CERTIKIT
Compliance made easy

Service Asset and Configuration Management Process

ITIL® 2011 Service Transition Process and Policy Pack v2

Implementation guidance

The header page and this section, up to and including Disclaimer, must be removed from the final version of the document. For more details on replacing the logo, yellow highlighted text, and certain generic terms, see the *Completion Instructions* document.

Purpose of this document

This document sets out the Service Asset and Configuration Management process including flowchart, activities, reporting and roles and responsibilities.

Areas of the ITIL® Framework addressed

The following areas of the ITIL Framework are addressed by this document:

- Service Transition: Service Asset and Configuration Management

General guidance

Service Asset and Configuration Management (SACM) is the foundation of several other key processes within the ITIL lifecycle suite, including change and release and deployment management. It is recommended that you implement them as a set since each relies so heavily on the others being in place.

The configuration management system (CMS), like the service knowledge management system (SKMS), should be seen as a set of data sources linked together using software tools, rather than as a single database, as the CMDB used to be described.

Automated software tools to discover and audit your IT estate will save a lot of time over a manual process of trying to keep track of your CIs. It is worth spending some time to investigate how such tools can be integrated into your IT service management system to provide a method of linking incident, problems and changes to CI records.

The integration of your procurement processes is also key so that new CIs are captured at the right time and all the necessary information is recorded in the CMS. The management of the movement of CIs as part of the service request fulfilment process must also be tightly controlled if the CMS is not to become increasingly out of date.

SACM is a difficult area to get right and so may take a while to implement and need more resources than expected, but it can add significant value to your service management capability.

Review frequency

We would recommend that this document is reviewed annually.

Document fields

This document may contain fields which need to be updated with your own information, including a field for Organization Name that is linked to the custom document property "Organization Name".

To update this field (and any others that may exist in this document):

1. Update the custom document property "Organization Name" by clicking File > Info > Properties > Advanced Properties > Custom > Organization Name.
2. Press Ctrl A on the keyboard to select all text in the document (or use Select, Select All via the Editing header on the Home tab).
3. Press F9 on the keyboard to update all fields.
4. When prompted, choose the option to just update TOC page numbers.

If you wish to permanently convert the fields in this document to text, for instance, so that they are no longer updateable, you will need to click into each occurrence of the field and press Ctrl Shift F9.

If you would like to make all fields in the document visible, go to File > Options > Advanced > Show document content > Field shading and set this to "Always". This can be useful to check you have updated all fields correctly.

Further detail on the above procedure can be found in the toolkit *Completion Instructions*. This document also contains guidance on working with the toolkit documents with an Apple Mac, and in Google Docs/Sheets.

Copyright notice

Licence terms

Disclaimer

Service Asset and Configuration Management Process

DOCUMENT REF	ITILST0502
VERSION	1
DATED	[Insert date]
DOCUMENT AUTHOR	[Insert name]
DOCUMENT OWNER	[Insert name/role]

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES

Distribution

NAME	TITLE

Approval

NAME	POSITION	SIGNATURE	DATE

Contents

Figures

Tables

1 Introduction

1.1 Vision statement

The vision of [Service Provider] in the area of service management is as follows:

[Insert the vision statement defined as part of service strategy]

This process forms a key part of the realisation of that vision.

1.2 Purpose

This document defines how the process of service asset and configuration management (SACM) is implemented within [Organization Name].

The purpose of the service asset and configuration management process according to ITIL® is:

> *"... to ensure that the assets required to deliver services are properly controlled and that accurate and reliable information about those assets is available when and where it is needed."*

Source: ITIL Service Transition Book 2011. Copyright © AXELOS Limited 2011. Reproduced under license from AXELOS.

1.3 Objectives

The objectives of the service asset and configuration management process are to:

- Identify, record and control information about configuration items that have value to the organization
- Create and maintain a configuration management system (CMS) that holds useful information about CIs and their relationships e.g. baselines and snapshots
- Ensure that the CMS stays up to date in the face of change by working closely with the change management process
- Provide useful information about the status, attributes and relationships of CIs to other processes such as release and deployment management, change management and capacity management

1.4 Scope

The scope of this process is defined according to the following parameters:

- Organizational
  - [List organizations and parts of those organizations covered]
- Geographical
  - [List locations from which requests for change will be accepted and managed]
- Services
  - [Define the services covered by the process]
- Technical
  - [If necessary, cover the technology that may give rise to changes managed via this process]

The following areas are specifically excluded from this process:

[Describe any areas that need to be clearly stated as outside the scope]

2 Service asset and configuration management process

2.1 Overview and process diagram

The process of service asset and configuration management is shown in Figure 1 and summarised below.

