Configuration Management Plan

*VAEC Amazon Web Services GovCloud High*

and VistA Adaptive Maintenance (VAM)



04/08/2019

Version *3.0*

Department of Veterans Affairs

*David Catanoso/VA Office of Information & Technology*

*Director, Enterprise Cloud Solutions Office*

Version History

| Date | Version | Description | Author |
| --- | --- | --- | --- |
| 5/31/2017 | 0.1 | Established initial template version with basic  content. | John Martoglio,  CSRA |
| 6/7/2017 | .2 | Included feedback from Keith, Carlos and  Ji. | John Martoglio,  CSRA |
| 6/27/2017 | 1.1 | Revised sections and content | Peter Davies,  MPG/CSRA |
| 8/28/2017 | 1.2 | Revised to match CONOPS documents | Peter Davies,  MPG/CSRA |
| 10/30/2017 | 1.3 | Various Updates | Wilbert  Francis/Daniel  Beaver,  MPG/CSRA |
| 10/30/2017 | 1.4 | Review | Peter Davies,  MPG/CSRA |
| 10/30/2018 | 1.5 | Revised content and formatting | Steven Quach  VAEC Security Team/Cognosante |
| 11/14/2018 | 2.0 | Updated and finalized for Signature | Steven Quach  VAEC Security Team/Cognosante  Organization 2 Author name - [System Acronym] |
| 4/11/2019 | 3.0 | General updates regarding orginaztion requirements | David Faulkner AbleVets Security - VAM |

Provide organization Author name and System Acronym in the document change control record table.

Entries in BLUE are instructions

Entries in RED are to be completed

Entries in BLACK are not to be changed, they are boiler plate

[Organization2] is the organization joining VAEC AZURE

All colored texts should be removed

Table of Contents

[1. Executive Summary 1](#_Toc528306960)

[2. Introduction 1](#_Toc528306961)

[2.1 Purpose of the Configuration Management Plan 1](#_Toc528306962)

[2.2 Scope of the Configuration Management Plan 1](#_Toc528306963)

[2.3 Structure of the Configuration Management Plan 2](#_Toc528306964)

[2.4 Compliance with IT Security Requirements 2](#_Toc528306965)

[2.4.1 Configuration Management Policy and Procedures 3](#_Toc528306966)

[2.4.2 Baseline Configuration 3](#_Toc528306967)

[2.4.3 Configuration Change Control 3](#_Toc528306968)

[2.4.4 Security Impact Analysis 4](#_Toc528306969)

[2.4.5 Access Restrictions for Change 4](#_Toc528306970)

[2.4.6 Configuration Settings 4](#_Toc528306971)

[2.4.7 Least Functionality 4](#_Toc528306972)

[2.4.8 Information System Component Inventory 5](#_Toc528306973)

[2.4.9 Configuration Management Plan 5](#_Toc528306974)

[2.4.10 Software Usage Restrictions 5](#_Toc528306975)

[2.4.11 User-installed Software 5](#_Toc528306976)

[3 Configuration Management Activities 17](#_Toc528306977)

[3.1 Roles and Responsibilities 17](#_Toc528306978)

[3.2 Communication 20](#_Toc528306979)

[3.3 System Configuration Baseline 20](#_Toc528306980)

[3.5 Release Management and Version Control 23](#_Toc528306981)

[3.5.1 Release Management 23](#_Toc528306982)

[3.5.1.1 Release Planning 23](#_Toc528306983)

[3.5.1.2 Security Impact Assessment 23](#_Toc528306984)

[3.5.1.3 Release Building 23](#_Toc528306985)

[3.5.1.4 Vulnerability Scanning 23](#_Toc528306986)

[3.5.1.5 User Acceptance Testing 24](#_Toc528306987)

[3.5.1.6 Release Deployment 24](#_Toc528306988)

[3.5.2 Version Control 24](#_Toc528306989)

[3.5.2.1 Versioning of Directories 24](#_Toc528306990)

[3.6 Configuration Management Resources 24](#_Toc528306991)

[APPENDIX A: CONFIGURATION MANAGEMENT PLAN APPROVAL 27](#_Toc528306992)

[Appendix B: References 29](#_Toc528306993)

[Appendix C: Key Terms 30](#_Toc528306994)

[Appendix D: Suggested Configuration Items Data Elements 32](#_Toc528306995)

[Appendix E: Current Configuration Baseline Report 37](#_Toc528306996)

[Appendix F: Change Order Approval Checklist 38](#_Toc528306997)

[Appendix G: Change Order Implementation Plan Template 39](#_Toc528306998)

[Appendix H: Business Case Justification 41](#_Toc528306999)

[Appendix I: Change Management Back-Out Plan Template 42](#_Toc528307000)

# Executive Summary

The Configuration Management Plan (CMP) is a security artifact that supports identification, control, and auditing of VA Enterprise Cloud (VAEC) and VistA Adaptive Maintenance (VAM) assets in an orderly and controlled manner. This artifact will also support the Authorizing Official with the information needed to maintain a robust continuous readiness and monitoring posture as the system moves through the lifecycle development process.

This document defines the change management process and evaluates change for potential adverse impacts. The VA Enterprise Cloud (VAEC) for Amazon Web Services (AWS) GovCloud High, hereafter known as VAEC AWS team, will determine the items to be managed, establish configuration baselines, and ensure modifications incorporate security considerations for security controls for the VAEC system in accordance with VA Continuous Readiness and Information Security Program (CRISP) Guidelines. Configuration Management (CM) is a security function within the System Development Life Cycle (SDLC) and has security implications if the baseline configurations are not managed and changes are not controlled.

The VAM – [Security Categoriztion – High] team, will determine the items to be managed, establish configuration baselines, and ensure modifications incorporate security considerations for security controls for the VAM system in accordance with VA Continuous Readiness and Information Security Program (CRISP) Guidelines. Configuration Management (CM) is a security function within the System Development Life Cycle (SDLC) and has security implications if the baseline configurations are not managed and changes are not controlled

This document is intended to be a living document. The final version will be placed under CM and the respective changes managed according to CM policies referenced.

# Introduction

## Purpose of the Configuration Management Plan

The overall objective of a CMP is to identify CM roles and responsibilities, resources, and formal processes and procedures to ensure that all proposed changes to a General Support System (GSS) / Major Application (MA) are evaluated and approved before implementation. This also includes the process used for controlling implementation, evaluation, and auditing of the CM processes and Configuration Items (CIs) to include maintaining a current baseline configuration of the system under Configuration Management Control. This CMP contains all the information pertinent to the VAEC.

## Scope of the Configuration Management Plan

The VAEC AWS GovCloud High CMP and VAM - [Security Categorization - High] document, along with the OIT CM Standard Operating Procedure (SOP), defines the Information System’s structure and methods for:

* Identifying, defining, and base-lining CIs
  + Creating CI Records
  + Identifying relationships
* Controlling modifications and releases of CIs
* Reporting and recording status of CIs and any requested modifications
* Ensuring completeness, consistency, and correctness of CIs
* Controlling storage, handling, and delivery of the CIs

## Structure of the Configuration Management Plan

The intended audience of the CMP is System Owners, Organizational Service Lines and divisions, Facility Chief Information Officers, System Administrators, Information Security Officers and Information Owners, Cloud Operations and Migration Services (COMS) staff, and Office of Information and Technology (OIT) staff within these identified areas responsible for the day-to-day maintenance of the configuration items.

This CMP, in conjunction with the Office of Information and Technology (OIT) Configuration and Change Management Process Documents, and Service, Delivery and Engineering (SDE) Change Management Policy and Standard Operating Procedures, identifies configuration management and change management roles and responsibilities and system relationships. In addition, the scope includes the automated tools and processes used to manage the information system baseline configuration.

## 2.4 Compliance with IT Security Requirements

The VAEC AWS CMP adheres to security requirements of the CM control family as prescribed in NIST SP 800-53 Rev. 4 and by the system’s FIPS 199 Security Categorization (SC) of **High**. The following table identifies the sections that contain control implementation statements that meets NIST SP 800-53 Rev. 4 CM control requirements.

**Table 2.4:** **Configuration Management Control Compliance**

|  |  |  |
| --- | --- | --- |
| **Control Number** | **Security Control Requirement** | **Section** |
| CM-1 | Configuration Management Policy and Procedures | *Section 2.4.1* |
| CM-2 | Baseline Configuration | *Section 2.4.2* |
| CM-3 | Configuration Change Control | *Section 2.4.3* |
| CM-4 | Security Impact Analysis | *Section 2.4.4* |
| CM-5 | Access Restrictions for Change | *Section 2.4.5* |
| CM-6 | Configuration Settings | *Section 2.4.6* |
| CM-7 | Least Functionality | *Section 2.4.7* |
| CM-8 | Information System Component Inventory | *Section 2.4.8* |
| CM-9 | Configuration Management Plan | *Entire Document* |
| CM-10 | Software Usage Restrictions | *Section 2.4.10* |
| CM-11 | User-installed Software | *Section 2.4.11* |

## 2.4.1 Configuration Management Policy and Procedures

**Control CM-1**

The VAEC inherits this control from OI&T. OI&T develops, documents, and disseminates policies and procedures enterprise-wide. In accordance with VA Directive and Handbook 6330, the Configuration Management Policy is reviewed every five (5) years. The VAEC develops and maintains SOPs as needed.

