Office of Information and Technology (OIT)

Change Management Process

Version 3.1

May 2014

Revision History

Date	Version	Description	Author
4/2010	1.0	Final version	Change Management TWG
1/2011	1.1	CR 7115 – Added instructions for updating document.	Approved by Mike LeRoy
6/2011	2.0	Replaced OI&T with OIT, modified roles to match ProPath map, Removed lead-time information, added suggested/recommended approval matrix based on priority/impact, changed highest priority from Emergency to Immediate. Added additional recommended fields for change order.	Approved by Integrated Technical Working Group
6/2012	3.0	Review and update of Priority, Urgency, Impact, and Risk tables	Russell McFall
5/2014	3.1	CR - CO213214FY14 submitted/approval for Review and update – Minor typographical and grammatical errors. No change to process Updated Concurrence and approval POCs	Russell McFall; Don Williamsen; Brenda Hall

Table of Contents

1. Introduction

1.1. Process Purpose

The purpose of the Change Management (ChM) process is to provide guidance for the management of changes to all Department of Veterans Affairs (VA) Information Technology (IT) environments. The process provided guidance on how to manage a change throughout its life cycle. This process applies to environments in production, development, and testing. The process is made up of interrelated activities, including activities that measure the effectiveness of the process, and it provides continued process improvement. In summary, the process captures the change request, categorizes it by Priority (Urgency + Impact) risk and complexity to the IT environment, acquires business and technical perspectives and identified changes to related system documentation that will need to be made to support the system (IT Security Plan, Configuration Management Plan, Continuity of Operations Plan (COOP), etc.) prior to granting official approval. The request is then scheduled, implemented, and verified during the Post Implementation Review (PIR) to determine whether it was successful. The process will communicate the status of the change among the participants and any actions required on their part.

The purpose of this document is to define the Change Management (ChM) process for the Department of Veterans Affairs (VA) Office of Information and Technology (OIT). This process applies to all VA IT assets under the management of OIT, its employees, its contract-based resources, and other third-party service providers.

This Process Document communicates the high-level process flow for OIT Change Management. This process is consistent with the Federal Information Security Management Act of 2002 (FISMA), 44 USC §3541-3549, and P.L. 107-347, Title III, and VA Directive 6500, Information Security Program, and VA Directive 6004, Configuration, Change, and Release Management Programs to provide a process infrastructure utilizing industry standards to support information technology management.

1.2. Scope

This process applies to all VA related components and information technology resources, including contracted Information Technology (IT) systems and services. This Change Management process supports the following general types of IT projects and activities on those systems:

- Software/Hardware Architecture and Design
- Software/Hardware Engineering
- Software/Hardware Development
- Application and General Support System Certification and Accreditation
- Electronic Documentation
- Environmental Changes

This Change Management process is applicable and appropriate for all type of IT assets. Its requirements communicate an overall process that is not constrained to nor assumes any one type of asset, project, or activity across VA.

1.3. Objectives

The Change Management process accomplishes the following objectives:

- Establish an OIT Change Management process
- Standardize methods and procedures that follow sound Change Management principles
- Communicate an adaptable framework for change management that allows OIT offices to incorporate the principles of change management into their business functions and work products as a routine procedure
- Allow OIT to reinforce a commitment of minimizing or preventing adverse effects on VA information systems, as a result of a lack of proper planning, documentation, and/or coordination through an approved standard process

1.4. Change Management Champion

This process is championed by the Assistant Secretary, Office of Information and Technology.

1.5. Change Management Process Document Modifications

This document has been placed under version control in the ProPath library. Access to the MS Word file under control (oit_change_management_process_document.doc) will be managed through the ProPath Change Request process. Approval of Change Requests affecting the Change Management Process must be obtained from the Integrated Technical Working Group (TWG).

ProPath Change Request Link: http://vaww.oed.oit.va.gov/process/change_control/

This file has been converted to a pdf and is available as read-only through the ProPath maps or the ProPath main page http://vaww.oed.oit.va.gov/process/propath/ via the Direct Access link.

2. Responsible, Accountable, Consulted, and Informed (RACI) Matrix

The purpose of the RACI Matrix is to create a matrix of activities and roles and sufficiently define the Responsible, Accountable, Consulted, and Informed (RACI) participation level.

This is accomplished by allocating, to each activity, task, or decision, the role that is accountable and/or responsible for the activity as well as those roles to be consulted with beforehand, or informed afterward.

Definitions for RACI are as follows:

> **Responsibility (R):** the correct execution of the process and activities. The person(s) or group(s) who actually execute the task are said to be responsible.
>
> **Accountability (A):** the ownership of the quality of the end result and process. For each activity, only one role (person or group) should be accountable.
>
> **Consulted (C):** involvement through input of knowledge and information. If the activity requires a response or input from a person or group, they are considered consulted.
>
> **Informed (I):** receiving information about process execution and quality. If the activity requires that a person or group receive information only (per activity or in summary form), then they are informed.

The below chart provides the suggested RACI Matrix for the *Change Management* Process. The “x-axis” of the RACI Matrix shows all of the relevant roles within the organization and appropriate touch points outside of the organization. The “y-axis” lists the activities, tasks, and decisions that make up the organization’s work.

RACI Matrix

PARTICIPATION CODES R = Responsible A = Accountable C = Consulted I = Informed	PROCESS ROLES												
ACTIVITIES	**Project Manager/System Owner**	**Change Initiator(End User)**	**Configuration Management Analyst Librarian**	**Change Submitter**	**Change Coordinator**	**Change Manager**	**Release Manager**	**Configuration Manager**	**CAB/Technical Subject Matter Expert (SME)**	**Appropriate Approval Authority**	**Business Partners**	**Implementer**	**Build Manager**
5.1. Initiate Change													
Creating a RFC	A	C	I	R	R	I			C		I		I
5.2 Analyze/Plan Change													
Standard Change Determination	A		I		R	C	I					R	
Emergency Change Determination	A	I	I	I	R	C	I			R		R	
Normal Change Determination	A		I		R	C	I						
Developing the Business Case Justification	A	C		C	R	C	I		C		C	C	
Technical, Customer and Security Impact Analysis	A	C		C	R	I	I		R		C	C	
Developing a Back-out plan	A	I		C	R	I	I		R	I		C	
Risk Analysis	A	C		C	R	I	I		R	I	C	C	
5.3 Approve Change													
IT Business Unit Manager Review and Approval	A	I		C	I	I			R		C		
Conducting the Peer Review and Approval	A				R	I			R			C	
Approvals Required for Change Based Priority (Urgency/Impact) and Risk Level	A	I		C	R	C			I	R	C		I
5.3.1 Emergency Change Procedures and Approval Process	A	C		R	R	R	I	I	C	R	I		
5.4. Fix/Develop Change													
Assign	A				R				I				I
Fix/Develop	A				I				R			R	
Build	A				I				R				R
Test	A	I		I	I	I			R		C	R	
5.5 Implement Change													
Obtain Release Package from Release Management	A	I	I	C	I	I	R		I			I	C
Final Planning	A	C		I	R	I				I	C	R	
Scheduling and Notifications	A	C		I	R	I				I	C	R	
Change Implementation	A	I	I	I	I	I				I	I	R	
5.6 Validate Change													

Change Verification	A	R			I	I			R	I	C	R	
Testing, Validation and Acceptance	A	R			C	I			R	I	C	C	
Accept Issues and Continue	A	R	I		R	I					C		
Monitor Change in Production Environment	A				R	I			R		C		
Hold Post Implementation Review	A	I			R	I			C		C	C	
Updating Configuration Management Database	A		R		C				R				
Close Change	A	I		I	C	R		I			I		I
6. Metrics													
Producing and Monitoring Metrics	A		I			R	I			I			
7. Process Verification													
Change Compliance	A					R				R			
Measuring Quality in the Change	A				R	R				I			

2.1. Process Roles and Responsibilities

Process roles and responsibilities are identified in the context of the management function and are not intended to correspond with organizational job titles. Specific roles have been defined according to industry best practices. In some cases, individuals may share a single role; and in other cases, an individual may assume multiple roles.

Table 1 lists the key roles and their descriptions for the Change Management process.

Table 2-1: Roles and Descriptions

ROLE	DESCRIPTION
Change Initiator (POC)	The Change Initiator is the primary point of contact (POC) that initiates a request for change representing the end user community. This person can be a business representative or a member of the IT organization. The initiator may be consulted during the analysis and implementation of a change, is kept informed of the status of the change and is also responsible for validating that the implemented change was successful in the eyes of the end user community.
Change Submitter	The Change Submitter (Requestor) receives a request for change (RFC) from the Change Initiator and performs the initial analysis to sufficiently document the request for change in the Change Management system. This is the individual that is requesting the Request For Change (RFC) on behalf of the Change Initiator (POC), and may be the same as Change Initiator (POC).
Change Management Process Owner	The Change Management Process Owner is accountable to senior management for proper governance, design, execution, and improvement of ChM processes in an OIT office.
Change Coordinator	The Change Coordinator is responsible for planning and implementing a change in the IT environment. This individual is identified for a particular change and assumes responsibilities upon receiving an approved RFC. The Change Coordinator is required to follow the approved change schedule. The Change Coordinator is responsible for planning and coordinating all of the phases of the change from submission through acceptance and documentation.
Release Manager	The Release Manager is responsible for planning, executing, and reporting on release-specific change requests/orders, and configuration item additions/modifications necessary to implement packaged change.
Change Manager	The Change Manager is responsible for ensuring proper introduction, execution, and status reporting of all Change Management (ChM) processes over Configuration Items (CIs) within their control. In addition, this individual is responsible for execution of verification and audits of ChM data and all coordination and communication regarding the status of all RFCs.
Configuration Management Analyst	The Configuration Analyst is responsible for performing daily CM operations for identification, control, status reporting, and audit of CIs under the leadership of the Configuration Manager.
Configuration Management	The Configuration Manager is responsible for ensuring proper introduction, execution, and

Manager	status reporting of all CM processes over CIs within their control. In addition this individual is responsible for execution of verification and audits of CI data and all coordination and communication regarding the status and availability of CIs.
Change Management Administrator	The Change Administrator is responsible for performing daily ChM operations for meeting facilitation, status reporting, data entry, and technical writing of ChM materials, under the leadership of the Change Manager.
Change Management Analyst	The Change Analyst is responsible for assisting Change Submitters/Coordinators, managing the change process and reporting to the Change Manager any deviations in the process.
Appropriate Approval Authority	The appropriate level of approval based on the Priority (Urgency and Impact), and risk the change will have on the organization. The approval could come from one or more of the listed: Project Manager, System Owner, Departmental Supervisor, Change Manager, Release Manager, or an established board set up to review and approve changes. **Change Management Governance Boards** – Change Management Governance Boards will be established for oversight of the VA OIT Change Management Process. The minimum number of governance boards necessary will be created to ensure representation of stakeholder organizations appropriate to the impact and risk of the Request for Change. **Executive Level Change Control Board (ECCB)** – Will enable executive-level decisions and may delegate authority to subordinate boards at their discretion. **National Change Control Board (NCCB)** – Will enable national-level decisions and may delegate authority to subordinate boards at their discretion. **Regional Change Control Board (RCCB)** – Will enable regional-level decisions and may delegate authority to subordinate boards if needed/required. **Emergency Change Committee (ECC)** – This is a subset of a Change Control Board (CCB) that deals only with Emergency Changes. The CCB/ECC meets on short notice to authorize or reject changes with emergency priority. They are responsible for adhering to the approved emergency escalation process. **Stakeholders** – Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), National Cemetery Administration (NCA), and other customers involved with the change.
Change Management System Administrator	The Change Management System Administrator provides subject matter expert knowledge on the ChM tool environment and its underlying databases.
Stakeholder	All people who have an interest in a change. Stakeholders may be interested in the activities, targets, resources, or deliverables of a change. Stakeholders may include customers, partners, employees, shareholders, owners, contractors, etc.
CAB/Technical SME	The Change Advisory Board (CAB) or Technical SME's are responsible for executing individual tasks within a RFC and ensuring they are completed according to the implementation plan.
Implementer	Technical SME responsible for the development of a fix, implementation, and validation of the technical part of the change
Project Manager/System Owner	Have overall accountability over changes made to their respective systems or processes. Verifies that the changes have been correctly implemented and have not caused any other related issues. The Project Manager or Systems Owner will ensure that proper change plans have been developed based on established National Policy and Procedures and are placed under configuration control.
Business Partners	Business Partners are those areas of the organization that need to be kept in the loop or that need to provide some level of review and feedback to changes affecting systems.

