

# **Office of Information and Technology (OIT)**

## **Configuration Management Process**



**Version 3.0**

**June 2011**

## Revision History

Date	Revision	Iteration	Description	Author
01/14/10	1.0		First Draft	Configuration Management TWG
03/18/10	2.0		Rewrite from F2F	Integrated TWG
01/12/11	2.1		CR 7115 – Added instruction for updating document.	Approved by Mike LeRoy
6/2011	3.0		Replaced OI&T with OIT, Modified RACI chart and Roles to match same wording as in ProPath Map, Added/Modified input/outputs for each to match ProPath Map.	Integrated Technical Working Group (TWG)

## Table of Contents

<b>Revision History .....</b>	<b>2</b>
<b>1. Introduction .....</b>	<b>1</b>
1.1. Process Purpose .....	1
1.2. Scope.....	1
1.3. Objectives .....	1
1.4. Configuration Management Champion.....	2
1.5. Config Management Process Document Modifications .....	2
<b>2. Responsible, Accountable, Consulted, and Informed (RACI) Matrix .....</b>	<b>3</b>
2.1. Process Roles and Responsibilities .....	4
<b>3. Configuration Management Process .....</b>	<b>5</b>
3.1. Configuration Management Process .....	7
3.2. Process Inputs.....	7
3.3. Process Outputs.....	8
3.4. Exit Criteria .....	9
<b>4. Related Processes .....</b>	<b>9</b>
<b>5. Configuration Management Process Steps .....</b>	<b>9</b>
5.1. Identify Configuration Items .....	9
5.1.1. Description .....	9
5.1.2. Inputs .....	9
5.1.3. Responsible Persons .....	10
5.1.4. Activities.....	10
5.1.5. Outputs .....	10
5.2. Place CIs Under Configuration Management Control .....	10
5.2.1. Description .....	10
5.2.2. Inputs .....	10
5.2.3. Responsible Persons .....	11
5.2.4. Activities.....	11
5.2.5. Outputs .....	11
5.3. Adopt Change Management Procedures .....	11
5.3.1. Description .....	11
5.3.2. Inputs .....	11
5.3.3. Responsible Persons .....	11

5.3.4.	Activities .....	11
5.3.5.	Outputs .....	11
5.4.	Verify and Audit Configuration Items .....	12
5.4.1.	Description .....	12
5.4.2.	Inputs .....	12
5.4.3.	Responsible Persons .....	12
5.4.4.	Activities .....	12
5.4.5.	Outputs .....	12
5.5.	Generate Reports .....	13
5.5.1.	Description .....	13
5.5.2.	Inputs .....	13
5.5.3.	Responsible Persons .....	13
5.5.4.	Activities .....	13
5.5.5.	Outputs .....	13
6.	Configuration Management Procedures .....	13
6.1.	Identify Configuration Items .....	13
6.1.1.	Inputs .....	13
6.1.2.	Responsible Persons .....	14
6.1.3.	Procedures .....	14
6.1.4.	Outputs .....	14
6.2.	Place CIs Under Configuration Management Control .....	14
6.2.1.	Inputs .....	14
6.2.2.	Responsible Persons .....	15
6.2.3.	Procedures .....	15
6.2.4.	Outputs .....	15
6.3.	Adopt Change Management Procedures .....	15
6.3.1.	Inputs .....	15
6.3.2.	Responsible Persons .....	16
6.3.3.	Procedures .....	16
6.3.4.	Outputs .....	16
6.4.	Verify and Audit Configuration Items .....	16
6.4.1.	Inputs .....	16
6.4.2.	Responsible Persons .....	17

6.4.3.	Procedures .....	17
6.4.4.	Outputs .....	17
6.5.	Generate Reports .....	17
6.5.1.	Inputs .....	17
6.5.2.	Responsible Persons .....	17
6.5.3.	Procedures .....	18
6.5.4.	Outputs .....	18
7.	Metrics.....	19
8.	Training and Tools.....	20
9.	Appendix A – Definitions and Acronyms .....	21
10.	Concurrence .....	22
11.	Appendix B – Family and Class Examples .....	23

