
VA Enterprise Design Patterns:

4. IT Service Management

4.2 Change Management

**Office of Technology Strategies (TS)
Architecture, Strategy, and Design (ASD)
Office of Information and Technology (OI&T)**

Version 1.0

Date Issued: November 6, 2015



THIS PAGE INTENTIONALLY LEFT BLANK FOR PRINTING PURPOSES

APPROVAL COORDINATION

**TIMOTHY L
MCGRAIL
111224**

Digitally signed by TIMOTHY L
MCGRAIL 111224
DN: dc=gov, dc=va, o=Internal,
ou=people,
0.9.2342.19200300.100.1.1=tim.mcg
rail@va.gov, cn=TIMOTHY L
MCGRAIL 111224
Date: 2015.11.12 15:36:04 -05'00'

Date:

Tim McGrail
Senior Program Analyst
ASD Technology Strategies

**PAUL A.
TIBBITS
116858**

Digitally signed by PAUL A. TIBBITS
116858
DN: dc=gov, dc=va, o=Internal,
ou=people,
0.9.2342.19200300.100.1.1=paul.tibbit
s@va.gov, cn=PAUL A. TIBBITS 116858
Reason: I am approving this
document.
Date: 2015.12.03 12:58:43 -05'00'

Date:

Paul A. Tibbits, M.D.
DCIO Architecture, Strategy, and Design

REVISION HISTORY

Version	Date	Organization	Notes
0.1		ASD TS	Initial Draft
0.5		ASD TS	Second draft document with updates made throughout document based upon initial internal/external stakeholder review and comment.
0.7		ASD TS	Third and final draft for stakeholder review prior to TS leadership approval/signature. Updates made following Public Forum collaborative feedback and working session.
1.0		ASD TS	Final version for TS leadership approval and signature, including all applicable updates addressing stakeholder feedback and Section 508 Compliance.

REVISION HISTORY APPROVALS

Version	Date	Approver	Role
0.1		Jacqueline Meadows-Stokes	ASD TS – Management and Program Analyst
0.5		Jacqueline Meadows-Stokes	ASD TS – Management and Program Analyst
0.7	9/2/2015	Jacqueline Meadows-Stokes	ASD TS – Management and Program Analyst
0.9		Tim McGrail	ASD TS – Senior Program Analyst
1.0		Paul A. Tibbits, M.D.	ASD – Deputy CIO

TABLE OF CONTENTS

Contents

1.0 INTRODUCTION 1

 1.1 BUSINESS NEED..... 1

 1.2 APPROACH..... 1

2.0 CURRENT CAPABILITIES AND LIMITATIONS 2

 2.1 THE CURRENT STATE OF CHANGE MANAGEMENT (CM) 2

3.0 FUTURE CAPABILITIES 3

 3.1 ALIGNMENT TO THE TECHNICAL REFERENCE MODEL (TRM) 8

4.0 USE CASES 9

APPENDIX A. DOCUMENT SCOPE 10

 SCOPE..... 10

 DOCUMENT DEVELOPMENT AND MAINTENANCE..... 11

APPENDIX B. DEFINITIONS 12

APPENDIX C. ACRONYMS 16

APPENDIX D. REFERENCES, STANDARDS, AND POLICIES 18

FIGURES

Figure 1: Current State of Change Management.....	3
Figure 2: Enterprise Change Management aligned with a Federated CMDB.....	5
Figure 3: Notional Enterprise Change Management Process.....	6
Figure 4: Change Management Use Case.....	10
Figure 5: Change Management Use Case.....	10

TABLES

Table 1: Representative VA Tool Categories and Approved Technologies.....	9
---	---

1.0 INTRODUCTION

The Office of the Inspector General (OIG), Federal Information Security Management Act (FISMA) and Federal, Identify, Credential, and Access Management (FICAM) audits reported a material weakness in change management controls. VA has not fully implemented procedures to enforce enterprise standard system development and change management controls for mission-critical systems. Software changes to mission-critical systems and infrastructure network devices do not follow standard software change control procedures. The OIG audit discovered numerous test plans, test results, and approvals either incomplete or missing. Lines of business have invested in several tools for asset discovery, data normalization, and configuration management that do not align with an enterprise change control policy.

1.1 Business Need

Enterprise change management ensures compliance with governance, legal, contractual, and regulatory requirements. By not enforcing a standardized change control methodology, system development projects may be inconsistently developed, tested, and migrated into production. This places VA systems at risk of unauthorized or unintended software modifications.

