VA Enterprise Design Patterns:
4. IT Service Management (ITSM)
4.3: Configuration Management

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

Version 0.7
Date Issued: September 2015

Draft

THIS PAGE INTENTIONALLY LEFT BLANK FOR PRINTING PURPOSES

Draft

APPROVAL COORDINATION

TIMOTHY L MCGRAIL 111224

Digitally signed by TIMOTHY L MCGRAIL 111224
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=tim.mcgrail@va.gov, cn=TIMOTHY L MCGRAIL 111224
Date: 2015.11.16 09:24:55 -05'00'

Date:

Tim McGrail
Senior Program Analyst
ASD Technology Strategies

PAUL A. TIBBITS 116858

Digitally signed by PAUL A. TIBBITS 116858
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=paul.tibbits@va.gov, cn=PAUL A. TIBBITS 116858
Reason: I am approving this document.
Date: 2015.12.03 13:00:46 -05'00'

Date:

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

REVISION HISTORY

Version	Date	Organization	Notes
0.1	May 2015	ASD TS	Initial Draft
0.5	July 2015	ASD TS	Second draft document with updates made throughout document based upon initial internal/external stakeholder review and comment.
0.7	September 2015	ASD TS	Third and final draft for stakeholder review prior to TS leadership approval/signature. Updates made following Public Forum collaborative feedback and working session.
1.0		ASD TS	Final version for TS leadership approval and signature, including all applicable updates addressing stakeholder feedback and Section 508 Compliance.

REVISION HISTORY APPROVALS

Version	Date	Approver	Role
0.1	May 2015	Jackie Meadows-Stokes	ITSM Design Pattern Lead
0.5	July 2015	Jackie Meadows-Stokes	ITSM Design Pattern Lead
0.7	September 2015	Jackie Meadows-Stokes	ITSM Design Pattern Lead
1.0			

Draft

TABLE OF CONTENTS

1 INTRODUCTION 1

1.1 Business Need 1

1.2 Approach 1

2 CURRENT CAPABILITIES AND LIMITATIONS 2

2.1 Inconsistent Baseline Configuration 2

2.2 Under-utilized Scanning and Discovery Tools 2

2.3 Multiple Configuration Management Databases 2

3 FUTURE CAPABILITIES 2

3.1 Enterprise-level Configuration Management Methodology 3

3.2 Standard Secure Baseline Configurations 4

3.3 Standard Automated Scanning and Discovery 5

3.4 Federated CMS 6

3.5 Alignment to the TRM 7

4 USE CASES 8

4.1 Drift Analysis of Veterans Immunizations Data Systems 8

4.2 Monitoring Prohibited Software Titles 9

APPENDIX A. DOCUMENT SCOPE 11

Scope 11

Document Development and Maintenance 11

APPENDIX B. DEFINITIONS 12

APPENDIX C. ACRONYMS 16

APPENDIX D. REFERENCES, STANDARDS, AND POLICIES 18

Draft

FIGURES

Figure 1: ITSM Configuration Management Phases per NIST SP 800-128 3
Figure 2: "To-be" Enterprise CMS Concept 6
Figure 3: Configuration Drift Analysis Use Case 9
Figure 4: Monitoring Prohibited Software Titles Use Case 10

TABLES

Table 1 – Representative VA Enterprise CM Tools 7

Draft

1 INTRODUCTION

A robust IT infrastructure that spans across numerous hosting environments requires a consistent approach to managing all of its service assets and configuration items (CI) to support VA's diverse business functions. This infrastructure requires a common set of IT service management (ITSM) tools and processes to ensure flexibility to changing business needs and to adhere to VA security policies. This document is part of a series of Enterprise Design Patterns that addresses specific ITSM capabilities that support VA's transition to enterprise services. The following sections establish a framework for enterprise-wide Configuration Management (CM) capabilities and addresses the following challenges::

- ITSM CM capabilities are not fully utilized and are dispersed geographically.
- Lack of standardized processes for IT service asset and CM.
- An enterprise-level Configuration Management System (CMS) has not been identified.
- Ownership and resources to manage an enterprise CMS have not been identified.