## 2.4.2 Baseline Configuration

**Control CM-2**

The VAEC develops, documents, and maintains configuration control, a current baseline configuration of the information system. Baseline configurations are developed and documented in the VAEC Configuration Management Plan.

* Code Baseline Configuration: GitHub Enterprise is used as the centralized repository and management of baselines.
* Servers: VA IBM BigFix is used to manage server configuration in accordance with VA CRISP Guidelines.

## 2.4.3 Configuration Change Control

**Control CM-3**

(a) The VAEC categorizes changes into two (2) categories. These are (1) changes that affect other VA information systems and (2) changes that affect the VAEC. For changes that only affect the VAEC, there are two (2) additional categories of changes:

**2.4.3.1** Changes that do not require CCB approval

* In accordance with the RACI chart, application support teams making changes to the Development and Staging environments.

**2.4.3.2** Changes that requires CCB approval

* All changes to the Production environment.
* Initial configuration of hosted application environment.
* All changes to Core Services.
* In accordance with the RACI chart, changes to hosted application environment is performed by the VAEC team.

(b) All configuration changes are documented and tracked in the Service Desk Manager (SDM) and Configuration Management Database (CMDB) (SDM and CMDB are defined in section 3.2).

(c) Based on the type of change, approval is required by the requisite CCB.

(d) In accordance with VA Handbook 6500, the VAEC will retain configuration-controlled records for five (5) years. The change request tickets are retained in the SDM and CMDB ticketing systems.

(e) All approved changes are reviewed prior to the closure of the change request ticket. IBM BigFix is used to identify and audit for unapproved changes.

(f) The VAEC coordinates and provides oversight for all configuration changes via a CCB.

## 2.4.4 Security Impact Analysis

**Control CM-4**

The VAEC utilizes a work flow change management process that includes a security review prior to approval. The security official will conduct a security impact assessment based on the probability and impact of the proposed change to the information system. This is documented in the CMP (referenced in Section 3.5.1.2).

## 2.4.5 Access Restrictions for Change

**Control CM-5**

The VAEC utilizes a work flow change management process that defines, documents, approves all proposed changes prior to implementation. Only system engineers have logical access to make changes to the operational environment. IBM BigFix is used to identify unapproved changes. The VA *ECSB Operations and Maintenance Responsibility Matrix(RACI)* documents authorized user(s) responsibilities.

## 2.4.6 Configuration Settings

**Control CM-6**

(a) The VAEC utilizes a gold image for initial baseline configurations. The baseline configuration settings are based on DISA STIGs and VA CRISP Guidelines.

* Windows Server 2012 and 2012 R2 DISA STIG – Version 2, Release 8, 28 Apr 2017
* Red Hat Enterprise Linux (RHEL) 7 DISA STIG – Version 1, Release 1, 13 Mar 2017

(b) The VAEC utilizes Ansible to deploy the gold image configuration settings.

(c) The VAEC conducts baseline configuration scans prior to a system going operational. Deviations from the gold image baseline are documented and approved prior to implementation into the operational environment.

(d) The VAEC utilizes IBM BigFix to monitor configuration settings.

## 2.4.7 Least Functionality

**Control CM-7**

(a) The VAEC operates under the principle of least functionality, where programs are executed with the minimum rights required. An RBAC methodology is used within the environment where programs are executed at the run-level of the authenticated user account.

(b) The VAEC only allows engineers to execute programs on servers in the environment that is required to complete their duties. Engineers must first login using non-privileged accounts and only escalate to privileged accounts, if needed.

## 2.4.8 Information System Component Inventory

**Control CM-8**

The VAEC maintains an online real-time inventory of system components inherited from VA Enterprise IBM BigFix and a cloud access security broker (CASB). The inventory includes network-based components and cloud services implemented. The real-time inventory list provides a level of granularity deemed necessary for tracking and reporting.

## 2.4.9 Configuration Management Plan

**Control CM-9**

The VAEC develops, documents, and implements a configuration management plan for the information system that:

(a) Addresses roles, responsibilities, and configuration management processes and procedures;

(b) Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

(c) Defines the configuration items for the information system and places the configuration items under configuration management; and

(d) Protects the configuration management plan from unauthorized disclosure and modification.

## 2.4.10 Software Usage Restrictions

**Control CM-10**

(a) The VAEC system engineers are the only personnel allowed to install software programs within the environment.

(b) The VAEC tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution.

(c) The VAEC does not utilize or permit the use of peer-to-peer file sharing technology.

## 2.4.11 User-installed Software

**Control CM-11**

The VAEC system engineers are the only personnel allowed to install software programs within the environment. System engineers are required to go through the CM approval process to install software.

Enter your organization Compliance with IT Security Requirements here.

The VAM CMP adheres to security requirements of the CM control family as prescribed in NIST SP 800-53 Rev. 4 and by the system’s FIPS 199 Security Categorization (SC) of [Security Categorization – High]. The following table identifies the sections that contain control implementation statements that meets NIST SP 800-53 Rev. 4 CM control requirements.

**Table 2.4: Configuration Management Control Compliance**

|  |  |  |
| --- | --- | --- |
| **Control Number** | **Security Control Requirement** | **Section** |
| CM- 02 | Baseline Configuration | *Section 2.4.12* |
| CM-03 | Configuration Change Control | *Section 2.4.13* |
| CM-04 | Security Impact Analysis | *Section 2.4.14* |
| CM-05 | Access Restriction for Change | *Section 2.4.15* |
| CM-06 | Configuration Settings | *Section 2.4.16* |
| CM-07 | Least Functionality | *Section 2.4.17* |
| CM-08 | Information Sytem Component Inventory | *Section 2.4.18* |

## 2.4.12 Security Control Requirement

**Control CM-02 Baseline Configuration**

VAM will develop, document, and maintain under configuration control, a current baseline configuration of the information system. Configuration management enables the organization to manage the VAM baseline. The baseline is updated when a change is implemented into Production or restored if a release in Production fails. Changes to the baseline are systematically monitored and controlled within the version control, change management, and configuration auditing functions.This control is provided VA-wide by the Service Delivery and Engineering (SDE), Enterprise Systems Engineering (ESE), Security Management Analytics (SMA); and EO Technical Security.

ESE owns the development and approval of all VA Baselines. The Baseline and Configuration Management (BCM) section within SMA was formed to serve as a liaison and one part of a governing body for the development, execution and review of configuration baselines. VA ESE-sanctioned baselines can be found here:

<https://vaww.sde.portal.va.gov/svcs/sma/BCM/SitePages/Home.aspx>

The SMA BCM section coordinates baseline requests by EO with ESE. To contact BCM, request a new baseline or request a change to an existing baseline, email BCM at vait.bcmintake@va.gov. EO information system baselines are maintained in the National Service Desk (NSD), CA Service Desk Manager (SDM) Configuration Management Database (CMDB) for all hosted systems, components, and configuration items (CI).

NSD SDM is the facilitator for baseline configuration by tracking authorized changes to EO information systems. Each Change Request (CR) details proposed changes and a back-out or recovery plan. All additions or changes to system/application baselines are maintained in CMDB under configuration and change control.

Service Desk (NSD), CA Service Desk Manager (SDM) Configuration Management Database (CMDB) for all hosted systems, components, and configuration items (CI).

NSD SDM is the facilitator for baseline configuration by tracking authorized changes to EO information systems. Each Change Request (CR) details proposed changes and a back-out or recovery plan. All additions or changes to system/application baselines are maintained in CMDB under configuration and change control.

VAM reviews and updates the baseline configuration of the information system annually and when directed by the VA; and as an integral part of information system component installations and upgrades.

ETM organization reviews and updates the baseline configuration of the information system at specified intervals; when required by defined events; and as an integral part of information system component installations. ETM has:

(i) Established and maintains baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles (SDLC); and

(ii) Established and enforces security configuration settings for information technology products employed in the information systems.

DCO utilizes a Configuration Management Database (CMDB) that serves as the system of record for all the related information including a current baseline configuration of DCO information systems and an inventory of constituent components as described in CFD Directive 6215. DCO has the ability to report on the current status and history of configuration items for ETM. The Configuration Management Team ensures all changes to configuration items are recorded and updated, accurately and timely. DCO documents and controls changes to ETM through Service Desk Manager (SDM). Officials approve changes through an automated change order workflow as described in CFD Directive 6220, Change Management.

