

---

A  
E  
T

# Configuration Management Process Guide

# Table of Contents

<b>1.</b>	<b>PREFACE .....</b>	<b>3</b>
<b>2.</b>	<b>MISSION.....</b>	<b>5</b>
<b>3.</b>	<b>OBJECTIVES.....</b>	<b>6</b>
3.1	INTRODUCTION.....	6
3.2	DEFINITIONS .....	6
3.3	OBJECTIVES .....	6
<b>4.</b>	<b>GUIDING PRINCIPLES.....</b>	<b>9</b>
4.1	INTRODUCTION.....	9
4.2	PRINCIPLES .....	9
<b>5.</b>	<b>SCOPE.....</b>	<b>11</b>
5.1	INTRODUCTION.....	11
5.2	XXXXX MANAGED ENVIRONMENT .....	11
5.3	HARDWARE CONFIGURATION ITEMS .....	11
5.4	SOFTWARE CONFIGURATION ITEMS .....	13
5.5	DOCUMENTATION CONFIGURATION ITEMS .....	14
<b>6.</b>	<b>PROCESS DESCRIPTION.....</b>	<b>15</b>
6.1	INTRODUCTION.....	15
6.2	PROCESS SUMMARY .....	15
6.3	CONFIGURATION MANAGEMENT PROCESS FLOW.....	17
6.4	CONFIGURATION MANAGEMENT SUB-PROCESSES.....	17
6.5	SUB PROCESS 1: PLAN AND MAINTAIN CONFIGURATION SCHEME ...	17
6.6	SUB PROCESS 2: MAINTAIN CONFIGURATION DATA.....	21
6.7	SUB PROCESS 3: AUDIT CONFIGURATION.....	25
6.8	SUB PROCESS 4: REPORTING CI INFORMATION.....	27
<b>7.</b>	<b>ROLES AND RESPONSIBILITIES .....</b>	<b>31</b>
<b>8.</b>	<b>MEASUREMENTS &amp; REPORTING .....</b>	<b>36</b>
8.1	INTRODUCTION.....	36
8.2	MEASUREMENTS .....	36
8.3	REPORTING .....	37
<b>9.</b>	<b>MEETINGS.....</b>	<b>42</b>
<b>10.</b>	<b>INTERRELATIONSHIPS WITH OTHER PROCESSES .....</b>	<b>44</b>

---

10.1	INTRODUCTION .....	44
10.2	SYSTEMS MANAGEMENT PROCESSES.....	44
10.3	BUSINESS MANAGEMENT PROCESSES.....	46
10.4	INTERRELATIONSHIP MATRIX .....	48

## Section

## 1

## 1. Preface

Successful management of business processes is dependent upon clear definition and consistent execution. This process guide is produced to reflect a management statement of direction. This guide binds the process by its scope and coverage, describes the major functions within the process, and sets forth standards for applying the process.

The following process has been designed to accommodate the various services offered by the XXXXX Information Technology (XXXXX I/T) organization. It encompasses both the components that may be deployed in the near-term and the strategies that may be pursued as the process matures. This process should be viewed as a “to-be” model towards which the organization evolves over time. For the sake of clarity, this guide refers to Information Technologies where applicable, in order to apply process concepts directly to XXXXX I/T.

While this guide serves as a road map for process deployment, it is also a living document. As process components are activated, a continuous improvement effort should be undertaken to capture lessons learned and opportunities to advance the process. When the process is fully deployed across XXXXX I/T, this guide should become a clear and consistent document of the accepted management approach in executing the process.

Most business processes are interdependent upon one another. Although this guide presents a comprehensive overview of a specific process, XXXXX I/T may discover other related processes that would benefit from an equally rigorous and disciplined approach in definition and documentation. In the sections describing “Scope and Coverage” and “Interrelationships with Other Processes,” this guide provides insights into some of these related processes.

In recognition of the unique requirements of different services, this process guide is structured to maintain a functional perspective of the process components. This guide aims to describe “What” functions need to be accomplished and not “How” those functions may be achieved via specific

tasks. Where appropriate, this guide may be supplemented with procedural amendments for a specific task or set of services.

## Section

## 2

## 2. Mission

In Defining the Mission of the Configuration Management Process, it was important to understand the business context in which it is being define. The key business drivers include:

- Integration of multiple gaming environments
- Support new technology deployments such as the Jupiter project (e-business services)
- Provide a foundation for improving customer satisfaction with IT services
- Improve operational effectiveness & efficiency through the implementation of standardized processes

With this in mind, the mission of this process was defined as follows:

*Configuration Management will cover the identification, recording, and reporting of all IT components within the XXXXX environment (including their current versions, constituent components, and relationships). Timely and accurate information will be provided to all processes requiring configuration information.*

Section  
3

## 3. Objectives

### 3.1 Introduction

The primary objectives of XXXXX Incorporated Information Technologies (XXXXX I/T) configuration management process is to identify, document and create a repository for all hardware and software configurations in the I/T environment and to provide configuration information to the help desk, change management, problem management, and other processes to effectively manage I/T resources.

### 3.2 Definitions

**Configuration Management:** Configuration Management can be defined as the logical and physical connectivity and relationships of physical assets and their internal characteristics.

.... IT IS NOT ....

**Procurement Management:** The purchase and receipt of a physical asset

**Asset Management:** The financial management of the physical asset

**Inventory Management:** The location of the physical asset (what and where)

**Release Management:** The controlled release of a software or documentation asset from development through test, and into production

### 3.3 Objectives

- With a clear understanding of the terms “configuration,” and “configuration management,” the objectives of the configuration management process can be defined:

The process for configuration management should be consistent across the organization, and should include standard documentation and reporting methods

Provide a single logical view of all IT components and connections needed to effectively deliver IT services to our customers. This view should include:

- A view of the authorized configuration. So, rather than reporting what is actually out there, the CMDB reflects the configuration we would like to see out there. Differences between the authorized and actual configuration are treated as exceptions that have to be resolved. In combination with data from other processes (change management, incident management, operations planning) the actual status at any given moment in time (past, present, future) can be reported, shown or predicted,
- An ability to identify, document, capture, organize and maintain readily accessible, accurate, and up-to-date information on configuration items, as identified in the process scope.
- An ability to store standard configuration scenarios (templates) to be used for procurement & project acquisitions

Timely and accurate configuration information is provided to all other processes within our environment

- The provision of prerequisite information to change management for activities such as device configuration, hardware additions and software distribution.
- The provision of consistent information to the help desk, problem management and incident management to effectively manage I/T resources and improve I/T client service delivery.
- Provide accurate and timely information on configuration to support any other Service Management process (i.e. Disaster Recovery, Capacity Planning, Procurement, Architectural Design, etc)
- Support the provision of business management impact information for decision making (i.e. change/problem device history for trend analysis and vendor management)

Reduce overall workload by integrating and automating existing configuration tools and procedures to support configuration management and other related processes

Provide a process that is adaptable enough to incorporate business or technology changes without significant rework



Provide the ability to verify configuration records against the infrastructure and correct any exceptions