1.1 Business Need

Recent VA Office of the Inspector General (OIG), Federal Information Security Management Act (FISMA) and Federal Identity, Credential, and Access Management (FICAM) identified "material weaknesses" stemming from a fragmented approach to IT asset management. These assets include all of the configuration items (CI) that make up IT services. A consistent approach and toolset for managing these CIs ensures that the entire infrastructure satisfies functional and non-functional requirements, which includes all Service Level Agreements (SLAs). As a result, all infrastructure hosting environments have unified control over potential vulnerabilities and unexpected configuration changes that inhibit VA's ability to meet customer expectations.

1.2 Approach

VA's near-term approach involves the following activities:

- Establishment of a standard CM methodology (ongoing)
- Evaluation of current CM toolset (ongoing)
- Selection of an enterprise-wide CM toolset (planned)
- National implementation of standard CM methodology and toolset (planned)

Deploying an enterprise-wide CM capability enables one logical view of all CIs and supports evaluation of all IT assets against the Technical Reference Model (TRM), as described in Section 3. All hosting environments use the same CM toolset, leverage the TRM, and follow the same methodology.

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

2 CURRENT CAPABILITIES AND LIMITATIONS

2.1 Inconsistent Baseline Configuration

The lack of a standard CM methodology poses risks to maintaining consistent configuration baselines that align to VA security policies. A 2013 FISMA audit revealed that VA had varying levels of compliance with United States Governance Configuration Baseline standards. It found that numerous network devices were not configured to a common security configuration standard. This has led to security vulnerabilities resulting from default network services, excessive permissions, weak administrator passwords, and outdated versions of network operating systems.

2.2 Underutilized Scanning and Discovery Tools

VA has invested in NESSUS, IBM Endpoint Manager, and Microsoft SCCM licenses that are not being fully utilized. These capabilities have not been fully implemented despite their ability to measure exposure, fix vulnerabilities automatically, validate security compliance, and generate alerts and reports for vulnerabilities.

IBM End Point Manager (IEM) scans the entire VA enterprise on a monthly basis. A semi-automated process has been implemented that takes results from IEM and other VA-owned tools. The results are normalized, reviewed, and assessed for false positives before an actionable list of items for further investigation is returned to field personnel.

Microsoft System Center Configuration Manager (SCCM) 2007 and 2012 are used to "push" patches to assets within the Microsoft platform. BMC Atrium Discovery and Dependency Mapping (ADDM) has been deployed at Enterprise Operations (EO) data centers and is primarily used to identify EO assets. ADDM has the ability to normalize data against a product catalog that is updated twice annually.

2.3 Multiple Configuration Management Databases

Different VA organizations use different CMS products, including disparate CM databases (CMDB) that cover different portions of VA's Configuration Items (CIs). VA does not have a complete list of the technical capabilities it requires from a CMDB system. As a result, OI&T cannot ensure that it possesses the optimal tool set to provide all needed capabilities without duplication or gaps.

3 FUTURE CAPABILITIES

A consistent Configuration Management (CM) approach throughout VA integrates with an overall ITSM enterprise framework and adheres to the following constraining principles:

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

- Enterprise-level CM methodology
- Standard secure baseline configurations
- Standard automated scanning and discovery tools
- Federated, enterprise-wide CMS tool

The following subsections provide guidance and additional resources for each principle.

3.1 Enterprise-level Configuration Management Methodology

The enterprise-wide CM approach aligns to the CM process already published in ProPath and aligned to NIST SP 800-128, as described in Appendix D. The following figure shows the high-level CM process based on NIST guidance.

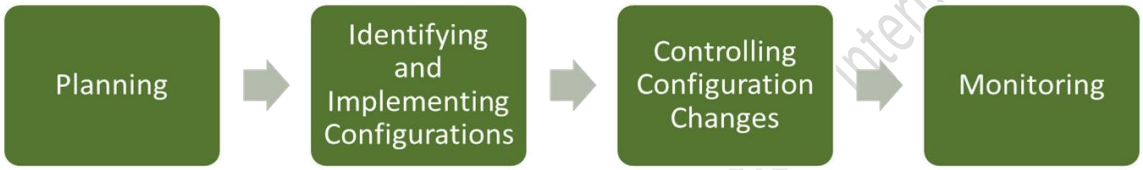

Figure 1: ITSM Configuration Management Phases per NIST SP 800-128

Implementation considerations for enterprise CM based on the four stages are listed below.