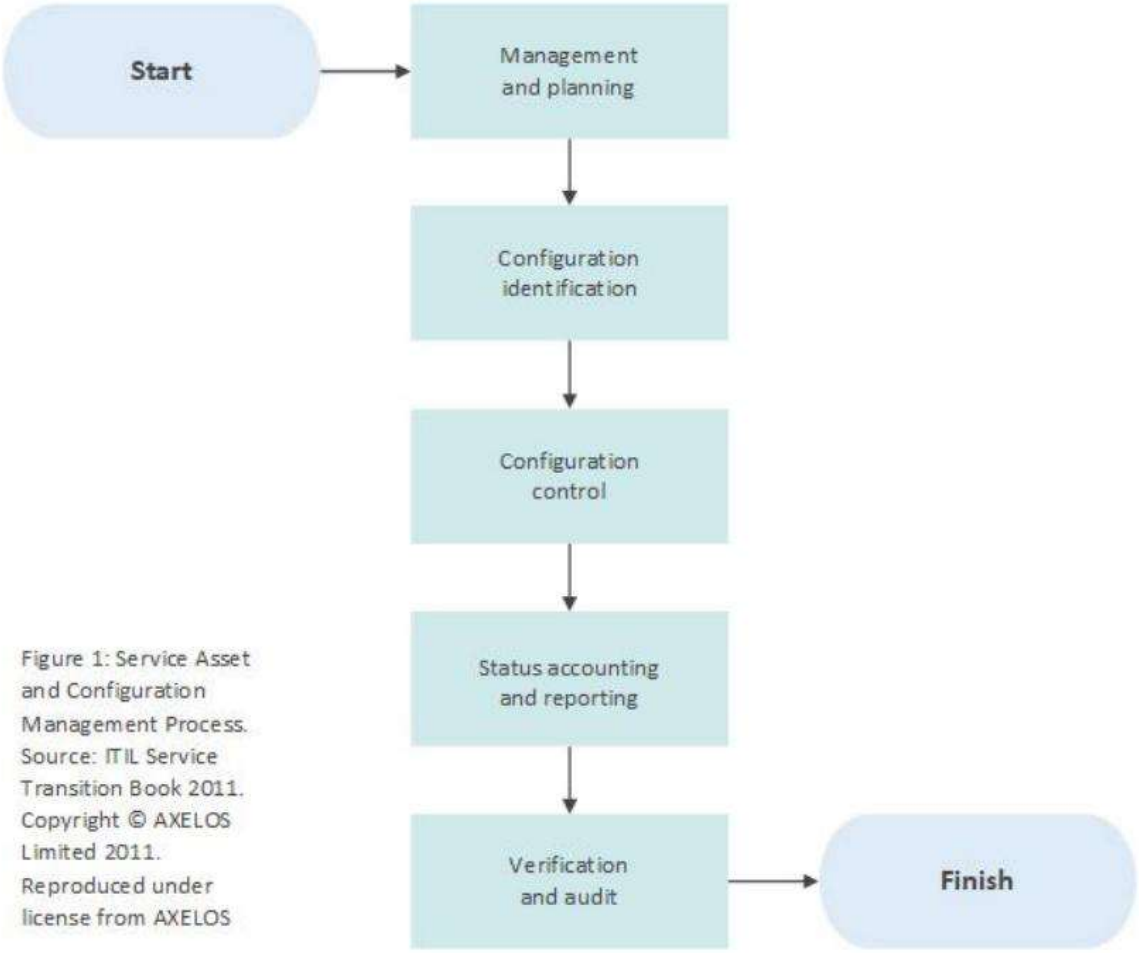

Figure 1: Service Asset and Configuration Management Process. Source: ITIL Service Transition Book 2011. Copyright © AXELOS Limited 2011. Reproduced under license from AXELOS

Figure 1: Service asset and configuration management process

Source: Based on ITIL Service Transition Book 2011. Copyright © AXELOS Limited 2011. Reproduced under license from AXELOS.

Management and planning will take place at two main levels. The first is at the overall management level and will encompass the definition of the approach for service asset and configuration management, including the creation of a policy and the configuration management system (CMS). The second level is at the start of a project for a new or changed service, during which a SACM plan will be defined for that specific project, including procedures for the identification of CIs and the establishment of baselines.

Configuration identification will involve the documentation of the individual CIs, including their attributes, unique identifiers, configuration structures and relationships.

Once the CIs have been identified, procedures will be defined for their proper control so that their integrity and that of the CMS records is maintained. Use of these procedures will ensure that all activity with regard to CIs, such as adding, modifying, replacing or removing them is carried out in a standardized way.

During their lifecycle, CIs will go through a series of statuses (e.g. draft, approved, withdrawn) which at key points need to be updated and reports produced for use in other service management processes e.g. release and deployment management.

Verification and audit of configuration records is essential to ensure that they stay accurate and reflect the real world. This may consist of physical audits at specific locations (e.g. for desktop computers and printers) and logical audits for software CIs and bespoke modules, in addition to other forms of verification where required.