VAM retains organization-defined previous versions older than current baseline versions to support rollback. A key part of the change management plan is to maintain previous versions of the VAM baselines in the VAM CM repository, so that the Platform may be rolled back to a previous state that has been snapped for backup.

This control is provided by Enterprise Operations (EO) and implemented by EIS personnel.

DCO retains older versions of baseline configurations as deemed necessary to support rollback. The CA Service Desk Manager (SDM) CMDB provides a list of changes in order that installation that can be reversed if rollback is necessary; records are kept for six (6) years.

ETM organization retains older versions of baseline configurations to support rollback as needed.Planned baselines, current baselines, and projected baselines for workstations, laptops, servers or COTS software are archived to separate locations and clearly identified through version control to ensure that only the most recent version is used. Older baselines are retained to allow and support a rollback if deemed necessary.

VAM:

a) Issues organization-defined information systems, system components, or devices with organization-defined configurations to individuals traveling to locations that the organization deems to be of significant risk.

b) Applies organization-defined security safeguards to the devices when the individuals return. Specially-configured mobile devices (laptops) are configured (hardened) in accordance VA policy and are provisioned with security technology to secure confidentiality, integrity, and availability.

Enterprise Operations does not issue information systems or devices to individuals traveling to locations with significant risk.

## 2.4.13 Configuration Change Control

**Control CM-03**

VAM:

(a)Determines the types of changes to the information system that are configuration-controlled.

(b)Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes, with explicit consideration for security impact analyses.

(c)Documents configuration change decisions associated with the information system.

(d)Implements approved configuration-controlled changes to the information system.

(e)Retains records of configuration-controlled changes to the information system for 12 months.

(f)Audits and reviews activities associated with configuration-controlled changes to the information system.

(g)Coordinates and provides oversight for configuration change control activities through the change control board (CCB) that will convene at determine designated time to review proposed changes.

This control is provided by SDE Enterprise Operations and implemented by DCO personnel.

EO:

a) Has determined the types of changes to information systems that are configuration controlled and escalates changes with VA-wide impact to the National Change Control Board (NCCB) according to predetermined escalation criteria;

b) Approves configuration-controlled changes to the system with explicit consideration for security impact analyses;

c) Documents approved configuration-controlled changes to systems using CA SDM and the CMDB;

d) Retains and reviews records of configuration-controlled changes to systems at the National Service Desk (NSD);

e) Audits activities associated with configuration-controlled changes to systems as a assigned task in the CO; and

f) Coordinates and provides oversight for configuration change control activities through the EO Operations Meeting that convenes weekly; or in response to an outage or security incident.

EO CCB:

VA Directive 6004 Configuration, Change, and Release Management Programs specifies that all computing system changes require an approved Change Request (CR) before the change is implemented; these changes are requested electronically via National Service Desk (NSD) CA Service Desk Manager (SDM) which maintains a record of all change requests. The CCB ensures that all CRs are documented, reviewed, and analyzed with explicit consideration for security impact analyses before the CO is closed. NSD SDM is the facilitator for configuration change control by tracking authorized changes to EO information systems. Changes are documented and tracked through SDM. Each CR details proposed changes and a back-out or recovery plan.Certain incident-related change control procedures are escalated to the VA-NSOC Change Control Request (CCR) process, particularly if NSOC services are impacted or required.

VAM:

a)Tests changes to the information system before implementing the changes on the operational system.

b)Validates changes to the information system before implementing the changes on the operational system.

c)Documents changes to the information system before implementing the changes on the operational system.

This control is provided by SDE Enterprise Operations and implemented by DCO personnel.

EO tests, validates and documents changes to the information system before implementing the changes on the operational system. Service Desk Manager (SDM) is a ticketing system maintaining configuration control of changes to a DCO information system.

Service Desk Manager (SDM) incorporates specific planning and coordination workflows to ensure that operational impact is reduced whenever any change, including security-related activities, occurs. These workflows enforce notification and approval procedures to effectively implement organizational planning and coordination.

Included in this process are a development and pre-production environment for testing prior to production implementation. All software upgrades and patches are applied to development and test environments and checked for effect prior to installation in the production environment. Changes to the information system are tracked and documented through SDM prior to implementing the changes. Development and pre-production environments exist for testing prior to production implementation. All hardware/software changes, upgrades and patches are applied first to these environments and checked for effect prior to installation in production.

http://vaww.nsd.va.gov/CAisd/pdmweb.exe"

This process is documented in AITC 6220 Directive on Change Management, and the accompanying 6220.01 Handbook on Change Management, which covers both emergency and routine situations.

## 2.4.14 Secuirty Impact Analysis

**Control CM-04**

VAM analyzes changes to the information system to determine potential security impacts prior to change implementation.

The VAM ISSO’s job is to assess security impacts of change requests that are presented to the CCB, where a description of the security impacts of the change is articulated by the security analyst. Any testing of the change and validation of those tests are presented during that time. The actual testing steps will depend on the scope of the change and devices/configurations impacted.

For significant changes, the VAM ISSO will perform additional testing, including scanning for vulnerabilities, documenting any findings, and identifying the mitigation steps prior to the change being implemented.

This control is provided by SDE Enterprise Operations and implemented by DCO personnel.

EO follows the CM process for all configuration management changes. Within the process, configuration changes are thoroughly monitored and documented. EO monitors changes to the information system and conducts assessments and analyses to determine the effects of changes that affect system performance, and user access. All change requests are recorded using CA SDM. The change control process requires conducting an impact analyses to determine the effect of proposed changes on existing security controls and infrastructure. This analysis is completed prior to implementing the change into production. The change control process requires conducting a security impact analyses to determine the effect of a proposed change(s) on the existing information system, security controls and infrastructure. The results of the impact analysis, done by EO for all potential changes, are included in the CR for all involved and interested parties to review prior to the disposition of the change request.

VAM defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

VAM maintains physical and logical access restrictions that have been established during changes to the information system. No change request will be considered that does not maintain the foundational access restrictions established by the VAM policy and ISSO oversight.

This control is provided by SDE Enterprise Operations and implemented by DCO personnel.

EO approves, and authorizes individual access privileges both at the system level and data level and enforces physical logical access controls. IT SMs/SAs are responsible for the monitoring of access restrictions. The change control process requires the CR to include the name of the individual(s) that will be tasked with implementing the change if approved. Before the CR has been closed the individual(s) that implemented the change is verified. Only authorized and documented individuals have been granted the rights and permissions to implement changes within the production environment. Access privileges to the information system for the implementation of changes are enforced through Active Directory. Individuals are given physical and logical access privileges when they are hired or may have these privileges changed when job responsibilities dictate. Access restrictions for system changes/upgrades are limited to program developers.

Data Center Operations (DCO) organization:

a) Approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and

b) Generates, retains, and reviews records reflecting all such changes.

In QRadar, the automated mechanism software employed by the DCO, provides utilization of centralized monitoring and provides automated review and alerting of system activity across the enterprise. QRadar securely collects, stores, reports and alerts on event data from Windows, Unix & Linux systems to by auditing access to critical VA systems and detecting inappropriate or suspicious access-related events.

DCO collects, analyzes, reports, and generates automated real-time alerts for all relevant access-related events across the network. The QRadar Log Manager scheduled collection of logs runs every 24 hrs.

Access to ETM assets is documented on VA Form 9957. No access is allowed unless it is properly documented. Only VA employees are allowed administrative privileges on the servers. Policy and procedures regarding Information System Configuration Security Management are formally documented in the following documents:

1) VA 6500 Handbook; and

2) DCO Handbook 6500.15, Information System Configuration Security Management, March 2012

In accordance with Directive 6500, access to DCO-managed general support system (including ETM) and other system resources are granted only to specifically identified and authorized personnel who have a demonstrated work-related requirement for such access on a "need to know" basis. Security audits are performed on a regular basis by DCO Security Services staff. These audits include monitoring for access to accounts that have the necessary privileges to perform configuration changes on the information system.

VAM:

a) Limits privileges to change information system components and system-related information within a production or operational environment.

b) Reviews and re-evaluates privileges at least quarterly.

The ISSO and VAM security team reviews and re-evaluates information system integrator privileges quarterly, according to the Continuous Monitoring activities.

## 2.4.15 Access Restriction for Change

**Control CM-05**

VAM defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

VAM maintains physical and logical access restrictions that have been established during changes to the information system. No change request will be considered that does not maintain the foundational access restrictions established by the VAM policy and ISSO oversight.

This control is provided by SDE Enterprise Operations and implemented by DCO personnel.

EO approves, and authorizes individual access privileges both at the system level and data level and enforces physical logical access controls. IT SMs/SAs are responsible for the monitoring of access restrictions. The change control process requires the CR to include the name of the individual(s) that will be tasked with implementing the change if approved. Before the CR has been closed the individual(s) that implemented the change is verified. Only authorized and documented individuals have been granted the rights and permissions to implement changes within the production environment. Access privileges to the information system for the implementation of changes are enforced through Active Directory. Individuals are given physical and logical access privileges when they are hired or may have these privileges changed when job responsibilities dictate. Access restrictions for system changes/upgrades are limited to program developers.

