CWDS
Knowledge Management ITIL Detailed Design

Created by:

Project Name: ***CWDS Service Desk Support Services***
Document ID: Knowledge Management Detailed Design.docx
Version: ***1.0***
Issue Date: **01/22/2018**

Revision History

Date	Version	Description	Author
27-Dec-17	1.0	Knowledge Management ITIL Detailed Design Plan	Jim McKennan

Approvals

Approver Name	Department/Role	Signature	Date

Table of Contents

1. Introduction

The purpose of this document is to provide a detailed design of the **CWDS** Knowledge Management (KM) process. It includes the detailed workflows, RACI (Responsible, Accountable, Consulted and Informed) matrices and procedure definitions for managing the KM process.

The content within this document is based on the ITIL® framework[1].

The following sections provide a detailed view of the **CWDS** Knowledge Management process. Each section contains a detailed process flow diagram, showing the procedure order, a RACI table and detailed procedure descriptions.

The procedure descriptions include title, purpose, policy statement, input, procedure or work instruction steps, output, audit/controls and metrics. This Detailed Design is largely beyond the scope of the ITIL Service Lifecycle books; however, it builds on the Knowledge Management High Level Design which follows ITIL[1] best practices.

1.1. Purpose

The purpose of the Knowledge Management (KM) Process is to share perspectives, ideas, experience and information; to ensure that these are available in the right place at the right time to enable informed decisions; and to improve OSI efficiency by reducing the need to rediscover knowledge.
The key objectives of KM are to:

- Improve the quality of management decision-making by ensuring that reliable and secure knowledge, information and data is available throughout the service lifecycle.
- Improve efficiency and quality of service.
- Increase user satisfaction and reduce cost.
- Ensure that staff have a clear and common understanding of the value that their services provide to customers and the ways in which benefits are realized from the use of those services.
- Maintain a Service Knowledge Management System (SKMS) that provides controlled access to knowledge, information and data that is appropriate for each audience.
- Gather, analyze, store, share use and maintain knowledge, information and data throughout OSI.

1.2. Scope

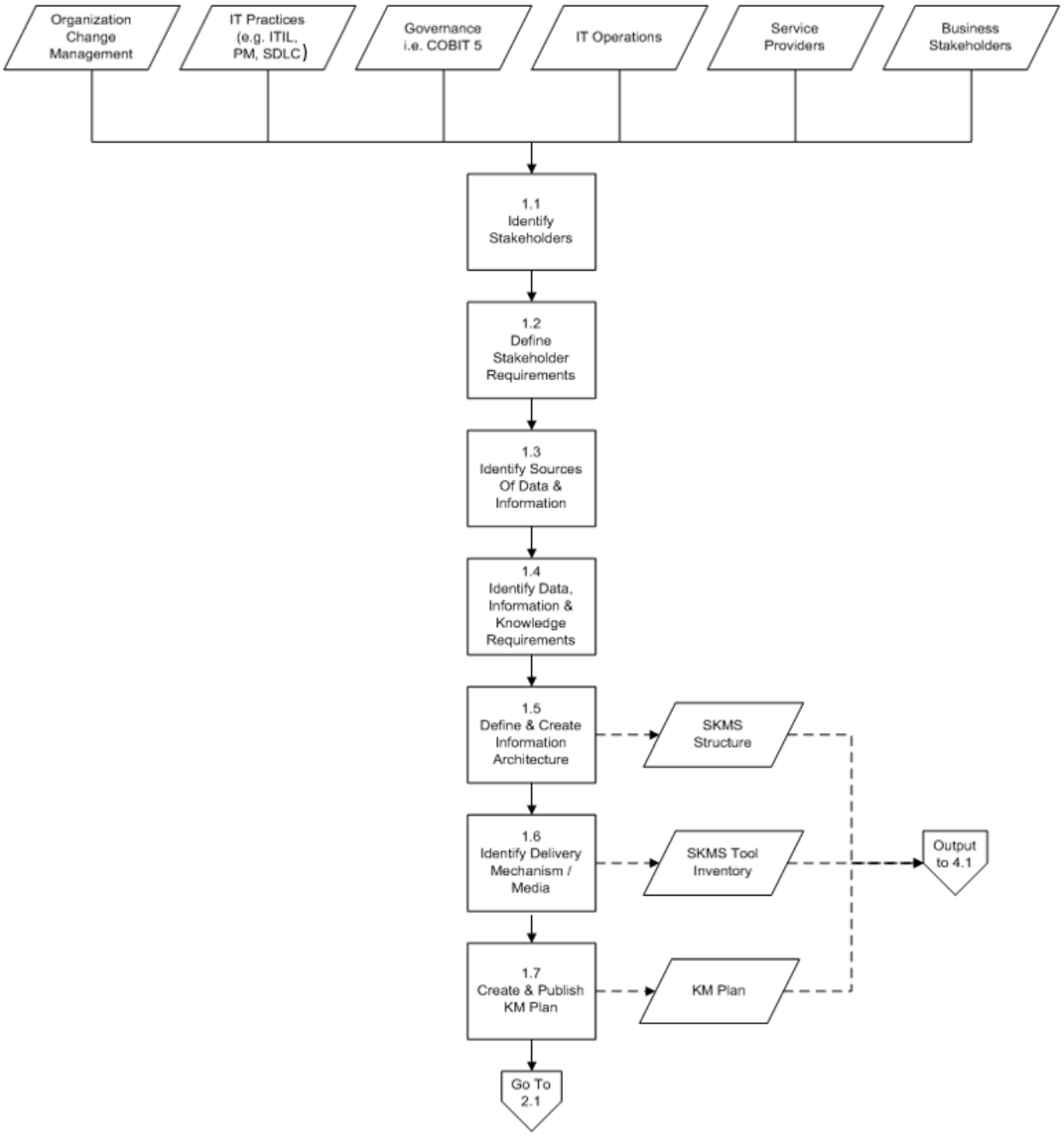
KM is a whole (ITIL) lifecycle-wide process that is relevant to all lifecycle stages and processes. KM includes oversight of the management of knowledge and the information and data from which that knowledge derives.