- Planning CM will:
  - Define how the types of assets and CIs are to be selected, grouped, classified, and defined by appropriate characteristics to ensure that they are manageable and traceable throughout their lifecycle.
  - Define the approach to identification, uniquely naming and labeling all the assets or service components of interest across the service lifecycle and the relationships between them.
  - Define the roles and responsibilities of the owner or custodian for configuration item type at each stage of its lifecycle (e.g., the service owner for a service package or release at each stage of the service lifecycle).
- An enterprise secure baseline will address configuration settings, software loads, patch levels, documentation, how information is physically or logically arranged, and how various security controls are implemented. Automation will enable tool interoperability and baseline configuration uniformity across the information system
- Changes to CIs are approved by the Change Advisory Board (CAB) (as documented in the Change Management Design Pattern) prior to their implementation except for routine changes. Access restrictions will be established, including:
  - Access controls
  - Process automation

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

    - Abstract layers
    - Change windows
    - Verification and audit activities to limit unauthorized and/or undocumented changes to the information systems
- Enterprise monitoring activities will validate that the information system adheres to organizational policies, procedures, and the approved secure baseline configuration. Monitoring identifies undiscovered/undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes that can expose organizations to increased risks.

3.2 Standard Secure Baseline Configurations

Enterprise Systems Engineering (ESE) manages all VA configuration baselines managed by the CMS described in Section 3.4. The Baseline and Configuration Management (BCM) section with Security Management and Analytics (SMA) was formed to serve as a liaison and one part of a governing body to develop, execute, and review all baselines. The SMA office's BCM section will triage and coordinate baseline requests on the user's behalf with ESE as well as create and submit action items for baseline updates.

Prioritization factors for implementing secure configurations in CIs include:

- System impact level – Implementing secure configurations in information systems with a high or moderate security impact level have priority over information systems with a low security impact level
- Risk assessments – Characterize information systems, IT products, or CIs with the most impact on security and organizational risk
- Vulnerability scanning – Characterize information systems, IT products, or CIs that are most vulnerable
- Degree of penetration – Represents the extent to which the same product is deployed within an information technology environment

<u>Test Configuration</u>

Configurations will be fully tested in a production environment to mitigate software compatibility and hardware device driver issues. Virtual environments will be used for testing secure configurations to determine functional impact on applications without having to configure actual machines. The test environment cannot be connected to the production environment to prevent unforeseen impacts to production or patient services. An isolated testing environment, clearly defined test parameters, specialized support hardware, knowledgeable staff, and appropriate change control processes will be put in place.

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

Resolve Issues and Document Deviations

Testing secure configuration implementations may introduce functional problems within the system or applications. These problems are examined individually and resolved or documented as a deviation from, or exception to, the established common secure configurations. When conflicts between applications and secure configurations cannot be resolved, deviations are documented and approved.

Implement Secure Configuration

After adequate testing has been performed and issues have been resolved, VA will be able to deploy new secure configurations.

Record and Approve the Baseline Configuration

The established and tested secure configuration represents the preliminary baseline configuration. This configuration is recorded to support:

- Configuration change control/security impact analysis
- Incident resolution
- Problem-solving
- Monitoring activities

Once recorded, the preliminary baseline configuration is approved by the CAB in accordance with organizationally-defined policy. Once approved, the preliminary baseline configuration becomes the initial baseline configuration for the information system and its constituent CIs. When a new baseline configuration is established, the implication is that all of the changes from the last baseline have been approved. Older versions of approved baseline configurations are maintained and made available for review or rollback as needed. The CAB manages prior versions of the baseline configurations in the enterprise CMS.

