If no, go to step 6.4, Develop and Coordinate Execution of Action Plan.
6.4	Develop and Coordinate Execution of Action Plan	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. The Deployment Manager notifies ChM of the execution of the action plan.
6.5	Document and Report Issues and Remediation Actions	The deployment team will document the results from each deployment step and develop remediation activities, as required. If no remediation is required, then the deployment is promoted to Early Life Support.



4.7 Early Life Support



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 RDM Manager negotiates with the stakeholders for release approval. Release approval may include known errors or back-out plans are invoked if a satisfactory release is not possible.



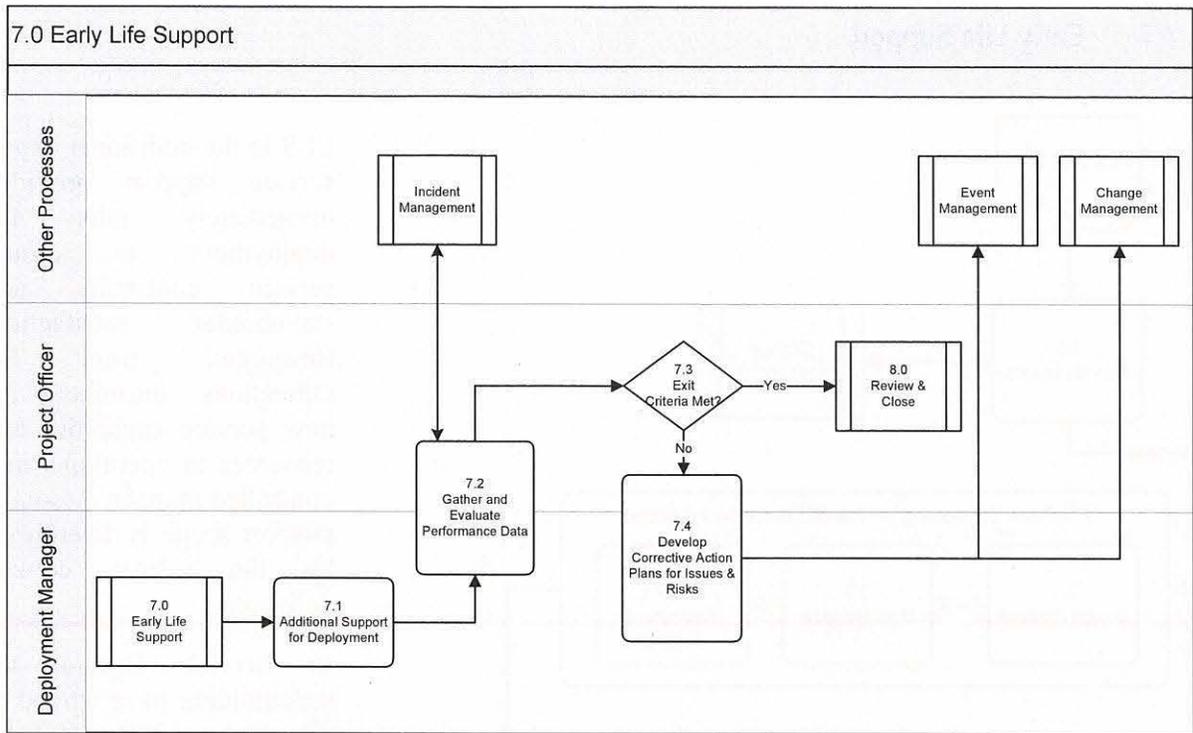


Figure 11. RDM Early Life Support Sub-Process

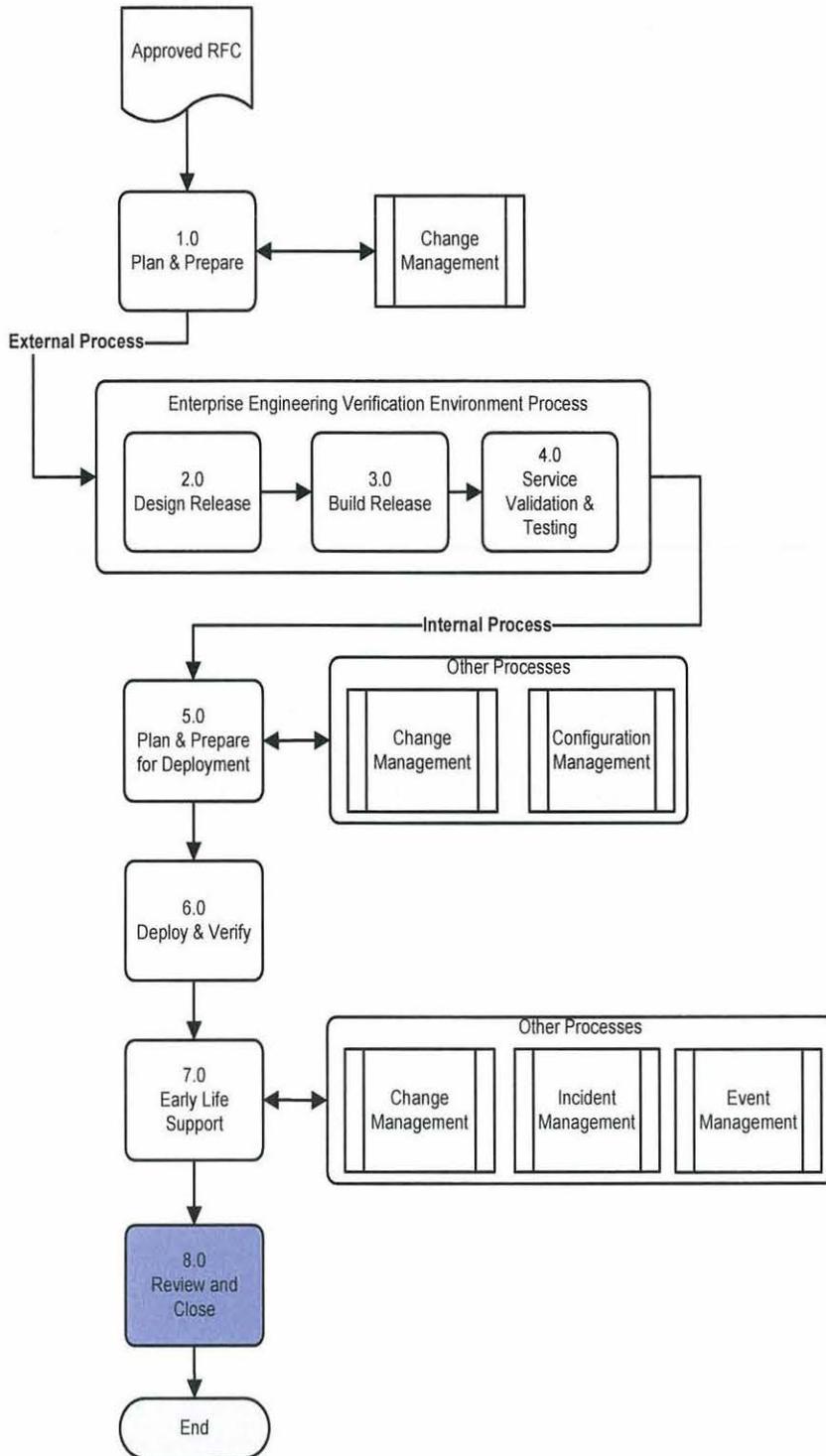
Table 14 describes the Early Life Support sub-process steps as depicted in Figure 11.

Table 14. 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.
7.2	Gather and Evaluate Performance Data	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.
7.3	Exit Criteria Met?	Exit criteria is defined in the PWIs. When ELS exit criteria is met, the release is promoted to Review and Close. If the exit criteria is not met, then move to 7.4 Develop Corrective Actions.
7.4	Develop Corrective Action Plans for Issues and Risks	If exit criterion is not met, corrective action plans are developed and implemented and forwarded to Change Management for review and disposition. Once a release has been successfully deployed into the environment, the deployment outcome is sent to both Event and Change Management.



4.8 Review and Close



The RDM 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 RDM 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 RDM Manager notifies the Project Officer who then 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.