2.2 Process triggers

The service asset and configuration management process is initiated as a result of one or more of the following triggers:

- Initiation of a project that requires the introduction or changing of CIs
- Requests from change management and release and deployment management
- Significant events such as an ITSCM or security incident
- Changes to legal, regulatory or contractual requirements
- In response to audit requirements

2.3 Process inputs

The process of service asset and configuration management requires a number of inputs in order to be able to function effectively. These may not always be available but will ideally be:

- Definitions of service asset and configuration management requirements from projects
- New configuration item details e.g. hardware manufacturer, model, serial number

- Requests for Change (RFCs)
- Audit records
- Hardware and software disposal records

2.4 Process activities

The individual process activities at each step are detailed as follows.

2.4.1 Management and planning

Planning of SACM will take place at the high level to establish and operate the process and at a lower level for individual projects.

The initial high-level planning of service asset and configuration management within [Organization Name] will establish the following factors:

- The scope of SACM and CIs to be recorded
- The objectives to be achieved
- Resources to be allocated both for initial setup and for on-going operation of the SACM process
- Tools to be used to identify, record, manage and report on configuration items within the CMS
- Timescales for the establishment of an effective process
- Roles and responsibilities in the configuration management process

This will include the definition of a SACM policy which describes the principles that will be adopted and the general rules that will be followed.

At the project level a SACM plan will be produced for each project that involves significant change within the areas in scope. This will set out the approach that will be taken to SACM within the project, including:

- Identification of configuration items
- Storage of CIs within the various environments used (development, test etc.)
- Check in/check out procedures for software components
- Configuration and management of build environments
- Definition of baselines and their timing within the project
- Approach to the retirement of replaced CIs

Project-specific procedures will be produced where required.

2.4.2 Configuration identification

Configuration Items (CIs) will be identified based on the following general principles:

- There will be three types of CI, namely hardware, software and documentation
- The level of CI will be determined according to the value of the information to the delivery of IT services
- The attributes recorded for each CI type will be determined based on a balance of usefulness and ease of maintenance

The following attributes will be recorded according to the CI type:

2.4.2.1 Hardware

The following types of configuration items will be recorded (this list will be updated as further types of hardware items are implemented):

- Desktop hardware
- Monitors
- Laptops
- Printers
- Servers
- Firewalls
- Routers
- Switches
- Other

The attributes listed below will be recorded.

ATTRIBUTE	DESCRIPTION
Asset Number	The asset number assigned to the CI
Description	A text description of the CI e.g. "Internet Router"
Status	Whether the CI is live, disposed etc.
Relationships	How this CI is related to other CIs and service components
Location/User	The current user or location of the CI
Type	The type of hardware e.g. desktop, router, laptop
Manufacturer	The manufacturer's name
Serial number	The unique manufacturers serial number
Model number	The manufacturers assigned full product code
Supply Date	The date the CI was supplied
Supplier	Where the CI was sourced from

ATTRIBUTE	DESCRIPTION
Cost	The costs of the CI when sourced
Purchase Order Number	Reference for the PO on which this CI was ordered
PO Date	Date of approval of the PO
Invoice #	If known
Invoice Date	If known
Date of Installation	The date the CI was installed into the live environment
Change Numbers	The numbers of all change records affecting this CI
Problem Numbers	The numbers of all problem and known error records affecting this CI
Incident Numbers	The numbers of all incident records affecting this CI
Comment	A free-format text field for any relevant information

Table 1: Hardware CI attributes

2.4.2.2 Software

All application software in use will be recorded as CIs in the CMDB. This includes server-based systems as well as desktop software such as office suites. The attributes listed below will be recorded.

ATTRIBUTE	DESCRIPTION
CI Name	The unique name by which this CI is known
Description	A text description of the CI
Status	Whether the CI is live, disposed etc.
Relationships	How this CI is related to other CIs and service components
Supplier	The supplier's name
Version number	The manufacturers assigned version number e.g. R33
DML Reference/location	The reference of this software item within the Definitive Media Library
Supply Date	The date the CI was supplied
Supplier	Where the CI was sourced from
Cost	The costs of the CI when sourced
Date of Installation	The date the CI was installed into the live environment
Maintenance/ Warranty Provider	Which organization provides maintenance/warranty services for this CI
Maintenance/ Warranty Contract Number	The contract number under which maintenance/warranty is provided
Maintenance/ Warranty Expiry Date	The date the relevant maintenance/warranty ends

ATTRIBUTE	DESCRIPTION
Change Numbers	The numbers of all change records affecting this CI
Problem Numbers	The numbers of all problem and known error records affecting this CI
Incident Numbers	The numbers of all incident records affecting this CI
Comment	A free-format text field for any relevant information

Table 2: Software CI attributes

2.4.2.3 Documentation

It is essential that correct versions of documentation are used and updated when their subject material changes. Requests for change must include the consideration of documentation so that it remains relevant to the area it covers.