1.3. Referenced Documents

ITIL Service Strategy 2011 Edition; ITIL Service Design 2011 Edition; ITIL Service Transition 2011 Edition; ITIL Service Operation 2011 Edition; ITIL Continual Service Improvement 2011 Edition; COBIT 5 (Control Objectives for Information and related Technology) “Enabling Processes” 2012, ISACA.

[1] ITIL® is a Registered Trade Mark of the AXELOS Limited.

2. Activity 1.0 – Knowledge Planning & Management



2.1. RACI Matrix

Process Roles / Process Activities	Knowledge Management Process Owner	Knowledge Management Process Manager	Knowledge Management Practitioner (Librarian)	Knowledge Artifact Owner	Knowledge Artifact Consumer	SKMS Tool Administrator	Business/User Stakeholders
1.1 Identify Stakeholders	A	R,C,I	R	C	C,I	C	C
1.2 Define Stakeholder Requirements	A	R,C,I	R	C	C,I	C	C
1.3 Identify Sources Of Data & Information	A	R,C,I	R	R,C	C,I	R,C	C
1.4 Identify Data, Information & Knowledge Requirements	A	R,C,I	R	R,C	C,I	C	C
1.5 Define & Create Information Architecture	A	R,C,I	R	C,I	C,I	C,I	C
1.6 Define Delivery Mechanisms/Media	A	R,C,I	R	C,I	C,I	C,I	C
1.7 Create & Publish KM Plan	A, I	R,C,I	R	I	C,I	C,I	C,I

Legend

R = Responsible: Executes the task
A = Accountable: Accountable for final result
C = Consulted: Consulted about the task to provide additional information
I = Informed: Needs to be kept up-to-date on activities/tasks

2.2. Procedure Descriptions

1.1	Identify Stakeholders
Purpose	Everyone who has responsibility for creating and managing knowledge and everyone who may be dependent on knowledge in the execution of their functions and roles are identified as a stakeholder in the process.
Policy Statement	The KM Process Owner ensures that all Stakeholders of the KM process are identified and updated on an ongoing basis.

Input	• Scope statement
	• Goals and Objectives statement
	• KM strategy
	• Organization chart
	• RACI Matrices for
	  o Functional job descriptions and deliverables
	  o Process role descriptions and deliverables

Procedure or Work Instruction Steps	Using the inputs, create a list of stakeholders in the KM process that includes the following information: • Name • Job title and function • Process role assignment(s) • Level of authority • Customers and users as consumers of knowledge (if in scope)
Output	Stakeholder names, job functions, process roles and deliverables
Metric	Number of stakeholders identified
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

1.2	Define Stakeholder Requirements
Purpose	To ensure that the specific knowledge requirements of all stakeholders are clearly defined and documented. In this way knowledge content and levels of access to the content can be appropriately planned and delivered.
Policy Statement	The KM Process Owner ensures that the specific requirements for all KM stakeholders will be defined and documented. Further, they will be used as the basis for the creation and management of all Knowledge Artifacts (KA) as well as access to those artifacts.
Input	Stakeholder names, job functions, process roles and deliverables
Procedure or Work Instruction Steps	• Consult with HR, corporate training to determine competency requirements of specific job functions • Identify and confirm existing knowledge content in use • Conduct stakeholder interviews to determine, for each specific responsibility identified in job functions and process roles, the type of knowledge required to support and enable successful execution of responsibilities

1.2	**Define Stakeholder Requirements**
	• Identify if there are gaps between information from interviews and existing HR/ IT training capabilities • Identify the ways in which the stakeholders access/ receive knowledge, how it is consumed • Identify the delivery mechanisms in use/ required for the successful role-based transfer of knowledge to stakeholders
Output	• Process specific knowledge requirements • Function specific knowledge requirements • Service specific knowledge requirements
Metric	Number of steps completed
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