## Section

## 4

## 4. Guiding Principles

### 4.1 Introduction

Why they are important and how they should be used

### 4.2 Principles

There will be one configuration management process (see Phase 1 in-scope items)

There will be a single process owner who will oversee the overall process and manage all changes to it and all linkages with other processes affecting it

All configuration information will be maintained in centralized repositories. This information will be available on demand to any process requiring it, including help desk, problem management, and change management

Only the Configuration Management Process Coordinator or designated service providers can update configuration information

Any configuration management tool will follow existing conceptual architecture principles supporting the ESM Domain architecture

All in-scope infrastructure elements required to go through Change management are covered by the Configuration Management process

The data in the CMDB should always accurately reflect the current (authorized) infrastructure status (this implies either automation or tool customization)

Configuration data will only be captured when there is a requirement from a service delivery & support process that can be supported by automation

The process should facilitate periodic review and validation of Configuration Items, Attributes, and Relationship requirements

The process should include procedures to validate and correct configuration data



## Section

## 5

## 5. Scope

### 5.1 Introduction

Because the configuration management process deals with I/T managed components within the XXXXX environment, it is imperative that XXXXX I/T personnel understand the scope of the process.

In this section, the scope of the process is outlined. This description includes areas that are both inside and outside of the process scope.

An important rule for determine if an Item is in scope is the Guiding Principle that states that: *“Configuration data will only be captured when there is a requirement from a service delivery & support process that can be supported by automation”*. This means that if there is no tool to verify the status of a Configuration Item, this item is out of scope. In this document the term auto-discovery is used to describe such tools.

### 5.2 XXXXX Managed Environment

Display logical architecture of IT environment here...

### 5.3 Hardware Configuration Items

#### **Introduction**

Because the CMDB will only contain Configuration Items of which the status can be verified in an automated fashion, one can read in the next tables which CIs are in scope.

The items are listed in four columns. The first one is to indicate if there is a tool that can provide auto-discovery for a Configuration Item. The second column lists if there are scripts or other means of verifying the status. The last two columns indicate if the status of a CI can be derived from an other administration.

**Change Initiated**

<b>Configuration Item (CI)</b>	<b>Auto Discovery</b>	<b>Scripts &amp; automation</b>	<b>Release Mgmt (DSL)</b>	<b>Doc Mgmt (DocSL)</b>
Computer Cluster	Yes			
Server	Yes			
Desktop	Yes			
Laptop		TBD		
Front End Processors	Yes			
Stand-Alone PC (network attached)	Yes			
Firewall	Yes			
Disk Farm	Yes			
Backup Unit	Yes			
Local Printer		TBD		
Network Printer	Yes			

**Change Initiated**

<b>Configuration Item (CI)</b>	<b>Auto Discovery</b>	<b>Scripts &amp; automation</b>	<b>Release Mgmt (DSL)</b>	<b>Doc Mgmt (DocSL)</b>
Palm Pilot		Later		
Router	Yes			
CISCO PIX	Yes			
Hub		TBD		
Switch		TBD		
Modems		TBD		
Local Directors		Later		
Patch Panel		Later		
Fax		Later		
Scanner		Later		
"Dumb" terminal		TBD		

Configuration Item (CI)	Change Initiated			
	Auto Discovery	Scripts & automation	Release Mgmt (DSL)	Doc Mgmt (DocSL)
Telephones		Later		
Cell Phones		Later		
Slot Machine		Later		
Retail Terminals		Later		
Switch Probes		Later		
FRAD		Later		
FDDI Lines		Later		
Leased Lines		Later		
PBX		Later		
UPS		Later		
Video Conference Equipment		Later		

## 5.4 Software Configuration Items

### Introduction

Configuration Item (CI)	Change Initiated			
	Auto Discovery	Scripts & automation	Release Mgmt (DSL)	Doc Mgmt (DocSL)
Operating System	Yes		TBD	
Programming Language	Yes		TBD	
System Tool	Yes		TBD	
Business App - Revenue Generating		TBD*	Later	
Business App - Business Enabling		TBD*	Later	
Application Database (SAN)		TBD*	Later	
External Interface			Later	
Application Module			Later	
Palm Software				

- \* includes current location and version information, but not version history or module hierarchy

## 5.5 Documentation Configuration Items

### Introduction

Configuration Item (CI)	Change Initiated			
	Auto Discovery	Scripts & automation	Release Mgmt (DSL)	Doc Mgmt (DocSL)
Service Level Agreement				Later
System Operations Guide				Later
Application Operations Guides				Later
Disaster Recovery Plan				Later
Software Licenses				Later
System Configuration Documents				Later

## Section

## 6

## 6. Process Description

### 6.1 Introduction

The detailed configuration management process is described in this section. A detailed explanation of the process and sub-processes is contained in the following pages and is meant to provide the participants in the configuration management process with an understanding of the general functional flow.

### 6.2 Process Summary

**Process Starts With**

- Change in Systems Management Controls
- Receipt of notice of a change in System or Service Design Information
- Initial capture of existing infrastructure
- Request for Change (Add, Modify, Remove a Configuration Item [CI])
- Requests for configuration information

**Ends With**

- Audit of configuration database against the installed infrastructure
- Creation of a logical representation of the current (and planned) infrastructure
- Provision of configuration information

**Process Design Includes**



- The complete lifecycle of a CI from planning through to retirement
- Flow of Data between the sub processes of the Configuration Management Process
- Flow of Data between the Configuration and other ESM Processes
- Activities per Sub process
- Roles per Activity

### **Process Design Excludes**

- Design activities for infrastructure components, both new or modifications to them
- Responsibility for authorization of changes
- Planning how and in what way configuration details should be represented

### **Process Controls**

- Service Management Controls
- Service Level Agreements
- Authorized Changes
- Infrastructure Design

### **Process Inputs**

- Configuration Details taken from Request For Changes [RFC]
- Verification Data taken from automated systems (auto discover)
- Verification Data taken from Physical checks
- Verification Data taken from Helpdesk calls

### **Process Outputs**

- Configuration Information
- Signalled differences between the authorized and actual configuration

## 6.3 Configuration Management Process Flow

Place ITIL Configuration Flow Here...

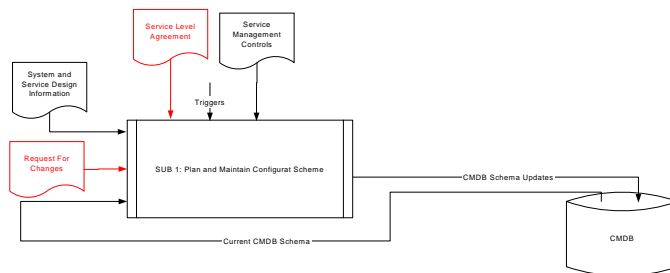
Figure 1. Configuration Management Sub-Process Flow

## 6.4 Configuration Management Sub-processes

The configuration management process itself can be broken down into several sub-processes:

- Sub 1: Plan and Maintain Configuration Scheme
- Sub 2: Maintain Configuration Data
- Sub 3: Audit Configuration
- Sub 4: Reporting Configuration Information

## 6.5 Sub Process 1: Plan and Maintain Configuration Scheme



### Purpose

The purpose of this Sub Process is to make sure that the schema of the Configuration Management Database [CMDB] is able to register all attributes and relationships a Configuration Item [CI] can have, and all policies involved with this. Therefore it needs to have knowledge about CIs and has to be kept informed about changes that influences CIs.