3. Change Management Process

The process outlined below is to be followed by all VA employees, contractors, and third parties responsible for implementing change to the IT infrastructure based on the scope outline in this document. The basic steps associated with the Change Management process for the Department of Veterans Affairs are listed below:

Initiate Change
Analyze/Plan Change
Approve Change
Fix/Develop Change
Implement Change
Validate Change

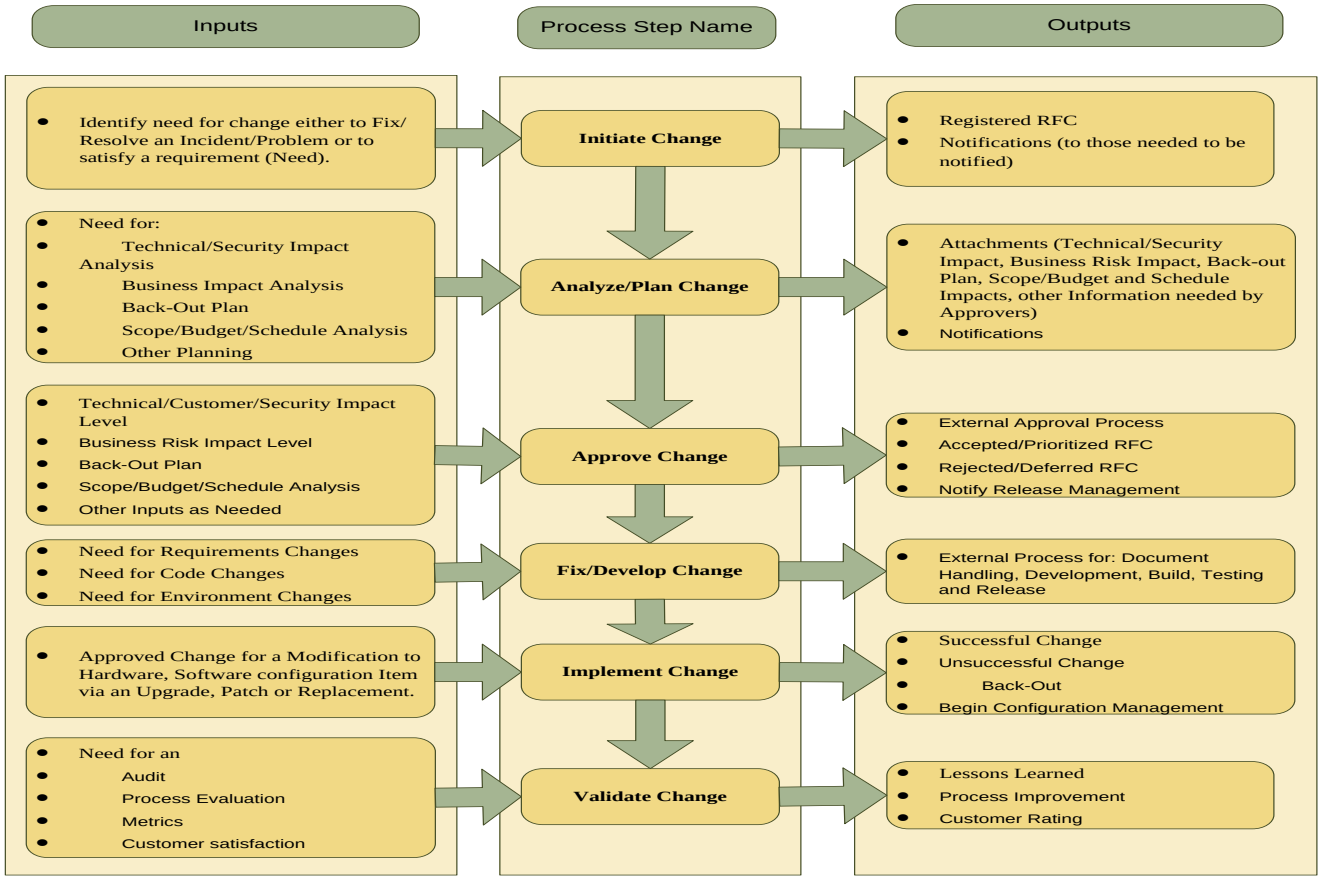


Figure 3-1: Change Management Process

3.1. Change Management Process Entry Criteria

Change Management enables beneficial changes to be made with minimal disruption to IT services.

3.1.1. Process Inputs

Below you will find a list of each of the Change Management Process steps along with its associated input

Initiate Change

- Action Items
- Establishing and updating a Baseline
- Business Need assessment
- Incidents
- Legislation
- Policy Change
- Problems
- Requests that affect more than one user
- Security Mandate
- Software Configuration Management Procedures
- Vulnerability Notifications
- ESE Process Documentation
- OIT Change Management Process Document

Analyze/Plan Change

- Input from Business Partners, Security, Engineering
- Request for Change
- Software Configuration Management Procedures
- OIT Change Management Process Document

Approve Change

- Request for Change
- OIT Change Management Process Document

Fix/Develop Change

- Request for Change
- Software Configuration Management Procedures
- OIT Change Management Process Document

Implement Change

- Approved Request for Change

Software Configuration Management Procedures
OIT Change Management Process Document

Validate Change

Request for Change
Software Configuration Management Procedures
OIT Change Management Process Document

3.1.2. Process Outputs

Below you will find a list of each of the Change Management Process steps along with its associated output

Initiate Change
- Notifications to affected and responsible entities
- Registered Request for Change

Analyze/Plan Change
- Business Case Justification
- Risk Assessment
- Updated Request for Change

Approve Change
- Approved/Rejected Request for Change
- Software Configuration Management Procedures

Fix/Develop Change
- Updated Request for Change

Implement Change
- Updated Implemented Request for Change

Validate Change
- Completed After-Action Report (if required)
- Completed (successfully or unsuccessfully) Request for Change
- Completed Test Results

3.1.3. Exit Criteria

Validate
- Successful change
- Unsuccessful change

Process Assessment

Lessons Learned

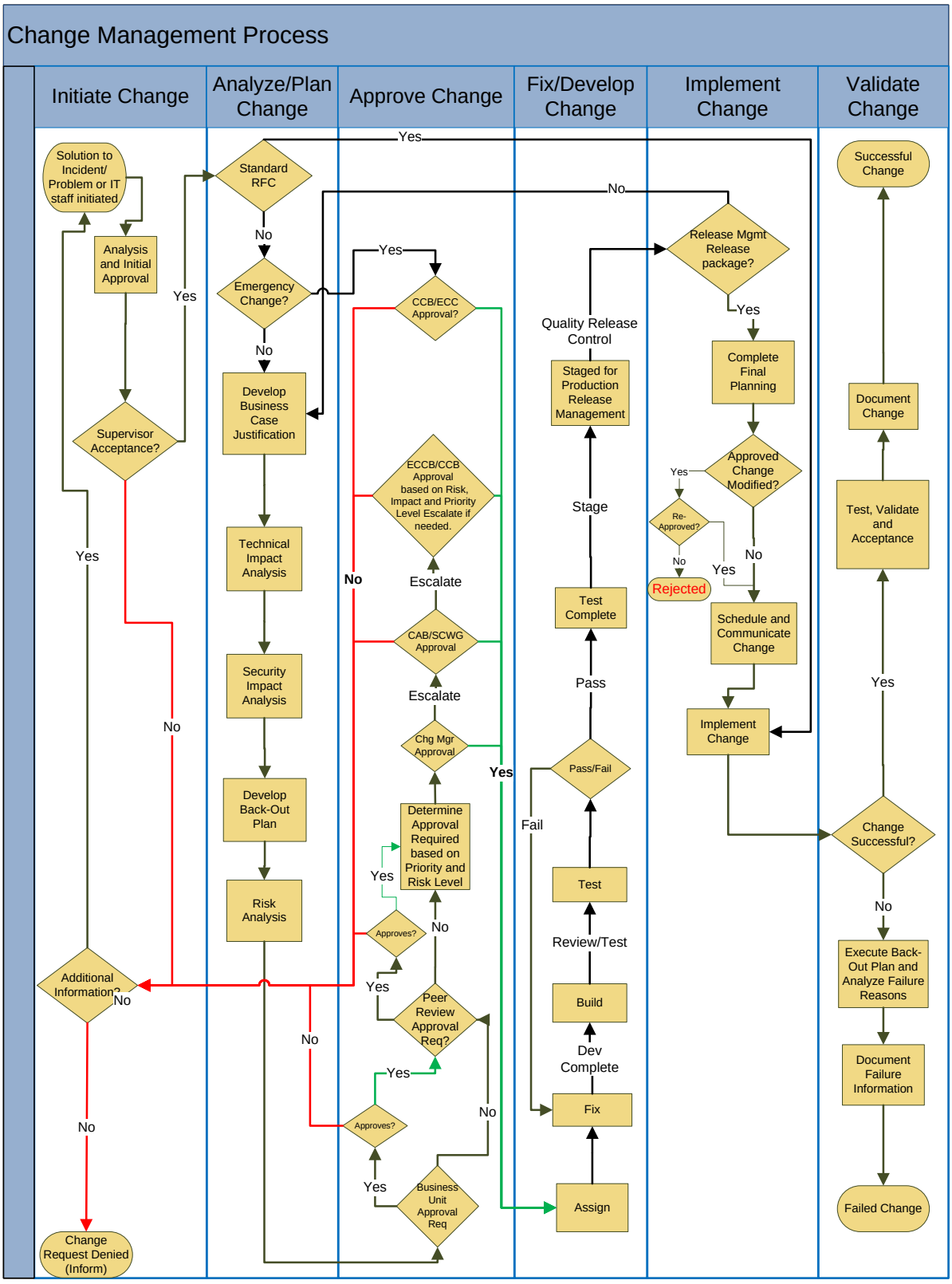
Process Improvement

Customer Rating

4. Related Processes

Incident Management
Problem Management
Release Management
Configuration Management
Risk Management
Security Management

5. Change Management Process Steps



5.1. Initiate Change (New Request for a Change)

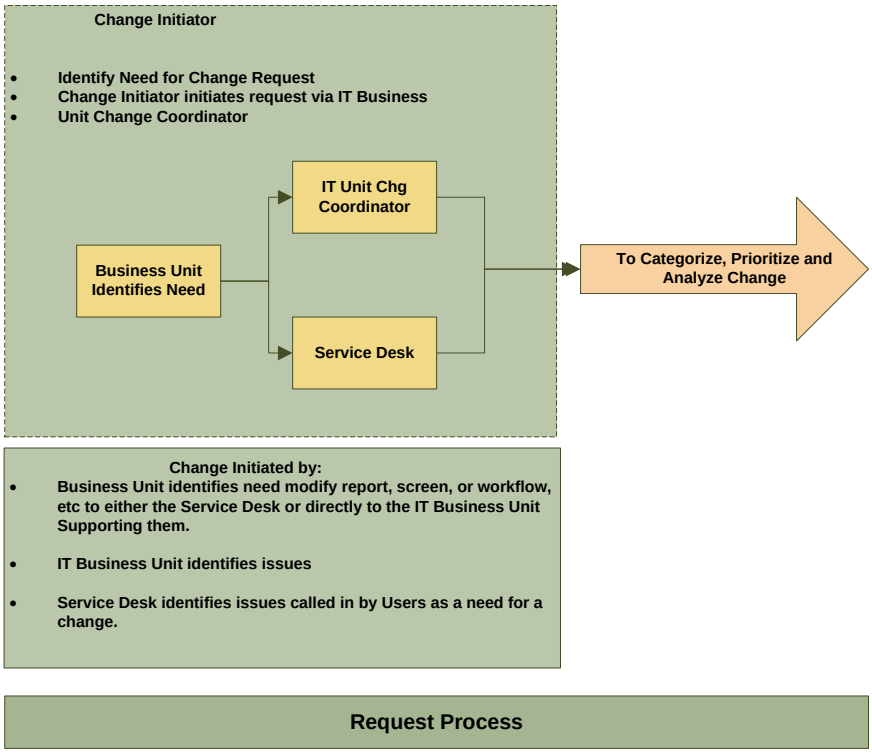
Within the Department of Veterans Affairs, changes are identified by the business customer, including Veterans Health Administration (VHA), Veterans Benefit Administration (VBA), and National Cemetery Administration (NCA), and by the internal OIT divisions, Data Centers, Service Lines (Systems, Network, Telephone, Facilities), or Help Desk/Service Desk. Anyone identifying a requirement for change functions as the Change Initiator and is responsible for providing the necessary information to identify the basic requirements associated with the change. It is critical that the change management process is consistent in quality and completeness and that it rejects invalid requests. Although a change request can be submitted by anyone within a business or IT unit, it will receive an initial review by the Change Coordinator within the appropriate IT business unit. The Change Coordinator will determine if there is sufficient information to create the change request and will create a new change request within the Change Management Process. They will contact the Change Initiator if additional information is required.