The attributes listed below will be recorded.

ATTRIBUTE	DESCRIPTION
CI Name	The unique name by which this CI is known
Description	A text description of the CI e.g. "Network Diagram"
Status	Whether the CI is live, disposed etc.
Relationships	How this CI is related to other CIs and service components
Supplier	The supplier's name (if supplied or internal if not)
Version number	The version number of the documentation
Reference/location	The location of this item of documentation within the filing structure
Date of Installation	The date the CI was accepted into the live environment
Change Numbers	The numbers of all change records affecting this CI
Problem Numbers	The numbers of all problem and known error records affecting this CI
Incident Numbers	The numbers of all incident records affecting this CI
Comment	A free-format text field for any relevant information

Table 3: Documentation CI attributes

2.4.3 Configuration control

On-going control of the configuration items recorded in the CMS will be exercised via the change management process. No CIs will be added, changed or removed unless the appropriate change management documentation has been completed and approved. Part of the change management process will be the updating of the CMS to ensure that it remains current and always reflects a true record of installed items.

Installation of common items such as desktop PCs and laptops will be treated as service requests and there will be an interface between the procurement process and SACM that ensures that items purchased are created as CIs when installed.

2.4.4 Status accounting and reporting

A set of reports will be regularly generated from the CMS in order to provide management information on the status of configuration items. These reports will include:

- List of all configuration items by site
- Rack listings by server room
- CIs having incidents associated with them
- CIs having problems associated with them
- CIs having changes associated with them
- Discrepancies between the recorded status of CIs and that most recently discovered by the automated asset management tool

Ad-hoc reports will also be required to satisfy information requirements for support contracts. These may require the creation of new reports.

Other reports may be required for:

- Equipment refresh programmes
- Financial or insurance purposes e.g. value of kit at a location

2.4.5 Verification and audit

An automated asset management software tool will be used to verify the hardware and software configurations of all CIs to which it has access. This exercise will be carried out on a monthly basis initially, with the frequency being adjusted according to the number of discrepancies found.

A programme of physical audits will be instituted to verify the data collected via the tool with the intention of visiting all locations within a specified period of time. This approach will be validated in the light of the results obtained – if the tool is found to maintain a very high degree of accuracy and completeness then the number of physical audits may be minimised. The IT service desk will also be used to verify data on an on-going basis when users report incidents.

Verification of CIs not covered by the software tool will be performed manually at least every six months.

2.5 Process outputs

The outputs of the service asset and configuration management process will be the following:

- New and updated configuration records
- Configuration baselines
- Status and accounting reports
- Relationship information for use in assessing changes
- An accurate CMS that provides input to the wider service knowledge management system (SKMS)

2.6 Service asset and configuration management tools

There are a number of key software tools that underpin an effective service asset and configuration management process. These are subject to change as requirements and technology are updated and so specific systems are not described here. However, the main types of tools that play a significant part in the process within [Organization Name] are as follows.

2.6.1 Configuration management system

The configuration management system (CMS) provides a way to store configuration records together with the attributes that are defined against them. It also allows relationships between CIs to be reflected so that a more effective impact assessment of changes can be made.

The CMS is interfaced with the incident, problem and change management tools so that records in each system can be linked together e.g. changes to a specific CI can be recorded and reported upon.

2.6.2 Automated asset management system

This system is capable of discovering assets located within the IT estate and automatically capturing key attributes of them such as their type, configuration and software versions. The automated asset management system works with the CMS to provide regular updates without the need to physically visit remote locations.

2.7 Communication and training

There are various forms of communication that must take place for the service asset and configuration management process to be effective. These are described below.

2.7.1 Communication with change management

SACM effectively provides a service to change management so that the potential impacts of changes can be better understood. SACM will obtain feedback from change management about the accuracy and usefulness of the information provided so that any required improvements can be identified.

Change management also provides updates to the CMS on a regular basis and the smoothness of the interface should be a subject of frequent communication.

For both these reasons the SACM process manager should be a regular attendee at Change Advisory Board (CAB) meetings.

2.7.2 Communication with IT teams

SACM needs to communicate the importance of keeping the CMS up to date to IT support teams so that there is no temptation to bypass change management and avoid updating the CMS. This will be done via awareness sessions delivered during team meetings and via other appropriate methods depending on the need.

2.7.3 Communication with projects

Project teams may need a significant degree of assistance with assessing and planning their configuration management requirements at the start of a project. This will depend upon the type and scope of the project but the SACM process manager's attendance at progress meetings may be useful to all parties involved.

2.7.4 Process performance

It is important that the performance of the service asset and configuration management process is monitored and reported upon on a regular basis in order to assess whether the process is operating as expected. The content of performance reports is set out in section 6 of this document, but it is vital that the reports are not only produced but are also communicated to the appropriate audience.