### Activities

A1.1 Run an Awareness Program

If change management will not be a part of the project office, we might need an awareness activity to promote the CMDB

A1.2 Gather & Review upcoming changes.

There has to be an active process of gathering changes. These changes can have several sources. -EWTA - Change Management – Projects. Each project that will be run must be examined for impact on the CMDB.

A1.3 Assess the impact of a change on the Schema of the CMDB.

Each identified change can potentially require a change for the policies or the schema of the CMDB. For instance when new infrastructure items are introduced, new CI types or new/different links between CIs.

A1.4 Design / Realize the changes needed on the Schema.

This activity designs and realizes the actual changes that are needed. This can also include conversions.

A1.5 Create and Maintain standard configurations ("Same-as").

Some configuration (parts) will be standardized. An example is the desktop. There will be a standard configuration, and a standard image installed on it. This activity defines those standards and maintains them as technology and requirements develop.

A1.6 Investigate the relationships types between new CI types.

There will be relations between CIs that cannot (easily) be automatically discovered. For instance which distributed database is being used by an application, or which network path a transaction takes to be processed. Still, it is very important to register these relationships for instance to do impact analysis. This activity analyses infrastructure designs, application architectures and work procedures to discover all the relationships a CI have with other CIs.

A1.7 Identify the owners of CI types.

For each CI type an owner has to be identified. This owner is the Subject Matter Expert for this CI type. The CI owner functions as a contact for information about the attributes, behaviour and relations of a CI type. This activity identifies and registers for each CI type an owner.

A1.8 Identify configuration Documentation for CI types.

Each CI type should be fully documented. The documentation should include the behaviour of a CI, information about the nature and values of attributes, and all relationships the CI has.

A1.9 Measure and report the performance of this sub process.

This activity measures and reports the performance of this sub process. The purpose is to have an objective way to measure the effectiveness of improvements to this process.

### **Key Performance Indicators**

- K1.1 Number of changes to the schema
- K1.2 Dates of latest changes.
- K1.3 Number of CI types without a identified owner
- K1.4 Number of CI types without configuration documentation
- K1.5 Number and severity of incidents related to missing attributes or registration of relationships

### **Controls**

#### C1.1 Service Management Controls

The Service Management Controls determine how configuration management is done. For instance the guiding principle “In phase one only Items that can be discovered (verified) automatically are put as a CI in the CMDB” determines the scope on CI type level.

#### C1.2 Service Level Agreements

The Service Level Agreements determine what, from a (IT) business perspective has to be registered.

### **Triggers**

- T1.1 New Request For Change [RFC]; Each Change has to be evaluated.
- T1.2 Changes in the infrastructure design that does not follow the change management process.
- T1.3 Changed Service Level Agreement
- T1.4 Changed Service Management Controls

### **Input**

- I1.1 Current CMDB Schema.
- I1.2 Request For Change  
A Request For Change from the Change Management Process
- I1.3 System and Service Design Information.  
A description of the Infrastructure design and changes to the Infrastructure that do not follow the Change Management Process.

### **Output**

- O1.1 CMDB Schema (updates)

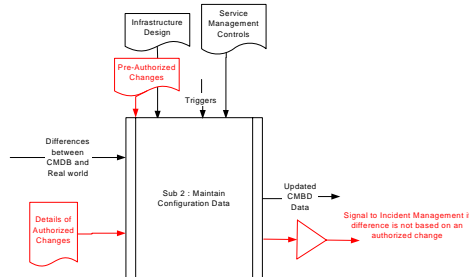
### **Skills (Roles)**

- S1.1 Process Owner (Management / Architect)
- S1.2 Database Specialist / Analyst
- S1.3 Infrastructure Specialist (Hardware, Software, Applications, Network)
- S1.4 Configuration Manager

**Tool Requirements**

- R1.1 Automated access to the change management / project information
- R1.2 Access to the CMDB schema
- R1.3 DB analysis/modeling functions
- R1.4 DB design functions
- R1.5 DB develop, test functions (develop/test/acceptation/production life cycle)
- R1.6 DB Conversion functions
  
- R1.7 A flexible Database (flexible for schema changes, relational versus Hierarchical)
- R1.8 The behaviour CMDB application must be controllable from the 'outside' (table driven, no recompiling after schema changes)
- R1.9 Possibility to register standard configurations (current done in EWTA)
- R1.10 Access to Infrastructure characteristics (network topology, application documentation)
- R1.11 Logging, tracking, reporting functions (# changes to schema, dates latest changes)

## 6.6 Sub process 2: Maintain Configuration Data



### Purpose

This Sub Process deals with registering information about the CIs that are managed by the Service Management System.

### Activities

A2.1 Identify authorized changes to the infrastructure (real world)  
 Changes to the infrastructure (real world) will be done based on a RFC (Request For Change) that has gone through the Change Management Process, and are therefore authorized. This activity identifies these changes and prepares them to be applied to the administered configuration in the CMDB.

A2.2 Identify list of pre-authorized types of changes.  
 There are changes to the infrastructure (real world) that do not go through the Change Management process, but are still to be administered in the CMDB. An example is the Token-ring port number a laptop connects to. This data is too volatile to be put through the Change Management Process. This means that if the validation process indicates that the administered configuration (CMDB) is not the same as the discovered infrastructure (real world) the new value is registered in the CMDB without raising an incident flag. This implies that in the example given, the token-ring port number of a laptop in the CMDB represents the 'last known' value, because changes on this attribute are pre-authorized. This activity identifies the list of pre-authorized changes. Maintains

A2.3 Validate changes (naming convention, completeness).  
 Authorized changes are validated on their completeness and compliance of the policies like the naming convention. This activity also validates the completeness of all documentation requirements and makes sure that the owners of each CI are known. This activity makes extensive use of Standard Configurations.

A2.4 Update the approved changes into the CMDB.  
 This activity updates the actual database entries based on the authorized changes. There are two techniques that can be used. Either the CMDB is

updated as soon as a change is authorized (the CMDB then reflects the authorized configuration). The other technique is to defer applying the change to the CMDB until the change is detected by the validation sub process. By combining the Change records, Configuration records of the CMDB this technique allows the CMDB to reflect the real world as closely as possible. Two special forms of RFCs are the “initial population of the CMDB” and the “synchronization population of the CMDB” actions. These actions can be considered as a sort of preauthorized change because all data is accepted without checking each update against a change in the RFC.

**A2.5 Create relationships between CIs.**

Since the auto-discover tools cannot discover all relationships between CIs, some relationships have to be maintained in the CMDB manual. This activity uses the change administration, or checks against standard configurations to determine the relationships a CI has with other CIs.