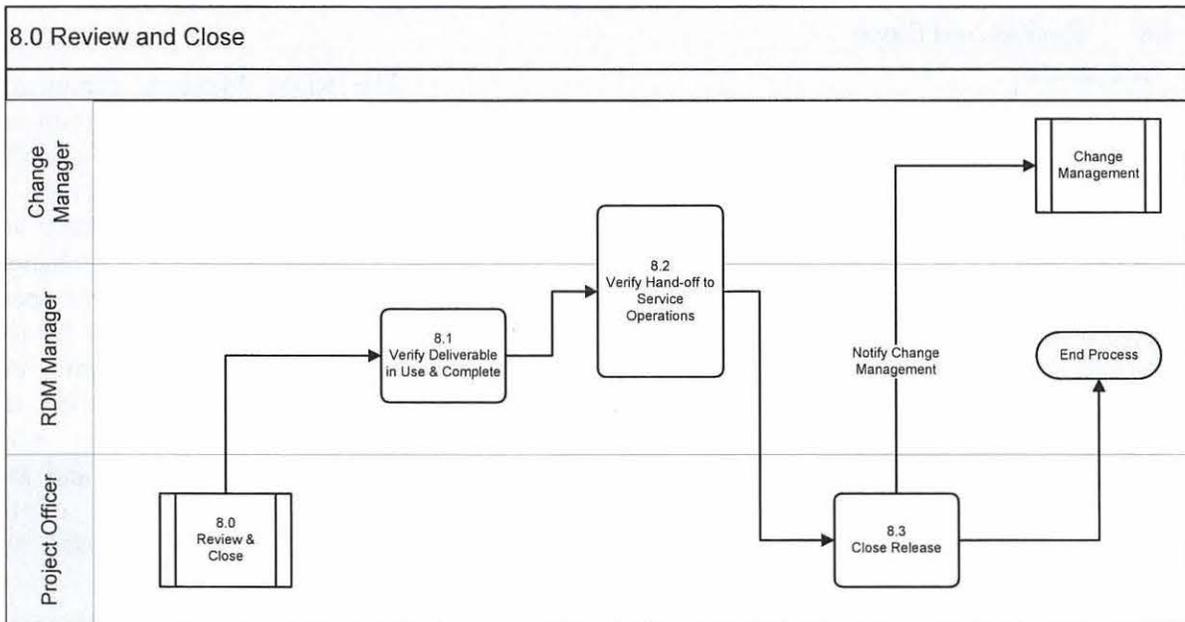


Figure 12. RDM Review and Close Sub-Process

Table 15 describes the Review and Close sub-process steps as depicted in Figure 12.

Table 15. RDM Review and Close Sub-Process Descriptions

8.0 Review and Close		
Number	Process Activity	Description
8.1	Verify Deliverable in Use and Complete	A deployment review is conducted, assessing the deliverable in accordance with established PWIs.
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 Project Officer closes the release , and ChM is notified that the release has been transitioned to Service Operations.



Appendix A – ACRONYMS

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

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



Appendix B – GLOSSARY

Term	Definition
Asset Management	Asset Management is the process responsible for tracking and reporting the financial value and ownership of assets throughout their lifecycle.
Back-out Plan	A Back-out Plan is developed in the Release planning phase. This plan provides a recovery plan to return to the original configuration or process if the release fails to achieve the planned outcome.
Change Schedule	A Change Schedule is a document that lists all approved changes and their planned implementation dates.
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 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.
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.



Term	Definition
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.
Governance	Governance is the process of ensuring policies and strategy are actually implemented and that required processes are correctly followed. Governance includes defining roles and responsibilities, measuring, and reporting and taking actions to resolve any issues identified.
Key Performance Indicator	A Key Performance Indicator (KPI) is a metric used to help manage a process, IT service, or activity. Many metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the process, IT service, or activity. KPIs are selected to ensure that efficiency, effectiveness, and cost effectiveness are all managed.
Known Error	A Known Error is a problem that has a documented root cause and a work-around. Known errors are created and managed throughout their lifecycle by Problem Management. Known errors may also be identified by SIE or suppliers.
Monitoring	Monitoring is the process of repeated observation of a CI, IT service, or process to detect events and to ensure that the current status is known.
Notification	Notification is a communication that provides information.
Process	A Process is a structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. A process may include any of the roles, responsibilities, tools, and management controls required to reliably deliver the outputs. A process may define policies, standards, guidelines, activities, and work instructions, if needed.
Quality Assurance	Quality Assurance (QA) is the process responsible for ensuring the quality of a product and also ensuring it will provide its intended value.
Role	A Role refers to a set of connected behaviors or actions that are performed by a person, team, or group in a specific context.
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 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.
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.



Term	Definition
Test Environment	A Test Environment is a controlled environment used to test CIs, builds, IT services, and processes.
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.