# 1. Introduction

## 1.1. Process Purpose

The purpose of the Configuration Management (CM) process is to identify, control, verify and track all versions, characteristics and attributes of hardware, firmware, software, documentation, processes, procedures and other components designated as Configuration Items (CIs) across all Department of Veterans Affairs (VA) Information Technology (IT) environments. The process manages a CI throughout its life cycle. This process applies to CIs in production, development, and testing. The process is made up of interrelated activities, including activities that measure the effectiveness for continued process improvement. In summary, the process identifies the CI and captures its attributes, relationships, versions, baselines and documents its authorization in IT environments with audits against official approvals. The CI is placed under change management to document its implementation life cycle. The process will communicate the status of the CI and any actions required.

The purpose of this document is to define the Configuration Management 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 Configuration 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 Configuration Management process supports the following general types of IT activities on those resources:

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

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

## 1.3. Objectives

The Configuration Management process accomplishes the following objectives:

- Establishes an OIT Configuration Management process
- Documents standardized repeatable methods and procedures that follow configuration management principles

- Communicates an adaptable framework for configuration management that allows OIT offices to incorporate the principles of configuration management into their business functions and work products as a routine procedure
- Allows OIT to reinforce a commitment to minimizing or preventing adverse affects on VA information systems, as a result of a lack of proper planning, documentation, and/or coordination through an approved standard process

## **1.4.Configuration Management Champion**

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

## **1.5.Config 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\_configuration\_management\_process\_document.doc) will be managed through the ProPath Change Request process. Approval of Change Requests affecting the Configuration Management Process document must be obtained from the Integrated Technical Working Group (TWG).

ProPath Change Request Link: [http://vaww.oed.oit.va.gov/process/change\\_control/](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 it 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.

Table 1 provides the suggested RACI Matrix for the Configuration 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.



**Table 1: RACI Matrix**

<b>PARTICIPATION CODES</b>				
<b>R = Responsible</b>				
<b>A = Accountable</b>				
<b>C = Consulted</b>				
<b>I = Informed</b>				
<b>ACTIVITIES</b>	<b>Project Manager/System Owner</b>	<b>Configuration Management Analyst</b>	<b>Configuration Management Manager</b>	<b>Stakeholder</b>
Identify Configuration Items	A	R	R	CI
Place CI Under Configuration Control	A	R	R	CI
Adopt Change Management Procedures	A	R	R	CI
Verify and Audit Configuration Items	A	C	R	CI
Generate Reports	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 2 lists the key roles and their descriptions for the Configuration Management process as referenced in Table 1 containing the Responsible, Accountable, Consulted, Informed (RACI) Matrix.