Service and infrastructure changes can be managed more effectively through enterprise change controls that will:

- Reduce failed changes and associated service disruption
- Decrease unauthorized changes
- Minimize unplanned outages
- Lower the number of emergency changes
- Reduce delayed project implementations

1.2 Approach

Change management is a control process responsible for ensuring that changes are business-aligned and do not pose undue risk. This Enterprise Design Pattern describes the process for establishing enterprise change management and defines the factors that are critical to its success.

The purpose of this document is to provide guidance on applying best practices to plan, implement, monitor, and improve enterprise change management. Process initiatives and service implementation efforts should align with the proposed framework. Supporting this purpose, the document will:

- Define best practices to drive the implementation of Enterprise Change Management
- Define the change control framework required to meet compliance with approved standards
- Recommend a set of milestones for implementation

2.0 CURRENT CAPABILITIES AND LIMITATIONS

2.1 The Current State of Change Management (CM)

- Absence of Enterprise CM Office: An Enterprise Level Program Office that oversees the VA Change and Configuration Management processes and ensures compliance needs to be established. While enterprise policy and OIT operational change management processes exist, they are not enforced consistently across the enterprise.
- Multiple change management systems and tools: Multiple change and configuration management tools are dispersed throughout the enterprise. These tools are not fully utilized, lack interoperability, and collect change information at varying levels.
 - Region four (4) uses Serena Tool
 - Enterprise Security System (ESS) uses Change Gear
 - Enterprise Systems Engineering (ESE) uses both CA and BMC Remedy
 - Office of Information Security (OIS) uses Government off the Shelf (GOTS) Product
 - Region three (3) uses CA and GOTS Product
 - Region two (2) uses CA tool not aligned to the current VA Data Centers
- Limitations of current change systems: Existing systems operate in silos. Change releases are implemented with no oversight. Separate processes exist for scheduling and release with little to no coordination on enterprise impact.