3.3 Standard Automated Scanning and Discovery

A fully automated scanning system that uses current implementations of discovery tools captures information across the entire enterprise. Endpoint discovery tools scan the entire enterprise and discover information on all endpoints. Captured information from the endpoint discovery tool goes to the data normalization toolset. This toolset includes server discovery that is capable of scanning the enterprise and discovering all server information across the enterprise. Automation tools are required to:

- Pull information from a variety of sources (e.g., different type of components, different operating systems, different platforms)
- Use open standards including XML and the Secure Content Automation Protocol (SCAP)
- Automatically detect and remediate changes from configuration or security baselines

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

- Include vendor-provided support (e.g., patches, updated vulnerability signatures)
- Allow for data consolidation into Security Information and Event Management (SIEM) tools and dashboard products
- Perform regular audit scans to demonstrate compliance with security policies

3.4 Federated CMS

A federated CMS integrates multiple autonomous database systems (CMDBs) into a single logical database, as shown in Figure 2. It creates a single federated environment where data stays in authoritative repositories that can be seamlessly accessed from external sources. Multiple Management Data Repositories (MDRs) are mapped to the CMS to improve communication between different repositories.

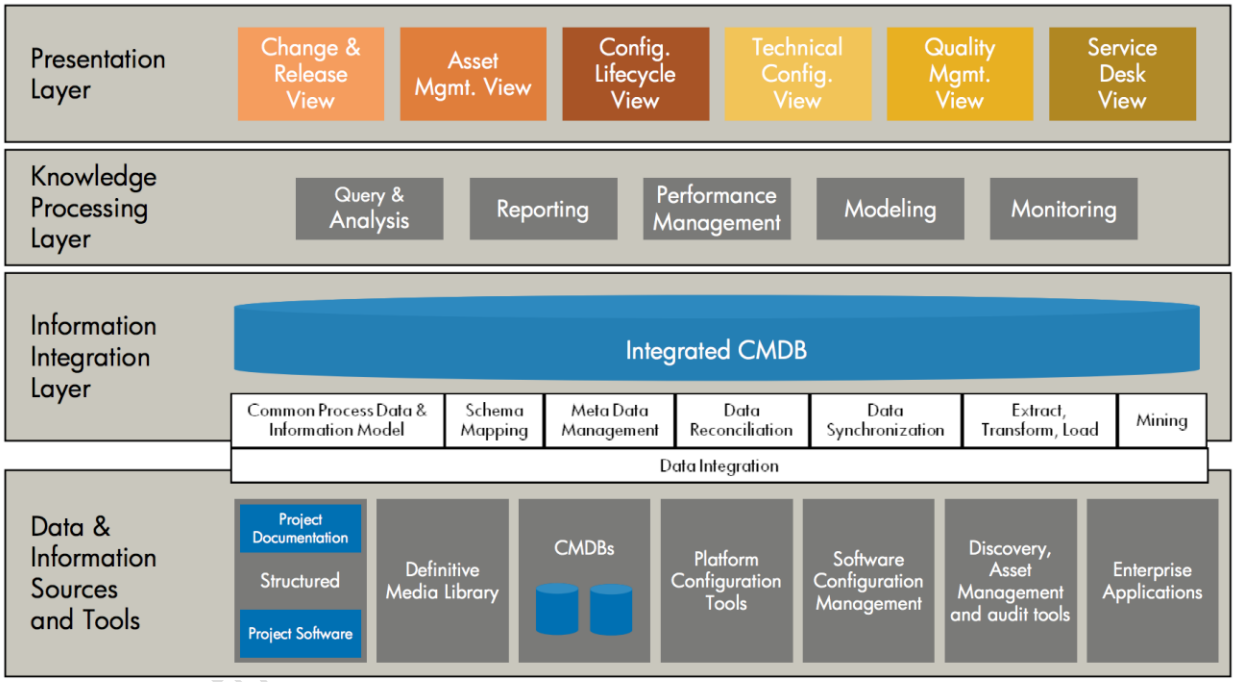

Figure 2: "To-be" Enterprise CMS Concept

The CMS houses reconciled and normalized data from federated CMDBs, and supports standard product catalog. The CMDB integrates with auto-discovery solutions and provides drift detection and analysis capabilities to ensure that the configuration remains compliant with internal policies and regulations. The CMS includes a configuration test environment in a centrally managed environment for testing IT products, tools, and proposed changes prior to being released into production. This testing environment evaluates:

- IT products proposed for approval and use within the organization

- Configuration settings for approved IT products
- Patches issued by suppliers prior to their rollout through the organization
- Validation of tools that detect unapproved configuration settings
- Verification of testing processes to validate approved configuration settings
- Security impact analyses