Inputs

Change Initiators can identify the need for a change through the Customer Help Desk/Service Desk or directly to a Change Coordinator in the IT Business Unit by phone or email.

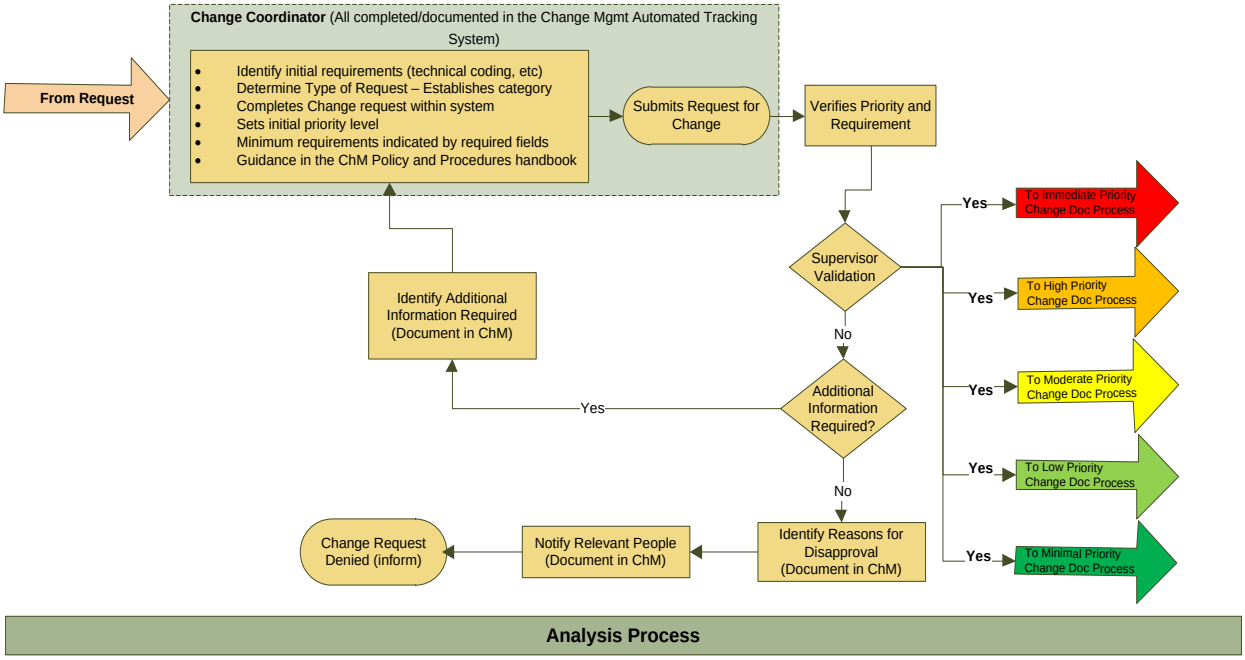
In the current change process, the IT Business Unit normally initiates changes based on their findings or a conversation with the relevant business unit. In these cases, the person in the IT Business Unit will function in the role of Change Initiator and may also function in the role of the Change Coordinator.

All documentation relevant to the change should be maintained together. Any documents created during the change process should be attached to the change record.



Analysis and Initial Validation Process: For the creation of the new change request, the Change Coordinator will collect additional information to help them further enhance the change parameters. This

additional information includes identifying specific coding or other technical requirements, and it establishes the initial priority and category. The diagram below shows a more detailed workflow of the analysis phase which includes the actual creation of the change request, establishment of the initial priority level, and the approval at the IT Manager level.



Responsible Persons

Change Submitter

Activities

Creating an RFC: The RFC is the document the OIT Change Coordinator creates that captures all of the relevant information regarding the proposed change. This information may range from basic facts regarding the change to more complex technical specifications necessary to complete the change.

The following are examples of the types of information/fields to be included, but are not limited to, in creating an RFC:

Change Request Number: a unique number that is used to identify the request for change.

Change Submitter (POC): submitter name and contact information.

Change Initiator (POC) (Affected End User)**:** name and contact information if different from Requestor.

Change Coordinator: name and contact information (Change Owner).

Organizational ID: a code that is standardized for the organization responsible for maintaining the Configuration Item (CI).

Change Type what is the type of change that is being documented.

- **Normal:** All changes follow a standardized change process model for the type of change being implemented. This process takes the change through its entire lifecycle; Registration, Analysis, Approval, Develop/Test/Build, Release Approval, Scheduling, Implementation and Verification.
- **Standard:** Is a change to a service or infrastructure for which the approach is pre-authorized by Change Management that has an accepted and established procedure to provide a specific change requirement.
- **Emergency:** Reserved for changes intended to repair an error in an IT service that is negatively impacting the business to a high degree. Changes that introduce immediate and required business improvements are handled as normal changes, assessed as having the highest urgency.

Category: This defines the change family, class and type, and serves as a means of classifying a change so that it can be searched on, reported on, etc. Categorization is described in the form of types of changes (*Change to Service Portfolio, Change to Service or Service Destination, Project Changes, User Access Requests, Operational Activity*). Process models are predefined steps that should be taken to handle a process or type of change in an agreed way/manner. These process models can be automated in a CMS tool but require unique names. Categorization naming convention is built into these process flows to standardize them. Since these process flows (workflows) have specific requirements for specific groups or individuals to perform tasks along the process path, they must be unique.

- Network/Infrastructure
- Security
- Clinical Applications
- Business Systems Applications
- Core Systems
- Client Technology
- Mobile Technology

Status - What is the current status of the change (Open, Approved, Pending Approval, Implementation in Progress, Backed out, Cancelled, Closed etc.). The status of the change order continuously changes through the life cycle of the change. It is imperative for the Change Manager to know at any given time which changes have entered into any of the following status types: Approved, Pending Approval, Schedule, or Pending Implementation. These statuses allow users to filter changes that have not been approved or are awaiting approval to be reviewed. Examples of suggested statuses include:

Table 5-1: Change Status

Status	Status Description
Analysis Review	Stage of the process when Business Case Justification, Technical Review, and Security Review are conducted.
Approval in Progress	Status of the change order during the approval process; this status is maintained while all approvals are being obtained.
Approved	Once all approvals have been obtained, the change order will be set to this status.
Backed out	This status indicates that the change order had to be backed out due to an unsuccessful change implementation.
Build	Stage of the process in which different artifacts/documents are gathered and one build is developed for release to the field.
Cancelled	This is used to cancel out a change order that is no longer needed or rejected.
CCB Review	After a CAB review, if a determination is made to have a Change Control Board review and approve the change order, this status should be used.
Closed	Final status of a change order once all stages of the change have been completed. The final status of a change should be closed if not backed out, rejected, or cancelled.
Development	Development of a solution.
Hold	If the change order needs to be placed on hold at any time during the life cycle of the change.
Implementation in Progress	The status of the change order should be placed into this status when it is being implemented.
Open	If a change order has to be re-opened for any reason, it must be placed in an open status.
Pending Implementation	Status changed to Pending Implementation delineates those that have been approved and are pending release approval, or scheduling. This status indicates that all tasks have been completed, and the change is pending the implementation status just before Implementation In Progress.
Pending Release	When the change is being assessed by the release process and is Pending Release, it enters this status.
Pending Scheduling	Stage of the process when the Change Coordinator ensures that the date selected for implementation can be accomplished and will not interfere with other changes.
Rejected	Change that the approving authority has deemed as not acceptable or has been rejected by the approval authority. If the change is not needed for whatever reason, use change status "Cancelled".
Request for Information or Needs Revision	The creator, Requestor, or task assignee may require additional information to make a determination on the change. This status should be used to communicate that additional information is needed to the Change Owner. .
Resolved	Once the change has been verified, the status should be changed to Resolved. This indicates that the change has been implemented, and the intent of the change has been obtained.
RFC	Request for Change - this is the initial status of a change order when it's created.
Scheduled	After approval, the change order will be scheduled. Once this has been completed, the status should be changed to Scheduled.
Suspended	If problems are noted or arise during the implementation of the change, the status should be modified to suspended.
Testing	The developed change is tested on test systems.
Updated	If the change order was placed in a needs revision status after it has been updated, the status should be changed to Updated.

Verification in Progress	Once the implementation has been completed, the status will be changed to Verification in Progress to identify those changes that have been implemented. They await final validation/verification that no issues have been found.

Trigger: What initiated the change (Purchase Order, Problem Report Number, Error Record, Business Need, and Legislation?)

Urgency: Identified by the numeric value that represents the description below. Urgency is described as how quickly a change must be put into effect to resolve a business or technical requirement.

Table 5-2: Urgency

Urgency	Urgency Definition
(1) Critical	Production System unavailable must be installed within **12 hrs but not later than 72 hrs.**
(2) Serious	Production System delayed (Potential Impact on Business Function) must be installed within **one week.**
(3) High	Production System delayed (Potential Impact on Business Function) must be installed within **two weeks.**
(4) Moderate	Production/Pre-Prod/Development – System not working within designated specifications (available No Business Impact) must be installed within **three to four weeks**.
(5) Minimal	Productions/Pre-Prod/Development – Request for service (No Business Impact) change can wait **four weeks or longer** before having to be implemented.

Impact: Measure of the criticality of an incident, problem, or change from a business perspective.

Table 5-3: Impact

Impact	Impact Definition
(1) Critical	A change where the impact could be severe, extensive, and involves a potential impact on the highest percentage of users on business-mission/special critical systems. Users experience a complete or substantial loss of service when using a production system, or a real or perceived data loss, or data corruption, makes an essential part of the production system unusable. This also applies to the inability to use a mission-critical application within a production system.
(2) Serious	Affects a high percentage of users. A change where the effect is widespread, but it is not massive. Affects users of Essential Business systems.
(3) High	Affects a moderate percentage of users or an event where the effect is widespread, but not massive.
(4) Moderate	Affects a smaller percentage of users, and the risk is less because of the organization's level of experience with the proposed change. Affects systems identified as Routine Support.
(5) Minimal	A pre-defined change type affecting the smallest percentage of users, consistently follows documented release process, and is pre-approved.

Priority: A value to identify the relative importance of a change. It is based on urgency and impact.

Table 5-4: Priority Matrix

Impact \ Urgency	1	2	3	4	5
1	1	1	2	3	3
2	1	1	2	3	4
3	2	2	3	4	4
4	3	3	4	4	5
5	3	4	4	5	5

Table 5-5: Priority Description

Priority Level	Priority Level Definition
(1) Immediate	Immediate change to a production system required to prevent a **SEVERITY 1** (SEV 1) incident from occurring, or restoration of services associated with an incident, or the absence of a required change will contribute to a system being placed at a high risk of an incident associated with it.
(2) High	Severity affecting many users or having an impact upon a large number of users. Could also be for certain defined major applications or hardware no matter how simple the change is. Highest priority for change-building, testing, and implementation resources should be allocated.
(3) Moderate	Moderate impact affecting less than 30% of users or having an impact upon a moderate number of users. Could also be for certain defined major applications or hardware no matter how simple the change is. Moderate priority for change-building, testing, and implementation resources should be allocated.
(4) Low	No severe impact. Rectification of an incident *cannot* be deferred until the next scheduled upgrade. Low priority for change-building, testing, and implementation resources should be allocated.
(5) Minimal	A change is justified as necessary, but can wait until the next scheduled release/upgrade to efficiently allocate resources. An issue that results in a minimal business impact for a Production System or Development System; may be assigned to an issue with no impact on quality, performance, or functionality of the software, or cases of general information requests, such as usage and configuration.

Organization: Who is the organization that is being affected by this change?

Risk: is numeric value that is derived by performing a risk assessment see Analyze/Plan Change section.

Environment: Identify the environment that this change is affecting: Production, Pre-Production, Test, Development, Non-Production.