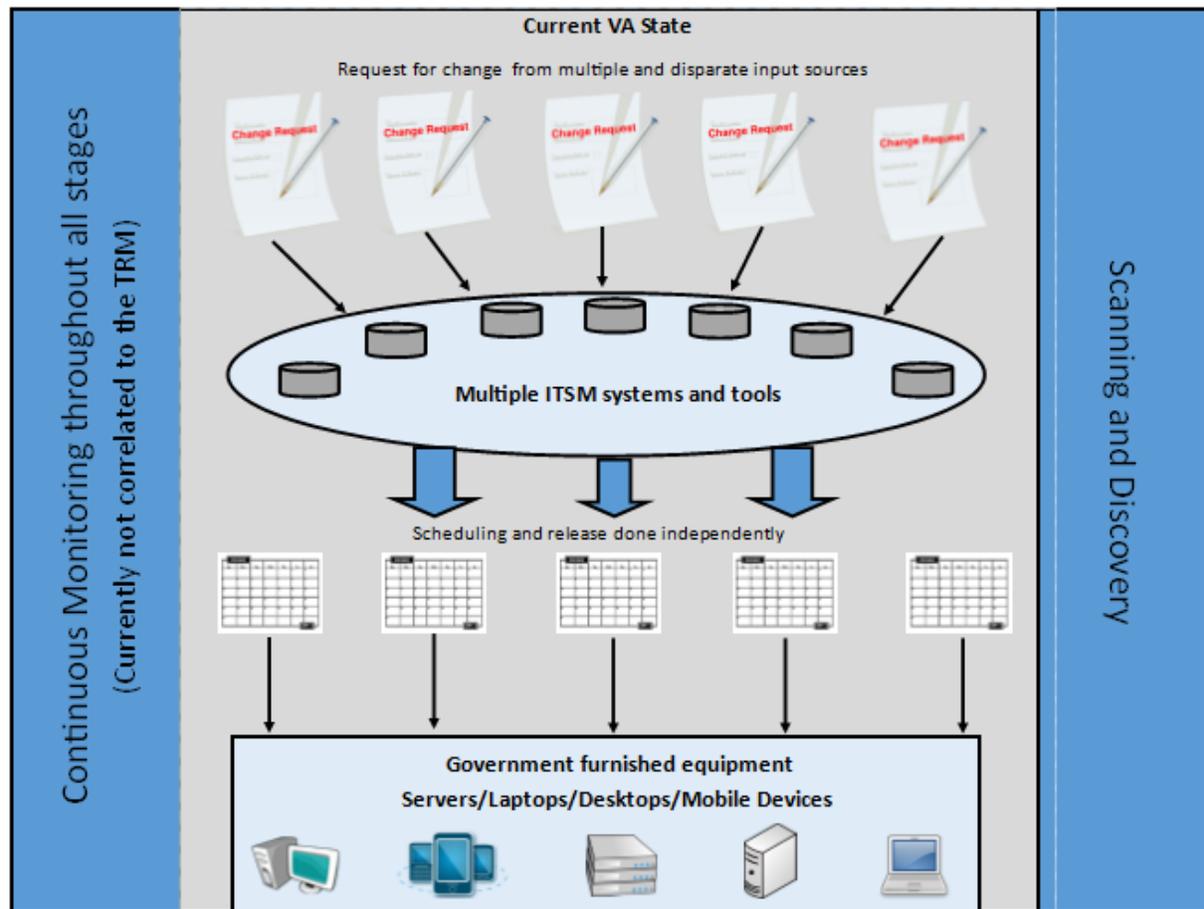


Figure 1: Current State of Change Management

As shown by Figure 1, changes are fed into the discovery tools but these changes are not reported to the Configuration Management Database (CMDB) to update the baseline of the affected Configuration Items (CI). These challenges and limitations present a loosely coupled infrastructure that:

- Provides a weakened defense against unauthorized change
- Non-compliance with baseline standards
- Increased security vulnerabilities such as malware, back-door attacks, and other harmful security threats due to non-standardized and enforced configuration control

3.0 FUTURE CAPABILITIES

Enterprise Change Management ensures all changes are assessed, approved, implemented, and reviewed in a controlled manner. As a result, any modification to the IT environment—whether it

involves an addition, maintenance, or deletion of a service or service component—is in line with the overall business strategy.

The goals of Enterprise Change Management are:

- Single source of Change Record Information across the enterprise
- Automated and integrated change record logging and tracking
- Single approval provided at appropriate change management jurisdiction level
- Authorization(s) provided at the appropriate change management jurisdiction levels
- Risk and Impact Assessment activities and Implementation activities documented and linked as part of the Change Record
- Change Status awareness throughout the lifecycle
- Standard management reusable reports

All CIs subject to change management require monitoring by an endpoint manager and scanning tool to maintain multiple standards mapped to the VA core policies, as shown in Figure 2. All data from each endpoint management and scanning tool is normalized into a standard dataset. This dataset is reconciled against a product catalog repository to validate each CI's current baseline adheres to the organization's policies, procedures, and federal laws. During this process, a relationship and dependency mapping between information system, its CIs, and information system components must be visible to examine the IT infrastructure of the VA network.

The standard change management process requires a change control process to track all changes from a Request for Change (RFC) aligned to a RACI matrix. This tracking requires a fully automated hybrid service desk manager tool.

A fully automated hybrid service desk manager tool connected to a federated CMDB will support change tracking. The CMDB requirements are as follows:

- Reflect all changes made to the CI from the time the CI entered the enterprise until its retirement
- Filter history for any category the administrator requires including priority, date created, and number of requests for changes (RFCs) by CI

The ITSM tools require a Process Flow Status Model that aligns to all change management process stages with mandatory fields assigned for compliance with the organization's auditing rules. The process flow model must indicate the status of the RFC and send triggers to each stakeholder outlined in the RACI matrix.