1.3	**Identify Sources Of Data & Information**
Purpose	Knowledge is derived from underlying data and information that is an outcome of service delivery activities across the entire service lifecycle. The sources of the underlying data and information will be identified and used to meet current and future needs for knowledge across the entire service lifecycle.
Policy Statement	The KM Process Owner ensures that all sources of data and information are identified and validated as reliable and trustworthy for the purposes of creating, transferring and maintaining all KA.
Input	• Systems management tools and database inventory • IT Service Management tools inventory • Monitoring tools inventory • Service Portfolio • Service Catalog • CMS/ CMDB

Procedure or Work Instruction Steps	• Identify sources of data and information through:
	  ○ Conducting interviews within Digital Service Groups
	  ○ Researching current tools in use that may be data sources/information, (e.g. ServiceNow, existing knowledge base maintained by IBM/OSI; application release notes, user guides etc.);
	  ○ Consulting with vendor management to identify external sources of knowledge (e.g. from vendors, web-sites etc.)
	• Document the nature of the data/information each contains and who manages the sources (e.g. Incident workarounds managed by Incident Management; Lessons Learned maintained by the Project Office, DevOps, Implementation Team, Digital Services)

Output	Inventory of data and information sources

1.3	Identify Sources Of Data & Information
Metric	Number of sources identified
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

1.4	Identify Data, Information & Knowledge Requirements
Purpose	To ensure the organization is capable of managing the source information for all KM content and that it can be converted into useful KA as required.
Policy Statement	The KM Process Owner ensures that Data and Information are managed and kept accurate, up-to-date and relevant for use across the service lifecycle as KA.
Input	• KM strategy • Inventory of information and data sources • KM information architecture • Stakeholder requirements documentation
Procedure or Work Instruction Steps	• Identify existing sources of information across the service lifecycle stages. For example: o Workarounds discovered and used in Incident Management o Defects identified in testing that will not be removed prior to deployment o List of known issues / bugs and workarounds (if any) o Change management submission requirements for a significant change o Lessons learned from DevOps, Implementation Team, Digital Services, etc. o Architecture standards to be followed by DevOps Team • Track and analyze number of changes, additions and deletions in data and information sources (e.g. service portfolio, service catalog, CMDB) • Validate the accuracy and relevance of the information and identify specific data/information that is needed to create KA • Review existing process outputs and service outcomes across the entire service lifecycle to identify the value and usefulness of existing knowledge, areas where knowledge content is inadequate, incorrect or not available o Analyze underlying data and information sources to ascertain areas of improvement needed o Analyze KA and compare to data sources to identify gaps and improvement opportunities o Prioritize improvement opportunities based on service impact of knowledge improvements o Work with process owners and Continual Service Improvement (CSI) to create action plans to address KM requirements

1.4	Identify Data, Information & Knowledge Requirements
Output	Requirements for input to design and creation of Data Architecture
Metric	Number of steps completed
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

1.5	Define & Create Information Architecture
Purpose	To ensure that Digital Services is capable of identifying, creating, managing and sharing knowledge for all stakeholders across the entire service lifecycle in a timely, efficient and cost effective manner. The information architecture will form the basis for the creation of the Service Knowledge Management System (SKMS).
Policy Statement	The KM Process Owner ensures that the information architecture is defined, documented and managed. This is to ensure that all tools needed and used to provide the underlying data and the information derived from that data can effectively deliver the required knowledge to the organization as needed. The architecture will be built on the data-information-knowledge-wisdom (DIKW) concept.
Input	• Data, information and knowledge requirements • Data repositories and tools that constitute the SKMS (e.g. ITSM tools such as ServiceNow and JIRA, systems management/monitoring tools)

