Configuration Management Plan

**Beneficiary Travel Self-Service System (BTSSS)**



**September 2017**

Version 3.04

Department of Veterans Affairs

Version History

| Date | Version | Description | Author |
| --- | --- | --- | --- |
| 9/18/2017 | 3.04 | September Monthly Update | Christina Silva |
| 8/31/2017 | 3.03 | CRMOL update | Christina Silva |
| 8/21/2017 | 3.02 | August Monthly Update | Christina Silva |
| 7/19/2017 | 3.01 | July Monthly Update | Christina Silva |
| 6/16/2017 | 2.03 | June Monthly Update | Christina Silva |
| 5/18/2017 | 2.02 | May Monthly Update | Christina Silva |
| 4/18/2017 | 2.01 | April Monthly Update | Christina Silva |
| 3/15/2017 | 1.03 | March Monthly Update | Christina Silva |
| 2/24/2017 | 1.02 | February Monthly Update | Christina Silva |
| 1/26/2016 | 1.01 | January Monthly Update | Christina Silva |
| 12/2/2016 | 0.04 | December Monthly Update | Scott Bartel |
| 10/31/2016 | 0.03 | Initial Release | Karen Shepherd |
| 10/28/2016 | 0.02 | Edited Document Per Comments | Karen Shepherd |
| 10/26/2016 | 0.01 | Initial Draft | Karen Shepherd |

Table of Contents

[1. Executive Summary 1](#_Toc493514719)

[2. Introduction 1](#_Toc493514720)

[2.1 Purpose of the Configuration Management Plan 1](#_Toc493514721)

[2.2 Scope of the Configuration Management Plan 2](#_Toc493514722)

[2.3 Structure of the Configuration Management Plan 2](#_Toc493514723)

[3 Configuration Management Activities 2](#_Toc493514724)

[3.1 Roles and Responsibilities 2](#_Toc493514725)

[3.2 Communication 4](#_Toc493514726)

[3.3 System Configuration Baseline 4](#_Toc493514727)

[3.4 Configuration Control Process (CCP) 5](#_Toc493514728)

[3.5 Configuration Management Resources 7](#_Toc493514729)

[APPENDIX A: CONFIGURATION MANAGEMENT PLAN APPROVAL 8](#_Toc493514730)

[Appendix B: References 9](#_Toc493514731)

[Appendix C: Key Terms 10](#_Toc493514732)

[Appendix D: Suggested Configuration Items Data Elements 11](#_Toc493514733)

[Appendix E: [Facility] Current Configuration Baseline Report 16](#_Toc493514734)

[Appendix F: Configuration Items (CI) Showing System Boundaries 17](#_Toc493514735)

[Appendix G: Change Order Approval Checklist 18](#_Toc493514736)

[Appendix H: Change Order Implementation Plan Template 19](#_Toc493514737)

[Appendix I: Business Case Justification 20](#_Toc493514738)

[Appendix J: Change Management Back-Out Plan Template 21](#_Toc493514739)

# Executive Summary

The implementation of a Beneficiary Travel Self-Service System (BTSSS) Solution serves to fulfill the Department of Veterans Affairs (VA) commitment to Veterans and to the American public to serve as good stewards of public resources.

This document will provide high level information on the Configuration Management (CM) processes implemented throughout all phases for the BTSSS software project including software, systems, and documentation. The process and procedures outlined in this document will conform with the existing VA CM tools and the overarching VA Configuration Management Plan (CMP) in the Rational repository. The CMP will also support the unified Veteran Information Portal (VIP) Release process utilizing agile development, frequent builds and releases, and a high level of integration with Agile Lifecycle Management (ALM) tools, with automated builds and testing. ALM and testing data will need to be stored in the VIP Rational Repository.

# Introduction

The Beneficiary Travel Self-Service System (BTSSS) will enable the VA to provide travel reimbursement to authorized Veterans and their beneficiaries at the point-of-care as well as through standard web browsers and the VetLink kiosk at various VA facilities. It will use state-of-the-art technology that will allow Veterans to submit expenses for travel reimbursement utilizing the BTSSS application and receive timely reimbursement via Electronic Funds Transfer (EFT).

The BTSSS software solution will be developed and implemented using Microsoft Dynamics 365 for Customer Service which is a COTS-based solution that provides strong customer support and access to a user community.

Due to this projects use of multiple third party vendors, the Configuration Management process will initially be split between multiple tools. However due to the VA’s requirement that all finalized code be stored within its Configuration Management Tool, this project will only be providing the final code releases in IBM Rational Team Concert (RTC).