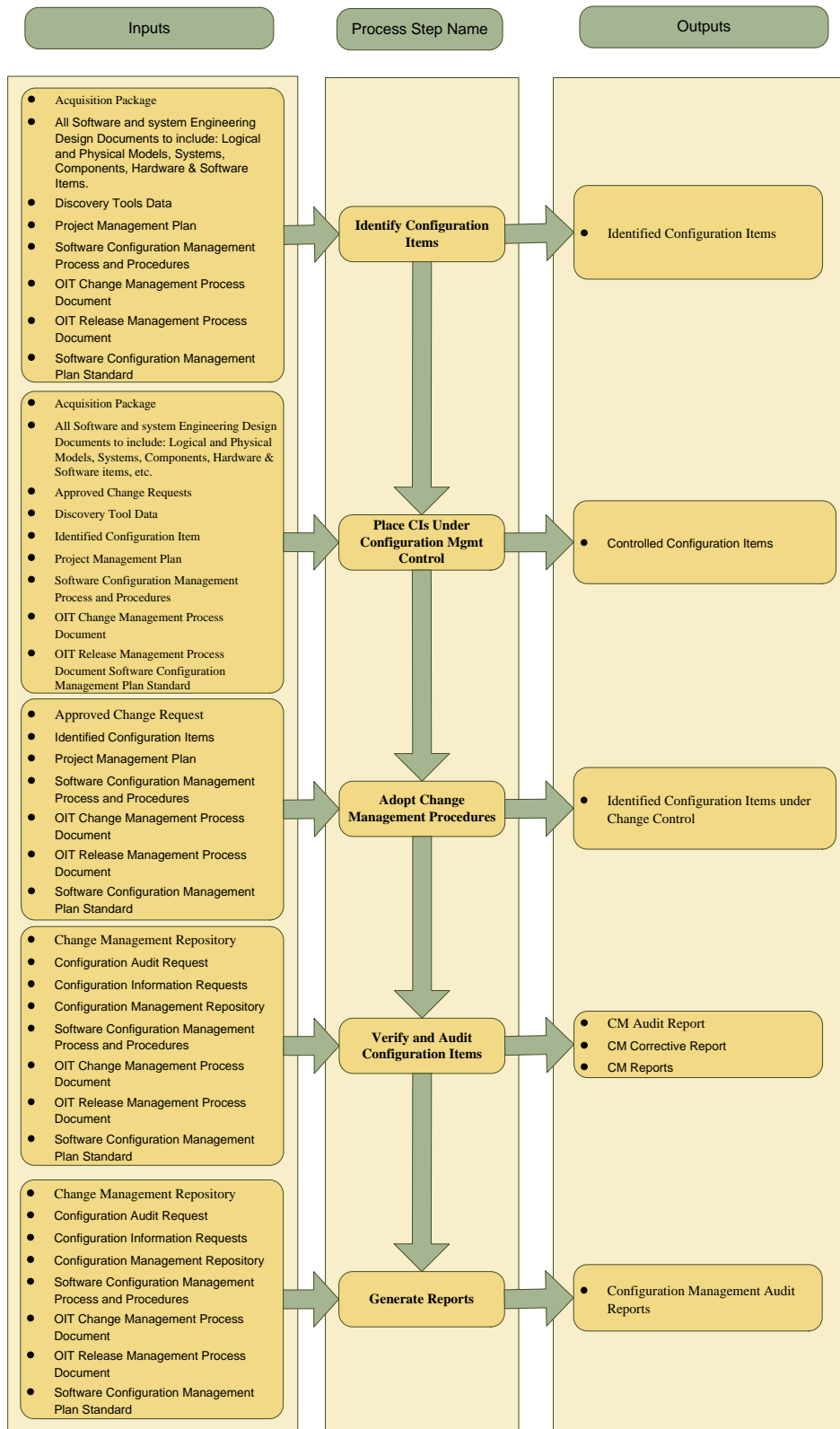
Table 2: Roles and Descriptions

ROLE	DESCRIPTION
CM Process Owner	The Configuration Management Process Owner is accountable to senior management for proper governance, design, execution, and improvement of CM processes in an OIT office.
Configuration Management Manager	The Configuration Management Manager is responsible for ensuring proper introduction, execution and 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.
Configuration Management Analyst	The Configuration Management Analyst is responsible for performing daily CM operations for identification, control, status reporting and audit of CIs under the leadership of the Configuration Manager.
Stakeholder	Any person who has an interest in a project, IT service, activity, deliverable, and resource.
Project Manager/System Owner	The Project Manager/System Owner is accountable to senior management for ensuring the Configuration Management Process is implemented

### 3. Configuration Management Process

The CM process outlined below is to be followed by all VA employees, contractors, and third parties who operate and or maintain IT resources and are responsible for implementing configuration management based on the scope outlined in this document. The basic steps associated with the CM process are listed below:

- Identify CI
- Place CI Under Configuration Control
- Adopt Change Management Procedures
- Verify and Audit CIs
- Generate Reports



**Figure 3: Configuration Management Process**

## 3.1.Configuration Management Process

Configuration Management enables the ability to maintain information of configuration items required to deliver IT services.