CMS drift management capabilities support verification and audit activities. Audits will ensure that the CMS is up to date and that the correct and approved CIs are in place. Drift management will perform audits and verification on a regular audit schedule.. Configuration audits take place:

- Shortly after implementation of a new CMS
- Before and after major changes to the IT infrastructure
- Before a software release or installation
- At random intervals
- At regular intervals
- When all is back to normal after a disaster recovery
- When any unauthorized CIs are detected

3.5 Alignment to the TRM

The enterprise CM toolset is bound by the approved products located in the TRM. The TRM will be updated to reflect the tool selection that meets the capability attributes in the previous sections. Future updates of this document will reflect the results of the tool selection effort. The following table references some of the CM tools approved for use in VA.

Table 1: Representative VA Enterprise CM Tools

Tool Category	Current Approved Technologies
Configuration Management Database (CMDB)	CA Service Desk Manager, BMC Remedy, Legacy CMDBs
Endpoint Manager	IEM, Microsoft SCCM
Relationship and Dependency Mapping	BMC ADDM, CA Configuration Automation
Configuration Change Control	CA Configuration Automation
Data Normalization	BMC ADDM, CA IT Asset Manager
Scanning and Discovery	Nessus, IEM, Microsoft SCCM, CA Configuration Automation

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

4 USE CASES

4.1 Drift Analysis of Veterans Immunizations Data Systems

The Veterans Health Information Systems and Technology Architecture (VistA) Immunization Enhancements (VIMM) project exposes immunization data through an application programming interface (API) that is accessible by internal clinician staff and external partner organizations (e.g., Walgreens). Enterprise CM methodologies and CMS support control of back-end IT infrastructure CIs that constitute the service. The service provides functionality to consumers per a Service Level Agreement (SLA), and significant configuration drift could cause a degradation of service and failure to meet the SLA. A high-level process flow for this use case (as shown in Figure 3) is as follows:

- Step 1: The CMS maintains information about the CIs and their "correct state" or target baseline in the IT infrastructure, and takes a snapshot of the CI baseline.
- Step 2: Discovery tools identify the status of the actual CI baseline in the IT infrastructure.
- Step 3: The CMS completes a "comparison job" to check against the target baseline.
- Step 4: The CMS determines the amount of drift that CIs made from the target state.
- Step 5: The CMS displays a drift report, and actions are taken to rectify the drift through incident management activities. No action is taken if the drift is insignificant.