## Purpose of the Configuration Management Plan

The overall objective of this CMP is to identify CM roles and responsibilities, resources, and formal processes and procedures to ensure that all development of the BTSSS software system are evaluated and approved before implementation. This also includes the processes and procedures for managing and controlling the development, delivery, and maintenance of all software and documentation products 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 also outlines the BTSSS organization, responsibilities, and requirements to be followed by teams producing or modifying software within the system. The BTSSS CMP will aid both management and technical staff in the production of high-quality software products and all the information pertinent to the BTSSS system.

## Scope of the Configuration Management Plan

The Beneficiary Travel Self-Service System (BTSSS) CMP document, along with the corresponding 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 required 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 are system owners, Organizational Service Lines and divisions, facility chief information officers, system administrators, information security officers and information owners, and Office of Information and Technology (OIT) staff within these identified areas responsible for the day-to-day maintenance of the configuration items on the BTSSS software development project. This includes others who have a requirement or need to develop, change, fix, or enhance software artifacts on the BTSSS software development project.

This CMP, in conjunction with the 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.

# Configuration Management Activities

## Roles and Responsibilities

Table : Roles and Responsibilities

| Role | Responsibility |
| --- | --- |
| Program Manager | • Oversees the software configuration management process.  • Ensures proper execution of the BTSSS Plan.  • Identify dependent projects. |
| Configuration Manager | • Develop and maintain Software Configuration Management (SCM) Procedures Manual and work instructions for each VA product they are assigned.  • Educates project team members in SCM “best practices.”  • Accountable for instituting the established processes and reporting progress statistics based on change requests.  • Identifies product baselines as necessary of all products within their assigned projects.  • Responsible for SCM audits and necessary status accounting related to the product.  • Maintains artifacts following proper version control procedures. |
| Software Change/Build Administrator | • Develops and maintains artifacts following proper version control procedures.  • Establishes, promotes, and releases baselines.  • Performs or validates interim and final builds.  • Identifies product baselines as necessary of all products within their assigned projects. |
| Development Manager/Technical Lead | • Prepares release package, release archives and Version Description Documents (VDD).  • Ensures all SCM Procedures Manual and work instructions are implemented and followed for all software, documentation, and/or any other components for which they are responsible.  • Ensures all developers’ work within the specified SCM process and related guidelines as specified in the SCM Procedures Manual and work instructions. |
| Developers/System Administration | • Develops and maintains artifacts following proper version control procedures using the SCM Procedures Manual and work instructions.  • Maintain accurate, detailed information for all assigned stories, in the Rational database, related to the applicable development detail of the Agile lifecycle.  • Provide impact analysis reporting problems or changes, including documentation of suggested solutions.  • Documentation of build, release, and installation instructions. |
| Software Quality Assurance Analyst/Testing Analyst | • Update stories assigned to them according to test activity results.  • Determines Pass/Fail for each story scheduled for a sprint release.  • Identifies defect(s) and/or enhancement(s) for any newly discovered problems during testing and creates stories or defects in Rational. |
| Technical Writer | • Develops technical deliverable documentation to support the software deliverables.  • Provides editing, formatting, and graphics support for documentation. |
| Implementation Team/Operations Team | • Coordinates the release and deployment of software updates to the existing BTSSS Customer Relationship Management (CRMOL) system.  • 365 Cloud |

## Communication

Communication within the BTSSS project will utilize the features within the Rational Configuration Management tool (RTC) that allows for tasks, work items, builds, and deployments to be processed through a life cycle. That cycle progression is accomplished by allocating to each activity, task, or decision the role that is accountable and/or responsible for it as well as those roles to be consulted with beforehand, or informed afterward. The OIT Configuration Management Process document provides a Responsible, Accountable, Consulted, and Informed (RACI) Matrix to define activities and roles.

BTSSS will utilize this matrix to define the roles and responsibilities within the project and will provide communication via daily scrum meetings, weekly team meetings, and various developer, test and deployment meetings as needed.

Requests for Change (RFC)/Stories are entered in 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.

## System Configuration Baseline

Configuration identification is the process of identifying, selecting, naming, and classifying the development items subject to change control. This involves defining the product structure and defining identification conventions to be used for baselines of products, documents, software builds, and releases packages. Items are normally placed under change control as soon as they are instantiated, as tracking the configuration and new contents and implementation status of new requirements going into an initial release is equally as important as tracking later changes.