## 3.2.Process Inputs

### Identify Configuration Items

- Acquisition Package
- All Software and system Engineering Design Documents to include: Logical and Physical Models, Systems, Components, Hardware and Software items, etc.
- Discovery Tools Data
- Project Management Plan
- Software Configuration Management Procedures
- OIT Change Management Process Document
- OIT Configuration Management Process Document
- OIT Release Management Process Document
- VA Directive 6004 Configuration, Change, and Release Management Programs
- Software Configuration Management Plan Standard

### Place CIs Under Configuration Mgmt Control

- Acquisition Package
- All Software and system Engineering Design Documents to include: Logical and Physical Models, Systems, Components, Hardware and Software items, etc.
- Approved Change Requests
- Discovery Tool Data
- Identified Configuration Item
- Project Management Plan
- Software Configuration Management Procedures
- OIT Change Management Process Document
- OIT Configuration Management Process Document
- OIT Release Management Process Document
- VA Directive 6004 Configuration, Change, and Release Management Programs
- Software Configuration Management Plan Standard

### Adopt Change Management Procedures

- Approved Change Requests
- Identified Configuration Items
- Project Management Plan
- Software Configuration Management Procedures

- OIT Change Management Processes Document
- OIT Configuration Management Process Document
- OIT Release Management Processes Document
- VA Directive 6004 Configuration, Change, and Release Management Programs
- Software Configuration Management Plan Standard

#### Verify and Audit Configuration Items

- Change Management Repository
- Configuration Audit Requests
- Configuration Information Requests
- Configuration Management Repository
- Software Configuration Management Procedures
- OIT Change Management Processes Document
- OIT Configuration Management Process Document
- OIT Release Management Processes Document
- VA Directive 6004 Configuration, Change, and Release Management Programs
- Software Configuration Management Plan Standard

#### Generate Reports

- Change Management Repository
- Configuration Audit Requests
- Configuration Information Requests
- Configuration Management Repository
- Software Configuration Management Procedures
- OIT Change Management Processes Document
- OIT Configuration Management Process Document
- OIT Release Management Processes Document
- VA Directive 6004 Configuration, Change, and Release Management Programs
- Software Configuration Management Plan Standard

### **3.3.Process Outputs**

#### Identify Configuration Items

- Identified Configuration Items

#### Place CIs Under Configuration Mgmt Control

- Controlled Configuration Items

#### Adopt Changed Management Procedures

- Identified CIs Under Change Control

Verify and Audit Configuration Items

- Appropriate level of Audit and Verification Required

Generate Reports

- Configuration Management Audit Reports

### **3.4.Exit Criteria**

CM processes and procedures are implemented and being followed.

## **4. Related Processes**

The CM process is dependent upon the following processes:

- Asset Management process
- Change Management process
- Incident Management
- Issue Management process
- Release Management process
- Solution Build Management process

## **5. Configuration Management Process Steps**

### **5.1.Identify Configuration Items**

#### **5.1.1.Description**

The Configuration Management Analyst works with the Project Team members to identify, select, name and classify the Configuration Items (CIs) subject to Change control within Office of Information and Technology (OIT). The lowest level CI is normally the smallest unit that will be changed independently of other components. CIs may vary widely in complexity, size and type (including but not limited to hardware, software, software builds, documentation, product baselines, release packages, etc.) to a single program module or a minor hardware CI.

#### **5.1.2.Inputs**

- Acquisition Package
- All Software and System Engineering Design Documents to include: Logical and Physical Models, Systems, Components, Hardware and Software items, etc.
- Discovery Tools Data
- Project Management Plan
- Software Configuration Management Procedures
- OIT Change Management Processes Document
- OIT Configuration Management Process Document

- OIT Release Management Processes Document
- VA Directive 6004 Configuration, Change, and Release Management Programs
- Software Configuration Management Plan Standard

### **5.1.3. Responsible Persons**

- Configuration Management Manager
- Configuration Management Analyst

### **5.1.4. Activities**

- Select CI
- Classify CI
- Name CI
- Gather Data

### **5.1.5. Outputs**

- Identified Configuration Items

## **5.2. Place CIs Under Configuration Management Control**

### **5.2.1. Description**

The Configuration Management Analyst ensures that Configuration Items (CIs) are managed and controlled according to the Configuration Management process. This activity updates existing CI information as well as any additions and/or retirement of CIs. Changes to CI information must be carefully controlled so that only approved changes are updated.