Table 5-6: Environment

Environment	Environment Definition
Production	Systems/applications that provide direct operational customer support.
Pre-Production	Supported projects/systems/applications where the developed solution in the test system is exercised. It runs on a same network as the production systems and has all the same requirements as the production systems.
Test	This environment is where an application is installed into a configuration which looks like the proposed production configuration.
Development	The environment where developers research, analyze and test the application and its components. Development may be hosted at any level of organization or a developer desktop.
Non-Production	All changes that do not meet the above descriptions will be categorized as non-production.

Change Need by Date: when will this change need to be implemented; this is normally a customer-driven date regarding when they would like to see the change implemented.

Change Order Summary: A title or short summary description of the change.

Change Description: Detailed information and identification of item(s) to be changed; A description of the desired outcome of the change.

Reason for Change: Document the Business Case Justification, this is the why we should implement this change, and what are the benefits of implementing the change.

Project Work Plan: This would include the Test Plan (how will this change be tested to ensure it will work). Define timeframe, resources, cost and effort on the quality of service. Provide requirements and detailed description.

Configuration Items: List of Configuration Items or, at a minimum, identification of the systems that are affected by the change.

Impact Description: Detailed information that will be used to determine the impact, priority and risk of a change. Include interfaces/interaction issues, organization/area being affected by change (Facility, VISN, Regional, Data Center, and National). Effects of not implementing the change (Business, Technical, Financial), would the change require consequential amendment to IT service continuity management plan, capacity plan, security plan, test plan. This is collected during the Analyze/Plan Change step of the process.

Installation Procedures: How will the change be installed/implemented, step-by-step procedures? This can be in the form of installation guides or cookbooks that are attached or referenced in the change request. This is collected during the Analyze/Plan Change step of the process.

Back-out/Remediation Procedures: Detailed plan to restore the system to the last approved state in case the change fails. Provide a level of effort to restore or implement a back-out plan (Easy, Difficult, or None). This is collected during the Analyze/Plan Change step of the process.

Approval Authority: Identify the level of approval required based on business requirements, priority, and risk of the change. See Roles for suggested levels of Approval Authority.

Incident/Problem Tracking Number: A tracking number for any incident or problem related to the change if applicable.

Initial Review and Validation

Review of the RFC

- Ensure mandatory data requirements are completed for submission.
- Confirm/Verify the impact of the change
    - Validate the RFC is appropriate.

Artifacts/Outputs

Notifications to affected and responsible entities.

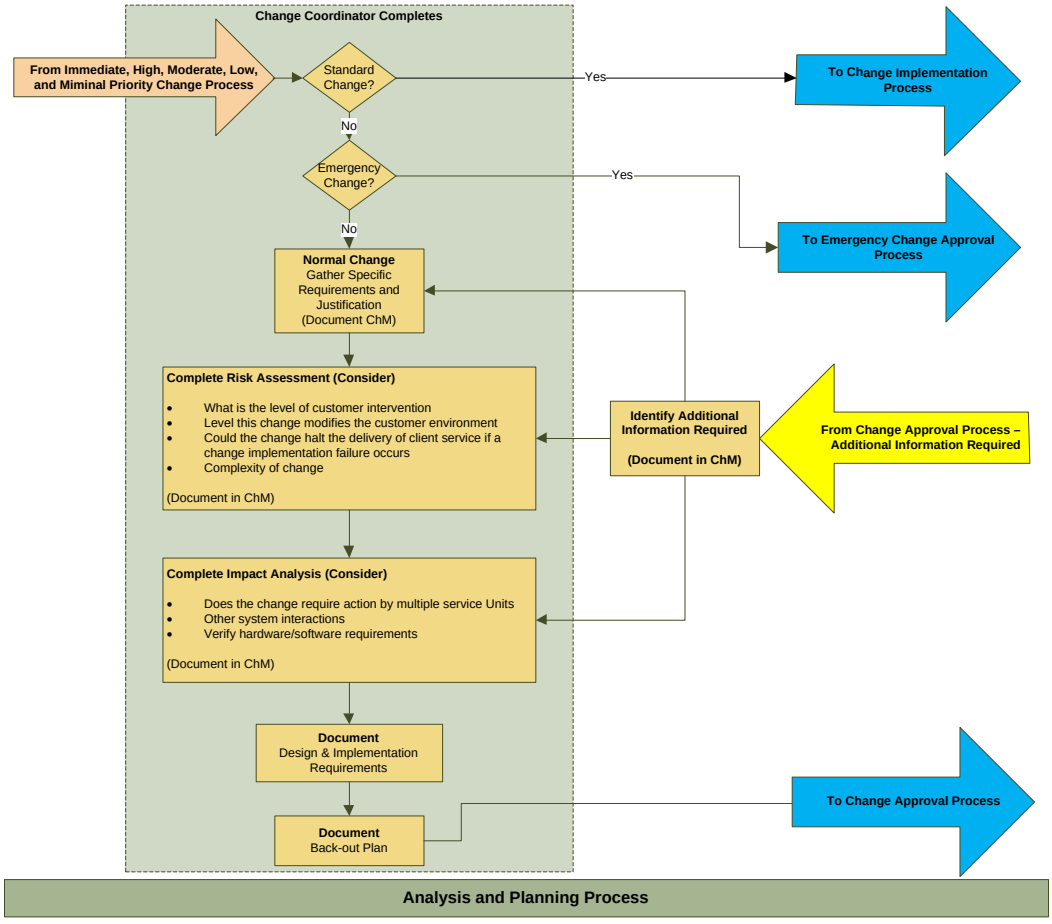
Registered Request for Change

5.2. **Analyze/Plan Change**

During this step in the process, the Change Coordinator, in concert with others involved with the change, will be developing a business case justification, performing a Technical Impact Analysis, and Business Risk and Impact Analysis. Once completed, a back-out plan is developed, and a determination will be made as to the lead time required based on the Priority and Risk levels.

Inputs

Analysis and Planning Process. During this phase of the process, the Change Coordinator will determine if the change is a standard change. If it is a standard change (see Definitions), it should be implemented as requested. Also, a determination is made if it is an emergency change. If it is an emergency change, it will be escalated to the ECC for approval and implementation. Emergency changes should only be initiated to implement changes to correct/fix problems causing production outages that need to be resolved immediately. See Emergency Change Process. If not a Standard change or Emergency change, it will follow a normal process. The Change Coordinator, with assistance from other process owners, develops a business case justification, which includes gathering specific change requirements and justification, in some cases determining if cost is a factor, and, if so, determining whether the cost of the change should be part of the change process. This would depend on the level of the organization at which the change is initiated. The Change Coordinator will also complete a risk and impact analysis, a documentation of design and implementation requirements document, and identify a back-out plan as required additional supporting documentation. All of the information collected during this stage should be documented in the Change Management System.



Responsible Persons

Change Coordinator

CAB/Technical Subject Matter Expert (SME)

Implementer

Activities

Standard Change Determination. If the change requested fits the definition of a Standard Change, it should be processed based on its documented and approved standard. Standard Changes are routine, everyday business changes that follow a documented release process. See Definitions & Acronyms.

Emergency Change Determination. If the change has been prioritized as an Emergency change, it should be escalated to the CCB/EC. The members of this board are responsible for reviewing and authorizing the change by ensuring that the change being implemented is due to a production outage, or may cause a production outage and needs to be implemented immediately. These types of changes are authorized by the CCB/EC and reviewed by the CCB and escalated to upper level NCCB/ECCB's as required based on the type of change.

Normal Change Determination

Developing the Business Case Justification. For all "Normal" Changes, the Change Coordinator must develop a Business Case justification, including the requirements of the change that will be attached to the RFC for consideration in the analysis portion of the process. The business case information is documented within the Request for Change. The following questions are relevant information that should be addressed during development of the business justification:

- Describe the requirements of the change.
- Describe effect the change may have upon the end user, business operation, and infrastructure, if known.
- Describe the impact on, and availability to, other services that run on the same infrastructure (or on software development projects).
- Describe the effect of not implementing the change.
- Estimate the IT, business, and other resources required to implement the change, covering the likely costs, the number and availability of people required, the elapsed time, and any new infrastructure elements required.
- Estimate any additional ongoing resources required if the change is implemented.
- Document downtime procedures.
- Document communication procedures; who needs to be notified in the event of scheduled/unscheduled down time and how.

Technical, Customer and Security Impact Analysis. This section describes the criteria a review must consider when evaluating the technical, customer, and security impact of a change. The impact analysis is documented within the RFC. After the Change Coordinator performs an initial review, the RFC will be categorized and prioritized based on the initial information provided. They may assign a resource depending on the type of change and complexity to perform a technical, customer, and security impact analysis of the change. This process is intended to evaluate and validate the technical and security feasibility, impact, and effect a change will have on the production environment and end user

productivity. A Technical, Customer, and Security Review should consider the following criteria while reviewing any change:

- Evaluate the change plans and gauge the impact and effect of the change during, and immediately following, the change implementation. Document a consensus of all affected departments, with agreement of requested change.
- Review by Security Infrastructure Team (SIT).
- Review the technical completeness of the change plan, including anticipated assets changed, impact on start-up or shut down of systems, impact on disaster recovery plans, back-up requirements, storage requirements, and operating system requirements.
- Architectural Review. Evaluate the technical feasibility of the change and the whole impact of the change in terms of: Performance, Capacity, Security and Operability. Document any shortfalls or exceptions.
- Validate technical aspects, feasibility, and plan.

After the technical, customer, and security impact assessments are complete, the reviewer will update the impact level to the change. The impact levels are described in the table below:

Table 5-7 Impact

Impact	Impact Definition
(1) Critical	A change where the impact could be severe, extensive, and involve a potential impact on the highest percentage of users on a business-mission/special critical system. Users experience a complete or substantial loss of service when using a production system, real or perceived data loss or data corruption making an essential part of the production system unusable, or the inability to use a mission-critical application within a production system.
(2) Serious	Affects a high percentage of users. A change where the effect is widespread, but not massive. Affects users of Essential Business systems.
(3) High	Affects a moderate percentage of users or where the effect is widespread, but not massive.
(4) Moderate	Affects a smaller percentage of users and risk is less because of the organization's experience level with the proposed change. Affects systems identified as Routine Support.
(5) Minimal	A pre-defined change type that affects the smallest percentage of users and consistently follows documented release process and are pre-approved.

Develop Back-Out Plan. Development of the back-out plan is essential to ensuring effective recovery in the event of a failed change. The back-out plan is primarily based on the technical, customer, and security impact analysis and the implementation plan.

- Document back-out criteria time constraints and procedures to return the service, system, application, or database to a working environment in the event that the implementation fails.
- How is the change to be removed?
- At what point is the decision made to back-out the change?
- What information should be gathered before back-out occurs to determine why the change needed to be backed out or why it affected the resources adversely?
- Part of a back-out plan should consist of a Management Escalation plan. The following guidelines and procedures should be followed when a change order requires Management Escalation.

- Deviations will be reviewed and considered in advance on an individual basis by the manager responsible for the system.
    - The Change Coordinator may establish an estimated completed date and time for implementation tasks within the change orders to ensure business goals, deadlines, and objectives are met. If this is required, the expectations must be defined within the order description or as a separate attachment. It is the responsibility of the Change Coordinator to notify the individual task assignees of the expected estimated completion times for specific tasks.
    - Supervisors are responsible for contacting the individuals responsible for the implementation to determine if the change order will be completed, needs to be backed out, or to have the overall estimated completion date changed.
    - If an implementation will not likely be accomplished by the target time, the Implementer will initiate the local incident response procedures at least 30 minutes before the scheduled completion time for the purpose of notifying the designated management chain of the delay.
    - The Service Desk or Change Coordinator will notify the Supervisor/Mgmt once it is completed. Documentation in the change order is required, and updates to any ANR should also be documented in the change order.

Risk Analysis. This section details the potential infrastructure, business risks, and impacts associated with a change, and the criteria necessary to assign a risk level to a change. The Change Coordinator works with the business units closely associated or impacted by the proposed change to conduct a risk analysis. The risk process evaluates the risk of the change as it relates to the ability of the VA and contractors to conduct business. The key objective is to confirm that the change is consistent with current business objectives. The following points should be considered while performing the risk assessment:

- Evaluate risk of implementing or not implementing the change.
- Describe the impact the change will make on the business unit's operation.
    - Service Level Agreement (SLA's)
    - Hours of availability
    - Backup Schedule
    - Maintenance Window
- Analyze timing of the change to resolve any conflicts and minimize impact.
- Identify and document the contacts for the change.
    - Application support contacts
    - Database support contacts
    - System support contacts
    - User Community contacts
- Ensure all affected parties are aware of the change and understand its impact.
- Determine if the implementation of the change conflicts with the business cycle.