Within the Rational Team Concert (RTC) repository, unique identifiers will be applied to products and their associated content. The following are the types of identifiers used in accordance with the formats defined in the applicable procedure documents:

1. File versions - Identifies the version or revision identifier of each software item that comprise the Product at any specific baseline. It allows identification of unique items that make up the inventory of a baseline. Software identification provides the foundation for traceability of related artifacts. The software identification version number is assigned by the version control automated tool and controlled in the development repository. The VDD lists all software, its version, and related change document numbers.
2. Change records– Identifies a set of work product versions created to resolve a specific Change Request. The identifier is created, controlled, and tracked by the Change Management System.
3. Baseline – Identifies a set of specifications or work products that has been formally reviewed and agreed upon, which serves as the basis for further development, and which can be changed only through change control procedures.
4. Build – Identifies a set of solution file versions used to build and assemble deployable packages.
5. Release Package – Identifies a set of deployable file versions and deliverable document versions that constitute a complete release package.
6. Release Candidate – Identifies the distribution of the baseline or application modifications to the baseline that is being staged for production before it become a Product Release.

For the BTSSS program all project related documents will be managed and controlled in the Rational Team Concert designated repository for that type of document. All project documentation must adhere to VA policy on protection of VA security and VA architecture content, desensitization of patient data content, Freedom of Information Act (FOIA) content redaction restrictions, 508 accessibility standards, and documentation standards where applicable.

Product Artifacts are those that change along with the developed product and most likely, will experience change over time and thus require baselining and Change Management. They also typically represent specific configurations and criteria required by the developed release of the product to which they are associated with and thus should be packaged and migrated through the same series of life cycles stages as all other baselined artifacts within the development environment architecture and utilities.

## Configuration Control Process (CCP)

OIT and SDE have established process and procedures that dictate the configuration change control for all hardware and software configuration items. A VA tool is used for requesting, approving, implementing, monitoring, and tracking, auditing and closing change orders affecting configuration items under change and configuration control.

* Step 1: Establish System Configuration Baseline
* Step 2: Review backlog, identify changes, and create change story
* Step 3: Identify change stories and plan Sprint
* Step 4: Perform configuration changes
* Step 5: Perform Security and Operational Impact Analysis
* Step 6: Implement configuration changes
* Step 7: Verify implemented changes are successful and did not introduce additional issues/incidents into the environment.
* Step 8: Perform Configuration Status Accounting
* Step 9: Conduct Retrospective which includes Configuration Verification and Audit.

All product assets are expected to be managed sufficiently to provide a stable, traceable, dependable, and secured development, test, and, production environment within VA and for VA information assets managed outside the VA for the purposes of conducting business with or on behalf of the VA. Configuration items in the scope of this document are defined as any object (software, hardware, data, documentation, environment configurations, etc.) that may experience change over time.

The act of creating any software deliverable implies that objects will be created and modified in the design and development process, which by definition become CIs along with the environments and documentation developed to support them. After development is complete, testing for validation and certification is required. This can only be accomplished accurately if the integrity of the software deliverable can be maintained through formal change control.

Formal change control involves the management of changes and versions to the CIs that are introduced to the baseline. Change control will also apply to product migration beyond development, to the various phases of testing and certification, and until it is released into a production environment.

There are at least two levels of change control that this document is addressing. The change control that takes place during the Software Development Life Cycle (SDLC) is managed with the SCM change management processes and procedures and the Operations change control is managed by OIT Change Management processes and procedures. The handoff between software development and OIT will be handled by assigned staff from both departments that the SCM Manager will coordinate.

The complexity involved in the Change Control process requires the implementation of formal processes and procedures to be documented in detail for each VA product in the SCM. Procedure Manual(s) and work instructions. These documents provide objectives, requirements, and step-by-step instruction on the performance of Change Control activities within the SCM Environment for each VA Product. The document will also provide sections with information on key process areas such as:

* The organization of personnel and the division of tasks for the VA team members.
* Decision criteria and escalation requirements specific to each level of change request review.
* The overall Change Management Process description and flow.
* The description of the change control tools and how the team will use them

## Configuration Management Resources

The Change Management Systems (CMS) is the automated mechanism that is used for tracking proposed changes to configuration items. Change orders are entered into the system and work orders assigned to the appropriate groups for review, approval, implementation, configuration status accounting and configuration verification. Changes are time stamped to provide a timeline and reviewed per local process and procedures to ensure that changes are processed correctly and are implemented to meet established requirements. Changes are not implemented without approval per OIT and SDE Change Management Policy and procedures.

Each area of the organization managing changes has a Change and Configuration Management Division that is responsible of ensuring that appropriate control is put in place to manage the configuration items per VA Handbook 6500 Configuration Management controls.

The VA utilizes the Rational Team Concert tools to manage all requirements, configuration items, tasks, activities, builds and testing. This all-encompassing tool provides project staff and VA management the ability to track any file, task, requirement or testing through the various stages of conception to delivery.