### **5.2.2. Inputs**

- Acquisition Package
- All Software and System Engineering Design Documents to include: Logical and Physical Models, Systems, Components, Hardware and Software items, etc.
- Approved Change Requests
- Discovery Tools Data
- Identified Configuration Item
- Project Management Plan
- Software Configuration Management Procedures
- OIT Change Management Process Document
- OIT Configuration Management Process Document
- OIT Release Management Process Document
- VA Directive 6004 Configuration, Change, and Release Management Programs
- Software Configuration Management Plan Standard

### **5.2.3.Responsible Persons**

- Configuration Management Manager
- Configuration Management Analyst

### **5.2.4. Activities**

- Manage Configuration Items
- Control Configuration Items

### **5.2.5.Outputs**

- Controlled Configuration Items

## **5.3.Adopt Change Management Procedures**

### **5.3.1.Description**

The Configuration Management Analyst follows established change management processes for Configuration Items (CIs) under Configuration Management control.

### **5.3.2.Inputs**

- Approved Change Request
- Identified Configuration Items
- Project Management Plan
- Software Configuration Management Procedures
- OIT Change Management Process Document
- OIT Configuration Management Process Document
- OIT Release Management Process Document
- VA Directive 6004 Configuration, Change, and Release Management Programs
- Software Configuration Management Plan Standard Change

### **5.3.3.Responsible Persons**

- Configuration Management Manager
- Configuration Management Analyst

### **5.3.4.Activities**

- Documents changes to Configuration Items per Change Management Process

### **5.3.5.Outputs**

- Modified Configuration Items under Change Control



## **5.4. Verify and Audit Configuration Items**

### **5.4.1. Description**

The Configuration Management Analyst conducts an audit and verifies the current state and status of Configuration Items (CIs). The intent is to ensure the CIs match the specifications and other documentation. The audits and reviews verify that the CIs are being properly managed within the defined processes. These audits vary in complexity and formality and are performed in conjunction with the Change Management process. The Configuration Management Analyst analyzes the information requested to determine the appropriate level of audit and verification. The data gathered from the analysis is used by the Configuration Management Analyst to determine the complexity of the audit and performs the audit according to established SOP's. Changes to the process may be warranted as a result of the audit.

### **5.4.2. Inputs**

- Change Management Repository
- Configuration Audit Request
- Configuration Information Requests
- Configuration Management Repository
- Software Configuration Management Procedures
- OIT Change Management Processes Document
- OIT Configuration Management Process Document
- OIT Release Management Processes Document
- Software Configuration Management Plan Standard

### **5.4.3. Responsible Persons**

- Configuration Management Manager

### **5.4.4. Activities**

- Analyze Request for Information
- Plan Audit
- Perform Audit

### **5.4.5. Outputs**

- Appropriate level of Audit and Verification required
- CM Audit Report
- CM Corrective Request
- CM Reports
- Process Improvement

## **5.5.Generate Reports**

### **5.5.1.Description**

The Configuration Management Analyst generates reports as required by the schedule or in response to individual requests.