- Validate that current business requirements and objectives are met.

When the Change Coordinator analyzes the change, they have the responsibility of initially assigning a risk level for all "Normal" changes. Depending on the line of business, risk levels are established based on the answers to questions like the following:

Table 5-8: Risk Overview

Customer and/or Client Impact

Risk	Risk Definition
Extreme (5)	Impacts several internal and/or external customers; major disruption to critical systems or impact to mission critical services, or disruption may have effect on patient safety.
High (4)	Impacts several internal customers significant disruption to critical systems or mission critical services
Medium (3)	Impacts a moderate number of internal customers; moderate impact to portions of a business unit or mission essential service. NOTE: If the customer impact is in a clinical setting or a benefits setting where the Veteran is waiting, or in a Veteran Facing application, it can never be rated less than Medium (3).
Low (2)	Impacts a minimal number of internal customers; minimal impact to a portion of a business unit or non-critical service.
None (1)	No Impact to internal customers, as well as no impact to critical systems or services.

IT Resource Risk

Risk	Risk Definition
Extreme (5)	Involves IT resources from more than two workgroups and crosses Regional/Organizational IT boundaries or involves expertise not currently staffed.
High (4)	Involves IT resources from more than two workgroups and within the same Region/Organization IT boundaries or involves expertise that has limited staffing.
Medium (3)	Involves IT resources from more than two workgroups within the same IT division or involves expertise that has limited staffing.
Low (2)	Involves IT resources from one workgroup within same IT division.
No Risk (1)	Involves a single IT resource from a workgroup.

Implementation Complexity

Risk	Risk Definition
Extreme (5)	High complexity requiring technical and business coordination.
High (4)	Significant complexity requiring technical and business coordination.
Medium (3)	Moderate complexity requiring technical coordination only.
Low (2)	Low Complexity requiring no technical coordination.
No Risk (1)	Maintenance type of change.

Duration of Change

Risk	Risk Definition
Extreme (5)	Change outage greater than **2 hours** and affecting customers during **Prime/Peak** times. Lengthy install and back-out.
High (4)	Change outage less than **2 hours** and affecting customers during **Prime/Peak** times or greater than **1** hour during **Non-Prime** times.
Moderate (3)	Change outage less than **1 hour** and affecting customers during **Prime/Peak** times or greater than **1 hour** during **Non-Prime** times.
Low (2)	Change outage less than **1 hour** during **Non-Prime** times and affecting customers during Non-Prime times.
No Risk (1)	No outage expected.

Security

Risk	Risk Definition
Extreme (5)	Affects critical data or server security and the back-out would likely extend the window timeframe.
High (4)	Affects mission essential data or server security and has moderate back-out plan which would not extend the window timeframe.
Moderate (3)	Affects non-critical data or server security and has moderate back-out plan which would not extend window timeframe.
Low (2)	No security issues and easy back-out plan.
No Risk (1)	No back-out plan needed.

Service Level Agreement Impact

Risk	Risk Definition
Extreme (5)	Impacts Mission Critical or Essential Systems SLA during business Prime/Peak times.
High (4)	Impacts Mission Critical Systems SLA during business Non-Prime/Peak times.
Moderate (3)	Impacts Mission Essential Systems SLA during business Non-Prime/Peak times.
Low (2)	Little measurable effect on SLA times.
No Risk (1)	No effect on SLA times.

Assessed risk and the related numerical value

Risk	Range	Description
Extreme (1)	25-30	Involves potential impact on the highest percentage of users or a business-critical system. The change may be new technology or a configuration change. It may involve downtime of a network or a service.
High (2)	19-24	Affects a high percentage of users. A change where the effect is widespread, but not massive. The change is a nonstandard change, such as a new product, new users, or network change, and may involve downtime of the network or a service.
Moderate (3)	11-18	Affects a smaller percentage of users, and the risk is less because of the organization's experience level with the proposed change.
Low (4)	7-10	Consistently follows documented release process and is pre-approved by the CCB. This type of change is performed on a routine basis and is part of the operational practice of the business. These types of changes conform to the requirements of a planned change, except they can be implemented without following a time constraint because they are routine. 100% of the changes submitted under this risk level do not cause any disruptions to the IT community. These types of changes have a minimal review and approval process.
No Risk (5)	1-6	This type of change has no impact on any production system.

Artifacts/Outputs

Business Case Justification

Updated Request for Change

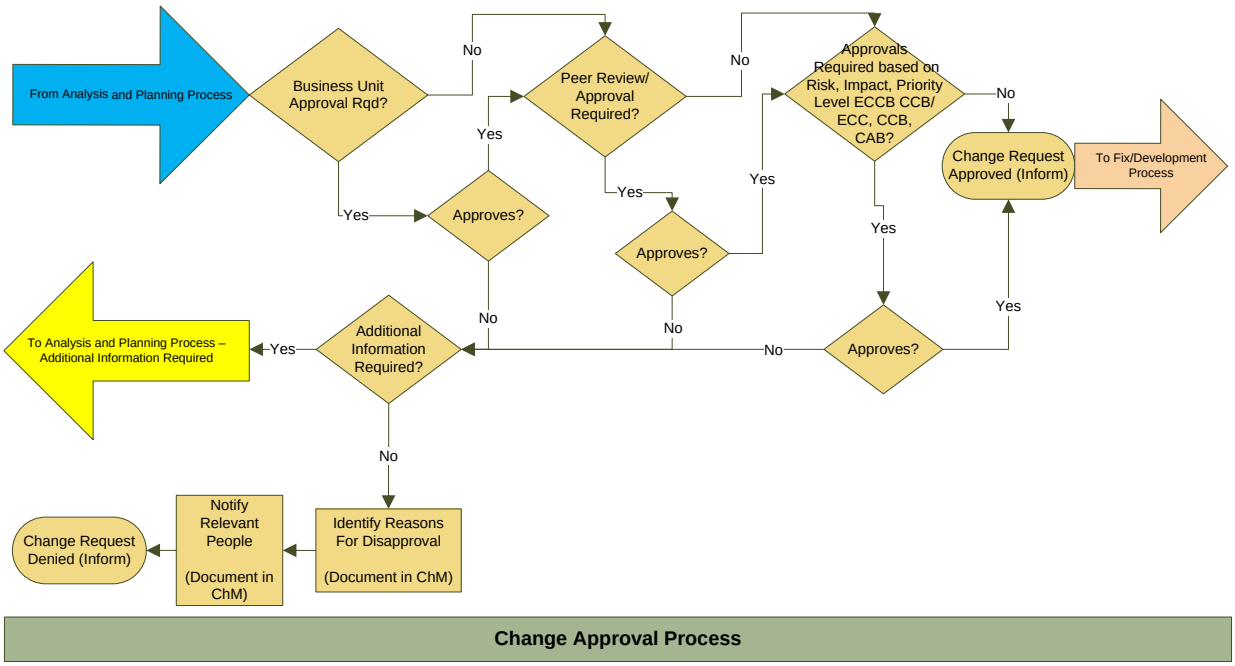
5.3. **Approve Change**

A determination is made if a Review by the IT Business Manager is required. If so, obtain approval. Following the completion of the IT Business Manager approval, determine if a peer review and approval should be conducted. Once completed, a determination will be made as to the approval level required prior to implementation.

Inputs

Change Approval Process. After a Normal change has been correctly categorized, prioritized, and analyzed by the Change Coordinator, the change must be authorized for development and implementation. The diagram below identifies the workflow associated with the change management approval at the VA.

All documentation relevant to the change should be maintained together. Any documents created during the change process should be attached to the change order record.



Responsible Persons

Change Coordinator

CAB/Technical Subject Matter Expert (SME)

Appropriate Approval Authority

- Change Manager
- Project Managers/System Owners
- IT Business Manager
- CCB
- NCCB

- ECCB
- Stakeholders (VHA, VBA, NCA, or other business representatives)

Activities

IT Business Unit Manager Review and Approval. Following the submission of the new RFC, it will be screened by the IT business unit manager who determines whether to authorize or deny the change based on the information in the new change order. This screening process must include a validation against business/IT needs, practices, and standards to ensure that the RFC is appropriate, and to ensure the request is complete, We don't want to introduce changes to our infrastructure that have not been vetted and approved for the organization. The manger can elect to approve, reject, or request additional information from the change initiator. The Change Initiator is notified of the progress of their request at all stages.

Conducting the peer review and approval. This step ensures that all of the technical components and notifications have been completed as required by the Change Advisory Board. This approval can be completed by anyone approved by the IT business unit manager and identified as a peer reviewer and approved in the Change Management System. Peer reviews and approvals are completed using a checklist which is attached to the change order.

Approvals Required for Change based on Priority (Urgency + Impact) and Risk Level. Appropriate Approval Authority is based on the Priority and Risk of a change or is determined by the specific process that is being followed, normally outlined within the Service/System Change Management Plan; if one was not developed, the following guidelines could be used to set a baseline for Appropriate Approval Authority. This Approval Authority is based on a change to a production environment but could be used to develop approvals required within other environments or levels of the organization. This intent is to ensure appropriate approvals have been obtained at the appropriate level of the organization and are documented and communicated. If the RFC is rejected, the RFC is closed, and the Change Initiator is informed of the decision. The reasons for rejection are added to the change order.

Table 5-9: Recommended/Suggested Approval Authority/Notification based on Priority and Risk

Organizational Level of the Change	Approval Authority	Priority	*Immediate*	*High*	*Moderate*	*Low*	*Minimal*	Risk	*Extreme*	*High*	*Moderate*	*Low*	*None*
Facility (Tier I)													
	FCIO		**A**	**A**	N	N	N		**A**	**A**	**N**	N	N
	IT Service Supervisor		N	N	**A**	**A**	A		N	N	A	**A**	**N**
	Service Line Manager		**A**	**A**	N	N	N		**A**	**A**	**A**	N	N
	Stakeholders		**A**	**A**	N	N	N		**A**	**A**	**N**	N	N
VISN (Tier II)													
	CTO		**A**	I	N	N	N		**A**	**N**	N	N	N
	NCIO		N	**A**	N	N	N		N	A	**A**	N	N
	Service Line Manager		N	N	**A**	**A**	A		N	N	N	**A**	**A**
	Stakeholders		**A**	**A**	N	N	N		**A**	**A**	**A**	N	N
Regional (Tier III)													
	RCCB		**A**	N	N	N	N		**A**	**N**	N	N	N
	CTO		N	**A**	N	N	N		N	A	**A**	N	N
	Service Line Manager		N	**A**	**A**	N	N		N	A	**A**	**A**	N
	Service Line Division Manager		N	N	**A**	**A**	N		N	N	N	**A**	**A**
	Change Manager		N	N	N	**A**	A		N	N	N	N	**A**
	Stakeholders		**A**	**A**	N	N	N		**A**	**A**	**A**	N	N
Data Center (Tier III)													
	CCB		**A**	N	N	N	N		**A**	**N**	N	N	N
	CTO		N	**A**	**A**	N	N		N	A	**A**	**A**	N
	Service Line Managers		N	**A**	**A**	N	N		N	A	**A**	**A**	N
	Program Manager		N	**A**	**A**	N	N		N	A	**A**	**A**	N
	System Owners		**A**	**A**	**A**	N	N		**A**	**A**	**A**	**A**	N
	Change Manager		N	N	N	**A**	A		N	N	N	N	**A**
	Stakeholders		**A**	**A**	N	N	**N**		**A**	**A**	**A**	N	N
National (Tier IV)													
	ECCB		**A**	N					**A**	**N**	N		
	NCCB		N	**A**					N	A	**A**	N	N
	SL Council		N	**A**	**A**	N	N		N	A	**A**	**A**	N
	Security Council		N	**A**	**A**	N	N		N	A	**A**	**A**	N
	National Program Managers		N	**A**	**A**	N	N		N	A	**A**	**A**	N
	System Owners		N	N	**A**	**A**	N		N	N	N	**A**	**A**
	National Change Manager		N	N	N	**A**	A		N	N	N	N	**A**
	Stakeholders		A	A	N	N	N		A	A	A	N	N

5.3.1. Emergency Change Procedures and Approval Process flow

This section details procedures to be followed when emergency production changes require implementation. Note: RFC involving development/pre-production (non-production impacting) and test (non-production impacting) technology systems (including applications) are not affected by the emergency change process. These changes can be done at any time without affecting other users, but they need to be tracked in the Change Management tool for documentation purposes.