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

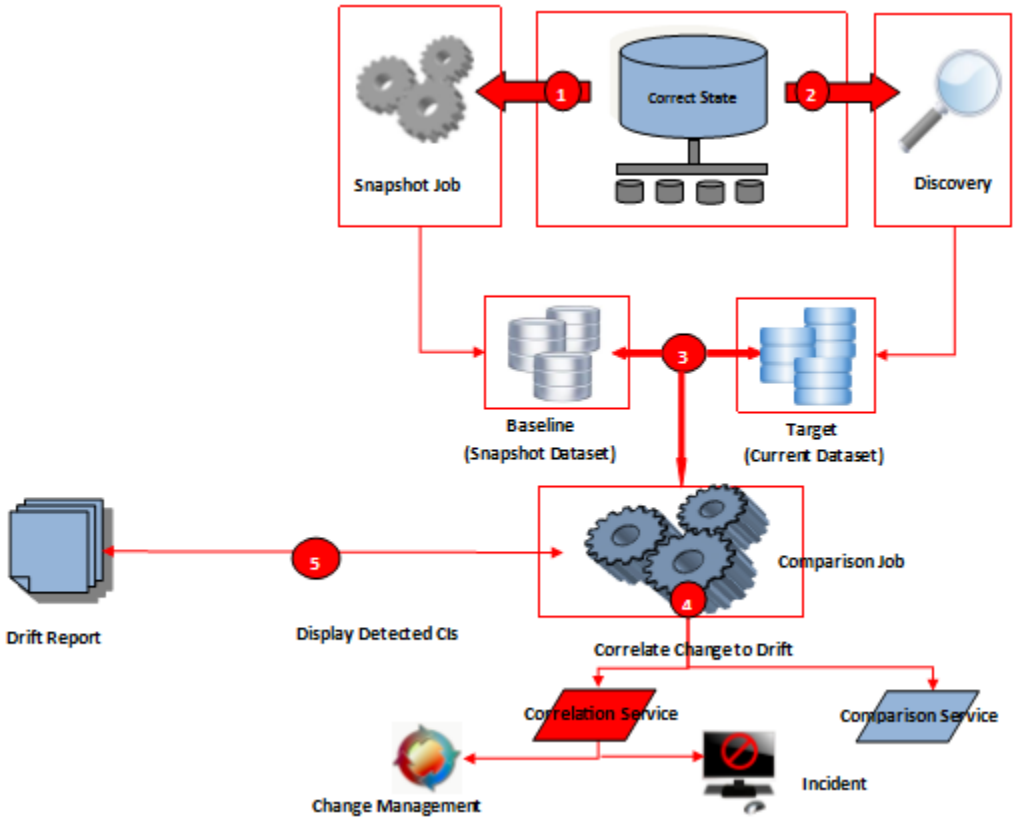

Figure 3: Configuration Drift Analysis Use Case

4.2 Monitoring Prohibited Software Titles

A user downloads a software program that is prohibited for specific use ("blacklisted" on the TRM) for his/her Government Furnished Equipment (GFE) laptop. The discovery tool identifies the software title and checks it against the TRM to determine whether it is authorized or prohibited. The software will automatically be removed if the user does not manually remove it. The CMS maintains data regarding blacklisted software titles . A high-level process flow for this use case (as shown in Figure 4) is as follows:

- Step 1: Endpoint discovery tools scan the entire enterprise and discover information on all endpoints.
- Step 2: The discovery tool produces software titles associated with each endpoint.
- Step 3: Software titles are checked against product catalog and TRM.
- Step 4: Software titles are either approved or prohibited based on results from product catalog and TRM.
- Step 5: Approved software titles are run on the system by a whitelisting tool.
- Step 6: Prohibited software titles go through an incident management process:
    - Email alert regarding prohibited software

- Initial analysis of prohibited software
- Initiate incident and create incident ticket
- Remediation and removal of prohibited software
- Assess TRM for alternate solutions
- Update ticket for resolution status and close

- Step 7: The enterprise CMS maintains data regarding the software titles.