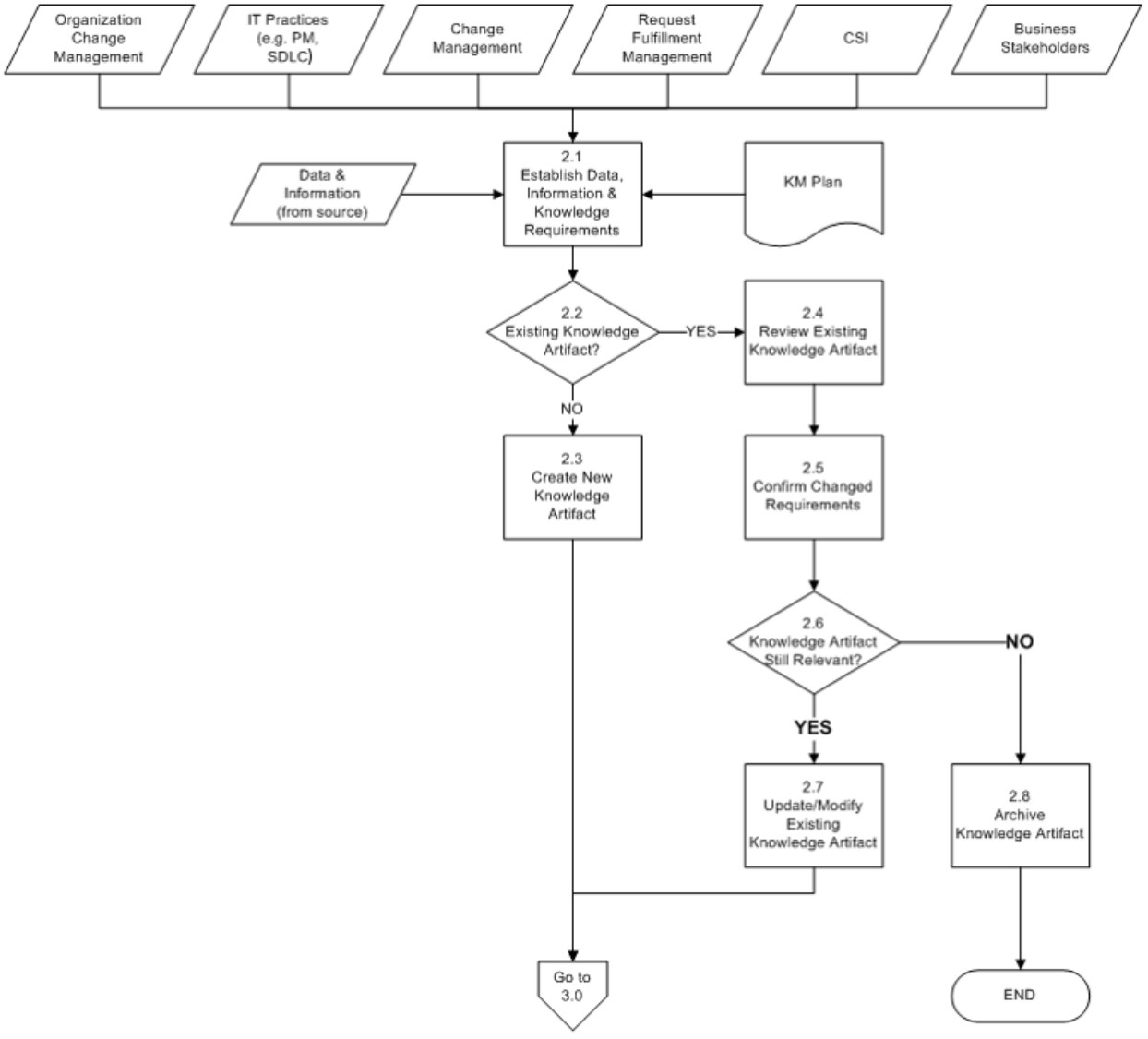
Procedure or Work Instruction Steps	• Create and regularly update a service management information model that enables creation, use and sharing of information that meets stakeholder needs
	• Adopt data classification schema that are in use across the organization
	• Define data classification schema based on service management principles and aligned with existing CMS and CMDB schema
	• Identify and document all tools in each layer of the information architecture for example:
	  o Data Layer: tools that discover, collect, protect, share, audit and archive the data
	  o Information Integration Layer: tools that enable data from multiple sources to be integrated, e.g. schema mapping, metadata management, reconciliation, extraction, transforming, mining
	  o Knowledge processing layer: tools for query and analysis, reporting, performance management, modeling, monitoring and alerting
	  o Presentation Layer: IT governance view, quality management view, service view, asset and configuration view, service desk and support view, self-service view

1.5	Define & Create Information Architecture
Output	• Information Architecture Documentation • Basis for definition and creation of SKMS
Metric	Number of tools identified and documented
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

1.6	Identify Delivery Mechanism / Media
Purpose	Knowledge transfer is enabled so all stakeholders will have access to the knowledge needed to successfully carry out specific tasks in the course of delivering quality service to the customer in a timely and cost effective manner.
Policy Statement	The KM Process Owner ensures that knowledge will be delivered to the stakeholders consuming the knowledge in accordance with its nature and use. This is in addition to the tools made available through the information architecture.
Input	• Information Architecture • Training Strategy and Plans • Communication Strategy and Plans • Operation and Support Plans • Process Management policies and procedures for all processes
Procedure or Work Instruction Steps	• Identify the current and planned knowledge transfer capabilities of the organization and how they can be leveraged to deliver knowledge • Identify learning styles, current practices and preferences of those receiving/using the knowledge • Establish the standards for delivering knowledge for each stakeholder group based on identified learning styles, current capabilities defined in the information architecture, and current organizational practices for communication and training, including such mechanisms as webinars, seminars, formal classroom training, Instructor-Led Online (ILO) or Self Paced Online training (SPO) • Create documentation such as job aids and user guides for self-help/ self-learning • Publish newsletters and journals • Promote learning via social media internally • Take into consideration requirements for confidentiality of information being made available to the staff • Identify gaps or opportunities to expand this capability
Output	Inventory of Knowledge Transfer Tools and Media, including identification of gaps in current capabilities
Metric	Number of steps completed
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

