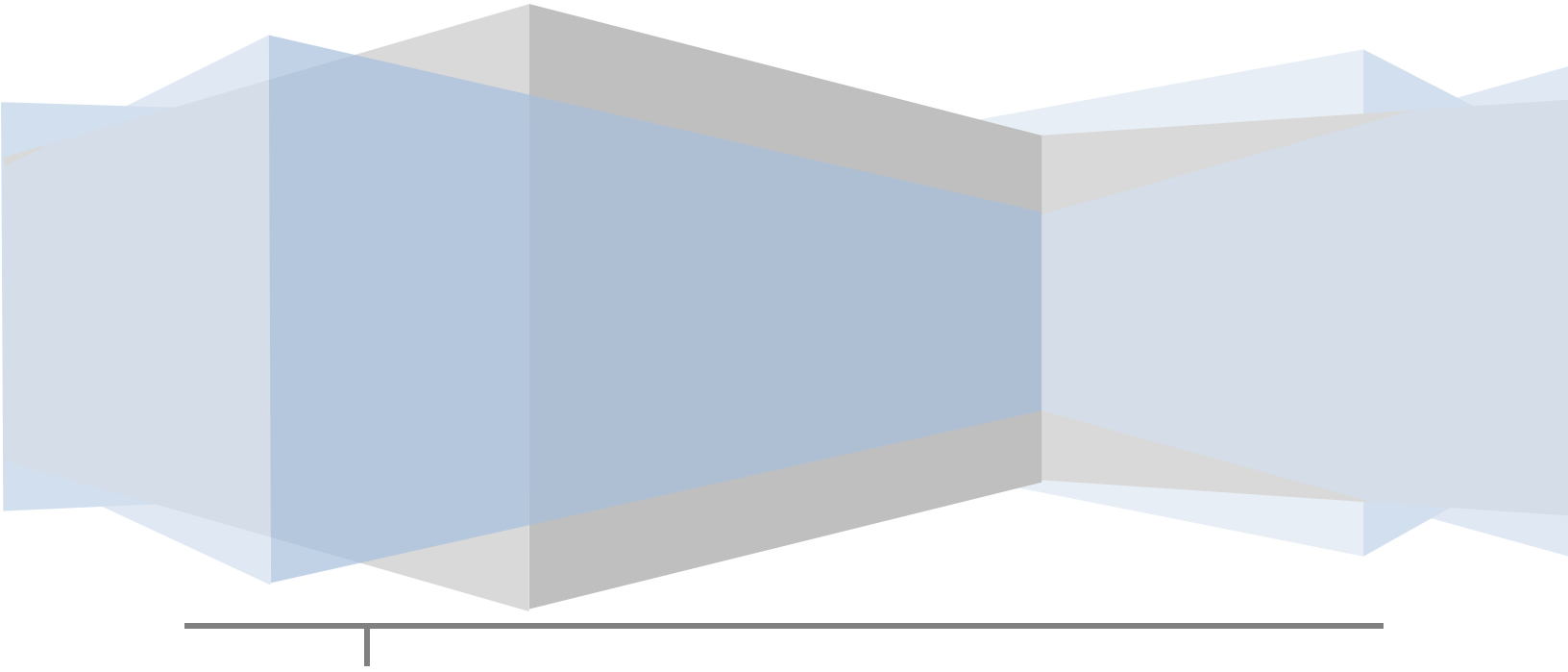
Configuration Management Process

Vanderbilt University IT

July 15, 2021



CONTENTS

Version History 3
Introduction 4
Objectives & Scope 5
Objectives 5
Scope 6
CI Categories 7
Process Flow 8
Initial population of the CMDB via Discovery/Upload 8
Maintaining the CMDB as part of Change Management 9
Verification & Audit Process 9
Roles & Responsiblities 10
CI Owner 10
Configuration Manager 10
Policies 11
CI Attributes 12
Common Attributes 12
Service Attributes 12
Key Performance Indicators 13

VERSION HISTORY

Date	Version	Who	Comments
8/15/2016	1.0	VMWare and Vanderbilt VUIT	First draft
8/25/2016	2.0	T. Osborne	Edits, Clarifications and CI Attributes
10/26/2016	2.1	T. Osborne	CI Attributes
12/19/2016	2.2	T. Osborne	CMDB processes updated
1/8/2021	2.3	T. Osborne	Updated CI categories
3/30/2021	3.0	T. Osborne/Taj Wolff	Remove references to Firescope, update process to indicate anyone with access can update the CMDB. Updated Service Attributes to reflect what is currently used in the tool.
7/15/2021	3.1	T. Osborne/Taj Wolff	Added previously unwritten policy to require change ticket when CI moves from New to Active status.

INTRODUCTION

This document describes the Configuration Management process and Configuration Management Database (CMDB) data dictionary that is implemented in Cherwell. It is based on the Information Technology Infrastructure Technology Library® (ITIL) and adapted to address VUIT's specific requirements.