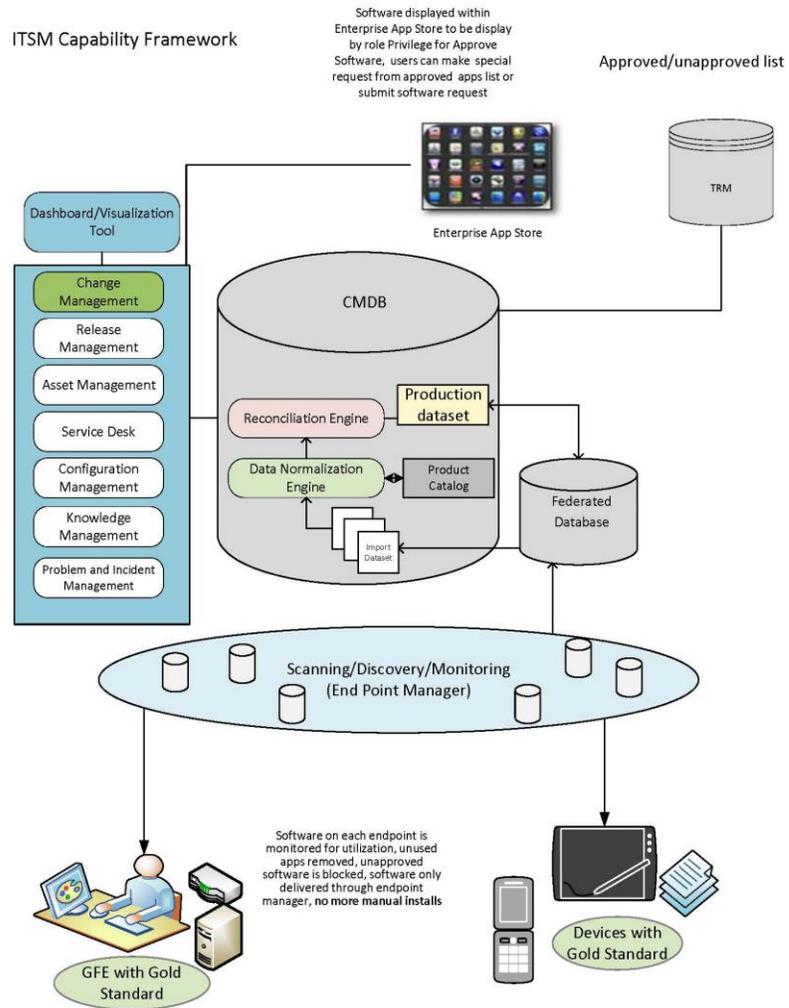


Figure 2: Enterprise Change Management aligned with a Federated CMDB

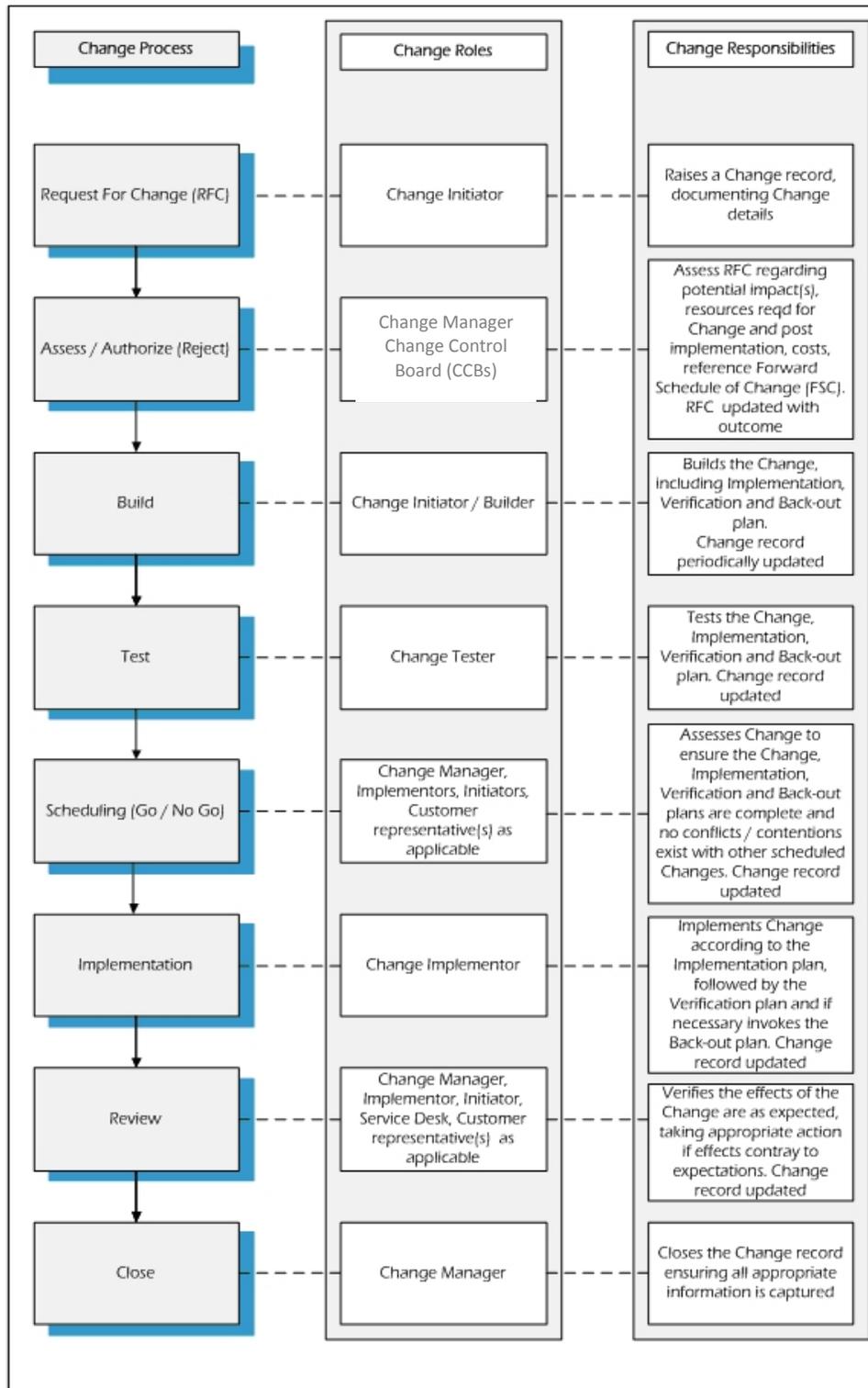


Figure 3: Notional Enterprise Change Management Process

- **Initiate RFC** - The goal of Change Management is to facilitate all RFCs through clear procedures, automation, and simple checks and balances. If RFC initiation is not managed properly, this could lead to misuse of the Change Management system. Clear policies will define who can create RFCs, scope of the RFCs, and the information required describe the requirement.
 - RFCs focus on improving productivity, a service request, an incident management, problem management or any type of request outlined within the change management process. This request will enable the organization to determine any ramifications of the changes prior to execution to mitigate a potential impact to the IT environment. RFC's are categorized as Normal, Standard, and Emergency. Routine or recurring changes considered to have minimal or no impact on business service can be considered for an automated process (depending on the type of RFC).
- **Analyze / Plan Change** - A comprehensive risk assessment, impact analysis and change plan will improve the change management process by providing accurate and reliable information. The change coordinator is required to route the RFC to the responsible groups for analysis and completion of the activity. This ensures complete visibility into the status of the RFC and identification of potential bottlenecks. Information for this section can be easily accessible from the CMDB. A standardized risk assessment provides technical, security, and business analysis as listed below:
 - A technical assessment provides technical risk analysis about change implementation and schedule conflict. This assessment, in conjunction with ITIL release management process will remediate issues and concerns and provide plans for back-out to restore the original baseline.
 - A security impact analysis assesses the change to information systems and the associated security ramifications.
 - A business assessment provides the potential impact of changes to the business in accordance with IT budget and cost with relations to the technical assessment for change.