**A2.6 Create soft-label.**

Each CI will be marked with a unique label. At this point it is not clear how the interface between Asset Management and Configuration Management will be defined and implemented. Ideally the asset-label would be used as part of the soft-label. The soft-label is not only unique for a CI but also unique for different versions / configurations of a CI. This way the various configurations of a CI through its lifecycle can be traced.

**A2.7 Signal to Incident Management.**

This activity takes the differences list [output from sub process 3: Audit Configuration] and verifies if each difference is based on an authorized change or a pre-authorized change. If a difference between the real world and the CMDB is not based on an authorized change, a signal is flagged for Incident Management.

**A2.8 Measure and report the performance of this sub process.**

This activity measures and reports the performance of this sub process. The purpose is to have an objective way to measure the effectiveness of improvements to this process.

**Key Performance Indicators**

K2.1 Number of modifications to the CMDB

K2.2 Number of incidents signalled.

- Indicative of unauthorized configuration changes
- Indicative of unsuccessful changes
- Indicative of planning problems for changes

K2.3 Number of incidents related to incorrect configuration information

**Inputs**

**I2.1 Differences between CMDB and Infrastructure.**

This list is created by Sub process 3: Audit Configuration through comparing CIs in the CMDB and CIs in the real world.

**I2.2 Details of Authorized changes.**

These are planned changes to the configuration against the differences are checked.

**Controls**

**C2.1 Service Management Controls**

The Service Management Controls determine the prerequisites for changes to be pre-authorized.

**C2.2 The Infrastructure Design**

The design determines which relations between CIs exist

**C2.3 Preauthorized changes.**

Some CI types have volatile attributes / relationships, changes are automatically authorized. For instance the type of the mouse attached to a Desktop.

**Triggers**

**T2.1 RFC [Request For Change];** The configuration changes resulting from an authorized change have to be registered into the CDMB if successfully implemented.

**T2.2**After each audit of the configuration the differences are evaluated and can result in updates of the CMDB.

**Output**

**O2.1** Updates on the CMDB data

**O2.2** Signals to Incident management

**Skills (Roles)**

**S2.1** Configuration Manager

**Tool Requirements**

**R2.1** Automated Access to Change tickets

**R2.2** Changes (fields) in recognisable and standard format

**R2.3** Automatic update CMDB if change and verification are in synch

**R2.4** Registration of change types (attribute- or relation-level) that are pre-authorized



R2.5 Automatic update CMDB if differences are matching a pre-authorized change

R2.6 Validation of Changes on field level (naming convention, valid value range), (semantic, and syntax validation) (mandatory fields entered) [responsibility of Change Management]

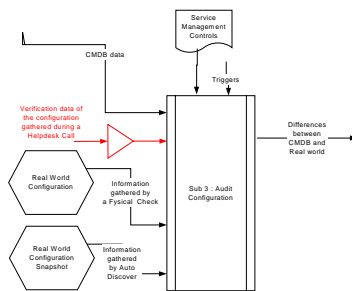
R2.7 Database generates a sequence number

R2.8 Asset tag registered as an attribute

R2.9 Ability to generate, fill appropriate fields) and route an incident ticket

R2.10 Logging, tracking, reporting functions (# updates in CMDB, # incidents signalled)

## 6.7 Sub Process 3: Audit Configuration



### Purpose

This Sub Process: -Gathers information about the real world, -Verifies and formats the data, compares it to the registered information in the CMDB, and creates a list of the differences. By doing so, it enables an audit of the real world configuration.

### Activities

A3.1 Run the auto-discover.

This activity runs Auto-discover to 'sniff' the 'real world' configuration, compares this to the configuration accordingly to the CMDB and creates a list of the differences.

A3.2 Verify CMDB on a Helpdesk call.

On a Helpdesk call, a helpdesk operator verifies the 'real world' configuration against the CMDB by questioning the customer and creates a list of differences.

A3.3 Verify CMDB by Physical checking the 'real world' configuration.

This activity consists of doing a physical check of the 'real world', comparing this to the configuration accordingly to the CMDB and creating a list of the differences.

A3.4 Measure and report the performance of this Sub process.

This activity measures and reports the performance of this sub process. The purpose it to have an objective way to measure the effectiveness of improvements to this process.

### Key Performance Indicators

K3.1 Number of CIs found by discovery activities

K3.2 Number of attributes found for each CI by discovery activities

K3.3 Number of relationships between CIs found by discovery activities

K3.4 Number of differences reported.

**Inputs**

- I3.1 Configuration Information from Helpdesk operator acquired from caller
- I3.2 Auto-discover tool output
- I3.3 Physical check results
- I3.4 CMDB data

**Output**

- O3.1 List of detected differences

**Controls**

C3.1 Service Management Controls

The Service Management Controls determine:

- The scope and timing of the auto-discover information: For instance once a day, 1/7 of the total configuration, or day one the servers, day two the desktops, day three the network, etc.)
- The scope of the auto-discover can be on-demand. For instance only the relevant configuration after a change.
- The scope and timing of the physical check.
- The scope and timing of audit after an implemented RFC.
- The scope of the questioning on a Helpdesk call.

**Triggers**

T3.1 Available information from an (automated) auto-discover action

T3.2 A Helpdesk call

T3.3 Available information of a physical check

T3.4 Request from Incident or Problem Management

T3.5 Verify CMDB after implementing RFC.

After the completion of a change (successful or unsuccessful) this trigger starts the comparing of the relevant 'real world' configuration to the CMDB to analyse the effects of the change and creates a potential list of differences.

T3.6 Populate initial CMDB.

This trigger starts an (one time) initial population of the CMDB based on the 'real world' configuration, verifies all the CIs on the list and use it as input for Sub process 2: Updating the CMDB.

T3.7 Synchronize CMDB.

After a major update (f.i. after defining a new CI type, or complementing the environment with a large number of CIs) do a Synchronization Population, verify the list and use it as input for Sub process 2.

**Skills (Roles)**

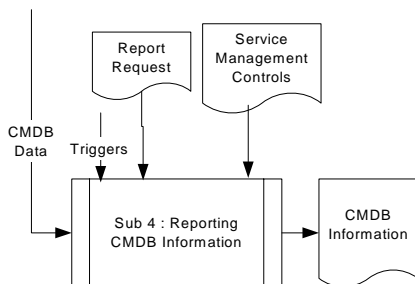
- S3.1 Operational Services Specialist (Systems Manager / Operator)
- S3.2 Helpdesk Operator
- S3.3 Configuration Manager

**Tool Requirements**

- R3.1 Automated discovery of a CI
- R3.2 Automated discovery of the value of attributes of a CI
- R3.3 Automated discovery of relations between CIs
- R3.4 Schedulable auto-discovery
- R3.5 Auto-discovery for a selection of CIs
- R3.6 Formatting the raw auto-discover information for comparison to CMDB
- R3.7 Automated Access to CMDB
- R3.8 Compare function (auto-discover data versus CMDB)
- R3.9 Generating a differences list
- R3.10 Generation a checklist from the CMDB used by the Physical checking activity
- R3.11 Ability to (easily) enter the data gathered by the Physical checking
- R3.12 Access to the CMDB data from the Helpdesk application (preferable integrated)
- R3.13 Ability to register the differences between the information the Helpdesk receives versus the information from the CMDB
- R3.14 Logging, tracking, reporting functions (# CI auto-discovered, # differences)

---

## 6.8 Sub process 4: Reporting CI Information



**Purpose**

This Sub Process generates all the necessary configuration reports.