This document is divided into the following sections:

Section	Description
Objectives and Scope	Specifies the objectives of the Configuration Management process and what is in and out of scope.
CI Categories	Major types of configuration items
Process Flow	Diagram illustrating how maintaining the CMDB will be integrated with Change Management. Also describes the CMDB Audit process.
Roles & Responsibilities	Describes the responsibilities for the roles within the Configuration Management process as well as the related Change Management roles.
Policies	Policies that support the Configuration Management process
Key Performance Indicators	Specifies the metrics for measuring the success of the Configuration Management process.

OBJECTIVES & SCOPE

The purpose of the Configuration Management process is to ensure that the assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed. This information includes details of how the assets have been configured and the relationships between assets.

This document uses the term Configuration Item (CI) to represent the asset. A CI may be hardware, software, documentation or an intangible concept. CIs are stored in the Configuration Management Database (CMDB).

OBJECTIVES

The specific objectives of the Configuration Management process are:

1. Establish a single enterprise CMDB, a source of truth, and retire disparate asset tracking tools
2. Establish a single standard Configuration Management process for maintaining the CMDB that integrates with the Change Management process
3. Eliminate the effort wasted on re-discovering relationships over-and-over again
4. Provide accurate configuration information to facilitate
    a. Systematic Change impact analysis
    b. Rapid Incident diagnoses including Security Incident Response
    c. Assist with Problem Management
    d. Help with analysis of our security posture and risks
    e. Source of information for querying, reporting and audits
    f. Identify our critical CIs
    g. Inter-operability, application rationalization. Process of cataloging and eliminating duplicate software applications
    h. Assist with Disaster Recovery planning, Business Continuity Planning, and Data Center moves
    i. Capacity management including how to adequately staff
5. Clarify who owns each Configuration Item and who to contact for support

SCOPE

The following CI Categories are in scope:

- All infrastructure and applications in the Data Center and cloud production environment.
- Infrastructure in the non-prod environments. This includes servers, network devices - basically non-application data center devices - that are in every environment (e.g. development, test, training, etc.).
- Applications in the non-prod environment will also be tracked but they will not be controlled by Change Management.
- Any CI that has a VUIT dependency

The following CI categories are out-of-scope but may be managed as assets:

- Workplace devices, e.g. laptops, desktops, etc. (future phase)
- Mobile devices, e.g. smart phones, tablets
- A/V equipment

CI CATEGORIES

The following table lists the main types of CIs:

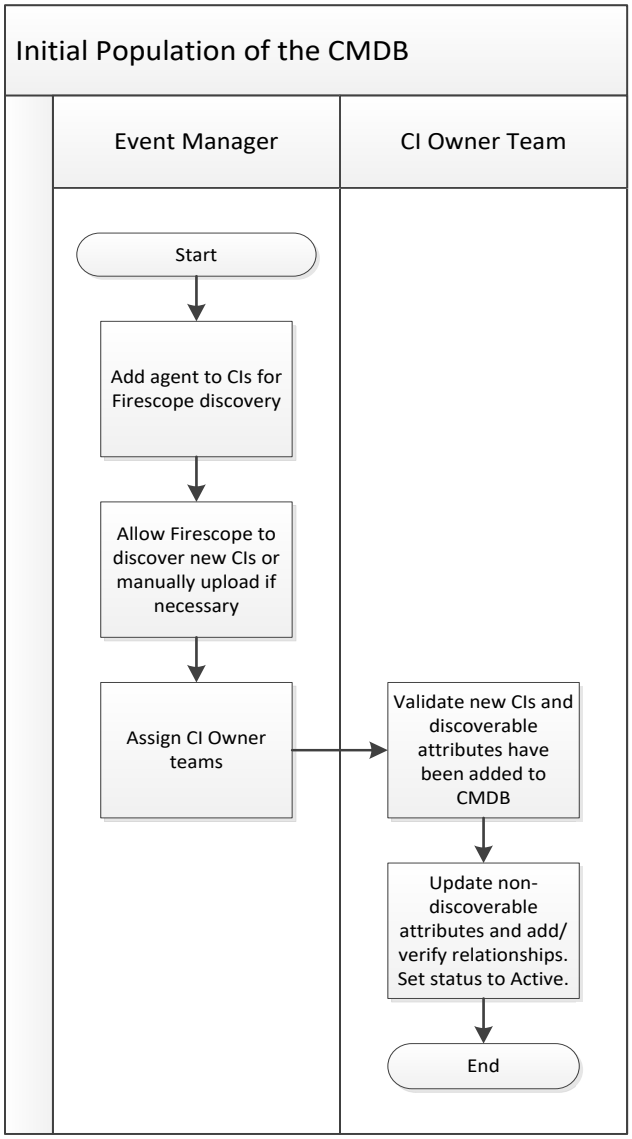
CI Category	Examples	Source
Network Device	Access points, firewalls, routers, switches, circuits, etc.	Netconfig
Server	Application server, file server, mail server, appliances, etc.	SCCM, Firescope (decommed)
Storage	SAN, NAS	Manual
Data Center & Facility Equipment	UPS, PDU, Racks, A/C Units, Cameras, Cable	Sunbird, Trellis (decommed)
SSL Certificate	SSL, WebCert, Self Signed, etc.	SerVU
Database	Oracle, MSSQL, MySQL, NoSQL, Hadoop	Manual
Middleware	Websphere, WebLogic, Apache	Manual
Application	SIS, ERP, HRIS, Exchange, SharePoint	VADR
Telephony Equipment	PBX	Manual
Classroom/Conference Technology	Projectors, video capture, wireless mics, digital signage, etc.	Spreadsheet

