



Process Guide

Configuration Management

Version: 1.1
CALGARY Release

Table of Contents

1	Introduction	3
1.1	Overview	3
1.2	Process Description	3
1.3	Process Goal	3
1.4	Process Objectives	3
1.5	Relationship with other processes	4
1.6	Principles and basic concepts	5
2	Process Roles	6
3	Configuration Management Activity Description	9
3.1	Process Overview	9
	Process Overview Activity Description	10
3.2	Process Planning and Design	11
	Process Planning and Design Activity Description	12
3.3	Configuration Identification	15
	Configuration Identification Activity Description	16
3.4	Configuration Control	17
	Configuration Control Activity Description	18
3.5	Status Accounting and Reporting	19
	Status Accounting and Reporting Activity Description	19
3.6	Verification and Audit	20
	Verification and Audit Activity Description	21
4	Process Control	22
4.1	KPIs	22
4.2	Reports & Homepage Gauges	23
	Appendix A: Document Conventions	25
	Appendix B: Glossary of Terms and Acronyms	26

List of Figures

Figure 1: Process Overview	9
Figure 2: Process Planning and Design	11
Figure 3: CMDB Structure Model Example	14
Figure 4: Configuration Identification	15

1 Introduction

The concepts described in this guide are aligned with ITIL 2011 and may reference capabilities that are dependent upon other ServiceNow applications. These references will be noted by *grey italicized font*.

This document assumes that the *ServiceNow Discovery* product is available and that the *Enterprise CMDB plugin* has been activated.

1.1 Overview

A process is defined as a set of linked activities that transform specified inputs into specified outputs, aimed at accomplishing an agreed-upon objective in a measurable manner. The Configuration Management process definition laid out in this document further breaks down these activities into actions and the role(s) responsible for their execution.

This document also describes how ServiceNow supports the Configuration Management process to identify, record, audit and verify assets and configuration items including their versions, baselines, components, attributes and relationships.

There are strong inter-process relationships between Configuration Management and the other IT service management processes. Configuration Management and the CMDB are the foundation to integrated ITSM processes, and should be considered at the very beginning of any IT service management transformation effort.

1.2 Process Description

A *configuration item* (CI) is any component or other service asset that needs to be managed in order to provide an IT service. Information about each CI is stored in a configuration record within the configuration management database (CMDB). The configuration management process is responsible for managing the life cycle of all configuration items and their relationships with one another.

1.3 Process Goal

The primary goal of the configuration management process is to support efficient and effective service management processes by providing accurate information about configuration items. This enables users of that information to make better decisions, and more effectively support the objectives and requirements of the business.

1.4 Process Objectives

The objectives of the Configuration Management process are to:

- Ensure that IT managed assets are identified, controlled and properly cared throughout their lifecycle.
- Identify, control, record, report, audit and verify services and other CIs, including versions, baselines, constituent components, their attributes and relationships.

- Account for, manage and protect the integrity of CIs, through the service lifecycle by working with change management to ensure that only authorized components are used and only authorized changes are made.
- Ensure the integrity of CIs and configurations required to control the services by establishing and maintaining an accurate and complete CMDB.
- Maintain accurate configuration information on the historical, planned and current state of services and CIs.
- Support efficient and effective service management processes by providing accurate configuration information for decision-making purposes.

1.5 Relationship with other processes

Process	Relation Description	Input	Output
Incident Management	The CMDB contains details of the infrastructure vital to efficient incident classification, initial support, investigation and diagnosis.		X
	When CI records are identified as inaccurate, incident records are created and assigned to configuration management for correction.	X	
Problem Management	CI details and relationship information aids in root cause analysis, impact evaluation, and solution development.		X
	Problem records are linked to relevant CI record(s).	X	
Change Management	The CMDB provides change management with the necessary information for the assessment of the risk and impact of proposed changes.		X
	New, changed or disposed configuration items. Change management ensures that the information related to impacted CIs is updated properly following the implementation of a change.	X	

1.6 Principles and basic concepts

Policies

Configuration management policies are needed to establish the objectives, scope and principles that govern the process and should be considered with the change management and release and deployment management policies because they are so closely related.

Configuration Management policies will be very dependent upon the organization's business drivers, contractual requirements, and on compliance to applicable laws, regulations and standards. Areas that are typically addressed by policies are:

- The need to comply with governance requirements, such as Sarbanes-Oxley, ISO/IEC 20000, or COBIT
- The need to deliver the capability, resources and warranties as defined by service level agreements and contracts.
- The level of control and requirements needed for traceability and auditability.
- The requirement to maintain adequate configuration information for internal and external stakeholders.
- Level of automation to reduce errors and costs.

Security Considerations

Security is a very important aspect of the CMDB design. This includes the design of authorizations, roles and access along with for all of the tools, data and components of the CMDB.

2 Process Roles

Each role is assigned to perform specific tasks within the process. Within a specific process, there can be more than one individual associated with a specific role. Additionally, a single individual can assume more than one role within the process although typically not at the same time. Depending on the structure and maturity of a process, all roles described may not exist in every organization.

The following describes the typical roles defined for service asset and configuration management:

Role	Description
Process Owner	<p>A Senior Manager with the ability and authority to ensure the process is rolled out and used by the entire IT organization.</p> <p>Responsible and Accountable for:</p> <ul style="list-style-type: none"> Defining the overall mission of the process. Establishing and communicating the process mission, goals and objectives to all stakeholders. Resolving any cross-functional (departmental) issues. Ensuring consistent execution of the process across the organization. Reporting on the effectiveness of the process to senior management. Initiating any process improvement initiatives.
Configuration Manager	<p>Responsible for:</p> <ul style="list-style-type: none"> Managing the day-to-day activities of the process. Gathering and reporting on process metrics. Tracking compliance to the process. Agreeing and defining the service assets that will be treated as configuration items. Defining the structure of the configuration management system, including CI types, naming conventions, attributes and relationships. Ensuring the integrity of the configuration management system, including the CI data model and relationships. Defining and coordinating Configuration Analyst activities and responsibilities. Planning and managing support for Configuration Management tools and processes.
Configuration Analyst	<p>This role supports (and takes direction from) the Configuration Manager as the primary 'representative' for a specific CI category.</p> <p>Responsible for:</p> <ul style="list-style-type: none"> Contributes to defining the structure of the configuration management system, including CI types, naming conventions, required and optional attributes and relationships. Records and maintains CIs (within scope) in the CMDB Training staff in Configuration Management principles, processes and procedures. Performing configuration audits.

Role	Description
CI Owner	The CI Owner is responsible for the supporting, maintaining, controlling and updating of a specific CI or CIs. The CI owner is accountable for all activities that directly affect the actual CI. This role is also responsible for all ITSM process activities associated with the maintenance and support of the CI.
Stakeholder	All persons who have an interest in the information contained in the CMDB. Stakeholders may include employees, customers, partners, CI owners, and others.
Change Management	<ul style="list-style-type: none"> • Ensure that Change Request is used for any change to an existing CI attribute or when a CI is added to the CMDB • Ensure that information in Requests for Change (RFC) are accurate • Matching RFCs against affected CIs • Validating all scheduled changes occur • Notifying Configuration management that changes are complete

2.1. RACI Matrix

Roles and responsibilities are assigned to specific process activities.