**Activities**

A4.1 Design / Implement Reports of Configuration Data.

This activity designs and implements reports to represent configuration data. The data can be presented in text, tables or graphics. These reports can be ‘canned reports’ (for frequent use) or a report for a specific request.

A4.2 Generate / Schedule Reports of Configuration Data

This activity generates a report or schedules the generation of a report. This can be on demand or for publication to a subscriber group. This activity also defines the timetable for generating standard reports, and maintains the list of subscriptions on periodically standard reports.

A4.3 Provide Configuration Data in downloadable form.

This activity generates configuration data in a downloadable form. For instance to import in a database program for analysis.

A4.4 Generate Change Impact reports. (Based on a RFC, list the effected CIs)

A4.5 Generate Detailed configuration reports for Incident / Problem Management

A4.6 Measure and report the performance of this Sub process.

This activity measures and reports the performance of this sub process. The purpose it to have an objective way to measure the effectiveness of improvements to this process.

**Key Performance Indicators**

K4.1 Number of reports generated

K4.2 Number of subscribers to regular reporting

K4.3 Number & content of ad hoc queries (can point to the need to define new standard reports)

**Inputs**

I 4.1 CMDB data

**Controls**

C4.1 Service Management Controls

- The data that will be made available in downloadable form
- The data that will be reported to subscribers
- The data that will be published, and how actual will it be
- Rules for who can be a subscriber

C4.2 Report Requests

- Reports can be for the all CIs, a group of CIs or for a single CI.
- A report can be fixed (canned) or created on the fly (ad hoc)

**Triggers**

T4.1 On-demand Reports

T4.2 Periodical Reports.

**Output**

O4.1 Configuration Reports

This can have many forms like text, tables or graphics. Special forms of a configuration reports are a RFC impact analyse and detailed reports used by Incident Control / Problem Management.

**Skills (Roles)**

S4.1 Database Specialist / Analyst

S4.2 Operational Services Specialist (Systems Manager / Operator)

S4.3 Configuration Manager

**Tool Requirements**

R4.1 Access to CMDB data (read-only?)

R4.2 Report generation functions

R4.3 Generate text

R4.4 Generate tables

R4.5 Generate graphics

R4.6 Schedule report generation

- R4.7 Parameterized Report generation (level of detail, scope)
- R4.8 On-line query facilities on CMDB data (several levels of actuality)
- R4.9 Download of parts of the CMDB
- R4.10 Provide copies of CMDB data (for instance generated at night)
- R4.11 Registration of the requested reports
- R4.12 Ability to subscribe to periodical standard reports
- R4.13 Creation of canned / prefab reports
- R4.14 Access to standard reports (posted on web, Mail list, paper)
- R4.15 Logging, tracking, reporting functions (number of reports generated, number of subscribers, number and content of ad hoc queries)

## Section

## 7

## 7. Roles and Responsibilities

This section describes the functions and activities to be performed by the individuals participating in the configuration management process. The Roles and responsibilities must be agreed to, documented, authorities understood, kept current, and all feel empowered to fulfill responsibilities and cross reporting boundaries.

The roles and responsibilities involved in the process are:

- Configuration Management Process Owner. [P\_owner]
- Configuration Management Coordinator. [P\_exec]  
Also called the Configuration Manager or the Process Executor
- Infrastructure (Network, Hardware, Software, Application) Specialist [Infra]
- Database Administrator [DB]
- Helpdesk / Service Desk [HD]
- Operational Services Specialist (systems manager / operator) [OPS]

The positions discussed refer to a functionality role and do not represent a one to one full time equivalent (FTE) position requirement. In most cases several roles may be assigned to a single person in the organization or several people may play a single role.



### Configuration Management Process Owner

The Configuration Management Process Owner is the XXXXX I/T designated management representative with ultimate responsibility and authority for the results of the configuration management process. The Configuration Management Process Owner must ensure business objectives of the XXXXX I/T organization are properly managed and supported by the process. The Configuration Management Process Owner has the following responsibilities:

- Prioritizes process investment, (responsible for cost and investment of the process).
- Acts as a final escalation point for configuration management process issues.
- Defines, prepares, and communicates new and changed policies.
- Approves new process definitions, requirements and requests for improvement.
- Assigns the Configuration Management Coordinator.
- Enforces the process throughout the organization.
- Ensures consistency with other processes.
- Approves or rejects process deviation requests<sup>1</sup>.
- Defines process measurements and associated targets.

### Configuration Management Coordinator

The Configuration Management Coordinator is responsible for the day-to-day management of the process. The Coordinator ensures adherence to the overall configuration management process. The Configuration Management Coordinator is responsible for the following:

- Provides central direction for the configuration management system including:

Identifying the requirements.

Creating the logical, operational design including tool and database usage.

Testing and implementing design.

Ensuring consistency across technical domains and compatibility of applications and systems configurations.

---

<sup>1</sup> A Process Deviation Request is a management approved request for a covered component of the XXXXX I/T production environment to be exempt from the provisions of the configuration management process.

- Manages/controls the day-to-day execution of configuration information management activities.
- Monitors how well the configuration management system is performing and takes corrective actions to improve according to the process effectiveness measurements.
- Manages process policies and standards.
- Assesses potential impacts to the process
- Ensures availability and accessibility of accurate configuration information and continuously maintains and updates information as required.
- Ensures tools are available and properly maintained.
- Ensures that configuration information management roles are correctly assigned and executed.
- Provides education of the process and tools.
- Communicates process status and changes to all process participants.
- Attends appropriate change, asset and problem management meetings.
- Resolves issues related to the process when the normal structure is not adequate.
- Escalates exceptions to upper management together with supporting facts and recommended actions.
- Analyzes configuration trends and reports.
- Surveys client satisfaction with the process.
- Manages retrieval of configuration information from installed components.
- Audits deviations between recorded and actual configurations.
- Issues appropriate notifications.
- Requests updates of configuration information and sends to 'validate and maintain sub-process.'

### Infrastructure Specialist

The Infrastructure Specialist provides the subject matter expertise about configuration characteristics. These characteristics are registered as the attributes of each Configuration Item and the relations between CIs. The Infrastructure Specialist has the following responsibilities:

- Provide knowledge about what information for each type of Configuration Item is relevant to be registered.

- Provide knowledge about the acceptable ranges for values of attributes for each type of Configuration Item.
- Provide knowledge about which relations to other types of Configuration Items are relevant to register.
- Provide knowledge about standard configurations and required components of standard configurations.