PROCESS FLOW

INITIAL POPULATION OF THE CMDB VIA FIRESCOPE/UPLOAD

The initial CMDB population was either performed via “discovery” automation (an integration between Firescope and Cherwell) or through a file upload. The CIs were assigned to a CI Owner, which is also known as Owned By team in Cherwell.

Most CIs were assigned to Owned By teams through the Contact field in the CMDB. The rest of the CIs were assigned manually. The CI Owner team will update all non-discoverable fields in the CMDB and verify or add the appropriate relationships.



ADDING A NEW CI TO THE CMDB

As a new CI goes through the installation stages within its project, the Project Manager will ensure that a task is created to manually create the CI in the CMDB. If it is a Virtual Machine, the CI will be created by an automated process. All others should be created manually if no automated process exists.

MAINTAINING THE CMDB

The responsibility of maintaining current, accurate information in the CMDB belongs to everyone. No change record will be necessary as the team member making the update will be recorded in a history field, along with the date/time and the fields that were edited.

VERIFICATION & AUDIT PROCESS

The CMDB verification and audit process is not automated in Cherwell. The Configuration Manager works with the CI Owner to create an audit plan. This plan includes preparing a list of CIs to be audited. After the audit is performed, the Configuration Manager will publish results in the ITSM Monthly Metrics report and/or send findings to appropriate leadership.

If exceptions were found during the audit, the CI Owner team from which exceptions were found researches the exception to determine the root cause. If necessary, the CI Owner team will update the Configuration Record so that an accurate representation of the IT environment exists.

ROLES & RESPONSIBLITIES

CI OWNER TEAM

The CI Owner will be the team that owns the CI.

1. Ensure that all of their CIs are recorded and the associated attributes and relationship information is accurate.
2. Perform CMDB audits as requested by the Configuration Manager.
3. Provide input to the Configuration Manager into what attributes and relationships need to be tracked within the CMDB.

REQUESTOR

1. When submitting a Request, associate all CIs that will be updated with all required information.
2. After the Request is fulfilled, validate the updates the appropriate CIs. When required, validate the updates to the CI attributes and relationships.

CONFIGURATION MANAGER

1. Own, maintain and continuously improve the Configuration Management process.
2. Sponsor improvement initiatives and drive the requirements for the CMDB.
3. Report on Configuration Management activities (number of CIs populated, number of CIs associated with Changes, number of CIs updated, etc.)
4. Sponsor initiatives to educate how to maintain the CMDB and utilize the CMDB information for decision making.
5. Trigger the CMDB audit process and define the scope of the audit based on input from CI Owners and IT management.
6. Prepare CMDB reports and queries as requested.

POLICIES

1. The CMDB must be an accurate reflection of the real world VUIT environment.
2. If VUIT staff member discovers that there is an error in CMDB information, he/she will inform the appropriate CI Owner team and the Configuration Manager.
3. The CMDB will be audited annually using the “Verification and Audit” procedures described in this document.
4. All CIs must have a change ticket entered in SerVU when that CI changes from New to Active status.

CI ATTRIBUTES

COMMON ATTRIBUTES

Attribute	Description
Friendly Name	Unique name
CI Owner	Lookup based on team.
Status	Drop down containing: • New • Active • Retired • Disposed
Environment	Drop down containing: • Non-Production • Production • Disaster Recovery

SERVICE ATTRIBUTES

Attribute	Description
Business Criticality	Drop down containing: • Low • Medium • High
FERPA	Drop down containing: • Yes • No
PCI	Drop down containing: • Yes • No
Service Consumers	Drop down containing: • Medical center
Service Affected/Service Category/Service Subcategory	Drop down containing: • Defined by the SLA/DR team

KEY PERFORMANCE INDICATORS

1. Number of CIs in the CMDB.
2. Reduction in the number of CIs that are not connected to any other CI.
3. Number of CIs linked to Incidents, Problems, and Changes.
4. Number of CIs in Active status in the CMDB.
5. Reduction in number of CIs that do not have an Owned by Team or accurate status.