Data Center Operations (DCO) organization:

a) Approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and

b) Generates, retains, and reviews records reflecting all such changes.

In QRadar, the automated mechanism software employed by the DCO, provides utilization of centralized monitoring and provides automated review and alerting of system activity across the enterprise. QRadar securely collects, stores, reports and alerts on event data from Windows, Unix & Linux systems to by auditing access to critical VA systems and detecting inappropriate or suspicious access-related events.

DCO collects, analyzes, reports, and generates automated real-time alerts for all relevant access-related events across the network. The QRadar Log Manager scheduled collection of logs runs every 24 hrs.

Access to ETM assets is documented on VA Form 9957. No access is allowed unless it is properly documented. Only VA employees are allowed administrative privileges on the servers. Policy and procedures regarding Information System Configuration Security Management are formally documented in the following documents:

1) VA 6500 Handbook; and

2) DCO Handbook 6500.15, Information System Configuration Security Management, March 2012

In accordance with Directive 6500, access to DCO-managed general support system (including ETM) and other system resources are granted only to specifically identified and authorized personnel who have a demonstrated work-related requirement for such access on a "need to know" basis. Security audits are performed on a regular basis by DCO Security Services staff. These audits include monitoring for access to accounts that have the necessary privileges to perform configuration changes on the information system.

VAM:

a) Limits privileges to change information system components and system-related information within a production or operational environment.

b) Reviews and re-evaluates privileges at least quarterly.

The ISSO and VAM security team reviews and re-evaluates information system integrator privileges quarterly, according to the Continuous Monitoring activities.

## 2.4.16 Configuration Settings

**Control CM-06**

VAM:

Establishes and documents configuration settings for information technology products employed within the information system using requirements and guidance that reflect the most restrictive mode consistent with operational requirements.

This control is provided by VA Enterprise Systems Engineering (ESE) and Enterprise Operations (EO); and implemented by EIS personnel.

EO-hosted information systems maintain the most current configuration and guides which are available to administrators. OIS Technical Security Package and Development Guidelines document the policies and procedures for developing and implementing installation packages within the DCO environment. Configuration Items are defined as each individual piece of hardware and software under the control of an information system. These baseline configurations and configuration settings (along with changes required for individual mission objectives) are recorded and stored within Change Control Records. Monitoring of configuration settings are done via CA Configuration Automation Agent (CCA) and IBM Tivoli Endpoint Manager (TEM/BigFix). If exceptions are required from the mandatory configuration settings, the requesting entity must follow the CCB process to get this exception(s) approved.

VA:OIT/SDE/ESE owns the development and approval of all VA Baselines. The Baseline and Configuration Management (BCM) section within Security Management & Analytics (SMA) was formed to serve as a liaison, and one part of a governing body, for the development, execution and review of all configuration baselines. All VA ESE-sanctioned baselines can be found here. Software standards documents can be found here. The SMA office's BCM section will triage and coordinate baseline requests on your behalf with ESE. To contact BCM, request a new baseline, request a change to an existing baseline, or have a question about VA baselines, email BCM at vait.bcmintake@va.gov

VA Configuration Management Policy specifies that all security settings be predefined and follow ESE Baselines, OIS recommended settings, system specific settings, and NIST required settings. All configuration settings are documented in OIS Technical Security Configuration Guides.

EO-managed information systems utilize the standard baselines, configuring the security settings to the most restrictive mode possible, consistent with operational requirements. CA SDM tracks changes to configuration settings in accordance with change control guidelines. Changes are documented in CMDB

## 2.4.17 Security Control Requirement

**Control CM-07 Least Functionality**VAM:

1. Configures the information system to provide only essential capabilities.

VAM’s approach is to take a white list approach and only enables those services and network ports that are required to operate the system. During initial component configuration (baseline configuration), System Administrators and Network Engineers turn off all unnecessary services.

1. Prohibits or restricts the use of the following functions, ports, protocols, and/or services United States Government Configuration Baseline (USGCB).

VAM configures the system according to industry best practices in order to provide only essential capabilities and specifically prohibits or restricts the use of the following functions: all ports, protocols, and/or services that are not explicitly required.

EO information systems are configured to provide essential capabilities and prohibit or restrict the use of services/applications that are deemed a high security risk. Configuration Build Documents implement Least-functionality.  Services and applications are allowed on an individual basis and only as required.  Approval to use non-essential services must go through the change control process. Feasibility studies and testing are conducted on high risk applications or services that may affect the performance or place sensitive data at risk.  SDE ESE and EO Technical Security establish standard baselines for devices which enforce least functionality.

Technical Security documents the configuration settings, utilizing standard build documents and Configuration Guides that implement best-practice. These configuration settings provide only essential capabilities and specifically prohibit and/or restrict the use of specific functions, ports, protocols, and/or services as defined by DCO organizational policy. The functions and services provided by ETM information system are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing, etc.)

VA-NSOC and EO Technical Security utilize Host-based Intrusion Prevention System (HIPS), which combines intrusion detection technology with a host-based firewall.  The baseline Real Secure Desktop policy will place the firewall in "cautious" mode, which blocks unsolicited inbound traffic to well-known ports except the following:  
 TCP/113 ident TCP/135 endpoint mapped TCP/139 NETBIOS session service TCP/445 NETBIOS-less SMB UDP/137 NETBIOS name service UDP/138 NETBIOS datagram service "

TCP/113 indent  
TCP/135 endpoint mapped  
TCP/139 NETBIOS session service  
TCP/445 NETBIOS-less SMB  
UDP/137 NETBIOS name service  
UDP/138 NETBIOS datagram service  
UDP/500 SIAM  
TCP/498 SIAM   
TCP/500 ISAKMP

System Administrators within DCO follow VA established configuration guidelines for their operating systems, databases, and applications. These configuration guidelines are posted on the Information Assurance Portal and provide guidance to use only essential capabilities and specifically prohibit and/or restricts the use of the following functions, ports, protocols, and/or services. These guidelines are specific to systems, servers, and workstations

## 2.4.18 Information Sytem Component Inventory Control CM-08 Information Secuity Component

VAM:

(a) Develops, and documents an inventory of information system components that:

(1) Accurately reflects the current information system;

(2) Includes all components within the authorization boundary of the information system;

(3) Is at the level of granularity deemed necessary for tracking and reporting; and

(4) Includes organization-defined information deemed necessary to achieve effective information system component accountability; and

(5) Reviews and updates the information system component inventory monthly.

This control is provided by SDE Enterprise Operations and implemented by DCO personnel.

EO System managers are responsible for documenting and maintaining a list of components installed or configured on Windows systems. The system inventory is updated as components are purchased and received as part of AEMS/MERS. The AEMS/MERS inventory accurately reflects the current information system components list and has been integrated with CMDB which can also receive updates from the CCA agent and Tivoli Endpoint Manager (TEM/BigFix) installed on EO Information Systems. Inventory for each application is reviewed by the system owner annually or whenever there is a significant change. The inventory of components includes any information determined to be necessary to achieve effective property accountability; and at the level of granularity deemed necessary for tracking and reporting.

VAM updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

VAM updates the inventory of information system components as an integral part of component installations, removals, and information system updates as part of the change management process.

ETM organization ensures:

a hardware, and firmware inventory has been developed and is being maintained;

The inventory includes the manufacturer, type, serial number, version number, location, and components required for contingency operations; and

Specific responsibilities and actions are defined for the implementation of the system component inventory control.

VAM:

(a) Employs automated mechanisms continuously, using automated mechanisms with a maximum five-minute delay in detection to detect the presence of unauthorized hardware, software, and firmware components within the information system.

(b) Takes the following actions when unauthorized components are detected (one or more): disables network access by such components; isolates the components; notifies security analysts.

This control is provided by SDE Enterprise Operations and implemented by DCO personnel.

EO:

a) Employs automated mechanisms quarterly to detect the addition of unauthorized components/devices into the information system. The detection of unauthorized network components is performed by two organizationally separated work centers; and

1. On a quarterly basis, The EO Technical Security work center uses Tenable Nessus in "Discovery" mode to detect any unauthorized components in the network; and

2. The Configuration Management (CM) work center uses the SolarWinds Orion networks discovery program and the VEEAM VMware reporting tool to search for unauthorized components;

b) Upon discovery of an unauthorized component two steps are immediately taken:

1. All open ports on the component are disabled;

2. A NSD SDM Change Order (CO) is opened.

The component is analyzed off line to determine the components"" characteristics. The CM work center and the appropriate technical work center, i.e. Windows/UNIX, etc., are assigned the CO to ensure a fully populated Configuration Item (CI) record entry is added to the CMDB.