### **Database Administrator [DB]**

The Database Administrator / Database Analyst provides support needed to build and maintain the configuration Database. The Database Administrator has the following responsibilities:

- Design a database schema that can support the Configuration Management requirements.
- Update the Configuration Management Database [CMDB] schema is needed.
- Maintain and optimize the CMDB
- Supply Support for Applications that need to access the CMDB

### **Helpdesk / Service Desk [HD]**

The Helpdesk is process / organization who interacts with users and customers. They are the first line support and next to using are also a source for information about the actual configurations that support to users. The Helpdesk has the following responsibilities:

- Verify the registered configuration of a user on each call to the Helpdesk.

### **Operational Services Specialist (systems manager / operator) [OPS]**

The Operational Service Specialist is responsible for the daily operations in the XXXXX's Data centers. This specialist will execute many tasks of the Configuration Management Process. The Operational Services Specialist has the following responsibilities:

- Execute all scheduled Configuration Management Reporting.
- Execute the auto-discover process.
- Execute Systems Management activities on the Configuration Management Application, Database and tools environment.



## Section

## 8

## 8. Measurements & Reporting

### 8.1 Introduction

Measurements and reporting are a necessary part of the configuration management process. They are key aspects in maintaining a continuous process improvement cycle. The Management Process Owner will conduct a periodic review of the configuration management process. The results of the self-assessment will be reported and analyzed with management.

The measurements and reporting of the configuration management process should address the status of the process at meeting or not meeting its defined objectives stated in Section 3 of this document.

### 8.2 Measurements

Next to the Key Performance Indicators mentioned in section 6 Process Description, there are some general measurements that can be used to measure the status of the process in the following areas.

#### Effectiveness

Indicators may be defined to control the level of effectiveness (is the process meeting or not meeting its objectives?) of the configuration management process:

- Number of configuration correction requests and the number of configuration requests.
- Percentage of processes that can obtain configuration information per the processes that require it.
- Percentage of captured component configurations per the number of known I/T managed components.

### Accuracy

Information accuracy indicators can be used as a way to audit configuration information management activities. Suggested indicators:

- Percentage of configuration correction requests per the number of configuration requests.
- Percentage of component records with an inaccurate configuration information as captured during the audit process. The Configuration Process Coordinator regularly selects a list of I/T managed components and manually verifies the captured information with actual information.

### Efficiency

These measurements help determine the level of automation implemented to support configuration management. As the configuration management process evolves, manual processes will become automated via system management tools. The efficiency of these tools must be continually measured to determine areas for improvement.

- Percentage of I/T managed component configurations gathered via automated methods versus I/T managed component configurations gathered manually.

## 8.3 Reporting

Reports are produced on a periodic basis to support the ongoing operation and measurement of the process. The following reports provide valuable information about the status of the process:

### Sub processes Key Performance Indicators

- K1.1 Number of changes to the schema
- K1.2 Dates of latest changes.
- K1.3 Number of CI types without a identified owner
- K1.4 Number of CI types without configuration documentation
- K1.5 Number and severity of incidents related to missing attributes or registration of relationships
  
- K2.1 Number of modifications to the CMDB
- K2.2 Number of incidents signalled.
  - Indicative of unauthorized configuration changes
  - Indicative of unsuccessful changes
  - Indicative of planning problems for changes
- K2.3 Number of incidents related to incorrect configuration information
  
- K3.1 Number of CIs found by discovery activities
- K3.2 Number of attributes found for each CI by discovery activities

- K3.3 Number of relationships between CIs found by discovery activities
- K3.4 Number of differences reported.

- K4.1 Number of reports generated
- K4.2 Number of subscribers to regular reporting
- K4.3 Number & content of ad hoc queries (can point to the need to define new standard reports)

Configuration Request Effectiveness Report

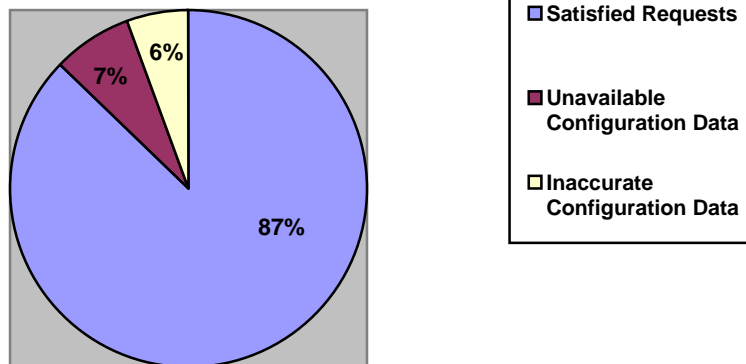
This report displays the number of configuration correction requests and the number of configuration requests. The table below gives an example.

Configuration Requests	124
Unavailable Configuration Information	10
Inaccurate Configuration Information	8
Satisfied Requests (Configuration Requests minus Unavailable and Inaccurate Configuration Information.	106

Configuration Request Accuracy Report

This report charts the number of configuration correction requests against the number of configuration requests. The difference between this number is assumed to be a satisfied request.

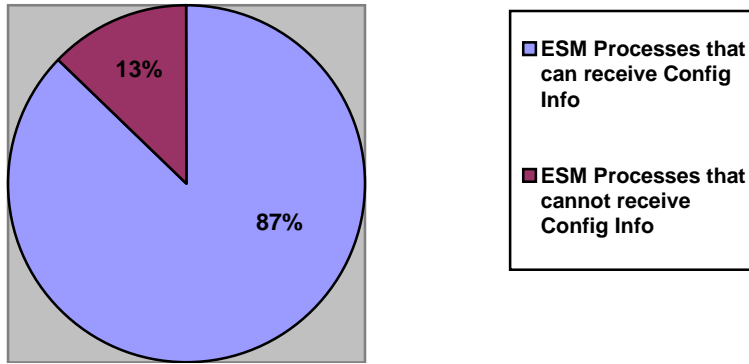
**Configuration Information Requests**



Configuration Information Availability Report

This report charts the percentage processes that can obtain configuration information verses those that cannot.