1.7	**Create & Publish KM Plan**
Purpose	Creation and maintenance of a relevant and executable KM Plan enabling a robust KM process.
Policy Statement	The KM Process Owner ensures that a current and up-to-date KM Plan is created and maintained.
Input	• KM Strategy • Stakeholder requirements • KM Scope statement • KM data sources inventory • Information Architecture (SKMS layers, Service Portfolio, Service Catalog, CMDB)
Procedure or Work Instruction Steps	• Define contents of the KM Plan • Define the media to be used and tool(s) to enable publication of the Plan • Identify resources required to produce the Plan • Write the Plan • Approve the Plan • Publish the Plan • Periodically review and update the Plan according to policy standards
Output	Fully documented KM Plan
Metric	Number of steps completed
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

3. Activity 2.0 – Manage Data, Information & Knowledge



3.1. RACI Matrix

Process Roles / Process Activities	Knowledge Management Process Owner	Knowledge Management Process Manager	Knowledge Management Practitioner (Librarian)	Knowledge Artifact Owner	Knowledge Artifact Consumer	SKMS Tool Administrator	Business/User Stakeholders
2.1 Establish Data, Information & Knowledge Requirements	A	R,C,I	R	C, I	C	C,I	C,I
2.2 Existing Knowledge Artifact?	A	R,C,I	R	C, I	C		C
2.3 Create New Knowledge Artifact	A	R,C,I	R	C, I	I	C	C,I
2.4 Review Existing Knowledge Artifact	A	C,I	R	C,I	C		
2.5 Confirm Changed Requirements	A	R,C,I	R	C,I	C		C
2.6 Knowledge Artifact Still Relevant?	A	C,I	R	C,I	C		C
2.7 Update/Modify Existing Knowledge Artifact	A	R,C,I	R,C	R	C,I		C,I
2.8 Archive Knowledge Artifact	A	C,I	R	C,I	I		

Legend

R = Responsible: Executes the task
A = Accountable: Accountable for final result
C = Consulted: Consulted about the task to provide additional information
I = Informed: Needs to be kept up-to-date on activities/tasks

3.2. Procedure Descriptions

2.1	Establish Data, Information & Knowledge Requirements
Purpose	To understand, define and document the requirements for specific KA needed to support effective and efficient delivery of services to the Stakeholders and Users. Requirements include specific content, format of the content, frequency of updates to content, sources of and audiences for content.
Policy Statement	The KM Process Owner ensures that requirements for knowledge are identified and documented.

Input	• Data and Information from source, e.g.:
	  o Stakeholder input/feedback
	  o Process outputs and outcomes, reports
	  o Data about usage of existing capabilities

Procedure or Work Instruction Steps	• Assess current KA to identify knowledge gaps and areas where knowledge is outdated or no longer relevant • Conduct review sessions with Process Owners/KM Process Managers, Service Owners, IT support staff and all functional areas of IT to determine needs • Review management reports and identify specific areas of need and specific requirements for KA content, format and category of the KA – e.g. technical, project, ITSM process, organizational, agreement, operations and information • Define reason for collection • Establish common and uniform content and format requirements based on category and reason for collection and expected purpose/use of artifacts • Establish requirements for data protection, privacy, security, ownership, agreement restrictions, rights of access, intellectual property and patents
Output	Documented, detailed and specific KA requirements
Metric	Number of steps completed
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

2.2	Existing Knowledge Artifact?
Purpose	To determine if a new KA is required or if a change to existing KA is required.
Policy Statement	If changes are required on an existing KA or if a new KA is required, the KM Process Owner ensures that it is identified.
Input	• KM Policy • KM Plan • KA requirements documentation
Procedure Or Work Instruction	• Review the KA requirements documentation and compare to the existing KA database information

2.2	**Existing Knowledge Artifact?**

Steps	• Determine if existing KA requires changes or if a new KA is required
	  o If changes to an existing KA required go to 2.4
	  o If a new KA is required go to 2.3

Output	Determination of existing KA or requirement for new KA
Metric	Number of steps completed
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

2.3	**Create New Knowledge Artifact**
Purpose	To create KA in a format that can be used to effectively manage and deliver services to the Users. This includes all functional areas of IT, all practices and processes being managed within OSI and any knowledge pertaining to external suppliers that is relevant to internal staff.
Policy Statement	The KM Process Owner ensures that any new KA are created and published in the appropriate media in accordance with policy standards.
Input	• KM Policy • KM Plan • KA requirements documentation • KA template