NOTE: Due to the detailed procedures outlined in CM-8(2)1 this issue rarely, to never, has occurred on the DCO's Production Network.

c) Additionally, the CM work center regularly audits the CMDB against Discovery tool reports.

VAM verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.

All components defined in the VAM architecture are inventoried as a part of the system definition and monitored by VAM.

An annual inventory (both physical and virtual) is conducted. That inventory is then reconciled against what is in the repository. Any discrepancies are researched and validated with the appropriate team(s). Resulting changes are then made to the repository.

This control is provided by SDE Enterprise Operations and implemented by DCO personnel.

EO ensures that an inventory containing hardware, software and firmware has been developed and is being maintained through the CMDB; and verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system. CMDB contains the manufacturer, type, serial number, version number, location, and components for contingency operations; specific responsibilities and actions are defined for the implementation of the system component inventory control. The verification that all system components are properly accounted for, secured and managed within Assessment & Authorization (A&A) boundaries is accomplished by VA Security Analysts operate in EO Systems Security, Information Assurance (IA) group. Each information system is assigned an analyst. To ensure compliance, the responsible analyst monitors all system components. IA Analysts are on the distribution lists for all CO which affect system components. If a system component is added or changed, it is the analyst's responsibility to make the appropriate modifications to relevant security artifacts.

# Configuration Management Activities

## 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.

Roles and responsibilities for the CCM programs as they pertain to the VAEC AWS are

found in the following SOPs:

* [OIT Configuration Management Process Document](https://vaww.sde.portal.va.gov/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/oit_configuration_management_process_document.pdf)
* [OIT Change Management Process Document](https://vaww.sde.portal.va.gov/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/oit_change_management_process_document.pdf)
* [SDE Field Operations Configuration Management Plan](https://vaww.sde.portal.va.gov/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/National%20Configuration%20Management%20Plan.doc)
* [SDE Change Management SOP](https://vaww.sde.portal.va.gov/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/National%20ChM%20Process%20SOP.pdf)

The following table includes defined roles and responsibilities of an organization in support of the CM process. The VAEC uses a Configuration Control Board (CCB) to manage change and includes an information technology expert as a key voting member of the board. The VAEC CM process defines the roles and responsibilities within the system lifecycle.

Table 3.1: Roles and Responsibilities

| Role | Responsibility | Name |
| --- | --- | --- |
| Configuration Control Board Chairperson | Responsible for chairing the configuration control board and ensuring the change has been reviewed and analyzed based on the requirements described in the charter | Cheryl Owsley |
| System Security Representative | Responsible for ensuring that the change has been reviewed and analyzed for impact to security | David Faulkner |
| Enterprise Architecture Representative | Responsible for ensuring that the change has been reviewed and analyzed for impact to the standards and guidelines in the enterprise architecture | Conor Dowling |
| Software Configuration Manager | Responsible for tracking software components, and building and promoting software releases | Conor Dowling |
| System Engineer | Responsible for tracking and maintenance of system components | Conor Dowling |
| Security Operations (SecOps) | Responsible for:   * Developing new security configuration baselines * Reviewing and discussing proposed submitted change(s) * Evaluating the impact of the change(s) to the existing security configuration baseline (both before and after testing should that occur) * Approving/Denying change(s) * Determining implementation approach * GitHub to ensure compliance | David Faulkner |
| Operations  (DevOps) | * Reviewing and discussing proposed submitted change(s) * Evaluating the impact of the change(s) to the existing * security configuration baseline (both before and after testing * should that occur) * Approving/Denying change(s) * Determining implementation approach * Implementing change (if approved) | Conor Dowling |

## 

## Enter your orgamization Roles and Responsibilities here.

Enter your orgamization Roles and Responsibilities in the table below.

Table 3.1: Roles and Responsibilities - VAM

| Role | Responsibility | Name |
| --- | --- | --- |
| System Owner | Signature Authority and Review | Christopher Brown |
| Information Security Officer | Signature Athority and Review | Bobbi Begay |
| Program Manager | Signature Athority and Review | Cheryl Owsley |
| Security | General Review and implementing Security-related details | David Faulkner |
| Development/Arch Lead | Implementation of configuration details | Conor Dowling |
|  |  |  |
|  |  |  |

Table 3.2: CCB Board Members

| Name | Title | Role |
| --- | --- | --- |
|  |  | CCB Chairman |
|  |  | CCB Voting Member |
|  |  | CCB Voting Member |
|  |  | CCB Non-Voting Member |

## Enter your orgamization CCB Board Members below

CCB Board Members VAM

| Name | Title | Role |
| --- | --- | --- |
|  |  | CCB Chairman |
|  |  | CCB Voting Member |
|  |  | CCB Voting Member |
|  |  | CCB Non-Voting Member |

Table 3.3: Change Review Team Members

| Name | Title | Role |
| --- | --- | --- |
|  |  | Code Reviewer |
|  |  | Vulnerability Scan Reviewer |
|  |  | Information Security Officer (ISO) |

## Enter your orgamization change review team Members in the table below

Table 3.3: Change Review Team Members [Organization 2 name/acronym]

| Name | Title | Role |
| --- | --- | --- |
|  |  | Code Reviewer |
|  |  | Vulnerability Scan Reviewer |
| Bobbi Begay | Information Security Officer (ISO) | Information Security Officer (ISO) |

## Communication

Requests for Change (RFC)/Change Orders are entered into the appropriate Change Management

System (VA) for review, approval, and implementation by the appropriate Servicing Divisions.

Change Control and Advisory Board reviews are required for changes that impose downtime for

the system or service or pose a risk or affect multiple facilities or services.  It is the responsibility

of the implementation team to notify potentially affected customers and personnel required to

provide support, e.g.,Organizational Servicing Divisions, Network Chief Information Officer

(NCIO), Facility Chief Information Officer (FCIO), etc.

The VAEC utilizes the Service Desk Manager (SDM) and Configuration Management Database

(CMDB) systems to document, approve and track all changes related to the system infrastructure

and/or applications. The SDM and CMDB provides a workflow that follows the VAEC process.

The VAEC team coordinates and provides oversight for configuration change control activities

through SDM and CMDB.

Enter your organization communication here.

## System Configuration Baseline

The system infrastructure is deployed to Amazon Web Services (AWS), which is

connected through VA’s Trusted Internet Connection (TIC) and VA National Security

Operations Center (NSOC) for security compliance.  The VAEC team and the IO Cloud

Architect team define and manage the baseline for the GSS.  All changes to the baseline are

documented, communicated and reviewed.  The baseline follows NIST 800-53 Rev 4 guidance and VA 6500 Handbook and policy for the creation, maintenance and sustainment of secure information systems. The system does not currently store PHI or PII at this time. Server configuration items (CI) are implemented in accordance with VA CRISP Guidelines for Windows and Linux based operating systems (OS). These configuration baselines are documented in Section 2.4.6.

## Enter your organization System Configuration Baseline here.

**3.4 Configuration Control Process (CCP)**

The VAEC has established processes and procedures that dictate the configuration change

control for all software configuration items.  The SDM and CMDB tools are used for requesting,

approving, implementing, monitoring, and tracking, auditing and closing change orders affecting

configuration items under change and configuration control.  The phases associated witht the

CCP are listed below with their accompanying process steps:

* **Phase 1: Initiate Change**

***Step 1: Establish System Configuration Baselines***

The VAEC utilizes a gold image based on the VA CRISP Guidelines for server

configuration baselines. The baseline configuration is developed and deployed using

Ansible Tower. Code baseline configurations are managed using GitHub.

* **Phase 2: Analyze/Plan Change**

***Step 2: Identify changes and complete Change Request***

Change request tickets are documented and tracked in the SDM and CMDB. Change

requests that affect VA Enterprise Services, such as network and Active Directory (AD),

requires the creation of a separate ticket for approval by the VA Enterprise Services

Change Control Board (ESCCB).

***Step 3: Submit Change Request***

Change requests are submitted using SDM and CMDB. Change requests must contain

the following items:

* Date
* Name of Requester
* Implementation Date
* Type of Change
* Environment(s) Affected (e.g. Development, Stage, Production: AWS)
* Description of Change
* Implementation Details/Instructions
* Rollback procedures
* Test Results (e.g., UAT)
* Code Review Results (if applicable)
* Vulnerability Scan Results (if applicable)

***Step 4: Evaluate Change Request***

The following review/evaluation activities occur:

* **Code:** Peer review and static code scans
* **Application:** Dynamic application scans
* **Servers:** Host-based vulnerability scans

***Step 5: Perform Security and Operational Impact Analysis***

The Change Review Team reviews proposed change requests and make recommendations to the CCB. The impact assessments (security and operational) will be conducted taking into consideration the probability of a negative effect of the change and impact to the system.