- **Approve Change** - The Approve Change stage involves the Enterprise Change Control Board ECCB, SMEs, Change Coordinators, Approval Stakeholders, and Change Manager to gain agreement with the recommended revision flowing from the Analyze / Plan Change stage. The RFC is prioritized depending on the severity of the change (e.g. Normal, Emergency).
- **Build** - Approved RFCs are assigned to a developer, programmer, technical writer, or other SME to create the change. The changes are compiled and packaged with appropriate 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. The

change to the CI creates a new baseline with supporting documentation which is approved by the Change Control Board (CCB).

- **Schedule / Implement Change** - Change implementation is a technical implementation that follows the guidelines established in the System Development Life Cycle (SDLC) and Project Management Procedures.
- **Validate** - The Change Manager reviews the change, tests and validates in a production environment, and monitors in real-time for any problems or issues after the approval of the implementation phase. The change request status is set pending additional reviews from the change manager, possible CCB stakeholders, and the change owners.

An effective Enterprise Change Management framework provides the flexibility to address processes, technology, and the human aspect of change. Key steps required to transition to an Enterprise wide Change Management process are:

1. Obtaining Executive and other Organizational Leadership/Stakeholder’s sponsorship
2. Establishing an Enterprise Change Control Office manage and oversee the CCB
3. Identifying and leveraging existing procedures, policies, tools, etc.
4. Ensuring new changes/requirements are aligned to the organization’s strategic vision and objectives
5. Identifying and documenting overall risks while specifying mitigation plans to address those risks

3.1 Alignment to the Technical Reference Model (TRM)

All projects are directed to use the approved tools and technologies located in the VA Technical Reference Model (TRM) to comply with VA Enterprise Architecture and the guidance provided in this document. Approved tools include:

Table 1: Representative VA Tool Categories and Approved Technologies

Tool Category	Example Approved Technologies
Asset Management	CA IT Asset Management, IBM Endpoint Manager, Atrium Discovery and Dependency Mapping
Data Center Automation Software	Microsoft System Center Configuration Manager (SCCM), BMC Application Automation
Disaster Recovery	Tivoli Storage Management, Bacula Enterprise
IT Service Desk	Cisco Agent Desktop, Remedy

Monitoring	Oracle Exadata, Strobe
System Change and Configuration Management	Hyena, VMware vSphere CLI (vCLI)

4.0 USE CASES

The following use case demonstrates the application of enterprise change management described in the previous section. Analyzing the impact of a change to IT service CIs represents a common use case for the change management process. According to the type of RFC, the National or Regional CCB approves the change to the specific CI if the impact analysis factor is considered minimal or poses no threat to the IT environment. The impact analysis works in conjunction with related ITIL service transition processes. The following steps represent change impact analysis at a high level:

1. Submitter packages a change order as an RFC
2. CCB retrieves and logs change order
3. CCB evaluates CI relationships affected by change order, using the CMDB
4. CCB determines whether change order conflicts with another change order or breaks a dependency in the CMDB
5. If Yes, then CCB rejects the change order
6. If No, then CCB approves the change order
7. CCB logs the decision and informs submitter of status of change order for both Steps 5 and 6
8. CMDB automatically updated to reflect CI changes resulting from change order

The following figure illustrates this use case:

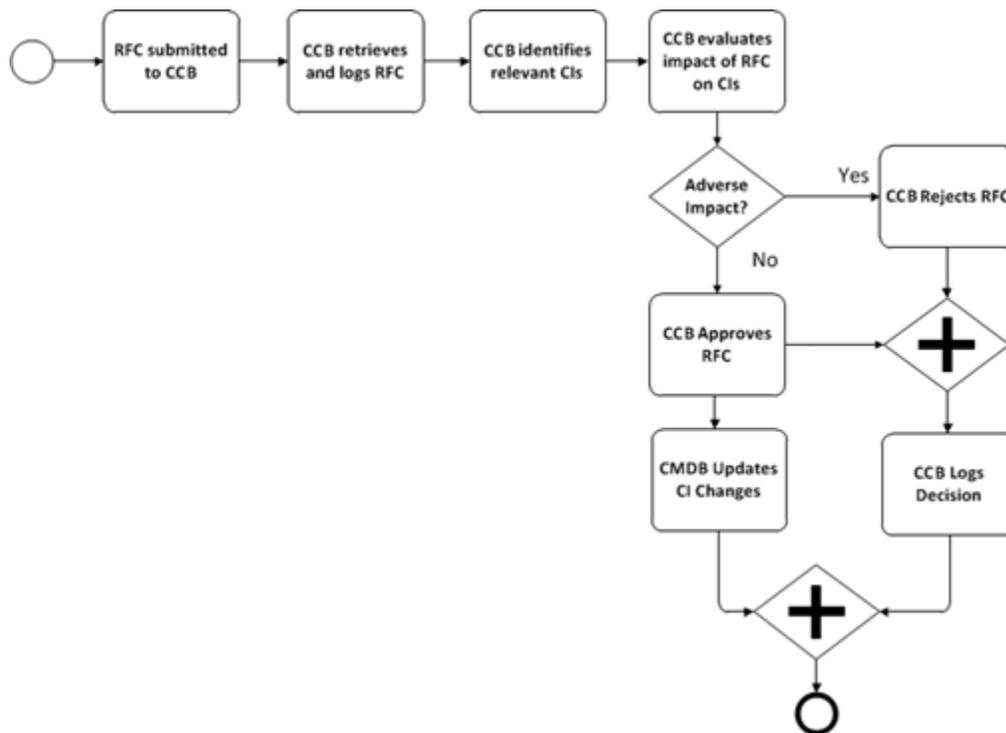


Figure 4: Change Management Use Case

This use case can also include real-time monitoring of the CIs, which in turn triggers changes to the IT infrastructure. Enterprise-wide ITSM tools support automated change detections, which can be packaged as an RFC for the CCB review and impact analysis. The CCB may also use ITSM tools to visualize the calendar of changes to mitigate risks to running critical business functions as changes are made. ITSM tools also support change collision detection, which prevents duplicate changes to CIs impacting the honoring of Service Level Agreements (SLA) with customers.