ID	Activities	Change Management	CI Owner	Stakeholders	Configuration Analyst	Configuration Manager	Process Owner
CFG	Process Planning and Design						
CFG P.1	Produce Configuration Management Plan			C	C	R	A/R
CFG P.2	Define CMDB Structure			C	C	R	A/R
CFG P.4	Determine CI Selection Guidelines			C	C	R	A/R
CFG P.3	Populate CMDB				C	A/R	
CFG P.4	Perform Initial Audit			C	R	A/R	C
CFG P.5	Baseline CMDB			I	I	A/R	I
CFG 1.0	Configuration Identification						
CFG 1.1	Evaluate New CI Type to be Created		C		R	A/R	
CFG 1.2	Assign Unique Identifier				R	A/R	
CFG 1.3	Specify Relevant Attributes		C		R	A/R	
CFG 1.4	Specify Appropriate Relationship(s)		C		R	A/R	
CFG 1.5	Publish New CI Type		I		R	A/R	I
CFG 2.0	Configuration Control						
CFG 2.1	Validate Update Request		C			A/R	
CFG 2.2	Validate CI Attributes		I		A/R		
CFG 2.3	Review Invalid Attributes		A/R		C		
CFG 2.4	Update CMDB		I		A/R		
CFG 3.0	Status Accounting and Reporting						
CFG 3.1	Authorize or Reject Report Request		I		R	A/R	
CFG 3.2	Create or Update Configuration Management Report				R	A/R	
CFG 3.3	Generate Configuration Management Report				R	A/R	
CFG 3.4	Distribute Configuration Management Report		I		R	A/R	
CFG 4.0	Verification and Audit						
CFG 4.1	Approve Verification & Audit Request					A/R	
CFG 4.2	Execute Audit				A/R	C	
CFG 4.3	Reconcile with CMDB				A/R		
CFG 4.4	Determine Corrective Action		A/R		I		
CFG 4.5	Initiate Corrective CMDB Action				A/R		
CFG 4.6	Execute Corrective Action		I		A/R		
	R: Responsible, A: Accountable C: Consulted, I: Informed						

3 Configuration Management Activity Description

3.1 Process Overview

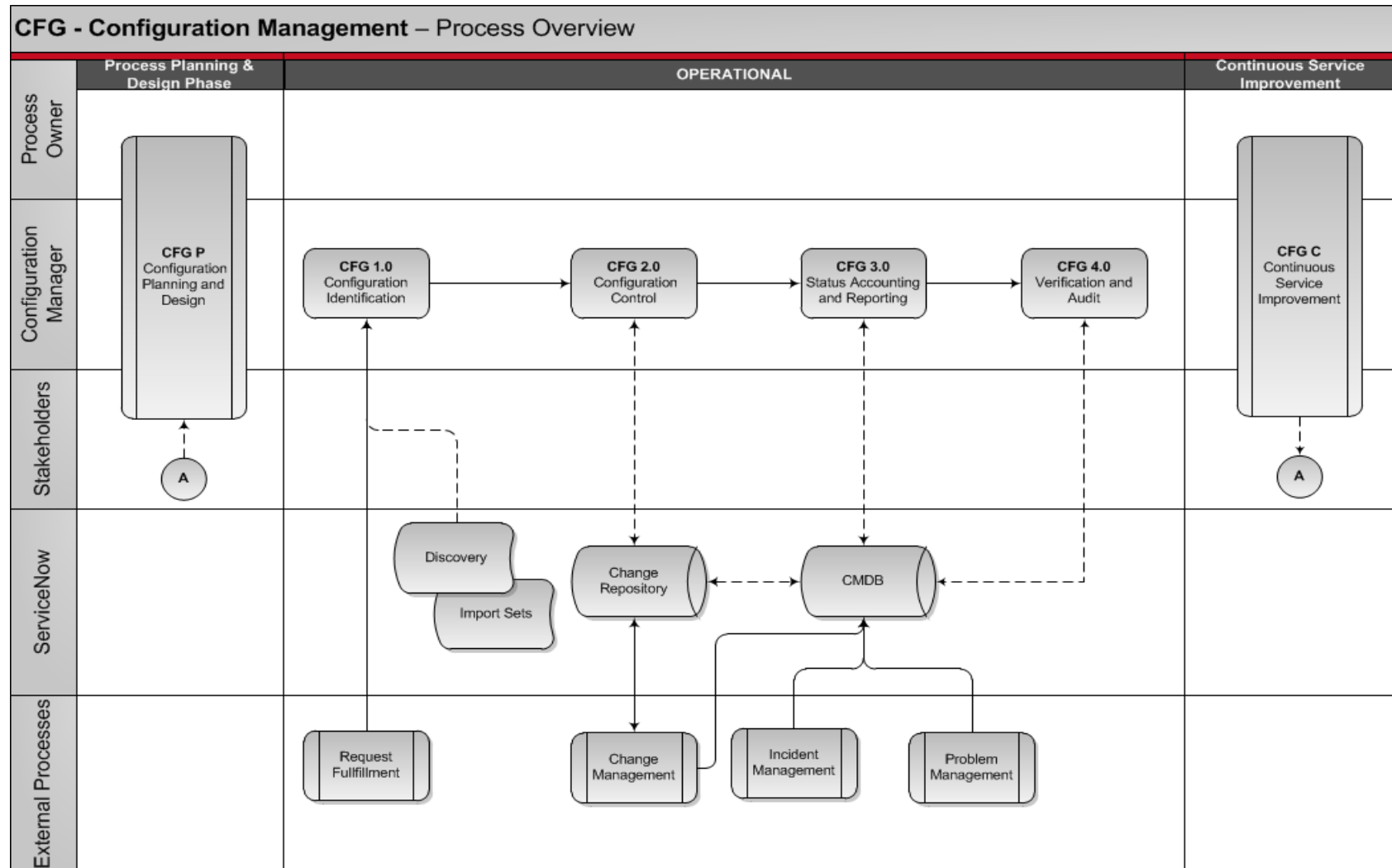


Figure 1: Process Overview

Process Overview Activity Description

ID	Activity	Description
CFG P	Process Planning and Design	The process planning and design Planning activity is the initial activity when the process is first being implemented. It is also being reviewed periodically (under Continuous Service Improvement initiatives), to keep the Configuration Management process in tune with the needs and capabilities of the business and all its supporting processes.
CFG 1.0	Configuration Identification	This activity determines the scope and criteria of CIs to be included in the CMDB. This includes the modeling of the infrastructure to determine what CIs will look like and how they are related to each other. It also includes the elaboration of naming conventions, enterprise taxonomy and the CI selection.
CFG 2.0	Configuration Control	Configuration Control is the activity responsible for ensuring that only authorized and identifiable CIs are in the infrastructure and that there is a corresponding accurate and complete CI record representing the CI in the CMDB. Updates to the CMDB are governed by the Configuration Control activity. Unauthorized Changes are forwarded to Change Management for instructions on how to proceed. Discrepancies and errors in the CI configuration are forwarded to the CI Owner for resolution.
CFG 3.0	Status Accounting and Reporting	This activity consists in the production of reports on the current, past and future status of the infrastructure and the CIs under the control of Configuration Management.
CFG 4.0	Verification & Audit	This activity involves the review and verification of the physical existence of CIs to check that they are correctly recorded in the CMDB. When discrepancies are found, Configuration Management consults Change Management for instructions on what corrective action to execute. There are two possible actions, update the CMDB to reflect what is actually in the infrastructure or change the CI to match the CMDB.
CFG C	Continuous Service Improvement	Ongoing activities to regularly measure and monitor the efficiency and effectiveness of the process and identify, plan and implement improvements.