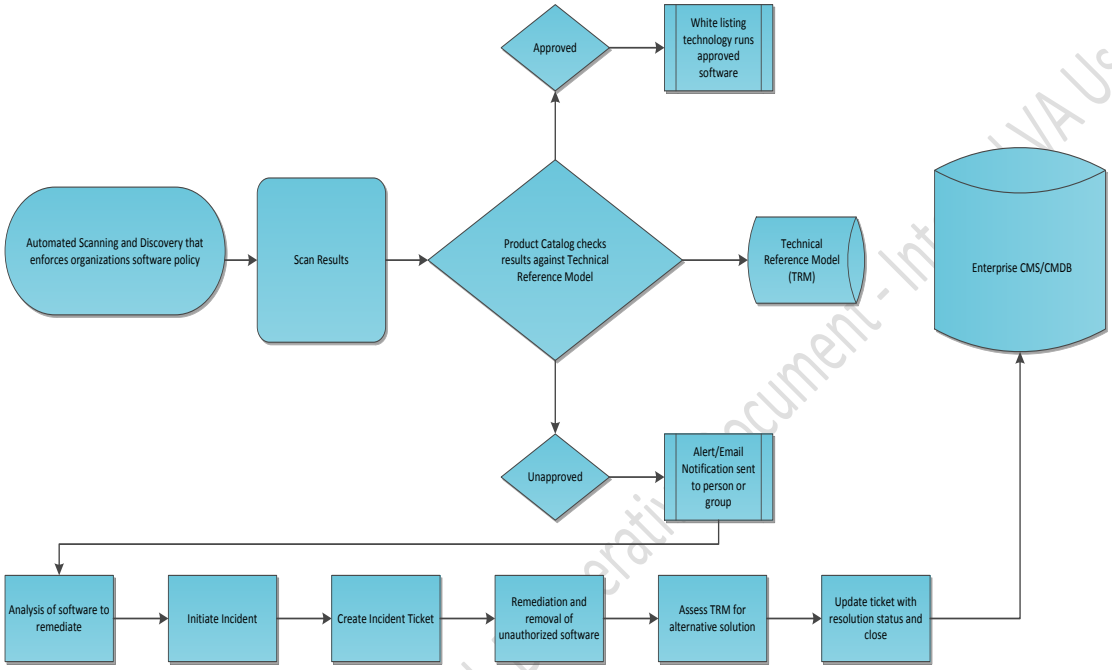

Figure 4: Monitoring Prohibited Software Titles Use Case

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

Appendix A. DOCUMENT SCOPE

Scope

This Enterprise Design Pattern provides a vendor-agnostic process framework, based on IT Infrastructure Library (ITIL) best practices and enterprise capabilities that VA will use to implement enterprise-wide IT service Configuration Management. This framework includes standardized processes and toolsets to manage VA's IT service configuration items, leading to reduction of security vulnerabilities and enhancements to customer support across all Lines of Business.

Document Development and Maintenance

This document was developed collaboratively with internal stakeholders from across the Department and included participation from all OI&T pillars and Administrations. Development of the document included engagements with industry experts to review, provide input, and comment on the proposed pattern. This document contains a revision history and revision approval logs to track all changes. Updates will be coordinated with the Government lead for this document, which will also facilitate stakeholder coordination and subsequent re-approval depending on the significance of the change.

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

Appendix B. Definitions

Name	Definition
Approved List	A list of discrete entities, such as hosts or applications that are known to be benign and are approved for use within an organization and/or information system.
Authentication (FIPS 200)	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Baseline Configuration	A set of specifications for a system, of Configuration Item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.
Configuration	The possible conditions, parameters, and specifications with which an information system or system component can be described of arranged.
Configuration Baseline	See "Baseline Configuration"
Configuration Change Control	Process for managing updates to the baseline configurations for the configuration items; and evaluation of all change requests and change proposals and their subsequent approval
Configuration Control (CNSSI-4009)	Process for controlling modifications to hardware, firmware, software and documentation to protect the information system against improper modifications before, during, and after system implementation.
Configuration Control Board	Establishment of and charter for a group of qualified people with responsibility for the process of controlling and approving changes throughout the development and operational lifecycle of products and systems; may also be referred to as a change control board;

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

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

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

Name	Definition
Information Technology(40 U.S.C., Sec. 1401)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the proceeding sentence, equipment is used by an executive agency if the equipment the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment, in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Patch	An additional piece of code developed to address a problem in an existing piece of software.
Remediation	The act of correcting vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, and uninstalling a software application.
Request for Change	▪ **Normal:** All changes follow a standardized change process model for the type of change being implemented. This process takes the change through its entire lifecycle; Registration, Analysis, Approval, Develop/Test/Build, Release Approval, Scheduling, Implementation and Verification. ▪ **Standard:** Is a change to a service or infrastructure for which the approach is pre-authorized by Change Management that has an accepted and established procedure to provide a specific change requirement. ▪ **Emergency:** Reserved for changes intended to repair an error in an IT service that is negatively impacting the business to a high degree. Changes that introduce immediate and required business improvements are handled as normal changes, assessed as having the highest urgency.
Risk	The probability that a particular threat will exploit a particular vulnerability.

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

Name	Definition
System	A set of IT assets, processes, applications, and related resources that are under the same direct management and budgetary control; have the same function or mission objective; have essentially the same security needs; and reside in the same general operation environment. When not used in this formal sense, the term is synonymous with the term" host". The context surrounding this word should make the definition clear or else should specify which definition is being used.
Systemic	An issue or vulnerability found through scanning or discovery that resides in multiple places throughout the enterprise.
System Owner	Individual with managerial, operational, technical, and often budgetary responsibility for all aspects of an information technology system.
Threat	Any circumstance or event, deliberate of unintentional, with the potential for causing harm to a system.
User	See "Information System User"
VA System Inventory (VASI)	VASI is an authoritative inventory of business-oriented applications and supporting databases that provides a comprehensive repository of basic information about VA systems; represents the relationships between systems and other VA data stores; and captures new systems.
Vulnerability	A Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat device.