An Emergency change is an immediate change to a production system that is required to restore services associated with an incident, or where the absence of a required change will contribute to a system being placed at high risk of having an incident associated with it.

The emergency change process allows the Department of Veterans Affairs and its systems and services to continue normal operations or restore them as quickly as possible by accelerating processes that follow the normal change process to the extent that time constraints permit. Emergency changes requiring quick and/or immediate implementation are generally more disruptive to the environment and more prone to failure. For this reason, emergency changes must be kept to a minimum and must adhere to the definition provided.

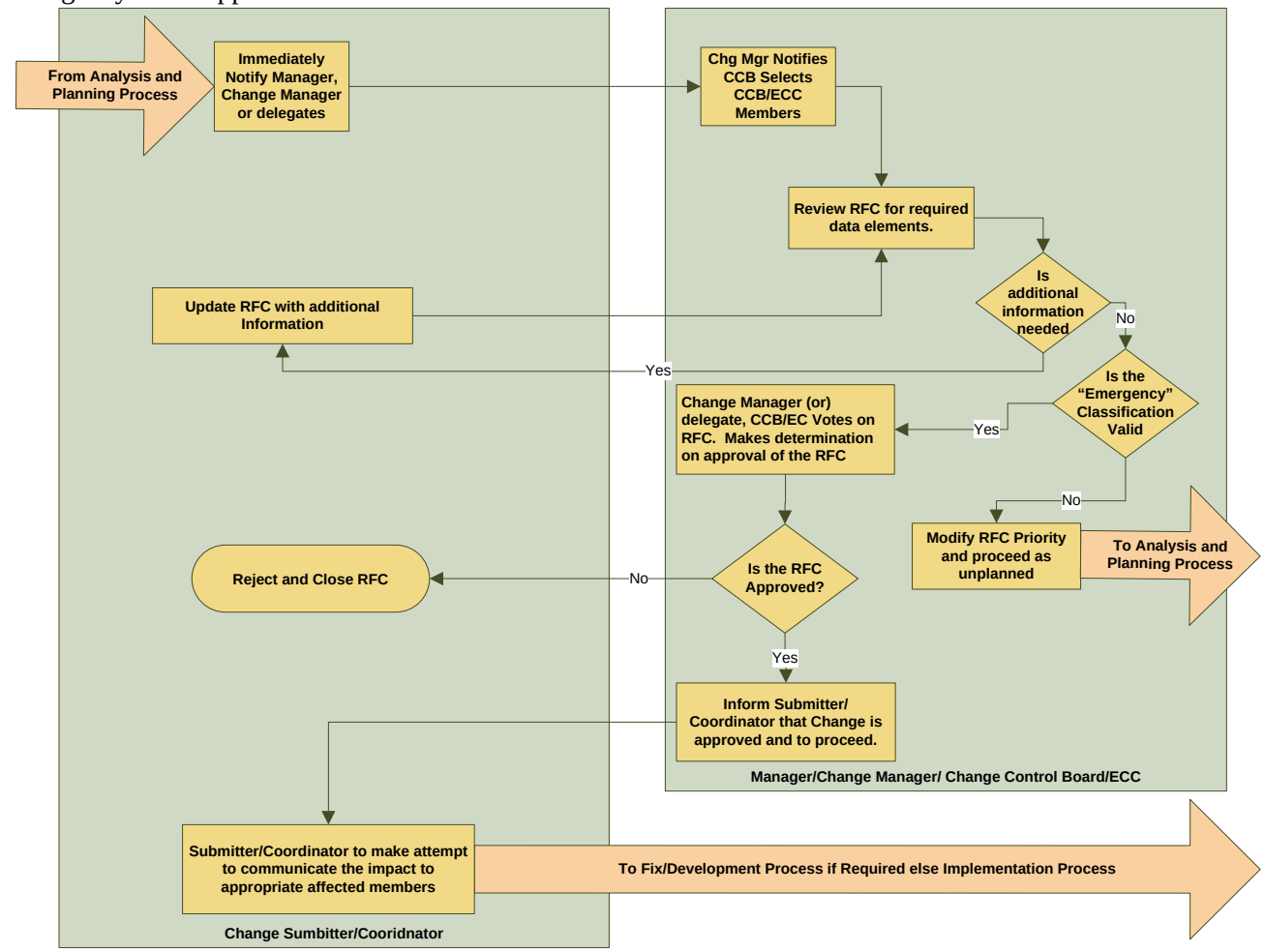
Every organization that performs emergency changes must document their emergency procedures and document the lines of authority that the approvals must follow. All emergency changes will adhere to the following guidelines:

- At a minimum, Emergency RFCs must be approved by the Service Line Manager(s) and the Change Manager (or their delegates) prior to work being performed. If the emergency change is being completed prior to it being entered into the Change Management System (CMS), verbal approval must be obtained and followed up with an email. Once the RFC is created in the Change Management System (CMS), the name of the individual who authorized the change must be entered into the description of the change.
- Without exception, the Emergency RFC must be entered into the Change Management System (CMS) as soon as time allows. The sooner it is documented, the sooner it can be communicated.
- All production emergency changes will be categorized with a Change Type of “Emergency.” This will initiate a notification to the Change Control Board. The Change Manager (or delegate) is responsible for reviewing emergency changes prior to or following the change being implemented. The changes may be recommended for further review by the CCB or ECC.
- The Change Manager is responsible for selecting ECC members, as necessary, if the standing CCB members are not available. The ECC has the same purpose and performs the same functions as the regular CCB to include full authority to approve or deny emergency changes.
- The reason for the emergency must be documented in the RFC (Order Description) with the details regarding why the change could not be completed using a non-emergency process.
- All emergency RFCs are required to follow the process workflow assigned to the selected change category/model, and all associated tasks must be completed prior to the RFC being closed.
- The Change Management process will comply with local and VA Emergency Notification Processes.
- In addition to adhering to the Emergency Notification Process, the change manager can serve as the incident manager and must communicate the impact and/or benefits of the requested change by contacting affected groups as soon as possible.

Affected groups may include but are not limited to the following:

- Primary assigned group responsible for implementing the change
- Project/Program Manager
- Service Desk/Help Desk
    - Impacted group(s)/Business Owner(s)
    - Impacted System, Database and Application Administrator(s)
    - Impacted affected end user

Emergency RFC Approval Process Flow



Emergency changes will follow the procedures defined as follows:

- The authorized change submitter registers the RFC and immediately notifies Manager and Change Manager of the emergency RFC.
- Update Status of RFC to "CCB Review."
- Change Manager and IT Manager review change and determine if:

    - Additional information is needed, and, if additional information is needed, contact the submitter or change coordinator.
    - Is the Emergency classification valid?
        - If not valid, update the Change Type to Normal and proceed as a normal change. Contact the Coordinator and provide feedback.
- If valid, the Change Manager identifies and communicates Emergency Change to the CCB/ECC members. The CCB/ECC will meet and review the RFC with the change coordinator. If additional information is needed, the Change Coordinator provides this information and updates the RFC. If no additional information is required, the CCB/ECC votes on the RFC.
    - If approved, the Change Coordinator is notified and proceeds with change.
    - Otherwise the change is rejected and closed. The decision must be documented in the RFC.
- The change order will remain open at least until the following business day for review and completion of all remaining workflow tasks.
- On the following business day, the CCB members will be notified of the RFC and, if required, will review the RFC with the Change Manager and others as needed. If additional information is requested, the Change Coordinator provides this information and updates the RFC.

Artifacts/Outputs

Approved/Rejected Request for Change

Software Configuration Management Procedures

5.4. Fix/Develop Change

A Fix and/or Development lifecycle to software code and similar configuration items in a Development environment follows processes put in place to ensure full compliance. All the steps of this phase may not be needed, for most solutions have been provided as a release for deployment into the Production environment. Approved changes (RFCs) are assigned to a developer, programmer, tech writer, or other Subject Matter Expert (SME) for resolution. Once resolved, the changes may be compiled and packaged with other changes and artifacts and delivered to testing as a build, modified work product, or configuration change. Testing verifies the fix, and the change is staged for production and packaged as a release candidate. New baselines are established, and substantiating documentation is produced. Subsequent processes are part of release management and quality release control.

Inputs

Fix/Develop Process. Approved changes (RFCs) are assigned to a developer, programmer, tech writer, or other SME for resolution. The Task Assignee then checks the artifact requiring change is checked-out of version control, makes the appropriate fix, and checks it back in. Changes to artifacts in the CMDB or in a version-controlled repository must be associated with an approved RFC, and that association provides an audit trail as to who made the change, what changed, when it changed, who approved it, who requested it, and so on.

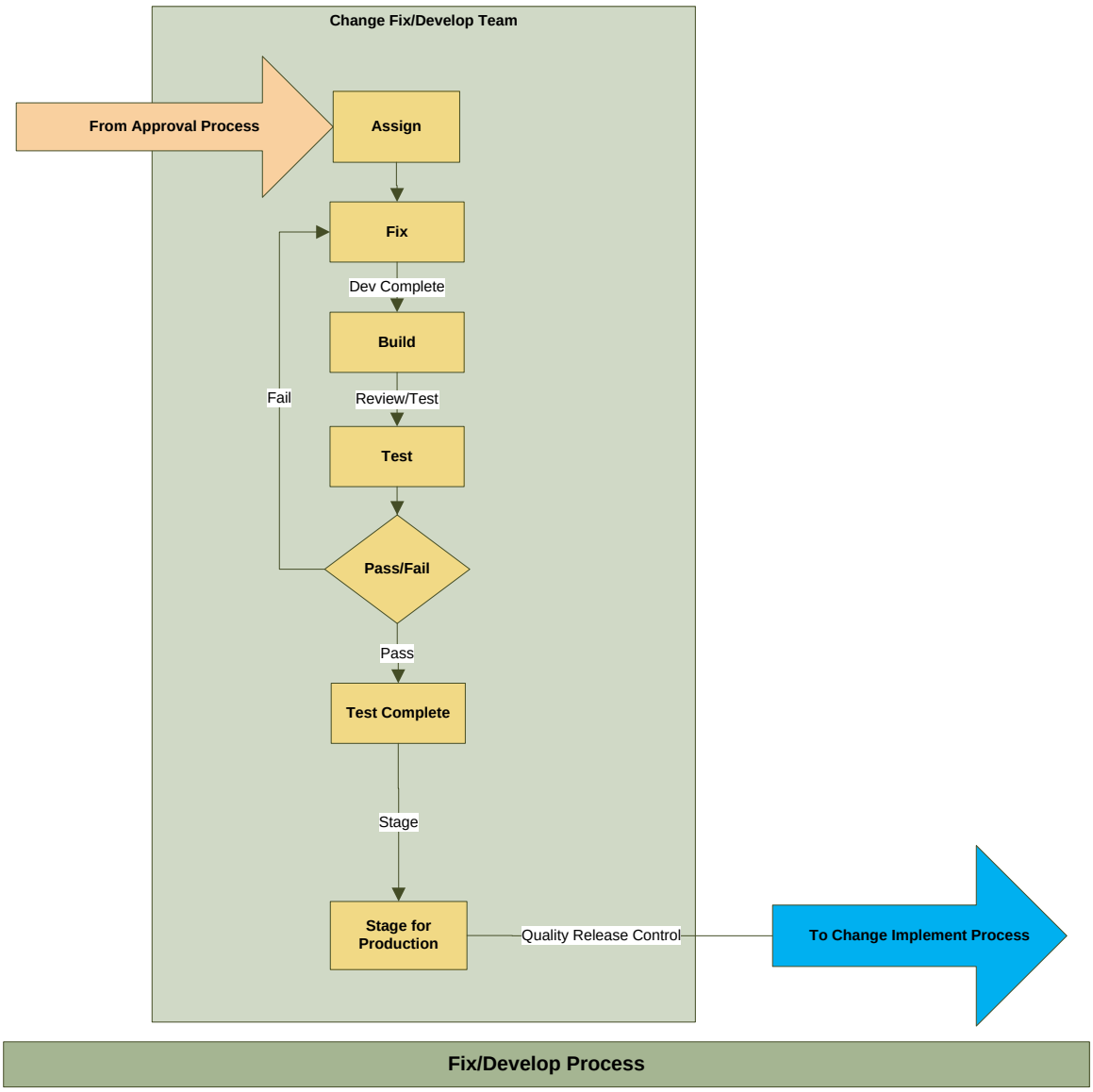
Build. Not all changes will require a build step, but most will pass through some configuration management process and audit before being handed off to testing. The build step audits the association between the approved change request and the change to the CMDB or versioned artifact. Typically, labels are applied, and changes are compiled and packaged in a controlled environment with a controlled process that records each step, maintains an audit trail, and restricts manual intervention. The build process controls the hand-off to testing, and it sends notifications about the build, what changed, and links to the associated RFCs.