3.2 Process Planning and Design

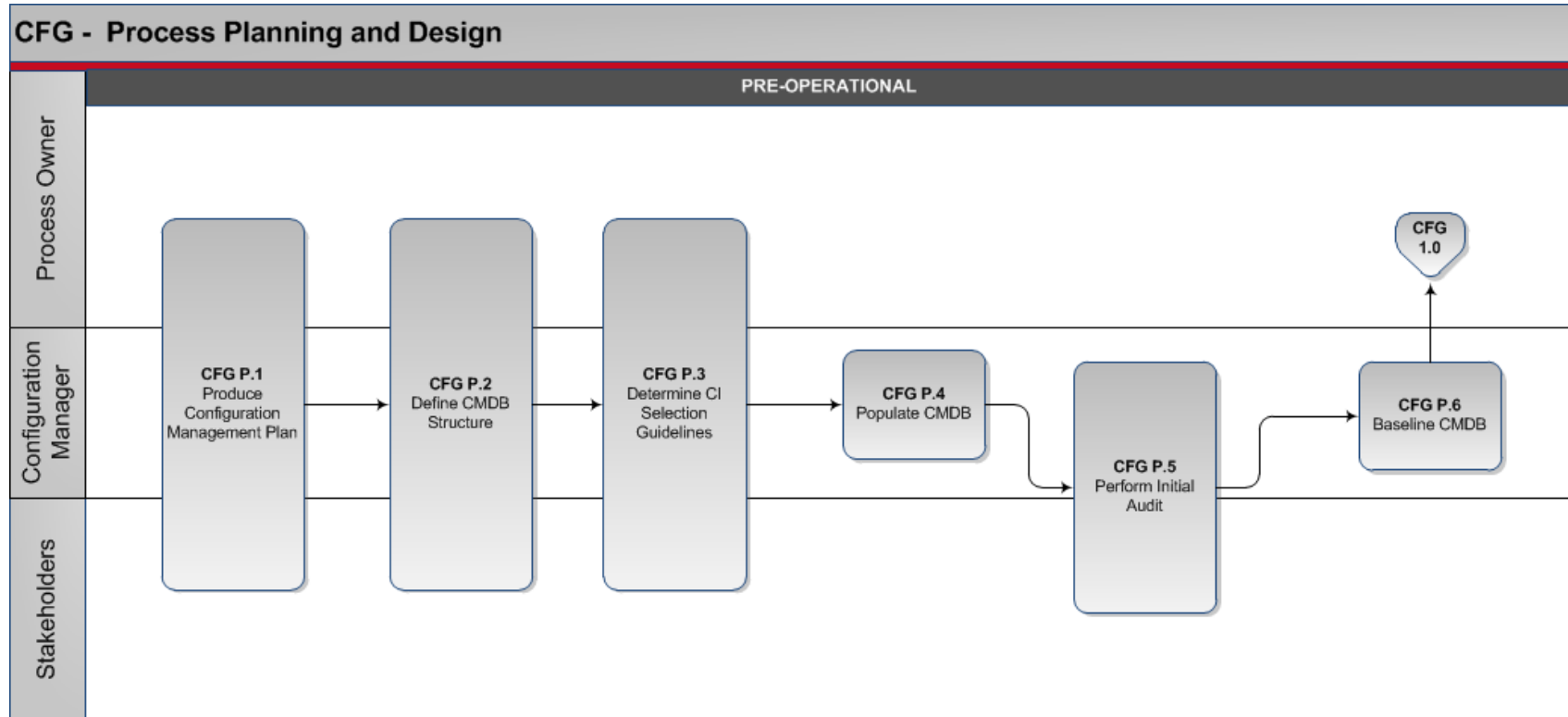


Figure 2: Process Planning and Design



In order for Configuration Management process to reflect enterprise goals and objectives It is important that a set of stakeholders be identified from a representative cross section of the organization. This stakeholder group should include members with both a good appreciation for the business needs as well as some knowledge of the technical aspects of managing the configurations of the IT infrastructure.

Process Planning and Design Activity Description

ID	Tasks	Description
CFG P.1	Produce Configuration Management Plan	<p>For the Configuration Management plan to reflect the business needs, and for the CMDB to efficiently support the business and its different services it is important that a set of stakeholders be identified from a representative cross section of the organization. The following items are examples of what the management team and stakeholders should define and document:</p> <ul style="list-style-type: none"> • Scope <ul style="list-style-type: none"> ○ Applicable services ○ Environments and infrastructure • Requirements <ul style="list-style-type: none"> ○ Link to policy, strategy ○ Link to business, service management and contractual requirements • Policies <ul style="list-style-type: none"> ○ Industry standards, e.g. ISO/IEC 20000 ○ Internal standards, e.g. hardware standards, desktop standards • Categorization and Prioritization of CIs • Labeling of CIs <ul style="list-style-type: none"> ○ As all physical device CIs should be labeled with a configuration identifier, plans should be made to label CIs and to maintain accuracy of their labels. • Naming Convention <ul style="list-style-type: none"> ○ Configuration Management must be able to uniquely identify each CI. Ideally the names should be automatically generated; otherwise the maintenance and effort to create and maintain names throughout the enterprise will be very substantial. • Attributes <ul style="list-style-type: none"> ○ Attributes describe the characteristics of a CI that are valuable to record and which will support Configuration Management and the ITSM processes it supports. <p>Relationships:</p> <p>Relationships provide structure to the CMDB; they represent how CIs relate to each other to deliver the services. They are also used to create service maps; analyze the impact of a change or an incident; evaluate the risk associated to a proposed change, and to build a logical model of the infrastructure. See Defining CI Relationships in the ServiceNow Wiki for a description of the ServiceNow tools and recommended approach for defining your CI relationships and making the CMDB a powerful decision tool.</p>

CFG P.2	Define CMDB Structure Model	<p>Defining the CMDB structure model is a key activity that contributes in making the CMDB a powerful decision support tool.</p> <p>However, because each customer has a unique environment, it is important that the appropriate level of information that is required for each CI types or classes is properly defined and agreed on by the different stakeholders.</p> <p>The CMDB structure model should describe the relationship and position of CIs in each structure. There should be service configuration structures that identify all the components in a particular service (see figure 3: CMDB Structure Model Example).</p>
CFG P.3	Determine CI Selection Guidelines	<p>The selection of CIs and level to which they are defined are very important parameters in the design of the CMDB. Selecting a CI level that is too granular can make the CMDB difficult to manage.</p> <p>On the opposite, a CMDB containing CIs at a high level may not meet the operational requirements of the supported processes.</p>
CFG P.4	Populate CMDB	<p>This activity involves the creation of CI records in the CMDB for each CI that has previously been identified as part of the initial integration. Consult the following Wiki articles to evaluate the different ways for importing data in the CMDB:</p> <ul style="list-style-type: none"> • Getting Started with Agentless Discovery describes how the Discovery plugin can collect information on network-connected hardware, the different applications and software that runs on that hardware and the relationships between all of the items found. • Importing Data Using Import Sets provides information on how to integrate data with existing external CMDBs or by simply using a CSV file.
CFG P.5	Perform Initial Audit	<p>To ensure the accuracy and of the imported data in the CMDB, perform an initial audit based on sampling criteria agreed in the Configuration Management Plan.</p> <p>Examples of sampling criteria could be:</p> <ul style="list-style-type: none"> • A predefined percentage of each CI category and their attributes to be captured • Only certain CI types or classes • Integrity of the relationships between CIs related to predefined service(s) <p>The results of the audit should be compiled and a report on the accuracy of the initial CMDB data should be submitted to all identified stakeholders for review.</p>
CFG P.6	Baseline CMDB	<p>To facilitate the tracking of the different changes that will be made in the CMDB, we recommend that a baseline of the audited CIs be made, before moving the initial data into the “Production” instance.</p> <p>Consult the Baseline CMDB article in the Wiki for more details and instructions.</p>