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

Appendix C. ACRONYMS

Acronym	Description
ADDM	Atrium Discovery and Dependency Mapping
ASD	Architecture, Strategy and Design
CA	CA Technologies
CA SDM	CA Service Desk Manager
CCB	Configuration Control Board
CERT	Computer Emergency Readiness Team
CI	Configuration Item
CIO	Chief Information Officer
CM	Configuration Management
CMDB	Configuration Management Database
COTS	Commercial Off-the-shelf
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
DHS	Department of Homeland Security
DOD	Department of Defense
EO	Enterprise Operations
ESE	Enterprise Systems Engineering
FEA	Federal Enterprise Architecture
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GOTS	Government Off-the-shelf
IEM	IBM Endpoint Manager
IS	Information System
IT	Information Technology
ITAM	Information Technology Asset Management
ITIL	Information Technology Infrastructure Library
MAC	Media Access Control
NCCB	National Change Control Board
NIST	National Institute of Standards and Technology
NSD	National Service Desk
OI&T	Office of Information and Technology

Draft

Acronym	Description
OIG	Office of the Inspector General
OIS	Office of Information Security
OMG	Office of Management and Budget
OVAL	Open Vulnerability Assessment Language
PD	Product Development
SCAP	Security Content Automation Protocol
SCCM	System Center Configuration Manager
SDE	Service Delivery Engineering
SIEM	Security Information and Event Management
SLA	Service Level Agreement
STIGs	Security Technical Information Guides
TRAC	Tasks, Reporting, Actions, Communications
TRM	Technical Reference Model
US-CERT	United Stated Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline
VA	Department of Veterans Affairs
VASI	Veterans Affairs Systems Inventory
XML	Extensible Markup Language

Draft

Appendix D. References, Standards, and Policies

This Enterprise Design Pattern is aligned to the following VA OI&T references and standards applicable to enterprise-wide CM:

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
1	VA	VA Directive 6004	Directive establishes VA policy and responsibilities regarding Configuration, Change, and Release Management Programs for implementation across VA.
2	VA	VA 6500 Handbook	Directive information security program. Defining overall security framework for VA.
3	NIST	SP 800-128	Guide for Security-Focused Configuration Management of Information Systems Provides guidelines for organizations responsible for managing and administrating the security of federal information systems and associated environments of operations
4	NIST	SP 800-63-2	Special Publication — Creating a Patch and Vulnerability Management Program Designed to assist organizations in implementing security patch and vulnerability remediation programs.
5	NIST	800-53	Recommended Security Controls for Federal Information Systems and Organizations Outlines the importance of deploying automated mechanisms to detect unauthorized components and configurations within agency networks
6	OMB	Memorandum M-14-04	FY2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management Provides guidance for Federal agencies to follow the report requirements under FISMA.

Draft

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
7	OMB	Memorandum M-02-01	Guidance for Preparing and Submitting Security Plans of Actions and Milestones Defines Management and Reporting Requirements for agency POA&Ms, including deficiency descriptions, remediation actions, required resources, and responsible parties.
8	White House	FISMA Act of 2002	Reauthorizes key sections of the Government Information Security Reform Act Provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets.
9	VA	CRISP	Intended to improve access controls, configurations management, contingency planning, and the security management of a large number of information technology systems.
10	OMB	E-Government Act of 2002	Public Law 107-347 Purpose is to improve the management and promotion of electronic government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a framework of measures that require using Internet-based information technology to improve citizen access to government information and services, and for other purposes.
11	VA	Change Plan – Process Template	This Standard Operating Procedure has been created to support and supplement the National Change Management Policy and Standard Document and is not intended to replace the overall management process of the Change Management Program this SOP expands and provides specific information related to the following process being placed under Change Control

Draft

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
12	VA	OI&T Enterprise Change Management Policy	This document establishes an OIT Enterprise Change Management policy ensuring changes to all information technology infrastructure and software configuration items (CIs) are managed and communicated in a disciplined and standardized manner to minimize risk, impact and optimize IT resources
13	VA	OI&T Change Management Process (ProPath)	The purpose of the Change Management (ChM) process is to provide guidance for the management of changes to all Department of Veterans Affairs (VA) Information Technology (IT) environments.
14	VA	SMA Security Baselines	The official versions of the baselines along with process information can be found at: http://vaww.sde.portal.va.gov/svcs/SMA/SitePages/Home.aspx

Draft