* **Phase 3: Approve Change**

***Step 6: Approve, Disapprove, Defer, or Refer Change Request***

All change requests are routed to the appropriate CCB.

* **Code:** VAEC CCB
* **Network: VA ESCCB1**
* **AD:** VA ESCCB
* **All other:** VAEC CCB
* **Phase 4: Fix/Develop Change**

***Step 7: Schedule Approved Change***

Configuration changes to the information system are approved through a general consensus by the CCB. The CCB consists of a chairperson and voting representatives as specified in Table 3.1. The chairperson makes the determining decision if a consensus cannot be reached. Changes to the VAEC environment are restricted to individuals who are authorized by the CCB.

***Step 8: Release Approved Change***

The VAEC release management process leverages the VA SDLC process to manage, plan, schedule and control software builds through different stages of the deployment process. Code release management and version control steps are identified in Section 3.5

* **Phase 5: Implement Change**

***Step 9: Implement Approved Change***

* Approved change requests are implemented after obtaining COMS and VA CCB management approval.
* **Code deployment:** hosted applications are deployed using GitHub.
* **Core Service changes:** are implemented by the VAEC team.
* **Phase 6: Validate Change**

***Step 10: Verify Implemented changes are successful and did not introduce additional issues/incidents into the environment.***

Changes are tested and validated after the change being implemented. Changes for hosted applications are verified by the Application Owner.

***Step 11: Perform Configuration Status Accounting***

The VA SDM and CMDB ticketing systems automatically records the changes and configuration change status. Records of configuration-controlled changes (requested, approved, disapproved, implemented and pending) are retained for at least one (1) year.

***Step 12: Conduct Configuration Verification and Audit***

Auditing of the VAEC configuration is conducted by the VAEC security team as part of continuous monitoring efforts. Additionally, VAEC personnel receive alerts for some changes to the environment. These may include:

* Infrastructure changes, such as starting and stopping of instances and cloud services
* Changes to key files and folders

## This is inherited through VAEC

## 3.5 Release Management and Version Control

The VAEC release management process seeks to manage, plan, schedule and control software

build through different stages from testing to deploying software releases. GitHub Enterprise is

used for source code repository and versioning. GitHub Enterprise provides code collaboration

and a secure code repository for hosted applications source code.

## 3.5.1 Release Management

## 3.5.1.1 Release Planning

Procedures for packaging and releasing software code are documented in the planning phase.

## 3.5.1.2 Security Impact Assessment

Throughout the SDLC, the ISO conducts security impact assessments (SIA). The phases include

requirement definitions and code release. During code release planning, the ISO will provide the

SIA.

## 3.5.1.3 Release Building

Code is packaged for release in this phase. The package is then deployed to the test/stage

environment for scanning and testing.

## 3.5.1.4 Vulnerability Scanning

In this phase, a scan is conducted to identify vulnerabilities. Identified vulnerabilities will be

remediated prior to release.

## 3.5.1.5 User Acceptance Testing

Application testing is conducted by end users. Feedback is then incorporated and necessary

changes are made prior to release.

## 3.5.1.6 Release Deployment

The release deployment step installs the software release in the production environment. Testing

is conducted subsequently to validate installation.

## 3.5.2 Version Control

## 3.5.2.1 Versioning of Directories

GitHub Enterprise versions directories as first-class objects.

* ***Copying, deleting, and renaming****–* Copying, deleting, and renaming are versioned

operations.

* ***Free-form versioned metadata ("properties***") – GitHub allows arbitrary metadata

("properties") to be attached to any file or directory. These properties are key/value pairs, and are versioned just like the objects they are attached to.

* ***Atomic commits*** – No part of a commit takes effect until the entire commit has

succeeded. Revision numbers are per-commit, not per-file, and commit's log message is

attached to its revision, not stored redundantly in all the files affected by that commit.

* ***Merge tracking*** – Provides automated assistance with managing the flow of changes between lines of development and with the merging of branches back into their sources.

## *This is inherited through VAEC*

## 3.6 Configuration Management Resources

The following tools ensure that appropriate control is in place to manage the configuration items in accordance with VA Handbook 6500 Configuration Management controls.

**GitHub Enterprise**

GitHub Enterprise will be used as a centralized distributed version control system/repository that securely stores application code and configuration items, as well as audit history. The VAEC will retain three (3) versions of code baseline configuration: Legacy, Pre-Production, and Production.

**Ansible Tower**

A scripting framework for deploying configuration item changes. The VAEC will utilize a gold image for initial baseline configuration. The gold image baseline configuration settings will be based on DISA STIGs and VA Continuous Readiness in Information Security Program (CRISP) Guidelines. Ansible Tower will be used to develop and deploy the VAEC gold image configuration and other server configuration.

Ansible playbooks are stored in GitHub. It also provides an enterprise framework for controlling, securing and managing the Ansible automation with a UI and RESTful API.

**AWS Cloud Formation**

AWS CloudFormation is a service that helps organizations model and set up their Amazon Web Services resources so that less time is spent managing resources. A CloudFormation template is simply a JSON (JavaScript Object Notation) or YAML-formatted text file that describes the AWS infrastructure needed to run an application or service along with any interconnection between them. Organizations create a template that describes all the AWS resources that they require and CloudFormation takes care of provisioning, dependencies and configuration of the resources.

**AWS OpsWorks**

AWS OpsWorks is a configuration management service that uses Chef, an automation platform that treats server configurations as code. OpsWorks uses Chef to automate how servers are configured, deployed, and managed across your Amazon Elastic Compute Cloud (Amazon EC2) instances or on-premises compute environments. AWS OpsWorks is an automation tool that gives the user workflow automation for continuous deployment, automated testing for compliance and security. OpsWorks gives the user full stack automation by handling operational tasks such as software and operating system configurations, package installations, database setups, and more.

**IBM BigFix**

IBM BigFix will be used to centrally manage, apply, monitor, and verify server configuration settings in accordance with VA CRISP Guidelines. It is an endpoint security and management platform that provides real-time visibility and control across endpoints, however they are connected. The VAEC will employ IBM BigFix to automatically maintain an up-to-date, complete, accurate, and readily available server baseline configuration. The VAEC retains three (3) versions of server baseline configurations: Legacy, Pre-Production, and Production. IBM BigFix is also employed to identify and audit for unauthorized configuration changes to operational systems. An alert will be sent to system engineers/administrators from BigFix if an unauthorized change occurs. The VA OI&T SDE and NSOC will employ automated mechanisms (SCCM, BigFix, etc.) to continuously detect the presence of unauthorized hardware, software, and firmware components within the information system (as a series of dashboards). The VAEC will maintain an online real-time inventory of system components utilizing IBM BigFix and a CASB. The inventory includes network-based components and cloud services implemented. The real-time inventory list provides a level of granularity deemed necessary for tracking and reporting.

**Tenable Nessus**

The Tenable Nessus scanner will be used to provide vulnerability management detection and auditing of assets within VAEC.

**BigFix SCCD**

BigFix SCCD scans will be used to identify policy-violating configurations (STIGS).

**McAfee VSE**

McAfee VSE active and full system scans will used to detect malware and potential attackers attempting to compromise the VAEC.

**Hewlett Packard Enterprise (HPE) Fortify**

Fortify Static Code Analyzer (SCA) identifies security vulnerabilities in source code early in the software development lifecycle (SDLC) and provides best practices so developers can code more securely. The HPE Fortify SCA is used by development groups and security professionals to analyze the source code of an application for security issues. The SCA identifies root causes of software security vulnerabilities, and delivers accurate, risk-ranked results with line-of-code remediation guidance, making it easy to address serious issues first.

**IBM Security AppScan Enterprise**

The IBM Security AppScan enables organizations to miti\\\gate application security risk, strengthen application security program management initiatives and achieve regulatory compliance. Security and development teams can collaborate, establish policies and scale testing throughout the application lifecycle. Enterprise dashboards classify and prioritize application assets based on business impact and identify high-risk areas, allowing to maximize remediation efforts. Performance metrics are provided that help monitor the progress of application security programs.

The IBM Security AppScan Enterprise delivers:

* **Scalable application security testing** using a variety of testing techniques.
* **Test policies, scan templates and vulnerability remediation advisories** to help implement application security programs.
* **Detailed security reports and enterprise level dashboards** to provide visibility of risk and compliance.

APPENDIX A: CONFIGURATION MANAGEMENT PLAN APPROVAL

The undersigned acknowledge that they have reviewed the ***VAEC AWS GovCloud High* Configuration Management Plan** and agree with the information presented within this document. Changes to this **Configuration Management Plan** will be coordinated with, and approved by, the undersigned, or their designated representatives.