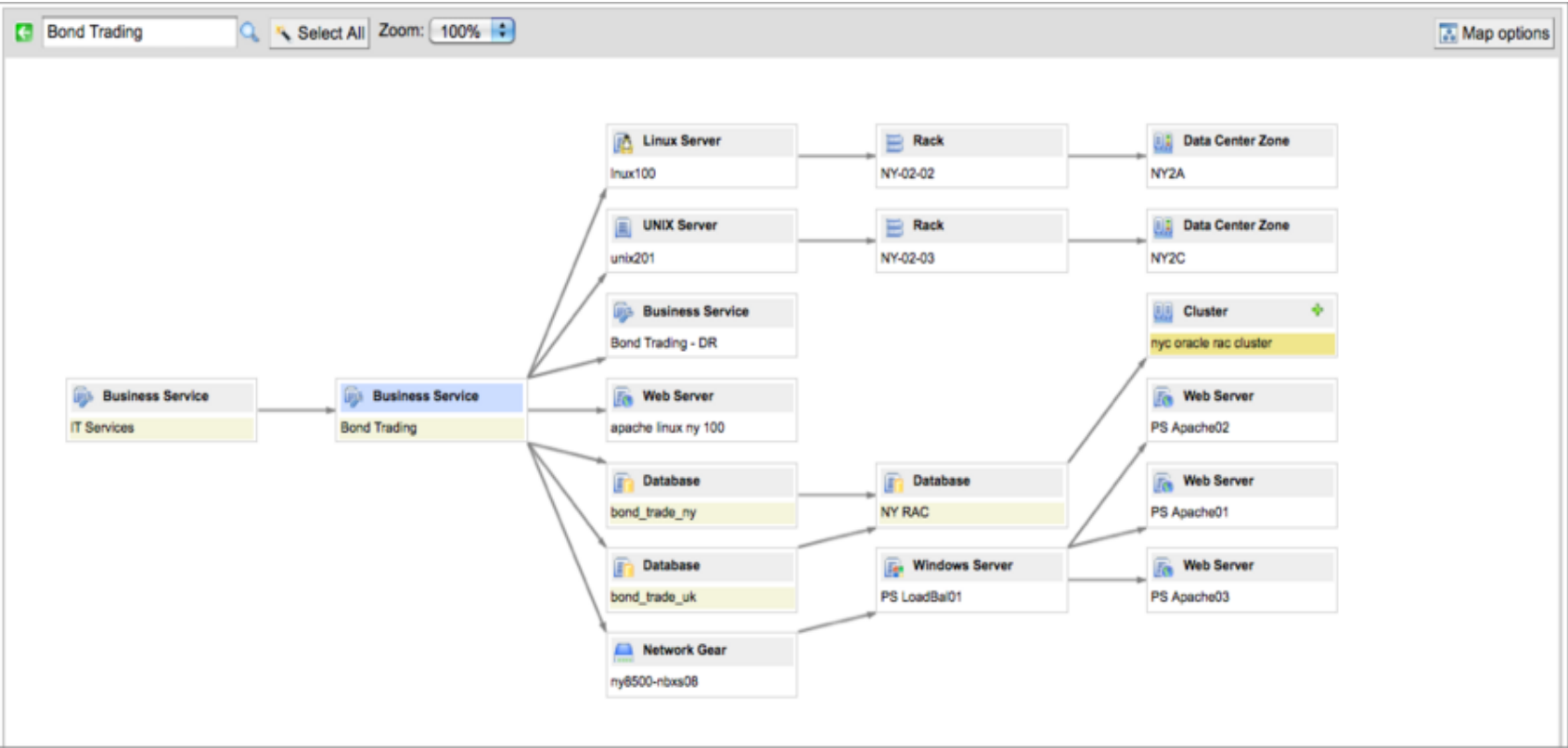


Figure 3: CMDB Structure Model Example

3.3 Configuration Identification

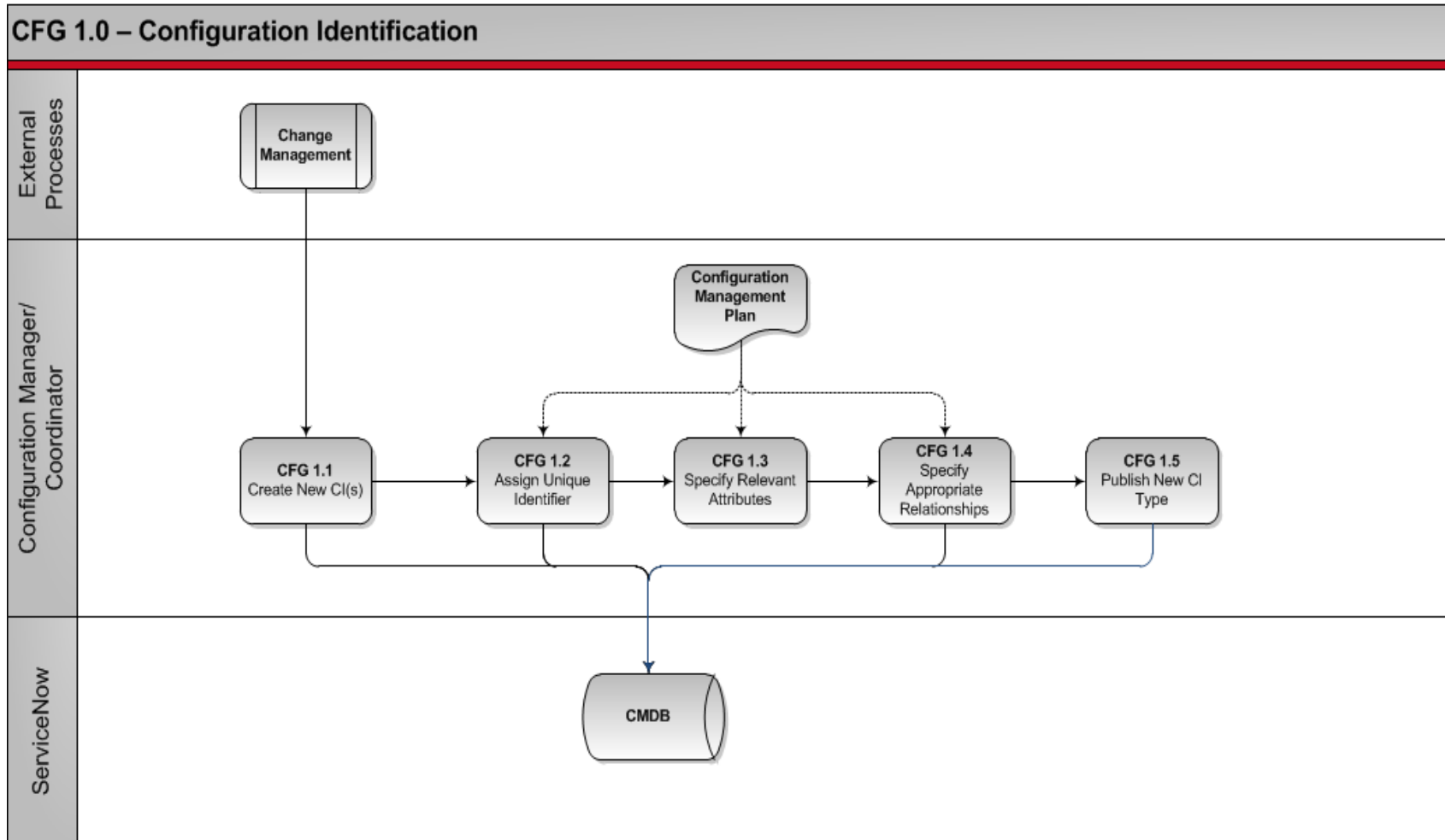


Figure 4: Configuration Identification

Configuration Identification Activity Description

ID	Tasks	Procedure	Primary Role	Input	Output
CFG 1.1	Evaluate New CI Type to be Created	This activity involves the addition or creation of new CI types, attributes or relationships that have not already been covered in the Configuration Management Plan. Evaluate the request and determine the new CI type to be created based on the information from the Configuration Plan.	Configuration Manager/ Coordinator	<ul style="list-style-type: none"> Change Request Configuration Management Plan 	New CI type identified
CFG 1.2	Assign Unique Identifier	Assign Unique Identifier to the New CI Type identified.	Configuration Manager/ Coordinator	New CI type identified	New CI type with assigned Unique Identifier
CFG 1.3	Specify Relevant Attributes	Identify the necessary attributes for the New CI Type. Consult the Reference Fields Wiki article for more information on creating reference fields on a table record.	Configuration Manager/ Coordinator	New CI type with assigned Unique Identifier	Defined attributes for new CI type
CFG 1.4	Specify Appropriate Relationship(s)	Specify the appropriate relationship(s) to be for the New CI Type.	Configuration Manager/ Coordinator	Defined attributes for New CI Type	New CI type associated with appropriate relationship(s)
CFG 1.5	Publish New CI Type	Publish the New CI type in the production CMDB.	Configuration Manager/ Coordinator	New CI type associated with appropriate relationship(s)	New CI Type Published