Procedure Or Work Instruction Steps	• Review requirements for the new KA
	• Identify the data and information that will underpin the KA
	• Identify the KA category and based on the category assigned, create KA to include the following information:
	  o Identification/ name
	  o Specific relevant knowledge in the KA template
	  o Media to be used to publish the KA
	  o Audience and specific access rights required to access the KA

Output	Fully documented KA and completed KA template
Metric	Number of steps completed
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

2.4	**Review Existing Knowledge Artifact**
Purpose	When there are changes to the underlying data and information, the KM Process Owner ensures that these changes are reviewed to determine what changes to the KA may be warranted.
Policy Statement	When notification is received about data and information changes, it is the responsibility of the KA Owner to ensure that the KA are reviewed and new requirements identified.
Input	Input from any identified source of data or information that supports the KA, such as ServiceNow, GitHub, WIKI's, service providers, regulatory bodies etc.
Procedure Or Work Instruction Steps	• Review sources of data and information that have been notified as changing • Match the data and information received with the appropriate KA • Compare new data and information received with that for existing KA to determine what changes are required to update or revise the knowledge artifact
Output	Reviewed data, information and KA
Metric	Number of steps completed
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

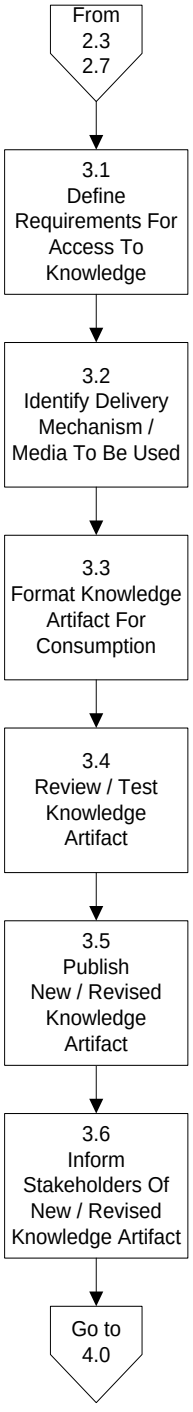
2.5	**Confirm Changed Requirements**
Purpose	To ensure that the appropriate and necessary changes to KA are identified and documented for further action and that the KA is still relevant and necessary.
Policy Statement	When notified of changes in underlying data and information the KA Process Owner ensures that changes to the KA being driven by the new data and information are defined.
Input	• New data and information • Existing KA
Procedure Or Work Instruction Steps	Analyze the data and information to confirm the changes that are required in the KA
Output	Analyzed data and information
Metric	Number of KA analyzed
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

2.6	**Knowledge Artifact Still Relevant?**
Purpose	To determine if the KA is still relevant and useful or if the KA is outdated and needs to be archived/replaced.
Policy Statement	When changed data and information for a KA is received the KA Process Owner must determine if the KA is still needed and relevant.
Input	• KA • Changed data and information that underpins the KA
Procedure Or Work Instruction Steps	• Analyze the changes in the data and information, comparing the current data and information with the changed data and information • Determine if the KA still meets the needs of the audience • If KA still relevant go to 2.7 • If KA is no longer relevant then go to 2.8
Output	Relevant and irrelevant KA
Metric	• Number of KA reviewed and deemed relevant • Number of KA ready to be retired/archived
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

2.7	**Update/ Modify Existing Knowledge Artifact**
Purpose	To ensure that when changes to underlying data and information occur, the knowledge artifact that is derived from that data is updated to reflect the current state.
Policy Statement	When underlying data and information require changes to the KA they support, the KA Process Owner ensures that the KA is updated accordingly.
Input	KA analyzed that were deemed relevant
Procedure Or Work Instruction Steps	• Identify the specific content changes to the knowledge required • Identify any changes or adjustments to the delivery of the knowledge itself • Update the KA content • Notify the ServiceNow Administrator/KA Owner of the changes required to deliver the knowledge to the audience
Output	Updated KA
Metric	Number of KA updated
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

2.8	**Archive Knowledge Artifact**
Purpose	To ensure that knowledge that is no longer valid or relevant is archived so that it is not available to anyone and cannot be used in error.
Policy Statement	When the KA is to be archived, the KM Process Owner ensures that the appropriate steps are taken to remove access to the KA itself.
Input	KA identified as no longer relevant
Procedure Or Work Instruction Steps	• Select the designated knowledge artifact • Change the status of the KA to 'retired' • Remove all access to the KA • Inform stakeholders of the KA that it has been archived and should no longer be relied on as up to date or used as a source of knowledge
Output	Archived KA
Metric	Number of archived KA
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