Appendix A. DOCUMENT SCOPE

Scope

Per the Federal Information System Controls Audit Manual (FISCAM) Audit Material Weaknesses #1 (Vulnerability Discovery and Remediation) and #6 (Unauthorized Software Discovery and Remediation), there needs to be an enterprise change management process. This document will ensure all changes to all information technology infrastructure and software CIs are managed and communicated in a disciplined and standardized manner to minimize risk, minimize impact and optimize IT Resources in accordance to the OI&T Enterprise Change Management Program Policy.

This document does not change the current change management process Standard Operation Procedure (SOP) that OI&T has established. It adds capabilities to the Product Development (PD) and Service Delivery and Engineering (SDE) guidance to develop an Enterprise Change Management Process across all the pillars of the Veterans Affairs (Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and National Cemetery Administration (NCA)).

Document Development and Maintenance

This document was developed collaboratively with internal stakeholders from across the Department and included participation from VA's Office of Information and Technology (OI&T), Product Development (PD), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE). Extensive input and participation was also received from VHA, VBA and NCA. In addition, the development effort included engagements with industry experts to review, provide input, and comment on the proposed pattern. This document contains a revision history and revision approval logs to track all changes. Updates will be coordinated with the Government lead for this document, which will also facilitate stakeholder coordination and subsequent re-approval depending on the significance of the change.

Appendix B. DEFINITIONS

Name	Definition
Approved List	A list of discrete entities, such as hosts or applications that are known to be benign and are approved for use within an organization and/or information system.
Authentication (FIPS 200)	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Baseline Configuration	A set of specifications for a system, of Configuration Item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.
Enterprise Change Control Board	A board delivering support to the Change Management team by approving requested changes and assisting in the assessment and prioritization of changes.
Configuration	The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged.
Configuration Baseline	See "Baseline Configuration"
Change Control Board	A board functioning to formally authorize all changes from the VA's baseline infrastructure. It is the systematic process of proposing, justifying, evaluating, validating, disposing of proposed changes, and implementing approved changes, as well as tracking the many changes affecting a configuration item's state. The Change Management team ensures the documentation and coordination of recommended engineering changes to configuration items.
Configuration Control (CNSSI-4009)	Process for controlling modifications to hardware, firmware, software and documentation to protect the information system against improper modifications before, during, and after system implementation.
Configuration Control Board	Establishment of and charter for a group of qualified people with responsibility for the process of controlling and approving changes throughout the development and operational lifecycle of products and systems; may also be referred to as a change control board;

Configuration Item	<p>An identifiable part of a system (e.g., hardware, software, firmware, documentation, or a combination thereof) that is a discrete target of configuration control processes.</p> <p>A Baseline Configuration is a set of specifications for a system, or CI within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.</p>
Configuration Identification	Methodology for selecting and naming configuration items
Configuration Management	A collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development and production life cycle.
Configuration Management Plan	A comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems.
Configuration Monitoring	Process for assessing or testing the level of compliance with the established baseline configuration and mechanisms for reporting on the configuration status of items placed under CM.
Enterprise Architecture	The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture.
False Positive	A result that indicates that a given condition is present when it is not.
Information System User (CNSSI-4009)	Individual or (system) process acting on behalf of an individual, authorized to access an information system.
Patch	An additional piece of code developed to address a problem in an existing piece of software.
Remediation	The act of correcting vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, and uninstalling a software application.

Request for Change	<ul style="list-style-type: none"> • 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.
Risk	The probability that a particular threat will exploit a particular vulnerability.
System	A set of IT assets, processes, applications, and related resources that are under the same direct management and budgetary control; have the same function or mission objective; have essentially the same security needs; and reside in the same general operation environment. When not used in this formal sense, the term is synonymous with the term "host". The context surrounding this word should make the definition clear or else should specify which definition is being used.
Systemic	An issue or vulnerability found through scanning or discovery that resides in multiple places throughout the enterprise.
System Owner	Individual with managerial, operational, technical, and often budgetary responsibility for all aspects of an information technology system.
Threat	Any circumstance or event, deliberate or unintentional, with the potential for causing harm to a system.
VASI	VASI is an authoritative inventory of business-oriented applications and supporting databases providing a comprehensive repository of basic information about VA systems; represents the relationships between systems and other VA data stores; and captures new systems.