3.4 Configuration Control

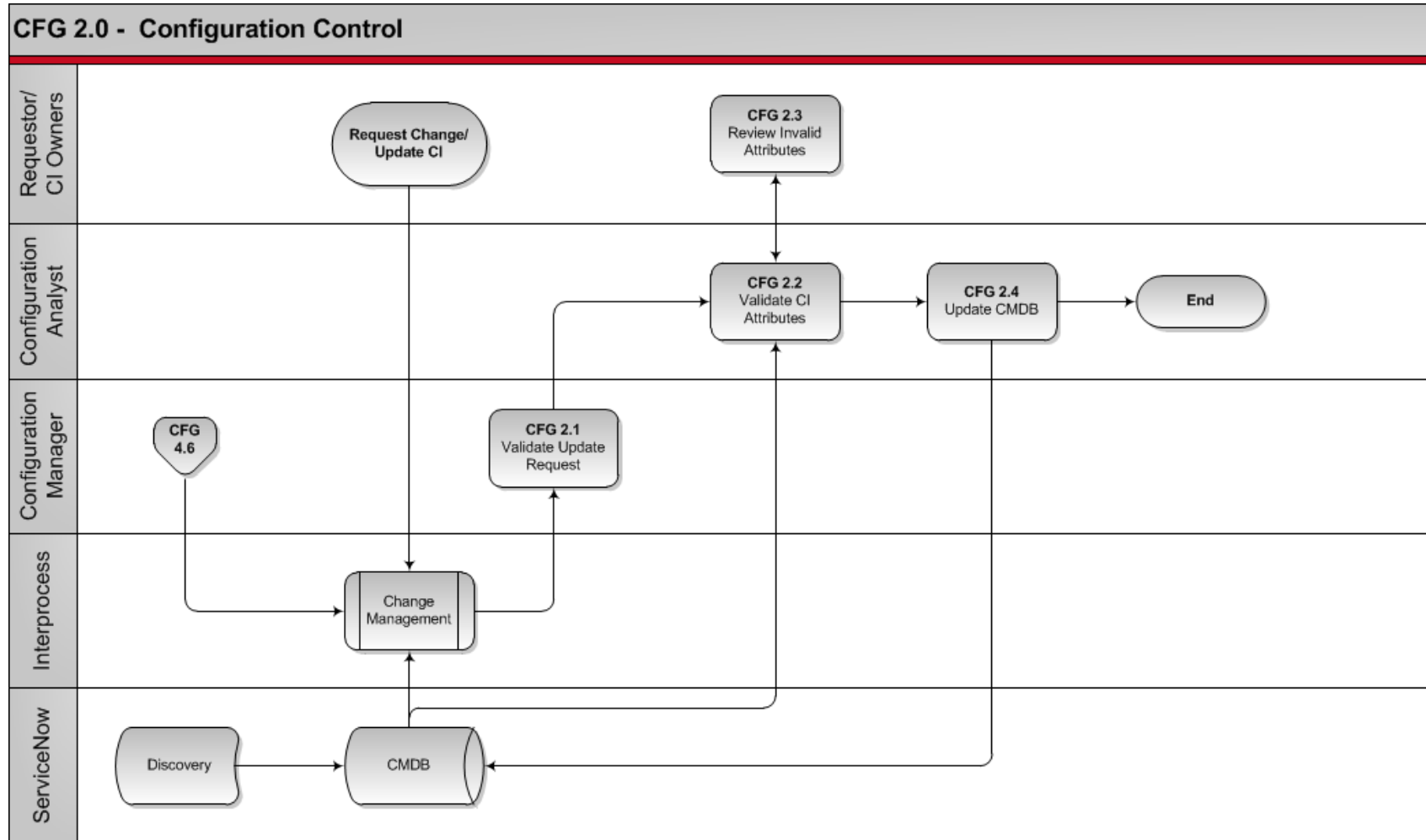


Figure 5: Configuration Control

Configuration Control Activity Description

ID	Tasks	Procedure	Primary Role	Input	Output
CFG 2.1	Validate Update Request	<p>The Configuration Manager receives a request to enter a new CI record or update an existing CI record.</p> <p>Authorized requests are prioritized and forwarded to a Configuration Management Analyst for further processing.</p> <p>Rejected requests are returned to the Requestor with an explanation of the rejection.</p> <p>In the case of new CI(s) identified by Discovery, verify that an authorized Request exists to justify the presence of the discovered CI(s).</p>	Configuration Manager	<p>Assigned Task from a Request for Change (RFC)</p> <p>New CI Identified by Discovery</p>	<p>Valid request ready to be processed</p> <p>OR</p> <p>Rejected request</p>
CFG 2.2	Validate CI Attributes	<p>For New CI Requests, validate that the proposed CI Attributes meet the requirements of Configuration Management as defined in the Configuration Management Plan.</p> <p>If all the proposed CI Attributes meet the criteria, the request is approved for updating the CMDB.</p> <p>For CI Attributes that fail to meet the Configuration Management Plan criteria, reject the request and inform the CI Owner with proper instructions.</p>	Configuration Analyst	Valid request ready to be processed	<p>New CI ready to be created in the CMDB</p> <p>OR</p> <p>CI with invalid attributes identified</p>
CFG 2.3	Review Invalid Attributes	Review the submitted instructions for defining proper CI attributes and submit a new request.	CI Owner	CI with invalid attributes identified	Revised Invalid attributes
CFG 2.4	Update CMDB	Publish the valid and authorized CI data into the CMDB.		New CI ready to be created in the CMDB	New CI published in the CMDB

3.5 Status Accounting and Reporting

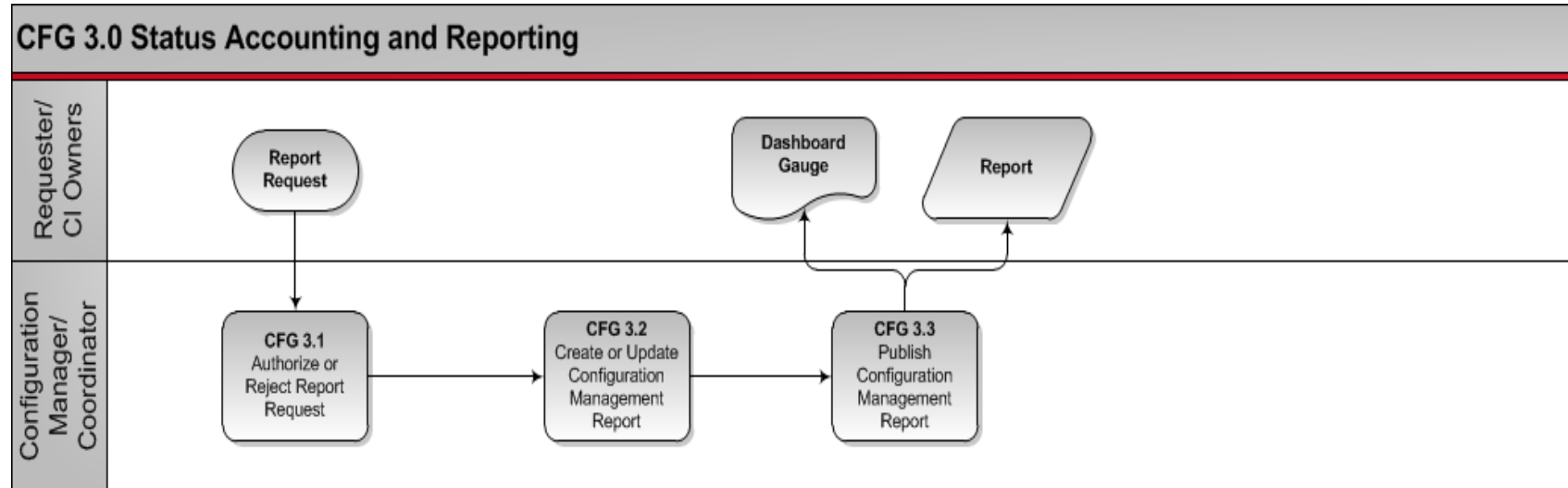


Figure 6: Status Accounting and Reporting

Status Accounting and Reporting Activity Description

ID	Tasks	Procedure	Primary Role	Input	Output
CFG 3.1	Validate Report Request	Review the submitted Report Request and validate if the request is for an existing report or gauge.	Requestor	New Configuration Management Report Request	Valid or Invalid Report Request
CFG 3.2	Create or Update Configuration Management Reports	For valid requests, create new Configuration report or gauge as requested. See the Creating Report Wiki article for more information for detailed procedures.	Configuration Manager/ Coordinator	Valid Report Request	New Configuration Management Report or Gauge read
CFG 3.3	Publish Configuration Management Report	Publish the created report or gauge and send the provided link to the requester.	Configuration Manager/ Coordinator	New Configuration Management Report or Gauge read	Published Report or Gauge accessible by requester