4. Activity 3.0 – Publish Knowledge



4.1. RACI Matrix

Process Roles / Process Activities	Knowledge Management Process Owner	Knowledge Management Process Manager	Knowledge Management Practitioner (Librarian)	Knowledge Artifact Owner	Knowledge Artifact Consumer	SKMS Tool Administrator	Business/User Stakeholders
3.1 Define Requirements For Access To Knowledge	A	R,C	R	C	C		C
3.2 Identify Delivery Mechanism/Media To Be Used	A	R,C	R	R,C	C,I		C
3.3 Format Knowledge Artifact For Consumption	A	R,C	R	R,C	C,I		C
3.4 Revie /Test Knowledge Artifact	A	R,I	R	R			
3.5 Publish New/Revised Knowledge Artifact	A	R,C,I	R	I	I		I
3.6 Inform Stakeholders of New/Revised Knowledge Artifact	A	R,C,I	R	C	I		C,I

Legend

R = Responsible: Executes the task
A = Accountable: Accountable for final result
C = Consulted: Consulted about the task to provide additional information
I = Informed: Needs to be kept up-to-date on activities/tasks

4.2. Procedure Descriptions

3.1	Define Requirements For Access To Knowledge
Purpose	The specific audience that requires access to specified KA is identified and defined to ensure they have the necessary information to make decisions, identify correct actions and execute tasks efficiently and effectively with positive results.
Policy Statement	The KM Process Owner ensures that the audience has been defined that requires access to knowledge. They also define the specific access requirements for that audience.
Input	• Security policy that defines information types for purposes of defining access rights to information • Stakeholder analysis • Roles and responsibilities of the audience
Procedure Or Work Instruction Steps	In order to make use of the KA, it must be accessible in a format that meets the specific needs of the intended audience. • Based on the identified roles and responsibilities of specific audience(s), and the KA requirements, identify the tool(s) to be used to gain access to the KA (such as ServiceNow, GitHub, WIKI, etc.) • Define the format of the knowledge to be accessed by the target audience • Confirm that the category of information for security purposes and the access rights of the audience are correctly aligned • For example, if the knowledge artifact explains how to apply a workaround to a specific incident then the KA must be accessible to the support role who would be assigned to apply the workaround • Determine who the audience is for the new or updated KA • Determine which tool(s) would be needed to access the data
Output	Defined requirements for access to modified/changed KA
Metric	Number of new access requirements
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

3.2	Identify Delivery Mechanism/ Media To Be Used
Purpose	To create KA in a format that can be used to effectively and efficiently manage and deliver services to the User. This includes all functional areas of IT, all practices and processes being managed within OSI and any knowledge pertaining to external suppliers that is relevant to internal staff.
Policy Statement	The KM Process Owner ensures that the KA are created and published in the appropriate media in accordance with policy standards.
Input	• KM Policy • KM Plan • KA requirements documentation
Procedure	• Based on the intended audience for/use-of the KA identify, the tool/

3.2	Identify Delivery Mechanism/ Media To Be Used
Or Work Instruction Steps	media to be employed to transfer knowledge to the audience • Use the data classification schema to ensure that KA in the same category are published in a consistent manner (i.e. specific category should have common templates for content delivery using the same format, same tools with same look and feel to users/consumers) • In many instances this will include multi-media, e.g. user guide in document format accompanied by interactive presentation that allows user to review the knowledge and answer a quiz about the knowledge and be given recognition for completion of the material
Output	List of tools/media to be used for knowledge transfer
Metric	Number of tools/media identified for knowledge transfer
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