This will include the management of IT concerning resource utilisation and allocation. Depending on the health of the process it may be appropriate to hold regular meetings with IT management to discuss the performance and agree any actions to improve it.

2.7.5 Training for service asset and configuration management

In addition to a well-defined process and appropriate software tools it is essential that the people aspects of service asset and configuration management are adequately addressed. The process requires that training be provided to all participants in order that it runs as smoothly as possible.

The main areas in which training will be required for service asset and configuration management are as follows.

- The service asset and configuration management process itself, including the activities, roles and responsibilities involved
- Service Asset and Configuration management software tools such as the configuration management system
- The basics of the technology and how it is implemented within [Organization Name]
- The business, its structure, locations, priorities and people

3 Roles and responsibilities

This section describes the main operational roles involved in the service asset and configuration management process, their interaction with the process and their detailed responsibilities.

3.1 Operational roles

The following main roles participate in the service asset and configuration management process:

- Process Owner
- Process Manager
- Configuration Analyst
- Configuration Librarian

There will also be interaction with IT and business management at various points in the process.

3.2 RACI matrix

The table below clarifies the responsibilities of these roles at each step of the service asset and configuration management process using the RACI system, i.e.:

- R: Responsible
- A: Accountable
- C: Consulted
- I: Informed

STEP	PROCESS OWNER	PROCESS MANAGER	CONFIG ANALYST	CONFIG LIBRARIAN
Management and Planning	A/R	R	C	I
Configuration Identification	I	A	R	C
Configuration Control	I	A	C	R
Status Accounting and Reporting	I	A	C	R
Verification and Audit	I	A	R	C

Table 4: RACI matrix

3.3 Service asset and configuration management process owner

The responsibilities of the service asset and configuration management process owner are:

- Sponsoring, designing and change managing the process and its metrics
- Defining the process strategy
- Assisting with process design
- Ensuring that appropriate process documentation is available and current
- Defining appropriate policies and standards to be employed throughout the process
- Periodically auditing the process to ensure compliance to policy and standards
- Periodically reviewing the process strategy to ensure that it is still appropriate and change as required
- Communicating process information or changes as appropriate to ensure awareness
- Providing process resources to support activities required throughout the service lifecycle
- Ensuring process technicians have the required knowledge and the required technical and business understanding to deliver the process and understand their role in the process
- Reviewing opportunities for process enhancements and for improving the efficiency and effectiveness of the process
- Addressing issues with the running of the process
- Identifying improvement opportunities for inclusion in the CSI register
- Making improvements to the process
- Working with other process owners to ensure there is an integrated approach to service asset and configuration management, change management, release and deployment management and knowledge management
- Agreeing and documenting the scope for SACM, including the policy for determining which service assets should be treated as configuration items

3.4 Service asset and configuration management process manager

The responsibilities of the service asset and configuration management process manager are:

- Working with the process owner to plan and co-ordinate all process activities
- Ensuring all activities are carried out as required throughout the service lifecycle
- Appointing people to the required roles
- Managing resources assigned to the process
- Working with service owners and other process managers to ensure the smooth running of services
- Monitoring and reporting on process performance

- Identifying improvement opportunities for inclusion in the CSI register
- Working with the CSI manager and process owner to review and prioritise improvements in the CSI register
- Making improvements to the process implementation
- Planning and managing support for service asset and configuration management tools and processes
- Coordinating interfaces between service asset and configuration management and other service management processes
- Driving the efficiency and effectiveness of the service asset and configuration management process
- Producing management information
- Managing the work of service asset and configuration management staff
- Monitoring the effectiveness of service asset and configuration management and making recommendations for improvement
- Developing and maintaining the service asset and configuration management systems
- Developing and maintaining the service asset and configuration management process and procedures

3.5 Configuration analyst

The responsibilities of the configuration analyst are:

- Proposing scope for service asset and configuration management
- Supporting the process owner and process manager in the creation of principles, processes and procedures
- Defining the structure of the configuration management system including CI types, naming conventions, required and optional attributes and relationships
- Training staff in SACM principles, processes and procedures
- Performing configuration audits

3.6 Configuration librarian

The responsibilities of the configuration librarian are:

- Controlling the receipt, identification, storage and withdrawal of all supported CIs
- Maintaining status information on CIs and providing this as appropriate

- Archiving superseded CIs
- Assisting in conduction configuration audits
- Identifying, recording, storing and distributing issues related to service asset and configuration management

4 Associated documentation

The following documentation is relevant to the service asset and configuration management process and should be read in conjunction with it:

DOCUMENT	REFERENCE	VERSION	LOCATION
ITIL Service Transition Book	ISBN number	2011	[Network drive location]
Change Management Process	ITILST0201	V1.0 Final	[Network drive location]
Problem Management Process	ITILSO0401	V1.0 Final	[Network drive location]
Incident Management Process	ITILSO0301	V1.0 Final	[Network drive location]
Configuration management system user guide			[Network drive location]
Configuration management system admin guide			[Network drive location]

Table 5: Associated documentation

In the event that any of these items is not available please contact the service asset and configuration management process manager.