3.6 Verification and Audit

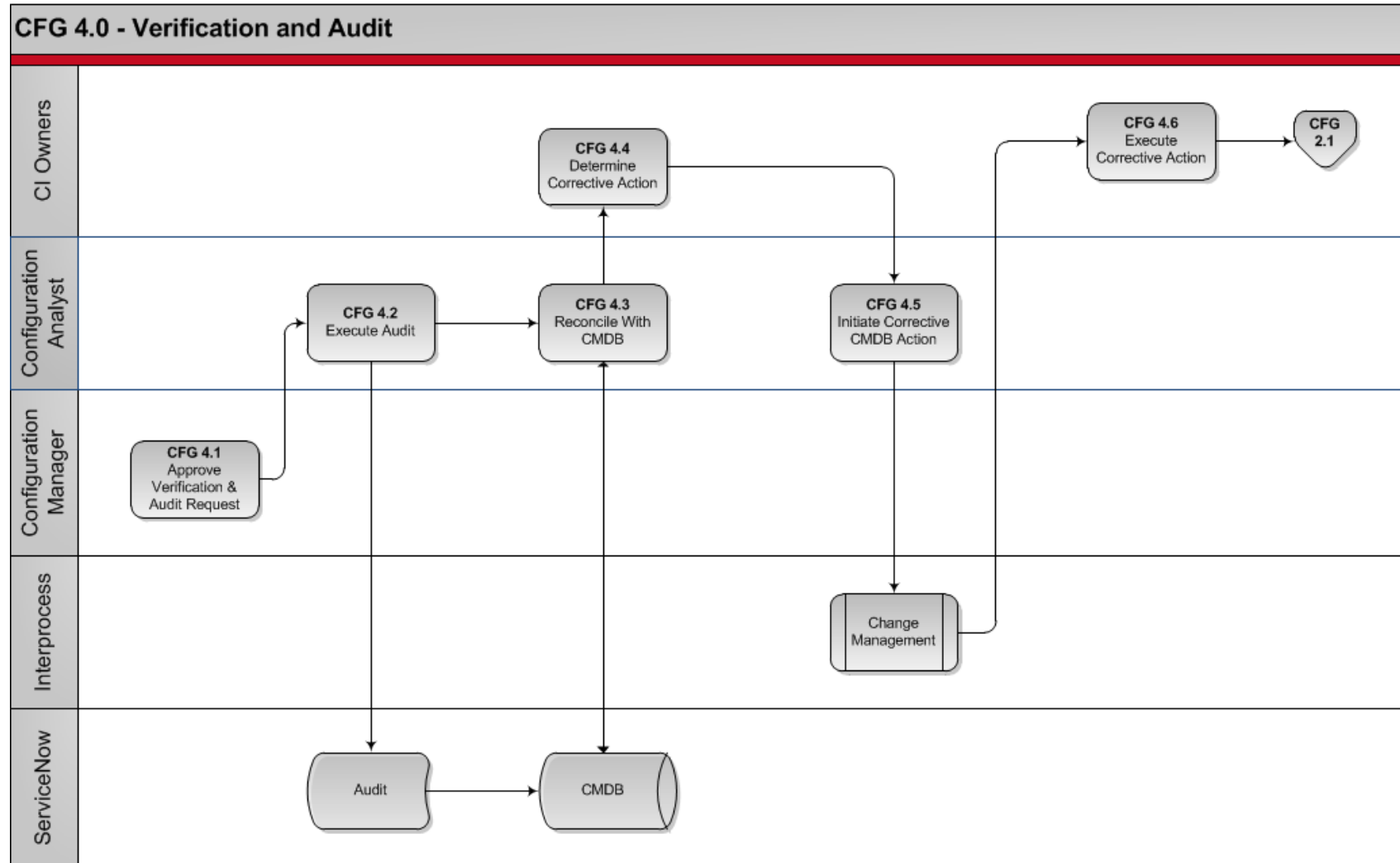


Figure 7: Verification and Audit

Verification and Audit Activity Description

ID	Tasks	Procedure	Primary Role	Input	Output
CFG 4.1	Authorize or Reject Verification Request	A request for Verification & Audit is approved or rejected by the Configuration Manager. Rejected requests are returned to the requestor with an explanation.	Configuration Manager	Request for Verification & Audit	Authorized Verification & Audit Request OR Rejection Information sent to requester
CFG 4.2	Execute Audit	Depending on the scope of the Verification or Audit Request, the Configuration Analysts performs a physical inspection or via Discovery.	Configuration Analyst	Authorized Verification & Audit Request	Documented results from verification & audit
CFG 4.3	Reconcile with CMDB	Review the compiled results from the audit and compare with CI Record information found in the production CMDB.	Configuration Analyst	Documented results from verification & audit	Reconciliation with production CMDB results
CFG 4.4	Determine Corrective Action	If discrepancies exist between the information contained in the CMDB and the actual CI(s), there are only two possible actions: <ul style="list-style-type: none"> • The most common action consists in updating the CMDB to reflect what is actually in the infrastructure • The second possible action would be to change the CI to match the information in the CMDB (e.g. an unauthorized and untested, perhaps unstable, CI is in production and must be removed). The task of correction is passed to the CI Owner. 	Configuration Analyst	Reconciliation with production CMDB results	CMDB information to be corrected OR CI to be modified to reflect information from CMDB
CFG 4.5	Update CMDB	Update the CMDB so that the CI record matches the "As Is" CI configuration in the infrastructure.	Configuration Analyst	CMDB information to be corrected	Corrected CMDB discrepancies
CFG 4.6	Execute Corrective CI Actions	Change the configuration of the actual CI so that it matches the CMDB CI record.	CI Owner	CI to be modified to reflect information from CMDB	CI matching information in CMDB CI record

4 Process Control

Process controls represent the policies and guiding principles on how the process will operate. Controls provide direction over the operation of processes and define constraints or boundaries within which the process must operate.

Name	Description
Audits	The frequency of configuration audits
Policies	Policies and criteria for the inclusion of a component and its attributes in the CMS.
Security Policies	Security policies governing access to the CMS.
Data Exchange Policies	Policy and criteria for the exchange of data between the CMDB and Configuration Systems Management repositories.
Scope	The scope of the Configuration Management process. Includes identification of what is included in and what is excluded from the Configuration Management process.
Change Management Policies	Change Management Policies and procedures.
Management Reports	The frequency and distribution for regularly produced management reports.
Database Backups	Frequency of CMS, CMDB and DSL housekeeping activities (i.e., backup, archive)
Systems Management Architecture	The architecture providing direction on how Systems Management tools and processes are to be selected, designed and integrated

4.1 KPIs

KPIs are best represented as trend lines and tracked over time. They provide information on the effectiveness of the process and the impact of continuous improvement efforts.

KPI/Metric	Purpose
Quality and accuracy of configuration information	Measure of how well an accurate and complete configuration management system is established and maintained.
Increase in re-use and redistribution of under-utilized resources and assets	Accounting for, managing and protecting the integrity of CIs throughout the service lifecycle
Reduced number of exceptions reported during configuration audits	Accounting for, managing and protecting the integrity of CIs throughout the service lifecycle