**SIGNATURE IN FILE AT ECSO**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: Date:

Print Name: Christopher Brown

Title: Director, Enterprise Cloud Solutions Office

Role: System Owner

**SIGNATURE IN FILE AT ECSO**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature:

Print Name: Bobbi Begay Date:

Title: Information Security Officer

Role: ISO

The undersigned acknowledge that they have reviewed theVAM [Security Categorization - High] **Configuration Management Plan** and agree with the information presented within this document. Changes to this **Configuration Management Plan** will be coordinated with, and approved by, the undersigned, or their designated representatives.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: Date:

Print Name: Cheryl Owsley

Title: Program Manager

Role: Program Manager

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature:

Print Name: Date:

Title:

Role:

Appendix B: References

The following table summarizes the documents referenced in this document.

| Document Name | Description | Location |
| --- | --- | --- |
| VA Directive 6500 | Managing Information Security Risk: VA Information Security Program | <http://www.va.gov/vapubs/landing2_relatedlinks.cfm> |
| VA Handbook 6500 | Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program | <http://www.va.gov/vapubs/landing2_relatedlinks.cfm> |
| OIT Configuration Management Process | OIT Configuration Management ProPath defined process and supporting document | [https://vaww.sde.portal.va.gov/](https://vaww.sde.portal.va.gov/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/oit_configuration_management_process_document.pdf)  [sites/fo/committees/ccb/CMDB/](https://vaww.sde.portal.va.gov/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/oit_configuration_management_process_document.pdf)  [Definitive%20Document%20Storage/](https://vaww.sde.portal.va.gov/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/oit_configuration_management_process_document.pdf)  [oit\_configuration\_management\_process](https://vaww.sde.portal.va.gov/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/oit_configuration_management_process_document.pdf)\_document.pdf |
| OIT Change Management Process Document | OIT Change Management ProPath defined process and supporting document | [https://vaww.sde.portal.va.gov/](https://vaww.sde.portal.va.gov/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/oit_configuration_management_process_document.pdf)  [sites/fo/committees/ccb/CMDB/](https://vaww.sde.portal.va.gov/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/oit_configuration_management_process_document.pdf)  [Definitive%20Document%20Storage/](https://vaww.sde.portal.va.gov/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/oit_configuration_management_process_document.pdf)  [oit\_change\_management\_process\_document.pdf](https://vaww.sde.portal.va.gov/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/oit_configuration_management_process_document.pdf) |
| SDE Change Management SOP | SDE Change Management Standard Operation Procedure | [https://vaww.sde.portal.va.gov/](https://vaww.sde.portal.va.gov/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/oit_configuration_management_process_document.pdf)  [sites/fo/committees/ccb/CMDB/](https://vaww.sde.portal.va.gov/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/oit_configuration_management_process_document.pdf)  [Definitive%20Document%20Storage/](https://vaww.sde.portal.va.gov/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/oit_configuration_management_process_document.pdf)  [National%20ChM%20Process%20SOP.pdf](https://vaww.sde.portal.va.gov/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/oit_configuration_management_process_document.pdf) |
| Master Test Plan | Master Test Plan Template | <http://vaww.oed.wss.va.gov/process/Library/master_test_plan_template.docx> |

Appendix C: Key Terms

The following table provides definitions and explanations for terms and acronyms relevant to the content presented within this document.

Enter additional key terms used in the table below.

| Term | Definition |
| --- | --- |
| [Insert Term] | <Provide definition of term and acronyms used in this document.> |
| ACL | Access Control List |
| AO | Authorizing Official |
| CAB | Change Advisory Board |
| CCP | Configuration Control Process |
| CI | Configuration Item |
| CM | Configuration Management |
| ChM | Change Management |
| CMDB | Configuration Management Database |
| CMP | Configuration Management Plan |
| CMS | Change Management System |
| COR | Contracting Officer Representative |
| CP | Contingency Plan |
| CTO | Chief Technology Officer |
| DRP | Disaster Recovery Plan |
| ESE | Enterprise System Engineering |
| FCIO | Facility, Chief Information Officer |
| FDCC | Federal Desktop Core Configuration |
| GPO | Group Policy Object |
| GRC | RiskVision Tool |
| GSS | General Support System |
| ISCPA | Information System Contingency Plan Assessment |
| IT | Information Technology |
| OIT | Office of Information & Technology |
| LAN | Local Area Network |
| MA | Major Application |
| MDIA | Medical Device Isolation Architecture |
| NCIO | Network, Chief Information Officer |
| RCCB | Region Change Control Board |
| RFC | Request for Change |
| SCCM | System Center Configuration Manager |
| SDE | Service Delivery and Engineering |
| SLM | Service Line Manager |
| SOP | Standard Operating Procedure |
| SSP | System Security Plan |
| TRM | Technical Reference Model |
| VA | Veterans Affairs |
| VISN | Veterans Integrated Service Network |
| WAN | Wide Area Network |
| WLAN | Wireless Local Area Network |

Appendix D: Suggested Configuration Items Data Elements

Suggested standard data elements (Data Type and CI Type) and what type of data would be collected and how it would be used.