5 Interfaces and dependencies

The service asset and configuration management process has a number of interfaces and dependencies with other processes within service management and the business. These are outlined here and are described in further detail in the relevant procedural documentation.

5.1 Other service management processes

ITIL LIFECYCLE STAGE	PROCESS	INPUTS TO SACM FROM THE NAMED PROCESS	OUTPUTS FROM SACM TO THE NAMED PROCESS
Service Strategy	Financial Management for IT Services	Requests for inventory and asset information Procurement information for new CIs	Reports for financial and insurance purposes
Service Design	Information Security Management	Security requirements for access to the CMS Security policies	Correct (unaltered) configuration information. Reports on detected configuration changes
	Availability Management	Changes to CIs to improve availability (via change management)	Reports on single points of failure from CI relationship information
	Capacity Management	Advance notice of required changes to configurations for capacity reasons	Details of installed configurations and capacities
	Design Coordination	Co-ordination of production of SACM plans	Information about existing configurations for planning purposes
	IT Service Continuity Management	Requirements for control of key spares and software in an ITSCM situation	Provision of key spares and other CIs needed during an ITSCM incident
Service Transition	Release and Deployment Management	Requirements for baselines and release packages	Tracking of CIs within releases and provision of the right versions of CIs when required
	Knowledge Management	Requirements for integration with the SKMS	The CMS forms a key part of the overall SKMS and provides information linked to other knowledge items within it
	Service Validation and Testing	Requirements for control of test CIs	Provision of correct CI versions for testing
	Change Management	Information about changes to CIs	Impact assessment of proposed changes
Service Operation	Incident Management	Incidents linked to CIs	Information about CIs for use in incident diagnosis

ITIL LIFECYCLE STAGE	PROCESS	INPUTS TO SACM FROM THE NAMED PROCESS	OUTPUTS FROM SACM TO THE NAMED PROCESS
	Problem Management	Problems linked to CIs	Reports on CIs with many incidents against them. Information about CIs for use in problem investigation
	Event Management	Events logged against CIs	Information about the CIs that need to be monitored
	Request Fulfilment	Service requests linked to CIs	Reports of service requests by CI
Continual Service Improvement	7 Step Improvement Process	Process improvements	Requirements for improvement, details of improvements made

Table 6: Interfaces with other service management processes

5.2 Business processes

[Business processes will obviously be numerous and highly industry- and organization-specific. We therefore recommend that you only address those that are closely linked to the process in question here.]

BUSINESS AREA	BUSINESS PROCESS	INPUTS TO SACM FROM THE NAMED PROCESS	OUTPUTS FROM SACM TO THE NAMED PROCESS
Human Resources			
Finance	Procurement	Details of new items purchased for creation of CIs within the CMS	Ad-hoc reports on asset location and allocation
	Fixed Asset Management	Reporting requirements	Reports on IT assets and their locations, ages, disposal etc.
Sales and Marketing			
Production/Operations			
Legal and Compliance	Insurance	Reporting requirements	Regular reports on asset location and value
Research and Development			
Distribution and Logistics			
Customer Services			
Purchasing			
Public Relations			
Administration			
[Insert further business processes here]			

Table 7: Interfaces with business processes

6 Process measurements and metrics

In order to determine whether the service asset and configuration management process is working effectively and achieving what we want it to achieve, we must first define our critical success factors and identify how we will determine if they are being fulfilled.

6.1 Critical success factors

The following factors are defined as critical to the success of the service asset and configuration management process:

REF	CRITICAL SUCCESS FACTOR
CSF1	Creation and maintenance of an effective, complete and accurate configuration management system (CMS)
CSF2	Provision of configuration information to other service management processes at the right place and at the right time
CSF3	Protection of the integrity of configuration items throughout their lifecycle

Table 8: Critical success factors

Achievement of these critical success factors will be measured via the use of relevant Key Performance Indicators (KPIs).

6.2 Key performance indicators

The following KPIs will be used on a regular basis to evidence the successful operation of the service asset and configuration management process:

CSF REF	KPI REF	KEY PERFORMANCE INDICATOR
CSF1	KPI1.1	Percentage discrepancies found during CMS audits
	KPI1.2	Number of complaints about inaccurate CMS records
	KPI1.3	User satisfaction with the CMS
CSF2	KPI2.1	Percentage of incidents for which configuration information was available
	KPI2.2	Number of successful impact analyses carried for change management
	KPI2.3	Number of access of the CMS by problem management
CSF3	KPI3.1	Number of configuration errors caused by inadequate protection of CIs

CSF REF	KPI REF	KEY PERFORMANCE INDICATOR
	KPI3.2	Completeness of the definitive media library (DML)

Table 9: Key performance indicators

6.3 Process reviews and audits

Reviews will be carried out by the process owner in conjunction with the process manager on a three-monthly basis to assess whether the service asset and configuration management process is operating effectively and delivering the desired results.