Number of RFCs without corresponding CI updated in CMDB	Measure of how well an accurate and complete configuration management system is established and maintained.





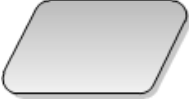


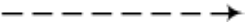

4.2 Reports & Homepage Gauges

There are numerous out-of-box reports available in ServiceNow that can be used to generate charts, publish to a URL, or schedule to be run and distributed at regular intervals. Users can also create custom reports. See [Creating Reports](#) in the Wiki for more detail on this capability.

In addition to reports, each user can create a personal homepage and add gauges containing up-to-the-minute information about the current status of records that exist in ServiceNow tables. See [Customizing Homepages](#) in the Wiki for details.

Appendices

Appendix A: Document Conventions

Symbol	Description
	Process start / end point: Represents the starting and ending point of the process.
	Process Activity/Task: Presents an activity or task that needs to be accomplished to produce a specific outcome.
	Predefined external process or organization: Indicated a contribution from an external process or organization.
	Decision: Indicates that a question needs to be answered in order to determine the in order to identify the following Activity/task in the process. The answers are indicated on the different connectors attached to the decision box. Every answer is linked to an associated Activity/task.
	System Action or Function: Indicates that an action is being performed in the system as an output of the previous activity and an input to the next.
	Off-page reference: Indicates a reference to another diagram within the same process. The number of the referenced diagram is indicated in the shape.
	On-page reference: Indicates a link to another activity within the same diagram.
	Association: Represented by a dotted or dashed line, it indicates an association or a relation between the connected, processes, tasks or activities.
	Sequence flow: Is represented with a solid line and arrowhead, and shows in which order the activities are performed.

Appendix B: Glossary of Terms and Acronyms

Term	Acronym	Definition
Alert		A notification that a threshold has been reached, something has changed, or a failure has occurred. Alerts are often created and managed by system management tools and are managed by the event management process.
Assessment		Inspection and analysis to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met.
Attribute		A piece of information about a configuration item. Examples are name, location, version number, and cost. Attributes of CIs are recorded in the configuration management database (CMDB).
Back-out		An activity that restores a service or other configuration item to a previous baseline. Back-out is used as a form of remediation when a change or release is not successful.
Baseline		<p>(ITIL <i>Continual Service Improvement</i>) (ITIL <i>Service Transition</i>) A snapshot that is used as a reference point. Many snapshots may be taken and recorded over time but only some will be used as baselines. For example:</p> <ul style="list-style-type: none"> ▪ An ITSM baseline can be used as a starting point to measure the effect of a service improvement plan ▪ A performance baseline can be used to measure changes in performance over the lifetime of an IT service ▪ A configuration baseline can be used as part of a back-out plan to enable the IT infrastructure to be restored to a known configuration if a change or release fails.
Category		A named group of things that have something in common. Categories are used to group similar things together.
Change		The addition, modification, or removal of anything that could have an effect on IT services.
Change Advisory Board	CAB	A group of people who support the assessment, prioritization, authorization, and scheduling of changes. A change advisory board is usually made up of representatives from all areas within the IT service provider, the business, and third parties such as suppliers.
Change Management	CHG	The process responsible for controlling the life cycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services.