### **5.5.2.Inputs**

- Change Management Repository
- Configuration Audit Request
- Configuration Information Requests
- Configuration Management Repository
- Software Configuration Management Procedures
- OIT Change Management Process Document
- OIT Configuration Management Process Document
- OIT Release Management Process Document
- VA Directive 6004 Configuration, Change, and Release Management Programs
- Software Configuration Management Plan Standard

### **5.5.3.Responsible Persons**

- Configuration Management Manager
- Configuration Management Analyst

### **5.5.4.Activities**

- Generate and Communicate Reports

### **5.5.5.Outputs**

- Configuration Management Audit Reports

## **6. Configuration Management Procedures**

### **6.1.Identify Configuration Items**

#### **6.1.1.Inputs**

- Acquisition Package
- All Software and System Engineering Design Documents to include: Logical and Physical Models, Systems, Components, Hardware and Software items, etc.
- Discovery Tools Data
- Project Management Plan
- Software Configuration Management Procedures

- OIT Change Management Processes Document
- OIT Configuration Management Process Document
- OIT Release Management Processes Document
- VA Directive 6004 Configuration, Change, and Release Management Programs
- Software Configuration Management Plan Standard

### **6.1.2.Responsible Persons**

- Configuration Management Manager
- Configuration Management Analyst

### **6.1.3.Procedures**

- Select CI

Identify which items in inventory will have the greatest potential impact on daily operations and operational readiness and stability. Consideration should be given to the impact on the business line, security, population, availability, and other direct dependencies. Examples of CIs include hardware, software, applications, network devices, infrastructure, and environmental devices.

- Classify CI

Classify CIs in one or more of the following ways: Family/Category, Class, and Type. For examples, see Appendix B.

- Name CI

Follow the acknowledged VA naming convention standards for the applicable CI classification.

- Gather Data

Identify which data sources will contain the data points that have the greatest potential impact on daily operations and operational readiness and stability.

### **6.1.4.Outputs**

- Identified CIs.

## **6.2.Place CIs Under Configuration Management Control**

### **6.2.1.Inputs**

- Acquisition Package
- All Software and System Engineering Design Documents to include: Logical and Physical Models, Systems, Components, Hardware and Software items, etc.
- Approved Change Requests
- Discovery Tools Data
- Identified Configuration Item

- Project Management Plan
- Software Configuration Management Procedures
- OIT Change Management Process Document
- OIT Configuration Management Process Document
- OIT Release Management Process Document
- VA Directive 6004 Configuration, Change, and Release Management Programs
- Software Configuration Management Plan Standard

### **6.2.2. Responsible Persons**

- Configuration Management Manager
- Configuration Management Analyst

### **6.2.3. Procedures**

Adopt Change Management procedures

Place CIs under configuration management control by following the change management process.

- Identify Specific Versions of Each CI
- Create a Baseline Based on the Controlled Version of the CI.

Adopt Change Control

Place CIs under configuration management control by following the change control process.

- Follow the Change Control Board Processes and Procedures
- Follow the Issue Management Processes and Procedures
- Follow the Risk Management Processes and Procedures
- Follow the Release Management Processes and Procedures
- Follow the Configuration Control Processes and Procedures
- Follow the Change Request Processes and Procedures
- Follow the Software Configuration Management Plan Standard
- Follow the Software Configuration Process and Procedures

### **6.2.4. Outputs**

- Controlled Configuration Items

## **6.3. Adopt Change Management Procedures**

### **6.3.1. Inputs**

- Approved Change Requests
- Identified Configuration Item

- Project Management Plan
- Software Configuration Management Procedures
- OIT Change Management Process Document
- OIT Configuration Management Process Document
- OIT Release Management Process Document
- VA Directive 6004 Configuration, Change, and Release Management Programs
- Software Configuration Management Plan Standard

### **6.3.2. Responsible Persons**

- Configuration Management Manager
- Configuration Management Analyst

### **6.3.3. Procedures**

Place CIs under configuration management control by following the change management process.

- Identify Specific Versions of Each CI
- Create a Baseline Based on the Controlled Version of the CI.

Place CIs under configuration management control by following the change control process.