Testing. All changes will undergo some level of testing depending on the complexity of the change. The changed artifact, work product, or build is delivered to Testing/SQA/QA. This phase focuses on conducting testing and quality assurance to ensure reliability and performance of all components of the organization's technology infrastructure. Tests, or work product reviews, are conducted to assure that requirements have been met, thresholds are satisfied, and that the process has been followed. The Change Coordinator will oversee the testing function, develop the test plan, and document its findings in the request for change to ensure proper review and approval by reviewing officials as to whether to advance the change to the next step.

Stage for Production. Changes that satisfy the testing requirement may be staged for production. In this step of the process, successful changes are assembled into a Release Candidate, or Release. The Release Candidate, or Release, is put through Quality Release Control to assure that everything in the Release is what went through testing. The Release package is handed off to Release Management to carry it through the next phase of the process and into the implementation. Release Management may go through many additional phases, such as Independent Verification and Validation (IVV), Stage 1 testing, IOC, and Pre-Production, before the Release is ultimately implemented into Production. Identified defects during the Release Process typically enter the system as new RFCs.

(**NOTE**: Typically this is a Product Development handoff to Enterprise Systems Engineering Release Management, but, in some cases where software development is being performed outside of Product Development, the same methods should be followed.)

All documentation relevant to the change should be maintained together. Any documents created during the change process should be attached to the change order.



Responsible Persons

Change Coordinator

CAB\Technical Subject Matter Expert (SME)

Implementer

Activities

Assign: If the RFC requires a code change, a document update, or a fix of any sort, the Change Coordinator assigns the approved change to an SME for resolution. Since not all RFCs require a Fix/Development step, this step may be skipped, but, in the event that a Fix/Development step is required, it typically follows a rigorous development lifecycle.

Fix/Develop: During this step in the process, the Task Assignee resolves the problem described in the RFC. Examples of fixes include, but are not limited to: code changes, document updates, process changes, and modifications to configuration items (CI). CIs are checked-out of the CMDB or version control system. Changes are made, and the CI is checked back in to the CMDB. The CMDB, or version control tracking system, records when the change was made, who made the change, what the change entailed, and other details of the change, and the changes are linked back to the RFC. Unified Change Management provides an audit trail to connect every change to an approved RFC.

Build: During this step in the process, one or more changes are combined into a change package, compiled, and packaged with documentation, third-party products, and other CIs as determined by the build process. Changes to CIs (source code, documents, models, images, etc.) are labeled. The label associates the build with the RFC, and the change made to the CI in the CMDB or in version control. The label provides the audit trail to assure that every change has an approved RFC. The build process is typically controlled by the configuration management in conjunction with the SME's to provide a controlled hand-off of the change, artifact, or build to the testing process owner.

Test: During this step of the process, the testing process owner will follow the developed test plan. There are several stages of testing documented within the Release Management Process that affect different areas of the organization. The results must always be documented within the appropriate request for change (RFC).

User Guide and Training

Training documentation for users and application support has been completed and distributed per training communication plan.

Designated staff has received training and has demonstrated required competency.

User documentation has been completed or updated.

Help Desk Documentation and Training

Help Desk documentation has been completed or updated and distributed two weeks in advance of the release date.

Help Desk staff has received training and has demonstrated required competency.

Installation Instructions / Production Operations Document

Detailed instructions for the implementation team have been provided. These include:

- Architecture overview (hardware, software) with diagram and interfaces.

- Environmental setup and configuration requirements
- Installation procedures
- Back-out procedures
- Interdependency details
- Logging retention/usage log availability

Artifacts/Outputs

Updated Request for Change

5.5. Implement Change

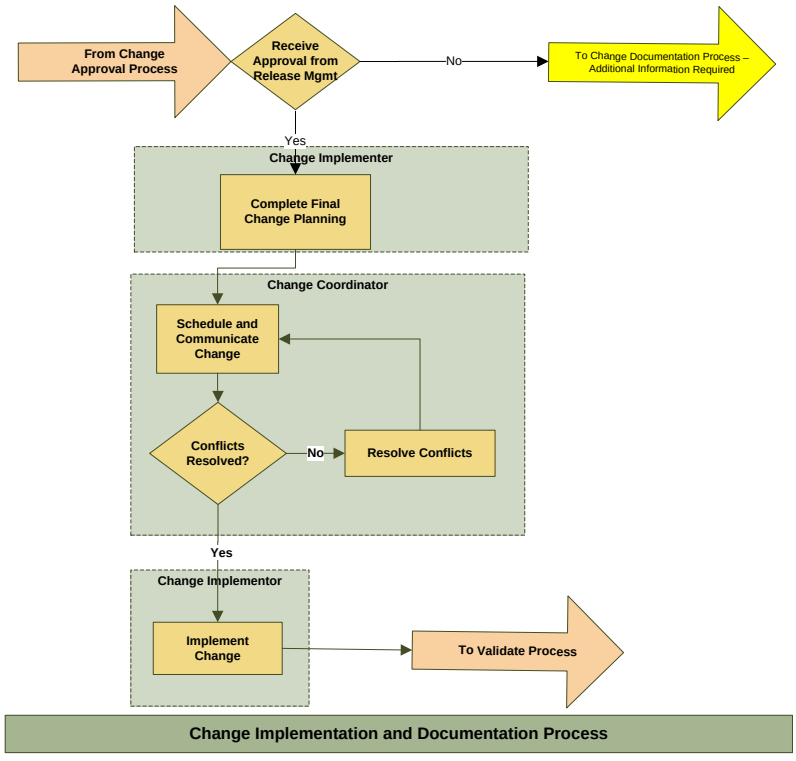
During this phase in the process, Release Management, in concert with the Implementation Manager, will ensure that release package is deployed to all host(s) identified on the rollout plan. The release package is deployed, as provided, without any modifications. The change Implementer will complete final planning, scheduling, notifying, and implementing the change, following any formal approval release communication process as required.

Inputs

Implementation and Documentation Process: Once the requested change has been developed, tested, and ready for release, it moves into the Implementation and Documentation phase. This phase is concerned with the steps necessary to successfully implement the change (See diagram below):

- Obtain release package from Release Management
- Complete final planning
- Establish the schedule and complete required notifications
- Complete the change implementation
- Validating the change in production
- Complete final change documentation

All documentation relevant to the change should be maintained together. Any documents created during the change process should be attached to the change order.



Responsible Persons

- Release Manager
- Change Coordinator
- Implementer

Activities

Obtain Release Package from Release Management. During this step in the process, the Release Manager will review the documentation of the change and ensure that all needed information has been provided.

Final Planning. During this step, the change coordinator reviews all comments and recommendations to ensure all required tasks have been completed. The change coordinator conducts this review with the IT business unit manager, the change implementer, and the change initiator. This phase is also used by the implementer to complete any final development necessary to complete the implementation. If modifications to the originally approved change have been made, re-approval will be required by the appropriate approval authority. If non-approval is received, the change will be rejected and closed out and the process re-started.

Scheduling and Notifications. The change coordinator in conjunction with the implementer establishes the appropriate schedule for the implementation of the change. The schedule is based on several factors including the change priority, risk, other changes being implemented, resources, maintenance windows and system availability. Once the schedule has been established the change coordinator ensures the change is noted on the consolidated change schedule and notifies all affected parties of the pending change.

Change Implementation. The change implementer implements the change in accordance with the implementation plan during the scheduled time. This is generally a technical implementation. Significant changes within the environment that require a major program development effort will follow the guidelines established in the System Development Life Cycle document and established Project Management Procedures. In general, these include the following requirements which all change implementations must follow:

- Review of the implementation project plan.
- Review of back-out plan.
- Verify release management testing was successful and documented.
- Applying the change to production.
- Validating the change in production.
- Resolving problems caused by the change.
- Writing a brief summary of the results.
- Updating the Change Management System with results of the implementation.
    - Failure of an implementation will normally require the Implementer to follow the back-out plan and follow a management escalation plan to ensure normal system restoration, operation as well as notification to all affected parties.

Artifacts/Output

Updated Implemented Request for Change

5.6. Validate Change

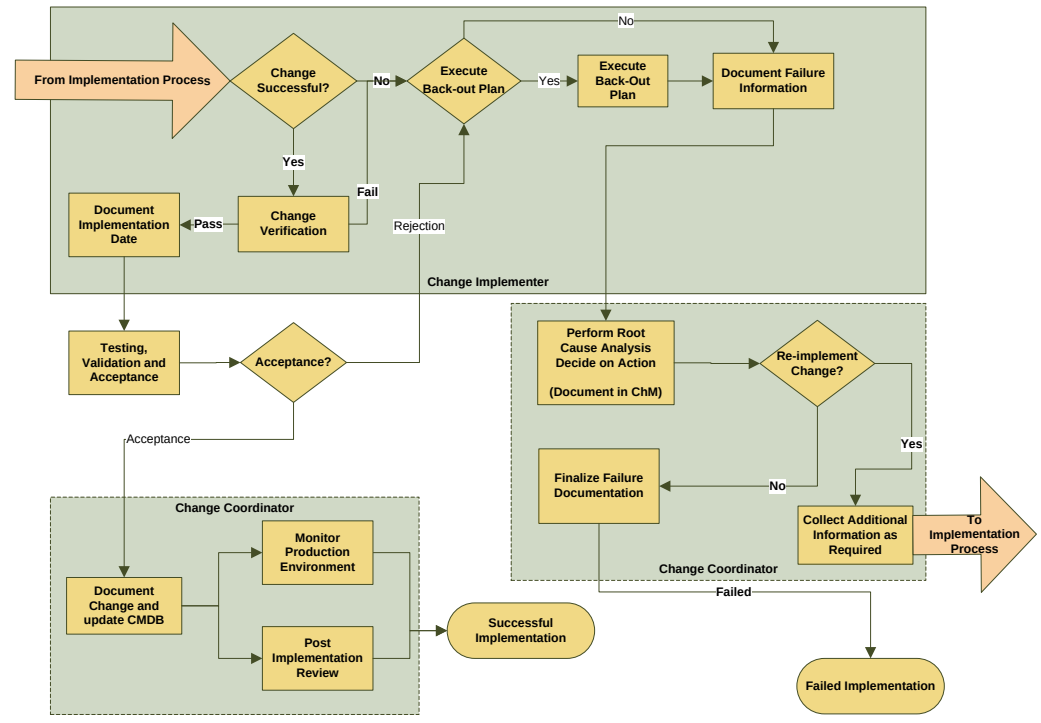
During this phase of the process the change will be tested, validated and accepted by the initiator also known as User Acceptance Testing, the change is verified and production environment monitored. A post implementation review is held to document any issues and if they are accepted. Configuration Management database is updated.

Inputs

Testing and Validation Process

During this step in the process the implementer and change initiator will test and validate that the implemented change has been successful and has not caused other problems. If problems are encountered a decision is made to back-out the change or to correct the problem and redeploy. User testing, validation and acceptance is initiated, once accepted the change order and CMDB will be updated. Monitoring will be performed based on the plan submitted with the change order. After testing, validation and monitoring the change will be documented and closed per the change manager. Below is a diagram that represents this phase of the process and each activity performed and the responsibility for those steps. See Activities below for detailed explanation of the steps.

All documentation relevant to the change should be maintained together. Any documents created during the change process should be attached to the change order.



Validation Process

Responsible Persons

- Implementer
- Change Initiator
- Change Coordinator
- CAB\Technical Subject Matter Expert (SME)

Activities

Change Verification. Following a change implementation, a change verification review must be conducted to determine if the change resulted in the desired outcome. In most cases, this review process might be very brief. For a routine change, where the effect has been small and the results relatively predictable, the review process will be limited to checking that the change has provided the user with the expected functionality. Failed changes must be thoroughly reviewed to identify the root cause of the failure.