APPENDIX A: CONFIGURATION MANAGEMENT PLAN APPROVAL

The undersigned acknowledge that they have reviewed the **BTSSS** **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:

Title:

Role:

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

Signature: Date:

Title:

Role:

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

Signature: Date:

Print Name:

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 | <https://DNS/vapubs/search_action.cfm?dType=2> |
| VA Handbook 6500 | Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program | https://www.DNS/vapubs/search\_action.cfm?dType=2 |
| OIT Configuration Management Process | OIT Configuration Management ProPath defined process and supporting document | [https://DNS/](https://dns/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/oit_configuration_management_process_document.pdf)  [sites/fo/committees/ccb/CMDB/](https://DNS/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://DNS/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://DNS/](https://DNS/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://DNS/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://DNSv/](https://DNS/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/oit_configuration_management_process_document.pdf)  [sites/fo/committees/ccb/CMDB/](https://DNS/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://DNS/sites/fo/committees/ccb/CMDB/Definitive%20Document%20Storage/oit_configuration_management_process_document.pdf) |
| Master Test Plan | Master Test Plan Template | https://DNS/sites/btsss/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2Fbtsss%2FShared%20Documents%2FData%20Library%2FProject%20Docs%2FMTP |

Appendix C: Key Terms

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

| Term | Definition |
| --- | --- |
| ALM | Agile Lifecycle Management |
| CAB | Change Advisory Board |
| CCB | Change Control Board |
| CCP | Configuration Control Process |
| CI | Configuration Item |
| CM | Configuration Management |
| CMS | Change Management Systems |
| CMDB | Configuration Management Database |
| CMP | Configuration Management Plan |
| COR | Contracting Officer Representative |
| CRMOL | Customer Relationship Management Online |
| DNS | Domain Name Service |
| FCIO | Facility Chief Information Officer |
| FOIA | Freedom of Information Act |
| IT | Information Technology |
| OIT | Office of Information & Technology |
| OS | Operating System |
| POC | Point of Contact |
| RACI | Responsible, Accountable, Consulted, and Informed |
| RFC | Request for Change |
| SCM | Software Configuration Management |
| SDE | Service Delivery and Engineering |
| SOP | Standard Operating Procedure |
| VA | Veterans Affairs |
| VDD | Version Description Documents |
| VIP | Veteran Information Portal |
| VISN | Veterans Integrated Service 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.

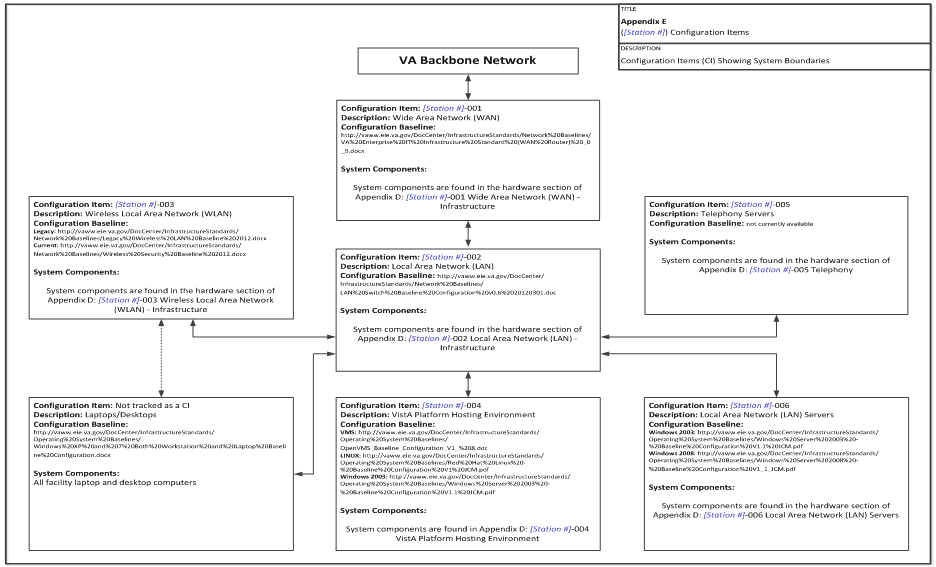
| Field Name | Data Type | CI Type | Description |
| --- | --- | --- | --- |
| Resource Name | *Indexed Text* | *Hardware / Software / Service / Document* | A unique name of the Configuration Item (CI). A name that represents the Resource and is easy to identify what it is; a key search field within 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 Information Technology (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 ava  ilable, 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 Point of Contact (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: [Facility] Current Configuration Baseline Report

The following table details the Hardware/Software and Services associated with the system under this CMP.



Appendix F: Configuration Items (CI) Showing System Boundaries





Appendix G: 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 Change Control Board (CCB) if this is a significant change/downtime required.**



Appendix H: 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

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

Identification of areas that might cause problems

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

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



Appendix I: 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 J: Change Management Back-Out Plan Template

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

Estimated time-frames for restoring service

Any pre-implementation work that will be required

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