Term	Acronym	Definition
Change Record		A record containing the details of a change. Each change record documents the life cycle of a single change. A change record is created for every request for change.
Change Request		See Request for Change.
Configuration Record	CI Record	A record containing the details of a configuration item. Each configuration record documents the lifecycle of a single configuration item. Configuration records are stored in a configuration management database and maintained as part of a configuration management system.
Configuration Type	CI Type	A category that is used to classify configuration items. The CI type identifies the required attributes and relationships for a configuration record. Common CI types include hardware, document, and user.
Classification		The act of assigning a category to something. Classification is used to ensure consistent management and reporting. CIs, incidents, problems, and changes are usually classified.
Closed		The final status in the life cycle of an incident, problem, or change. When the status is closed, no further action is taken.
Closure		The act of changing the status of an incident, problem, or change to closed.
Configuration Item	CI	Any component or other service asset that needs to be managed in order to deliver an IT service. Information about each configuration item is recorded in a configuration record within the configuration management system and is maintained throughout its life cycle by service asset and configuration management.
Configuration Management Database	CMDB	A database used to store configuration records throughout their life cycle. The configuration management system maintains one or more CMDBs. Each CMDB stores attributes of CIs and relationships with other CIs.
Configuration Management System	CMS	A set of tools, data, and information that is used to support service asset and configuration management. The CMS is part of an overall service knowledge management and includes tools for collecting, storing, managing, updating, analyzing, and presenting data about all configuration items and their relationships. The CMS also includes information about incidents, problems, known errors, changes, and releases. It may contain data about employees, suppliers, locations, business units, customers, and users. The CMS is maintained by service asset and configuration management and is used by all IT service management processes.

Term	Acronym	Definition
Configuration Record		A record containing the details of a configuration item. Each configuration record documents the life cycle of a single configuration item.
Continual Service Improvement	CSI	Ensures that services are aligned with changing business needs by identifying and implementing improvements to IT services that support business processes. The performance of the IT service provider is continually measured and improvements are made to processes, IT services, and IT infrastructure in order to increase efficiency, effectiveness, and cost effectiveness.
Customer		Someone who buys goods or services. The customer of an IT service provider is the person or group who defines and agrees to the service level targets. The term is also sometimes used informally to mean user, for example, 'This is a customer-focused organization.'
Diagnosis		A stage in the incident and problem life cycles. The purpose of diagnosis is to identify a workaround for an incident or the root cause of a problem.
Effectiveness		A measure of whether the objectives of a process, service, or activity have been achieved. An effective process or activity is one that achieves its agreed objectives. <i>See also</i> Key Performance Indicator.
Efficiency		A measure of whether the right amount of resource has been used to deliver a process, service, or activity.
Emergency Change		A change that must be introduced as soon as possible, for example to resolve a major incident or implement a security patch. The change management process normally has a specific procedure for handling emergency changes.
Employee Self Service	ESS	A module in ServiceNow that allows users to make requests, view articles, log incidents, and search the knowledge base through a user-friendly website called the Employee Self-Service Portal (ESS Portal).
Event		A change of state that has significance for the management of an IT service or other configuration item. The term is also used to mean an alert or notification created by any IT service, configuration item, or monitoring tool.
Impact		A measure of the effect of an incident, problem, or change on business processes. Impact is often based on how service levels will be affected. Impact and urgency are used to assign priority.
Incident		An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident.

Term	Acronym	Definition
Key Performance Indicator	KPI	A metric that is used to help manage an IT service, process, plan, project, or other activity. Many metrics may be measured, but only the most important of these are defined as key performance indicators and used to actively manage and report on the process, IT service, or activity. They should be selected to ensure that efficiency, effectiveness, and cost effectiveness are all managed.
Known Error	KE	A problem that has a documented root cause and a workaround. Known errors are created and managed throughout their life cycle by problem management. Development groups or suppliers may also identify known errors.
Major Incident		The highest category of impact for an incident. A major incident results in significant disruption to the business.
Metric		Something that is measured and reported to help manage a process, IT service, or activity.
Policy		Formally documented management expectations and intentions. Policies are used to direct decisions and to ensure consistent development and implementation of processes, standards, roles, activities, IT infrastructure, and so on.
Post-implementation Review	PIR	A review that takes place after a change or a project has been implemented. It determines if the change or project was successful and identifies opportunities for improvement.
Priority		A category used to identify the relative importance of an incident, problem, or change. Priority is based on impact and urgency, and is used to identify required times for actions to be taken. For example, the SLA may state that priority 2 incidents must be resolved within 12 hours.
Problem		A cause of one or more incidents. The cause is not usually known at the time a problem record is created. The problem management process is responsible for further investigation.
RACI	RACI	A model used to help define roles and responsibilities. RACI stands for responsible, accountable, consulted, and informed.
Release		One or more changes to in IT service that are built, tested, and deployed together. A single release may include changes to hardware, software, documentation, process, and other components.
Request for Change	RFC	A formal detailed proposal for a change to be made. The term is often misused to mean change record or the change itself.
Restore		Taking action to return an IT service to the users after repair and recovery from an incident. This is the primary objective of incident management.

Term	Acronym	Definition
Risk		A possible event that could cause harm or loss or affect the ability to achieve objectives. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred.
Role		A set of responsibilities, activities, and authorities assigned to a person or team. A role is defined in a process or function. One person or team may have multiple roles. For example, a single person may carry out the role of configuration manager and change manager.
Root Cause		The underlying or original cause of an incident or problem.
Root Cause Analysis	RCA	An activity that identifies the root cause of an incident or problem. Root cause analysis typically concentrates on IT infrastructure failures.
Service		A means of delivering value to customers by facilitating the outcomes customers want to achieve without the ownership of specific costs and risks.
Service Desk		The single point of contact between the service provider and the users. A typical service desk manages incidents and service requests, and also handles communication with the users.
Service Level		Measured and reported achievement against one or more service level targets.
Service Level Agreement	SLA	An agreement between an IT service provider and a customer. A service level agreement describes the IT service; documents service level targets, and specifies the responsibilities of the IT service provider and the customer.
Service Request		A formal request from a user for something to be provided, for example, a request for information or advice; to reset a password; or to install a workstation for a new user.
Stakeholder		A person who has an interest in an organization, project, or IT service. Stakeholders may be interested in the activities, targets, resources, or deliverables. Stakeholders may include customers, partners, employees, shareholders, owners, or others.
User		A person who uses the IT service on a day-to-day basis. Users are distinct from customers, as some customers do not use the IT service directly.
Workaround		Reducing or eliminating the impact of an incident or problem for which a full resolution is not yet available, for example, by restarting a failed configuration item. Workarounds for problems are documented in known error records. Workarounds for incidents that do not have associated problem records are documented in the incident record.

Source: ITIL® glossary and abbreviations

© Crown copyright 2011. All rights reserved. Material is reproduced with the permission of the Cabinet Office under delegated authority from the Controller of HMSO.

ITIL® is a registered trade mark of the Cabinet Office