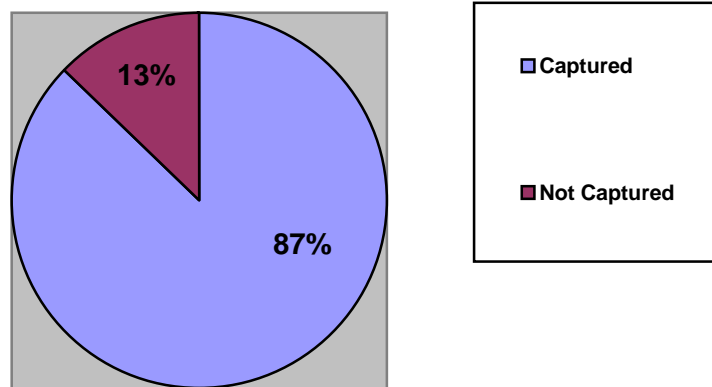
### Configuration Information Availability to Other Processes



### Captured Configuration Information Report

This report charts percentage of captured component configurations per the number of known I/T managed components

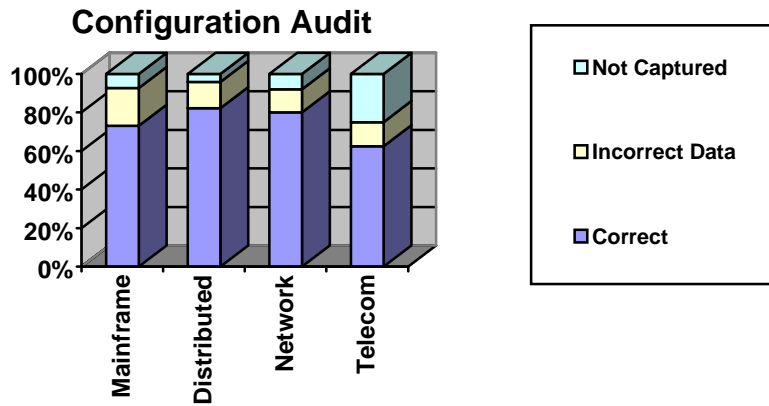
### Captured Configuration Information for I/T Managed Components



### Configuration Data Accuracy Audit Report

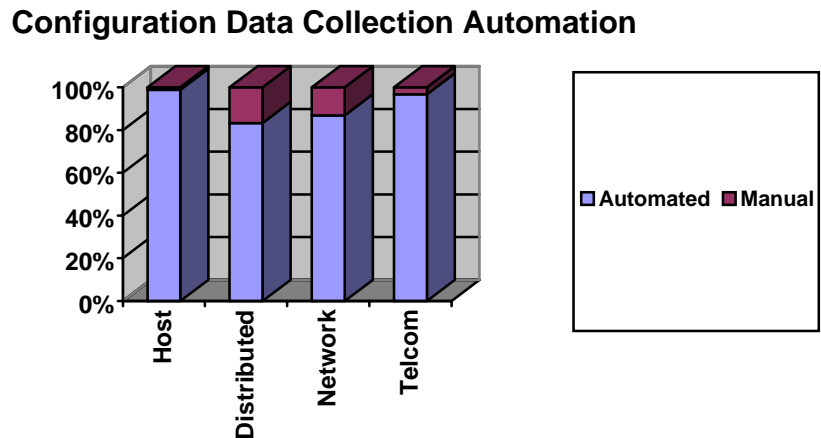
This report displays the accuracy of the data for I/T managed components that. The information should be captured during audits of the configuration information. The report could look something like the bar chart below.





Configuration data capture automation report

It indicates the configuration data that is captured automatically verses data captured manually. The report indicates the level of automation in the configuration management process. The information should be gathered by collecting the number of records in the database of each type of component where data is collected automatically and compare it to the number of known components of each type in the environment. The report could look something like the bar chart below.



Below are descriptions of the log files that are created by the process. The information in the logs could be use to generate the reports above or any new reports.

Configuration History Log

This log lists new and updated configurations, stored to reflect the evolution of hardware, software, and network configurations. This information may be used for back-out procedures. The report may specify whether the updates were triggered by discovered configuration information or by change execution results.

### Configuration Error Log

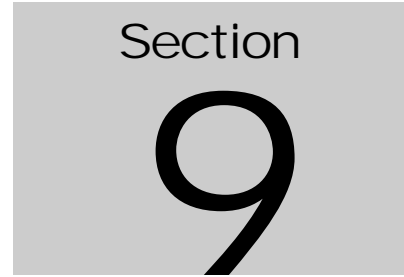
This log lists errors when attempting to enter new and updated configuration information into the configuration database. It also logs an event when information that should be in the database cannot be retrieved. The configuration Error Log should be reviewed within 1 day of an error and should be resolved within 5 working days.

### New Configuration Information Log

This log lists the new configuration information that has been implemented.

### Changed Configuration Information Log

This log lists the planned configuration changes that have been implemented and not implemented due to problems. This report also lists the unplanned configuration changes. The changed configuration information log should be reviewed within 1 day of an unplanned change and should be resolved within 5 working days.



## 9. Meetings

This section outlines topics to be covered in configuration management meetings. The names, criteria and/or guidelines for the meetings are shown below. Next to these meetings there is a requirement for input from Configuration Management during Change Advisory Board meetings where Request For Changes are evaluated.

- Configuration Management Meeting (monthly).
- Configuration Management Process Improvement Meeting (yearly or as needed).

### Configuration Management Meeting

The purpose of this meeting is to resolve configuration management issues. These meetings should be attended by the Configuration Management Process Coordinator, Configuration Management I/T Strategic Business Unit representatives, and other appropriate attendees. The meeting should be held monthly or as needed.

The following is an example of the format/agenda of the configuration management meeting.

- Review configuration management reports and resolve issues
- Identify and resolve failures of the process to meet its design
- Review configuration management strategy.

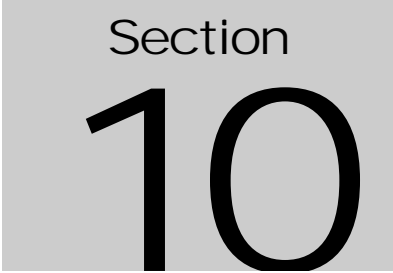
### Configuration Management Process Improvement Meeting

The purpose of this meeting is to review trends relating to the configuration management process and to determine if improvements are necessary. Recommendations for improvement are reviewed and a determination is made as to a corrective course of action. Plans and expected results are reviewed. In addition, this meeting can be a forum for the Configuration Management I/T Strategic Business Unit representatives to share ideas for improvements with the Management Process Owner and encourage open communication. This meeting is chaired by the Configuration Management

Process Owner and attended by the Configuration Management Coordinator, Configuration Management I/T Strategic Business Unit representatives and other appropriate attendees. The meeting should be held quarterly or upon request.

The following is an example of the format/agenda of the process improvement meeting.

- Communicate problem areas: process, documentation, tools, data entry fields, data integrity, reports etc.
- Suggested areas for improvement.
- Review new reporting requirements.
- Provide feedback on the execution of the process.
- Document and communicate improvement plans.

A gray rectangular box containing the text "Section" in a small, black, sans-serif font at the top, and the number "10" in a large, bold, black, sans-serif font below it.