An unsuccessful change will require a decision to either execute the back-out plan or to document the failure and workaround.

If a re-implementation is performed it should be documented and communicated.

A determination should be made with the coordination of the Supervisor and Change Coordinator to either perform an immediate re-implementation, or re-scheduling the change.

If decision to immediately re-implement, any extension of down time should be coordinated and communicated to the appropriate customer, end user, program manager etc.

Testing, Validation, and Acceptance. Once a change has been implemented, the IT Business responsible for the change and end users who will be affected by the change will conduct testing following the test plan developed during the change development phase. Accurate documentation and analysis of any discrepancies are documented in the change order.

The Change Coordinator will rate the change with one of the following ratings.

- Acceptance – with no comments.
- Acceptance – with minor exceptions (note that these exceptions will either be fixed under the current change or may require the creation of another new change).
- Rejection – Normally used only if the implementation change doesn't meet the required business needs. This results in a failed change determination and must be thoroughly reviewed to identify the root cause of the failure. This normally results in the creation of new change request.

Accept Issues and Continue. Even if a change has not fully met the desired objectives for the change, the review may still determine that the change should not be backed out and that it is not desirable or cost-effective to make more changes. Instead, there may be options available to work around the deficiencies of the system. Such workarounds should be coordinated and documented with the customer. If there are user workarounds, the service desk should be informed so that the information can be easily made available to the users. If the workaround is an additional manual process that some IT staff needs to take, document the workaround and inform the responsible parties.

Monitor Change in Production Environment. In order to determine whether the deployed change has been effective, it is necessary to monitor the changes in the production environment. For a small change, this may consist of checking on the desired functionality. For larger changes, it might require the monitoring of network and server information, performance data, event logs, or response times. The change coordinator will typically determine the best tool needed based on the specific change.

Hold Post-Implementation Review. At a minimum all Emergency changes and Immediate Priority and High Risk changes must go through a Post Implementation Review. The Appropriate Change Control Board (CCB) should make a determination as to what types of changes that will required a Post-Implementation Review, and documented as part of their charter. The Change Coordinator is responsible for ensuring that a post-implementation review is completed and presented to the appropriate CCB. The findings of the post-implementation review are documented within the Change Management System of record. After enough information has been gathered from monitoring to determine the effectiveness of the change, a post-implementation review is held.

The CCB Chairperson or Change Coordinator will schedule and moderate the review meeting for large changes. During the review, reference must be made to the original RFC, which states the objectives of the change and offers some measurable indicators for gauging the effectiveness of the change. The measured effects of the change can be compared with the expected effects in order to decide whether the change has met its objectives.

In addition to making a success or failure decision on the change implementation, the review will also consider how the change request was developed and whether it was implemented as scheduled. This exercise will result in the documentation of lessons learned from the change.

Post Implementation feedback is then distributed to all parties involved in the change to encourage and enable future process improvements.

Updating Configuration Management Database for items that will need to be manually updated in the CMDB the process should allow for the responsible configuration management to update the database with the changes made. The Change Coordinator is responsible for gathering all information and sending it to the Configuration management Librarian responsible for entry into the CMDB.

Artifacts/Outputs

Completed after Action Report (if required)
Completed (successfully or unsuccessfully) Request for Change

6. Metrics

Metrics are a system of parameters or methods for quantitative and periodic assessment of a process that is to be measured. It includes procedures necessary to carry out such measurement and procedures for the interpretation of the assessment in the light of previous or comparable assessments. Metrics are usually specialized by the subject area, in which case they are valid only within a certain domain and cannot be directly benchmarked or interpreted outside it. The collection and analysis of metrics provides a factual method of evaluating the quality of the product or system.

The list of reports below is recommended but not inclusive of all reports that should be developed. This section will need revision at semi-annual intervals. The Change Management Reports include:

- Reasons for Change.
- Number of successful changes.
- Percentage of changes on time.
- Number and percentage of failed changes.
- Number of changes backed-out, together with the reason (e.g., incorrect assessment, bad build).
- Number of Incidents traced to the change and the reasons.
- Outages during changes.
- Number of RFCs (and any trends in origination).
- Number and percentage of emergency changes
- Number of implemented changes reviewed, and the size of review backlogs.
- Number of pending implementation changes
- Date from previous periods (last period, last year) for comparison.
- Number and percentage of Cancelled RFCs
- Number and percentage of rejected RFCs.
- Number of changes per category.
- Average number of days it takes for CCBs to process changes.
- Number of delayed CAB/CCB action items.
- Number of unauthorized changes.
- CAB/CCB attendance.
- Customer satisfaction.
- Time to successful change completion.
- Number of failed changes with no back-out plan.

The above reports can be used as basis for assessing the efficiency and effectiveness of the Change Management process.

7. Process Verification

Change Compliance This section describes the activities necessary for the Change Organization to audit their effectiveness of change. The Change Manager will conduct a monthly audit to evaluate change compliance and will be submitted to the appropriate CCB. The NCCB will perform a monthly evaluation by management to ensure compliance VA wide. Some areas that may be examined include:

Appropriate CCB's minutes and Forward Scheduling Calendar (FSC).

Perform a random review of change orders and related documentation.

When review and analyze Change Management reports based on the following criteria:

- All RFCs have been correctly logged, assessed and executed.
- FSC has been adhered to, or there is a good reason why not.
- All items raised at CCB meetings have been followed up and resolved.
- All change reviews have been carried out on time.
- All documentation is accurate, up-to-date and complete.
- All CIs have been updated in the CMDB.

Measuring Quality in the Change. Reports from the Change Management System (CMS) will provide information about past and current changes. This information will permit the evaluation of the impact of changes, dependencies and trends for all levels of the organization. Notification will be provided as requested or previously agreed, to Business Owners by Change Manager.

8. Training and Tools

8.1. Training

- OIT Change Management Process Training
- CA Service Desk Manager Analyst Training

8.2. Tools

- CA Service Desk Manager (SDM).

9. Concurrence

Integrated Technical Working Group Members		
Name	Title	Organization
Mike Leroy	Enterprise Process Manager	Service Delivery and Engineering
Jeff Rabinowitz	Enterprise Process Management	Service Delivery and Engineering
Mitzi Arth	Manager, LRM Change and Configuration Management	Enterprise Service Engineering
James Magness	Application/Build Manager	Enterprise Operations
Andrea Kucharski	Service Line Manager, Support Services	National Service Desk
Russell McFall	Lead, Change, Configuration and Release Management	Field Operations, Technology Management
Julie Harvey	Director, Product Assessment Division	Product Development
Phyllis Denson	Business Process Mgmt Analyst	VHA, Office of Health Information

10. Approval

Name	Title	Organization
christopher.shorter@va.gov Digitally signed by christopher.shorter@va.gov DN: cn=christopher.shorter@va.gov Date: 2014.07.08 14:05:26 -04'00' Christopher Shorter	Executive Director of Enterprise Operations	Enterprise Operations

11. Definitions and Acronyms

For additional definitions and acronyms, please refer to the Glossary and Acronyms spreadsheet on the IG Audit SharePoint site.

This temporary link will be used until the joint Glossary and Acronyms document is completed and posted to its permanent location:

Link #1 is the Technical Work Group's definitions:

http://vaww.infoshare.va.gov/EPG/VAIGADP/Shared%20Documents/Finalized%20TWG%20Documents/Glossary_and_Acronyms.xls

Link #2 is the OIT Master Glossary:

http://vaww.oed.wss.va.gov/process/Library/master_glossary/masterglossary.htm

11.1. Definitions

Term	Definition
Change	Any new IT component deliberately introduced to the IT environment that may affect an IT service level or otherwise affect the functioning of the environment or one of its components.
Change Category	The measurement of the potential impact a particular change may have on IT and the business. The change complexity and resources required, including people, money, and time, are measured to determine the category. The risk and the deployment, including potential service downtime, is also a factor**.**
Change Priority	A change classification that determines the speed with which a requested change is to be approved and deployed. The urgency of the need for the solution and the business risk of not implementing the change are the main criteria used to determine the priority.
Change Order	The record within the Automated Change Management Module that contains all of the information relative to a change. This information includes justification, risk and impact analysis, approvals, phases, and tasks associated with accomplishing the change.
Configuration Item (CI)	An IT component that is under configuration management control. Each CI can be composed of other CIs. CIs may vary widely in complexity, size, and type, from an entire system (including all hardware, software, and documentation) to a single software module or minor hardware component.
Emergency Changes	Is an immediate change to a production system that is required to restore services associated with an incident causing loss of service or severe usability problems to a mission-critical system, or some equally serious problem, or where the absence of a required change will contribute to a system being place at a high risk of having an incident associated with it. Immediate action required. Emergency meetings of the CCB or CCB/ECC may need to be convened. Resources may need to be immediately allocated to deploy such authorized changes. Failure to fix the identified problem will result in the production system becoming or staying non-operational.
Forward Schedule of Changes (FSC)	The FSC shows when all changes are to take place within the entire Customer IT infrastructure. This single glance at the change schedule makes it possible to see the available change windows. Scheduling changes against the FSC also ensures that multiple, interdependent changes are not scheduled at the same time.
Planned Changes	These types of changes allow for timely approvals and notifications to the customer of expected outages. See related table in this Process Document for standard lead times depending on the Priority and Risk associated to it.
Release	A collection of one or more changes that includes new and/or changed Configuration Items (CIs)

	that are tested and then introduced into the production environment.
Request for Change (RFC)	This is the formal change request, including a description of the change, components affected, business need, cost estimates, risk assessment, resource requirements, and approval status.
Standard Changes	Consistently follows documented release process and are pre-approved by the CCB or CAB. This type of change is performed on a routine basis and is part of the operational practice of the business. These types of changes conform to the requirements of a planned change, except they can be implemented without following a time constraint because they are routine and 100% of the changes submitted under this category do not cause any disruptions to the IT community. These types of changes have a minimal review and approval process.
Unplanned Changes	These types of changes cause a disruption to the IT community due to the unexpectedness of it and the lack of resources. Timely notification is also a key factor of the customer's expectations to maintain the system at a specific level of availability.

11.2. Acronyms

Acronym	Definition
AAR	**After Action Report**
ANR	**Automated Notification Reporting**
APP	**Application**
AUS	**Austin**
CAB	**Change Advisory Board**
CCB	**Change Control Board**
CI	**Configuration Item**
CMDB	**Configuration Management Database**
CMS	**Change Management System**
DB	**Database**
DOC	**Documentation**
EDB	**Enrollment Database**
ECC	**Emergency Change Committee**
ECCB	**Executive Change Control Board**
ECWG	**Executive Change Work Group**
ESM	**Enterprise Storage Management**
FISMA	**Federal Information Security Management Act of 2002**
FSC	**Forward Schedule of Changes**
GSS	**General Support Systems**
HDR	**Health Data Repository**
HIN	**Hines**
HTH	**Home TeleHealth**
HW	**Hardware**
INFRA	**Infrastructure**
IP	**Internet Protocol**
IT	**Information Technology**
ITIL	**Information Technology Infrastructure Library**
IVV	**Independent Verification and Validation**
LAN	**Local Area Network**
MA	**Major Application**
NCA	**National Cemetery Administration**
OIT	**Office of Information and Technology**
OS	**Operating System**
PlantMgmt	**Plant Management**
PHI	**Philadelphia**

POC	**Point of Contact**
PortDev	**Portable Devices**
PIR	**Post Implementation Review**
RACI	**Responsible, Accountable, Consulted and Informed**
RDI	**Remote Data Interoperability**
RFC	**Request for Change**
SAQ	**Software Quality Assurance**
SCCB	**Subordinate Change Control Board**
SCWG	**Subordinate Change Work Group**
SIT	**Security Infrastructure Team**
SLA	**Service Level Agreement**
SME	**Subject Matter Expert**
SptContract	**Support Contracts**
SQL	**Structured Query Language**
SVS	**Services**
SW	**Software**
SYS	**Systems**
T and E	**Test and Evaluation**
TELCO	**Telecommunications**
VA	**Department of Veterans Affairs**
VBA	**Veterans Benefit Administration**
VHA	**Veterans Health Administration**
VIE	**VistA Interface Engine**
VistA	**Veterans Health Information Systems and Technology Architecture**
WAN	**Wide Area Network**