| Field Name | Data Type | CI Type | Description |
| --- | --- | --- | --- |
| Resource Name | *Indexed Text* | *Hardware / Software / Service / Document* | A unique name of the Configuration Item (CI). A name that represents the Resource and is easy to identify what it is; a key search field within the Configuration Management Database (CMDB). |
| DNS Name | *Indexed Text* | *Hardware* | The name of the CI as identified within your Domain Name Service (DNS); this helps with association of services or servers to a CI. |
| Status | *Lookup Table* | *Hardware / Software / Service / Document* | The current status of the CI. For example: when first added to the CMDB, the CI may be in a status of Registered, then later it may be Accepted. This identifies how the record moves through the status/lifecycle; if a change is being performed on the CI the status would be changed to Change in Progress, thus identifying CI’s that are currently undergoing some form of a change. |
| Description | *Free Text Multiple Lines* | *Hardware / Software / Service / Document* | A short description that will provide additional feedback to the end user when looking up the CI. |
| CI Type | *Lookup Table* | *Hardware / Software / Service / Document* | This is the type that the CI belongs to. See list of suggested family types. |
| Asset Class | *Lookup Table* | *Hardware / Software / Service / Document* | This is the classification of the configuration item; it is related to the family, but is a more specific classification of an asset. This is the sub-type that the CI belongs to; it is used to group common types on configuration items. An example would be “Laptop”; the “Laptop” Class is within the hardware Type. |
| Comments | *Free Text Multiple Lines* | *Hardware / Software / Service / Document* | Comments regarding the specific CI; notes that need to be part of the record history but are not within the Description of the CI. |
| COR | *Contact Table Lookup* | *Hardware / Software / Service* | Contracting Officer Representative (COR) associated with this particular purchase or CI. |
| Customer Name | *Contact Table Lookup* | *Hardware / Software / Service / Document* | Name of the Customer point of contact for issues with the CI. This person or group is the primary focus point when issues or changes are related to the CI. |
| Customer Organization | *Lookup Table* | *Hardware / Software / Service / Document* | Name of the Organization that the customer belongs to. Provides reporting information about what CI’s are associated to a specific organization. |
| Deployed Date | *Date* | *Hardware / Software / Service / Document* | The date that a service, system, etc. was deployed to the production environment. |
| Financial Reference | *Free Text* | *Hardware / Software* | A Purchase Order that was used to obtain the hardware or software. It is useful when looking up other information that may be found in related databases like the Asset Management system. |
| Function | *Lookup Table* | *Hardware* | The function or purpose that the hardware Configuration Item serves. |
| Host Name | *Free Text* | *Hardware* | In some cases, like UNIX, there is a purpose to identify the host name; this is on the same as DNS Name. |
| License Count | *Numeric* | *Software* | A number of copies that a particular license allows the owner to distribute. It can be used to determine if additional software licenses are needed or if there are too many licenses unused. |
| Type of Licenses | Lookup Table | Software | The type of license that has been procured, perpetual or recurring. |
| License Key Maintained By | *Contact table Lookup* | *Software* | Who maintains the Software License Key that is used to install the software? |
| Lifecycle Date | *Date* | *Hardware / Software / Service* | This is a date in the future derived from the install date and IT equipment life expectancy. |
| Location | *Lookup Table* | *Hardware / Software / Service / Document* | The location where this particular CI is hosted or installed. More specific location fields may be needed, such as room, floor, and rack as part of the physical location. |
| Maintenance Organization | *Lookup Table* | *Hardware / Software / Service* | Name of the Organization that has Maintenance responsibility over the CI; normally found within the Operations and Maintenance (O&M) Plan. |
| Maintenance Vendor | *Lookup Table* | *Hardware / Software / Service* | The vendor that would support the Maintenance Organization with a Warranty or other type of maintenance agreement. |
| Manufacturer | *Lookup Table* | *Hardware / Software* | Manufacturer of the CI being entered into the CMDB. Name used for reporting maintenance contracts or other data related to a specific manufacturer. |
| Model | *Lookup Table* | *Hardware / Software* | The manufacturer’s model name for the device. Relates to the manufacturer; used for reporting and for maintenance contracts. |
| Version Number | *Free Text* | *Software / Document* | Version Number of software or documents. This provides a baseline as to what version of software is installed/authorized in production or the version of a document that was approved and published. No version changes unless there is a change process for it. |
| Maintenance Window | *Free Text* | *Hardware / Software / Service* | Maintenance windows are established based on Service Level Agreements (SLA’s) or other agreements for specific services that are available to the end user. The Maintenance windows that are associated with the CI’s should clearly state if they are recurring maintenance windows, the days of the week that they are available, and the hours of the day that they can be used. Example: Recurring - Monday – Friday 7 to 11 PM Contact *(name or role of the person that should be contacted to validate/verify the maintenance window).* |
| Operating System | *Look Up Table* | *Hardware / Software* | Identifies the Operating System (OS) running on the server, virtual machine, laptops or workstations. It is used for patching, SA assignment, reporting purposes, licensing, etc. NOTE: If this information is available from other tools that can report this information and is not needed as part of internal reporting or linked to other fields that are not part of the external data source, then this field could be left out. |
| Published Date | *Date* | *Document* | The date that a document was published for general consumption. |
| Region | *Lookup Table* | *Hardware / Software / Service / Document* | OIT is broken out into different regional areas. Most have their own processes and procedures or have equipment and software that is regionalized. If the CMDB holds cross-regional CI’s these should be identified for reporting purposes; otherwise, the Organizational field should provide the needed feedback. |
| Relationships | *Lookup Table* | *Hardware / Software / Service / Document* | Field is a one-to-many relationship used to identify a relationship between 2 or more CI’s and the type of relationship that the CI has. This relationship could be with contacts, other hardware, software, services or document CI’s. An example of types of relationships are listed below:  Changes Approved By  Connects To  Is Documented By  Runs/Runs On |
| Renewal Date | *Date* | *Hardware / Software* | A renewal date is used to establish when a particular CI’s maintenance agreement will expire and would require renewal to continue with the service. |
| Cost of Maintenance Agreement | *Numbers* | *Hardware / Software* | Recurring cost of maintenance agreements purchased under the contract. |
| Responsible Organization | *Lookup Table* | *Hardware / Software / Service / Document* | The Organization that has responsibility over the CI. It may be the same as maintenance or customer organization or a different one. |
| Responsible Owner | *Contact Lookup Table* | *Hardware / Software / Service / Document* | A primary point of contact who has been identified as the POC for the Responsible Organization. |
| Responsible Vendor | *Lookup Table* | *Hardware / Software* | The Responsible Vendor for a particular CI may be the same as Maintenance Vendor or may be a different vendor if maintenance is sub-contracted out by the Primary Responsible Vendor. |
| Secondary Contact | *Contact Lookup Table* | *Hardware / Software / Service / Document* | This would be an alternate Point of Contact that could be contacted in the absence of the Primary POC, |
| Serial Number | *Alpha-Numeric Free Text* | *Hardware* | Serial Numbers are unique identification elements that are directly related to asset management; but by including it within your CMDB you could link to other databases that track their CI’s by Serial Number. |
| Service Line | *Lookup Table* | *Hardware / Software / Service / Document* | Support is broken down by Service Lines within OIT Field Operations, providing a Service Line associated to the CI would expedite maintenance issues and provide reporting capabilities on the type and number of CI’s being maintained by a particular service line. |
| Service Line Team/Division | *Lookup Table* | *Hardware / Software / Service / Document* | As Service Lines are stood up, so are the Service Line Teams/Divisions that support the service line and have a more defined scope of their responsibilities. Capturing this type of information would provide you with the same information as Service Line would but allow you to break it down by the Service Line Team Division. |
| Source Supplier | *Lookup Table* | *Hardware* | Used for hardware support, this is the vendor that purchased the equipment from the manufacturer. It is received obtained from the Purchase Order Contract. |
| Created By | *System Contact Field* | *Hardware / Software / Service / Document* | This is an audit field; it captures the name of the person that created the record. This should be a system field and captured based on who was logged in during the creation of the record. |
| Created Date | *System Date Field* | *Hardware / Software / Service / Document* | Initial date of creation of the Configuration Item Record. |
| Modified By | *System Contact Field* | *Hardware / Software / Service / Document* | This is an audit field; the person who last edited the record would be listed. This should be a system field and captured based on who was logged in during the modification. |
| Modified Date | *System Date Field* | *Hardware / Software / Service / Document* | Date the Configuration Item Record was last modified. |

Appendix E: Current Configuration Baseline Report

The following table details the Software and Services associated with the system(s) under this CMP.

|  |  |  |
| --- | --- | --- |
| # | **Core Services** | **Tools/Software** |
| 1 | Server Configuration Management Service | Ansible Tower, SCCM, IBM BigFix, and Nessus |
| 2 | Code Configuration and Release Management Services | GitHub |
| 3 | Authentication Services | VA AD Service, AWS IAM, and CA-SiteMinder |
| 4 | Auditing Service | Splunk, AWS CloudWatch, AWS CloudTrail |
| 5 | Monitoring Service | Splunk, Nessus, AWS CloudWatch |
| 6 | Vulnerability Scanning Service | WASA Services (App Detective, Tenable Security Center, HP Fortify), Nessus, and McAfee VSE |
| 7 | JumpBox Service | Linux and Windows servers |

Enter details of Software and Services associated with the system(s) under this CMP.

VAM

|  |  |  |
| --- | --- | --- |
| # | **Core Services** | **Tools/Software** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |
| 6 |  |  |
| 7 |  |  |

Appendix F: Change Order Approval Checklist

Reviewer and Approver must be different (the person putting together the plan, and the person approving the plan)

Correct location entered?

Change Order description contains required information

What is being done?

The business case for doing it.

What is the impact of the change (what services will be impacted and what will the impact most likely be)?

What else may be impacted?

What will occur if we don’t do the change?

The implementation plan should be attached, never be pasted, into the description.

Were the customers/stakeholders notified as per the Change Advisory Board (CAB) process?

CAB notification in the ticket.

Facility OIT response or ignore entered as a log comment.

Is the implementation plan attached?

Is the Notification and Escalation section complete?

Does the implementation plan provide sufficient detail so that a peer who is unfamiliar with the particular facility where the implementation is taking place could execute the plan?

Does the implementation plan include a test plan that contains checkpoints for verification, coordination, or implementing back-out?

Are verification steps (Test Plan) included?

Do the verification steps ensure the customers are functioning and not just the item modified is working?

Is the back-out plan attached?

Is the notification plan included?

Are verification steps included?

Do the verification steps ensure the customers are functioning, the services impacted are operational, and not just the item modified is working?

Is the need by date realistic?

Is there an implementation date/time prior to the need by date?

**If everything is accurate and all documentation attached, change Status to Approved and/or escalate to next level CCB if this is a significant change/downtime required.**



Appendix G: Change Order Implementation Plan Template

Local facility Notification and Escalation Contacts

|  |  |  |
| --- | --- | --- |
| Name/Role | Business | After-hours |
| John Doe, FCIO | 333-345-6789 | 333-987-6543 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

VISN/Service Line Notification and Escalation Contacts

|  |  |  |
| --- | --- | --- |
| Name/Role | Business | After-hours |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Any pre-implementation work that will be required

Enter required pre-implementation work here

Step-by-step guidance for what needs to be done including time estimates, escalation and coordination points

Enter step-by-step guidance here

Identification of areas that might cause problems

*Enter Identification of areas that might cause problems here*

Identification of roll-back points and/or criteria for initiating the Back-out plan

Enter Identification of roll-back points and/or criteria for initiating the Back-out plan here

Test/validation steps for the verification phase – include validation that customers are functioning and not just the item modified (See Master Test Plan Template)

Enter Test/validation steps for the verification phase



Appendix H: Business Case Justification

1. Please provide a detailed description of this change.
2. List the requirements needed for the change (i.e., servers, switches, software, etc.).
3. Describe the effect the change may have upon the end user, business operation, and infrastructure, if known.
4. Describe the impact on and the availability to other services that run on the same infrastructure (or on software development projects).
5. Describe the effect of not implementing the change.
6. Estimate the IT, business, and other resources required to implement the change, including the likely costs, the number and availability of people required, the elapsed time, and any new infrastructure elements required.
7. Estimate any additional ongoing resources required if the change is implemented.
8. Document downtime procedures.

Document communication procedures (i.e., who needs to be notified in the event of scheduled/unscheduled downtime and how to notify this person).



Appendix I: Change Management Back-Out Plan Template

| Change Order | Affected Systems |
| --- | --- |
|  |  |

Estimated time-frames for restoring service

Enter estimates here

Any pre-implementation work that will be required

Enter pre-implementation work here

Step-by-step guidance to restore service to the pre-change state

Enter step-by-step guidance here