## 10. Interrelationships with Other Processes

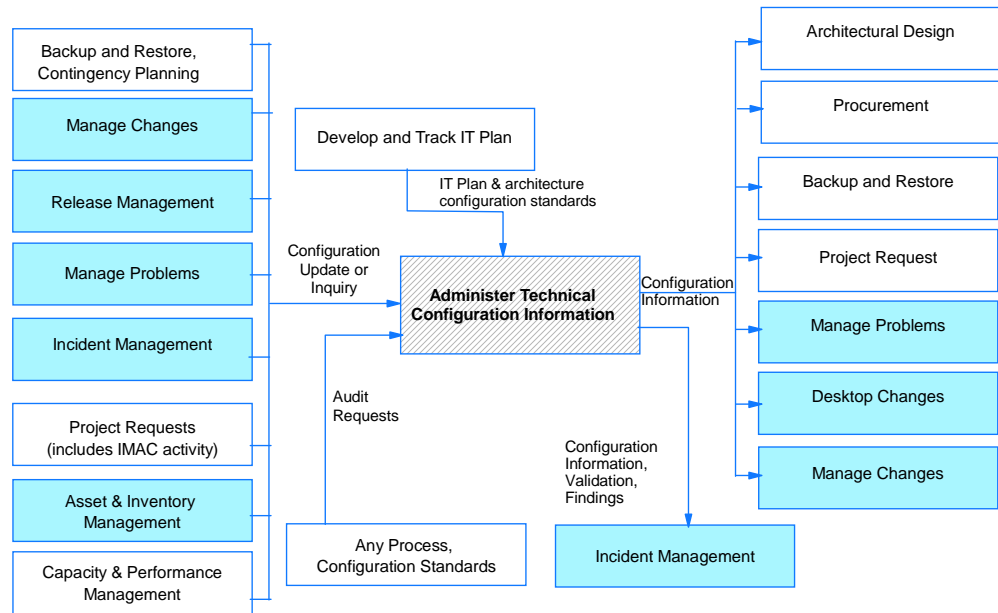
### 10.1 Introduction

When operating within the configuration management process, it is imperative that all participants have a clear understanding of how the process interacts with other disciplines within the XXXXX I/T environment.

### 10.2 Systems Management Processes

Systems Management (SM) processes represent a set of integrated management processes governing the delivery of IS services. The processes are change management, incident management, problem management, service level management, capacity management, performance management and recovery management. Because the configuration management process may interact with these processes, it is important to understand the interrelationships between them.

Key interfaces are maintained with the areas listed below. Depending on the final organization, responsibility for these disciplines and functions may reside either in a single department with a single individual, across many departments, or any effective combination. It is not the organization that is important, but the effective execution of configuration management responsibilities.



Each process should answer the question: “What will be provided to configuration management process and what is expected from the configuration management process?”

The following is a description of the SM processes that interrelate with the configuration management process.

Incident Management

This process invokes configuration management to retrieve configuration information needed deal with an incident. It receives from configuration management signals about deviations between authorized and actual status of configurations.

Problem Management

This process invokes configuration management when hardware and software information is requested to assist with problem determination and resolution.

Change Management

This process invokes configuration management when a change request to implement a new component or affecting an existing component configuration is executed. The record is updated and the New or Changed Configuration Information Log is updated with an expected configuration change entry.

### Service Level Management

This process invokes configuration management when measuring the performance of the configuration management process.

### Recovery Management

This process invokes configuration management when hardware or software failures occur and configuration information is required to restore operation.

### Performance Management

This process invokes configuration management when there is a need to tune various components

### Capacity Management

This process invokes configuration management when there is a need to upgrade component capacity.

### Security Management

The security management process ensures the confidentiality and integrity of information technology assets, and manages the registration or enrollment of people and programs to access controlled information system resources. This process invokes configuration management when system configuration information is needed to register clients to appropriate services using relevant registration products.

### Software Distribution Management

The software distribution management process enables software to be deployed on I/T managed components. This process will require information from the configuration management process to determine if software distributions are necessary or possible.

## 10.3 Business Management Processes

While SM focus on management of the I/T environment, the XXXXX I/T organization is also subject to the guidelines of many other business processes. In addition, the concepts and constructs of the configuration management process can be applied across the entire XXXXX I/T environment beyond I/T services.

The following is a description of the SM processes that interrelate with the configuration management process.

### Help Desk

This process invokes configuration management when help desk personnel request hardware and software information to assist with problem determination.

### Information Technology Planning

Information Technology Planning encompasses the activities pursued by XXXXX I/T management to identify and fulfill the technology requirements for their service offerings, and to integrate those requirements into the existing environment. The configuration management process should attempt to fulfill XXXXX I/T management requirements.

### Business Planning

Business Planning encompasses the activities pursued by client organizations to identify and fulfill the functional requirements for their business needs, and to integrate those requirements into their existing environment. In Change Management, Business Planning contributes to identification of the assessment criteria for categorizing and mitigating potential business risks in introducing a proposed change. The configuration management process should attempt to fulfill XXXXX I/T management requirements.

### Service Delivery

Service Delivery encompasses the operational procedures and practices executed by XXXXX I/T to effect delivery of a particular service. While the process does not impose specific requirements on “how” a service is to be executed, it does present guidance on the management disciplines surrounding those services. Thus, this Process Guide represents a mode of management and not a prescription for execution.

### Project Requests

Service Request encompasses the procedures and practices deployed by XXXXX I/T in response to the service needs of a client. Service request also encompasses the reporting and authorization procedures deployed by the client prior to contacting XXXXX I/T. In configuration management, service request may generate a requirement that is subject to the discipline of this process.

### Asset Management

The asset management process maintains all information regarding technology assets, including leased and purchased assets, licenses and inventory (including location) from the time an asset is received until its retirement. The asset management process and configuration management process should share databases so that there is one source to retrieve information about I/T managed components.



## 10.4 Interrelationship Matrix

The configuration management process has data and functional dependencies on other management processes. This matrix outlines the inputs and outputs to the Configuration Management process in relation to other XXXXX I/T management processes.

<b>Process</b>	<b>Input or control provided to Configuration Management</b>	<b>Outputs received from Configuration Management</b>
<b>Help Desk</b>	Configuration information request, including client or service criteria needed to retrieve the requested information.	Configuration information about the components used to deliver services to clients calling the Help Desk.
	Configuration requirements when client requests imply new or upgraded configurations.	Notification to requirement submitter.
	Severity and Priority information of each configuration component based on service level objectives.	
<b>Problem Management</b>	Configuration information request to analyze and resolve problems.	Configuration information required to analyze and resolve problems.
	Request for information to determine the priority and severity of a failing component.	Priority and Severity Information for a failing component.
		Configuration information to determine the components that are affected as the result of another failing component.
		Exception Log of missing or incorrect configuration

		information that is created as a result of the Capture Configuration Information Sub-Process
		Error Log of errors that were created when the Configuration Data Base was updated or new records or fields were created.
<b>Change Management</b>	Change request, approval, schedule to the Analyze Configuration Information sub-process to make changes/additions to the configuration information.	Change Request from the Implement (Design and Plan) Sub Process to make changes/additions to the Configuration Information.
	Change notification from an implemented change to ensure that the Configuration database is updated.	Configuration Management supplies requested Configuration Information
	Request for Information to determine the impact of a proposed change.	Information to Change Management to determine impact and risk assessments.
	Change review status, especially feedback from technical review.	Configuration implementation plan for configurations that need staged implementation (i.e. require more than one change).
	Change execution reports are needed to reflect actual configurations in the information base.	Prepared change ready to be implemented.
<b>Backup &amp; Restore Management</b>	Configuration Requirement for backup, archive and retrieval configurations	Configuration information about vital components.