Vulnerability	A Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat device.
---------------	--

Appendix C. ACRONYMS

The following table provides a list of acronyms that are applicable to and used within this Enterprise Design Pattern document.

Acronym	Description
ADDM	Atrium Discovery and Dependency Mapping
ASD	Architecture, Strategy and Design
CA	CA Technologies
ECCB	Enterprise Change Control Board
CA SDM	CA Service Desk Manager
CCB	Change Control Board
CERT	Computer Emergency Readiness Team
CI	Configuration Item
CIO	Chief Information Officer
CM	Configuration Management
CMDB	Configuration Management Database
COTS	Commercial Off-the-shelf
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
DHS	Department of Homeland Security
DOD	Department of Defense
EO	Enterprise Operations
FEA	Federal Enterprise Architecture

Acronym	Description
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GOTS	Government Off-the-shelf
IBM EPM	IBM Endpoint Manager
IS	Information System
IT	Information Technology
ITAM	Information Technology Asset Management
ITIL	Information Technology Infrastructure Library
LOB	Line-of-Business
MAC	Media Access Control
NIST	National Institute of Standards and Technology
NSD	National Service Desk
OI&T	Office of Information and Technology
OIG	Office of the Inspector General
OIS	Office of Information Security
OMG	Office of Management and Budget
OVAL	Open Vulnerability Assessment Language
PD	Product Development
SCAP	Security Content Automation Protocol
SCCM	System Center Configuration Manager

Acronym	Description
SDE	Service Delivery Engineering
SIEM	Security Information and Event Management
SLA	Service Level Agreement
TRM	Technical Reference Model
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline
VA	Department of Veterans Affairs
VASI	Veterans Affairs Systems Inventory
XML	Extensible Markup Language

Appendix D. REFERENCES, STANDARDS, AND POLICIES

This Enterprise Design Pattern is aligned to the following VA OI&T references and standards applicable to all new applications being developed in the VA, and are aligned to the VA ETA:

This Enterprise Design Pattern is aligned to the following VA OI&T references and standards applicable to all new applications being developed in the VA, which were gathered and reviewed from:

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
1	VA	VA Directive 6004	Directive establishes VA policy and responsibilities regarding Configuration, Change, and Release Management Programs for implementation across VA.
2	VA	VA 6500 Handbook	Directive information security program. Defining overall security framework for VA.
3	NIST	800-128	Guide for Security-Focused Configuration Management of Information Systems Provides guidelines for organizations responsible for managing and administrating the security of federal

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
			information systems and associated environments of operations
4	NIST	SP 800-63-2	Special Publication — Creating a Patch and Vulnerability Management Program Designed to assist organizations in implementing security patch and vulnerability remediation programs.
5	NIST	800-53	Recommended Security Controls for Federal Information Systems and Organizations Outlines the importance of deploying automated mechanisms to detect unauthorized components and configurations within agency networks
6	OMB	Memorandum M-14-04	FY2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management Provides guidance for Federal agencies to follow the report requirements under FISMA.
7	OMB	Memorandum M-02-01	Guidance for Preparing and Submitting Security Plans of Actions and Milestones Defines Management and Reporting Requirements for agency POA&Ms, including deficiency descriptions, remediation actions, required resources, and responsible parties.
8	White House	FISMA Act of 2002	Reauthorizes key sections of the Government Information Security Reform Act Provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets.
9	VA	CRISP	Intended to improve access controls, configurations management, contingency planning, and the security management of a large number of information technology systems.
10	Congress	E-Government Act of 2002	Public Law 107-347 Purpose is to improve the management and promotion of electronic government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a framework of measures that require using Internet-based information technology to improve citizen access to government information and services, and for other purposes.

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
11	VA	Change Plan – Process Template	This Standard Operating Procedure has been created to support and supplement the National Change Management Policy and Standard Document and is not intended to replace the overall management process of the Change Management Program this SOP expands and provides specific information related to the following process being placed under Change Control
12	VA	OIT Enterprise Change Management Policy	This document establishes an OIT Enterprise Change Management policy ensuring changes to all information technology infrastructure and software configuration items (CIs) are managed and communicated in a disciplined and standardized manner to minimize risk, impact and optimize IT resources
13	VA	OIT Change Management Process	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.
14	VA	TRM	

Working Draft, Pre-Decisional, Deliberative Document - Internal Use Only