- Follow the Change Control Board Processes and Procedures
- Follow the Issue Management Processes and Procedures
- Follow the Risk Management Processes and Procedures
- Follow the Release Management Processes and Procedures
- Follow the Configuration Control Processes and Procedures
- Follow the Change Request Processes and Procedures
- Follow the Software Configuration Management Plan Standard
- Follow the Software Configuration Process and Procedures

### **6.3.4. Outputs**

- Modified Configuration Items under Change Control

## **6.4. Verify and Audit Configuration Items**

### **6.4.1. Inputs**

- Change Management Repository
- Configuration Audit Request
- Configuration Information Requests
- Configuration Management Repository
- Software Configuration Management Procedures
- OIT Change Management Processes Document
- OIT Configuration Management Process Document

- OIT Release Management Processes Document
- VA Directive 6004 Configuration, Change, and Release Management Programs
- Software Configuration Management Plan Standard

### **6.4.2. Responsible Persons**

- Configuration Management Manager

### **6.4.3. Procedures**

- Analyze Request for Information  
Analyze the information requested to determine the appropriate level of audit and verification needed.
- Plan Audit  
Plan the formality of the audit based on the audience.  
Use the data gathered from the analysis to determine the complexity of the audit.
- Perform Audit  
Perform the audit per the request based on the analysis and the plan.

### **6.4.4. Outputs**

- Appropriate level of Audit and Verification required

## **6.5. Generate Reports**

### **6.5.1. Inputs**

- Change Management Repository
- Configuration Audit Requests
- Configuration Information Requests
- Configuration Management Repository
- Software Configuration Management Procedures
- OIT Change Management Process Document
- OIT Configuration Management Process Document
- OIT Release Management Process Document
- VA Directive 6004 Configuration, Change, and Release Management Programs
- Software Configuration Management Plan Standard

### **6.5.2. Responsible Persons**

- Configuration Management Analyst

### **6.5.3.Procedures**

- Generate and communicate reports

Create reports as required by the schedule or in response to individual requests

### **6.5.4.Outputs**

- Configuration Management Audit Reports

## 7. Metrics

Metrics are a system of parameters or methods for quantitative and periodic assessment of a process that are to be measured. The collection and analysis of metrics provides a factual method of evaluating the quality of a process, product, or system.

For example, some typical metrics attributable to configuration management may include:

- Number of CIs in VA CM METADATA REPOSITORY
- Number of CIs by family/class category
- Number of CIs Audited
- Number of CI Errors Discovered
- Number of CI Changes
- Number of CI Changes without corresponding RFC
- Number of Incidents Related to Inaccurate CI Information
- Number of Change Failures Related to Inaccurate CI Information
- Number of CIs without Assigned Ownership
- Key Performance Indicators (KPIs)
- VA CM METADATA REPOSITORY Accuracy Ratio
- VA CM METADATA REPOSITORY Completeness Ratio
- CI Ownership Rate



## **8. Training and Tools**

When resources are in place, training plans will be developed and executed.

## 9. Appendix A – Definitions and Acronyms

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 Groups definitions:

[http://vaww.infoshare.va.gov/EPG/VAIGADP/Shared%20Documents/Finalized%20TWG%20Documents/Glossary\\_and\\_Acronyms.xls](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](http://vaww.oed.wss.va.gov/process/Library/master_glossary/masterglossary.htm)

## 10. Concurrency

<a href="#">Integrated Technical Working Group Members</a>		
Name	Title	Organization
<a href="#">Mike Leroy</a>	Enterprise Process Manager	Service Delivery and Engineering
<a href="#">Jeff Rabinowitz</a>	Enterprise Process Management	Service Delivery and Engineering
<a href="#">Mitzi Arth</a>	Manager, LRM Change and Configuration Management	Enterprise Service Engineering
<a href="#">Julie Harvey</a>	Director, Product Assessment Division	Product Development
<a href="#">Phyllis Denson</a>	Business Process Mgmt Analyst	VHA, Office of Health Information
<a href="#">Andrea Kucharski</a>	Chief, Configuration Management	National Service Desk
<a href="#">Russell McFall</a>	Lead, Change, Configuration and Release Management	Field Operations, Technology Management