These reviews will have the following as input:

- Follow-up action list from previous reviews
- Relevant changes and developments within the business and IT
- KPI reports from the previous period
- Details of all complaints logged during the period
- Internal and external audit reports
- Feedback from users and customers
- Identified opportunities for improvement

Each review will be documented by the process owner and actions arising agreed and published.

Audits will be carried out on an annual basis by the internal auditing department. The scope and timing of the audit will be agreed in advance. Recommendations from the audit will be published and actions discussed and agreed with the process owner.

All actions will be followed up by the internal auditor within the agreed timescales for each action.

7 Process reporting

It is important that regular reports are produced for two main reasons:

1. To help to assess whether the service asset and configuration management process is meeting its critical success factors (see section 6.1 above)
2. To assist the process manager in the day-to-day management of the service asset and configuration management process and its resourcing

These two purposes may require different views of the information available and will need to be produced at varying frequencies for differing audiences.

The format of the reports produced will also be subject to regular review and amendment as requirements become clearer and the available reporting technology within the business matures. What must be avoided is the continued production of reports that are not read and serve no purpose. It is up to the process owner, in consultation with the process manager, to ensure that all reporting remains focussed and relevant.

The following tables show the reports that will be produced together with their purpose, method of production, data source, audience and frequency. Some of the reports listed will be used for multiple purposes.

7.1 Process reports

The following reports are produced by the process manager and are intended to help the process owner assess whether the CSFs for service asset and configuration management are being met.

REF	REPORT TITLE	DESCRIPTION	METHOD OF PRODUCTION	DATA SOURCE	FREQ	AUDIENCE
CSFR1	Audit Report	Percentage discrepancies found during CMS audits	Figures taken from audit spreadsheet	Audit report	Ad-hoc	Process Owner
CSFR2	Complaints	Number of complaints about inaccurate CMS records	Report from complaints system	Complaints database	Monthly	Process Owner
CSFR3	User Satisfaction	User satisfaction with the CMS	Summary report from user satisfaction returns	User satisfaction spreadsheet	Six-Monthly	Process Owner
CSFR4	Incident Usage	Percentage of incidents for which configuration information was available	Report from incident management system	Incident management database	Monthly	Process Owner

REF	REPORT TITLE	DESCRIPTION	METHOD OF PRODUCTION	DATA SOURCE	FREQ	AUDIENCE
CSFR5	Change Usage	Number of successful impact analyses carried for change management	Report from change management system	Change management database	Monthly	Process Owner
CSFR6	Problem Usage	Number of access of the CMS by problem management	Report from problem management system	Problem management database	Monthly	Process Owner
CSFR7	Error Report	Number of configuration errors caused by inadequate protection of CIs	Report from incident management system	Incident management database	Monthly	Process Owner
CSFR8	DML Report	Completeness of the definitive media library (DML)	Comparison of number of items held against target number	CMS	Six-Monthly	Process Owner
CSFR13	[Insert further reports]					

Table 10: Process reports

7.2 Operational reports

The following reports are to provide further ongoing operational information to the process manager. They are in addition to the relevant process reports described above.

REF	REPORT TITLE	DESCRIPTION	METHOD OF PRODUCTION	DATA SOURCE	FREQ	AUDIENCE
OPR1	Capacity	Number of configuration records in the CMS (trend)	Report from CMS	CMS	Monthly	Change Manager
OPR2	CI Types	Breakdown of types of CIs held in CMS	Report from CMS	CMS	Monthly	Change Manager
OPR3	CI Status	Breakdown of statuses of CIs held in CMS	Report from CMS	CMS	Monthly	Change Manager
	[Insert further reports]					

Table 11: Operational reports

8 Glossary, abbreviations and references

8.1 Glossary

For a full list of terms used and their definitions within ITIL, please refer to the back of any of the books in the ITIL Lifecycle Suite 2011.

The following subset of terms is specifically relevant to this document:

TERM	MEANING
Assembly	A configuration item (CI) that is made up of other CIs
Assessment	Inspection and analysis to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency or effectiveness targets are being met
Asset	Any resource or capability
Asset management	A generic activity or process for tracking and reporting the value and ownership of assets throughout their lifecycle
Attribute	A piece of information about a configuration item
Audit	Formal inspection and verification 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
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	A snapshot that is used as a reference point
Build	The activity of assembling a number of configuration items to create part of an IT service.
Category	A named group of things that have something in common
Change	The addition, modification, or removal of anything that could have an effect on IT services
Change advisory board (CAB)	A group of people that support the assessment, prioritisation, authorisation and scheduling of changes
Change history	Information about all changes made to a configuration item during its life
Change management	The process responsible for controlling the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services
Change model	A repeatable way of dealing with a particular category of change
Change proposal	A document that includes a high-level description of a potential service introduction or significant change, along with a corresponding business case and an expected implementation schedule
Change record	A record containing the details of a change
Change schedule	A document that lists all authorised changes and their planned implementation dates, as well as the estimated dates of longer-term changes
CI type	A category that is used to classify configuration items