## 11. Appendix B – Family and Class Examples

FAMILY	CLASS	DEFINITION
Document	Business Continuity Plan	This is a document that describes how a system will be recovered in the event of a disaster. This record will point to the location of the plan and be related to the system(s) it supports.
Document	Certification and Accreditation	This is a document that describes the necessary elements to certify a system and gain an Authority to Operate. This record will point to the location of the CA and be related to the system(s) it supports.
Document	Release Management Plan	This is a document that describes the approved methodology to release a system, updates to a system, and patches to a system, into each type of environment (test, pre-production, and production). This record will point to the location of the Release Management Plan and be related to the system(s) it supports.
Document	Configuration Management Plan	This is a document that describes how a system is initially configured, the approvers for changes to the configuration and what release management plan is used for the release of a system into each type of environment. This record will point to the location of the Configuration Management Plan and be related to the system(s) it supports.
Hardware	Mainframe	This is a physical device that is used to run programs and process data. This record will contain configuration details about the device and be related to the Software Applications running on the system, to the Documents that support its operation and to the Services that it is supporting.
Hardware	Console	This is a physical device that is used to manage a piece of hardware. The relationships for this Configuration Item will be simple but is needed in support of business continuity. This CI should be related to the hardware it supports, the business continuity plan of the hardware it supports and the Service(s) that it supports.
Hardware	Server	This is a physical configuration item that used to run software and process data. This record will contain configuration details about the device and be related to the Software Applications running on the system, to the Documents that support its operation and to the Services that it is supporting. This CI could be federated out to a discovery tool for deeper configuration details than what is managed within the CI record.
Hardware	Storage	This is a physical configuration item that used to run store data. This record will contain configuration details about the device and be related to the Software Applications running on the system, to the Documents that support its operation and to the Services that it is supporting. This CI could be federated out to a discovery tool for deeper configuration details than what is managed within the CI record.

FAMILY	CLASS	DEFINITION
Hardware	Virtual Machine	This is a logical configuration item that used to run software and process data and which is housed in a physical device. This record will contain configuration details about the device and be related to the physical device it is housed in, Software Applications running on the system, to the Documents that support its operation and to the Services that it is supporting. This CI could be federated out to a discovery tool for deeper configuration details than what is managed within the CI record.
Hardware	Router	This is a physical configuration item that routes data from one system to another. This record will contain configuration details about the device and be related to the devices it connects to, to the Documents that support its operation and to the Services that it is supporting. This CI could be federated out to a discovery tool for deeper configuration details than what is managed within the CI record.
Hardware	Firewall	This is a physical configuration item that protects systems from incoming data feed from one system to another. This record will contain configuration details about the device and be related to the devices it connects to, to the Documents that support its operation and to the Services that it is supporting. This CI could be federated out to a discovery tool for deeper configuration details than what is managed within the CI record.
Service	Internal Service	This is a grouping of configuration items that provide a service to the Department of Veterans Affairs – such as BlackBerry Services. This CI should be related to the hardware, software, documents and services it supports.
Service	Customer Service	This is a grouping of configuration items that supports the customers of the Department of Veterans Affairs – such as Health Data Repository (HDR). This CI should be related to the hardware, software, documents and services it supports.
Software	Application	This is software that is purchased by the Department of Veterans Affairs that is not a COTS Product and not fully developed by the Department of Veterans Affairs. This CI should be related to the hardware it is running on, to the Service it supports and to any Documents.
Software	COTS	This is Commercial Off The Shelf software that is licensed to the Department of Veterans Affairs. This CI should be related to the hardware it is running on, to the Service it supports and to any Documents.
Software	In-House	This is software that is developed by the Department of Veterans Affairs. This CI should be related to the hardware it is running on, to the Service it supports and to any Documents.

FAMILY	CLASS	DEFINITION
Telecom	PBX	This is a telephone system that is used to manage a grouping of phones for a logical location. This CI should be related to the Services it supports any related hardware or software and documents such as a business continuity plan in the event of a disaster.
Telecom	Modem	This is a data transport methodology that allows remote systems to connect to managed devices. This CI should be related to both the external system and the internal system, any supporting documentation and the internal service it supports.