TERM	MEANING
Component CI	A configuration item that is part of an assembly
Configuration	A generic term used to describe a group of configuration items that work together to deliver an IT service, or a recognizable part of an IT service
Configuration baseline	The baseline of a configuration that has been formally agreed and is managed through the change management process
Configuration identification	The activity responsible for collecting information about configuration items and their relationships, and loading this information into the configuration management database
Configuration item	Any component or other service asset that needs to be managed in order to deliver an IT service
Configuration management database (CMDB)	A database used to store configuration records throughout their lifecycle
Configuration management system (CMS)	A set of tools, data and information that is used to support service asset and configuration management
Configuration record	A record containing the details of a configuration item
Configuration structure	The hierarchy and other relationships between all the configuration items that comprise a configuration
Continual service improvement	A stage in the lifecycle of a service. Continual service improvement ensures that services are aligned with changing business needs by identifying and implementing improvements to IT services that support business processes
Definitive media library (DML)	One or more locations in which the definitive and authorized versions of all software configuration items are securely stored
Deployment	The activity responsible for the movement of new or changed hardware, software, documentation, process etc. to the live environment
Emergency change	A change that must be introduced as soon as possible – for example to resolve a major incident or implement a security patch
Emergency CAB	A subgroup of the Change Advisory Board that makes decisions about emergency changes
Escalation	An activity that obtains additional resources when these are needed to meet service level targets or customer expectations.
Financial management	A generic term used to describe the function and processes responsible for managing an organization's budgeting, accounting and charging requirements
Fixed asset	A tangible business asset that has a long-term useful life (for example a building, a piece of land, a server or a software license)
Fixed asset management	The process responsible for tracking and reporting the value and ownership of fixed assets throughout their lifecycle
Impact	A measure of the effect of an incident, problem or change on business processes
Incident	An unplanned interruption to an IT service or reduction in the quality of an IT service
Incident management	The process responsible for managing the lifecycle of all incidents

TERM	MEANING
Integrity	A security principle that ensures data and configuration items are modified only by authorized personnel and activities
IT service	A service provided by an IT service provider. An IT service is made up of a combination of information technology, people and processes
Key performance indicator	A metric that is used to help manage an IT service, process, plan, project, or other activity
Model	A representation of a system, process, IT service, configuration item etc. that is used to help understand or predict future behaviour
Normal change	A change that is not an emergency or a standard change
Post-implementation review (PIR)	A review that take place after a change or a project has been implemented
Priority	A category used to identify the relative importance of an incident, problem or change
Problem	A cause of one or more incidents
Release	One or more changes to an IT service that are built, tested and deployed together
Remediation	Actions taken to recover after a failed change or release
Request for change (RFC)	A formal proposal for a change to be made
Service desk	The single point of contact between the service provider and the users
Service knowledge management system (SKMS)	A set of tools and databases that is used to manage knowledge, information and data
Service level agreement	An agreement between an IT service provider and a customer
Snapshot	The current state of a configuration item, process or any other set of data recorded at a specific point in time
Status accounting	The activity responsible for recording and reporting the lifecycle of each configuration item
Urgency	A measure of how long it will be until an incident, problem or change has a significant impact on the business
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
Verification and audit	The activities responsible for ensuring that information in the configuration management system is accurate and that all configuration items have been identified and recorded
Version	A version is used to identify a specific baseline of a configuration item
Vision	A description of what the organization intends to become in the future

Table 12: Glossary of relevant terms

8.2 Abbreviations

The following abbreviations are used in this document:

- CAB: Change Advisory Board
- CI: Configuration Item
- CMDB: Configuration Management Database
- CMS: Configuration Management System
- CSF: Critical Success Factor
- CSI: Continual Service Improvement
- DML: Definitive Media Library
- IT: Information Technology
- ITIL: Information Technology Infrastructure Library
- ITSCM: IT Service Continuity Management
- PO: Purchase Order
- RFC: Request for Change
- SACM: Service Asset and Configuration Management
- SKMS: Service Knowledge Management System

8.3 References

The following sources have been used in the creation of this process document and should be consulted for more information on particular aspects of it:

- ITIL Service Transition Book 2011. Copyright © AXELOS Limited 2011
- [Organization Name] IT organization structure, published dd/mm/yyyy
- [Organization Name] Business Strategy yyyy-yyyy
- [Organization Name] IT Strategy yyyy-yyyy
- [Organization Name] IT Service Management Strategy yyyy-yyyy