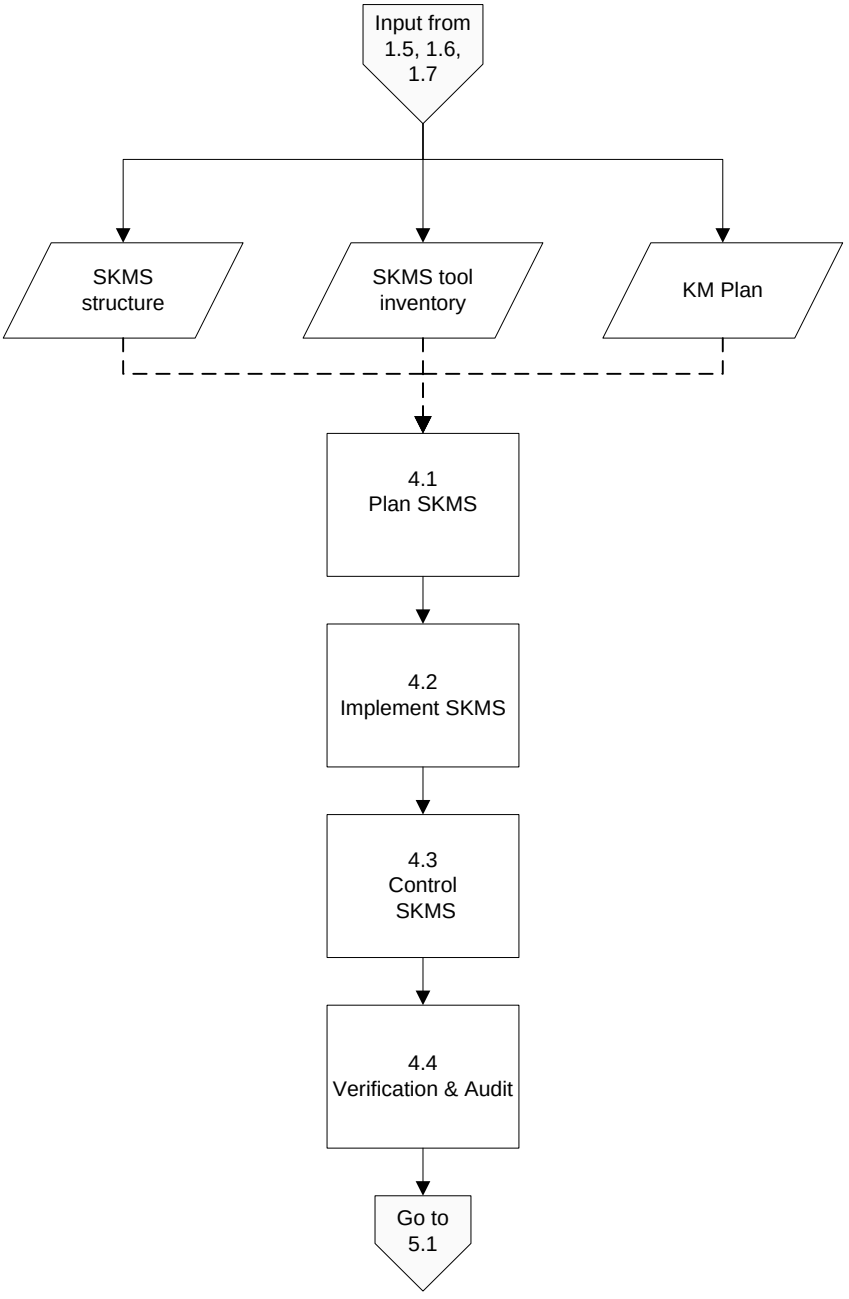
3.3	Format Knowledge Artifact For Consumption
Purpose	Create the KA in a format that supports the requirements of the audience
Policy Statement	The KM Process Owner ensures the KA is fit for use and fit for purpose by formatting the KA in the appropriate tool (ServiceNow, GitHub, WIKI) to be accessed by the consuming audience.
Input	KA requirements document
Procedure Or Work Instruction Steps	• Using the designated tool/media, format the knowledge content • E.g.: A workaround is documented for use to resolve a bug in a new application being launched; this knowledge will be shared with the Service Desk and other operational support teams prior to release
Output	Completed KA ready for testing/review
Metric	Number or completed KA ready for testing/review
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

3.4	**Review/Test Knowledge Artifact**
Purpose	The KA is reviewed and where appropriate/necessary it is tested to ensure that access by audience is assured and that the content of the KA meets stakeholder needs.
Policy Statement	The KM Process Owner ensures that the KA is reviewed/tested so that the KA can be accessed in a timely manner and it meets the needs of the audience.
Input	• Knowledge requirements • Knowledge artifact
Procedure Or Work Instruction Steps	Conduct a formal test of the KA to ensure that it is accessible to its intended audience, that it displays content that is accurate, useable and in the format required by the audience
Output	Tested KA
Metric	• Number of KA tested • Number failed • Number passed
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

3.5	**Publish New/Revised Knowledge Artifact**
Purpose	Publication of a new or revised KA is the actual means by which the knowledge is made available to its intended audience in a format that meets the audience's specific requirements.
Policy Statement	The KM Process Owner ensures that the new or revised KA is published in ServiceNow, GitHub, WIKI, etc.
Input	• KA content • KA requirements
Procedure Or Work Instruction Steps	Finalize the KA in ServiceNow, GitHub, WIKI and change the status of the KA to operational
Output	Operational KA in ServiceNow, GitHub, WIKI, etc.
Metric	Number of KA state changed to operational
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

3.6	**Inform Stakeholders of New/Revised Knowledge Artifact**
Purpose	Stakeholders of each KA that is created, modified or archived are advised of the status changes of existing KA under their control.
Policy Statement	The KM Process Owner ensures that all stakeholders are informed of new KA as well as changes to existing KA.
Input	• Audience list • KA published list
Procedure Or Work Instruction Steps	• Announce the updated or new KA with instructions for who can access the knowledge and for what reasons the knowledge is to be used; include specific work instructions as needed to support this activity • Develop and execute a Communications Plan to advertise the publication of new or updated KA. This includes relevant details for those who will manage the knowledge content, those that may use the content to deliver training and those that will consume the content for a specific intended purpose
Output	• Communication Plan • Announcements regarding new or updated KA
Metric	Number of announcements regarding new or updated KA
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

5. Activity 4.0 – Manage SKMS



5.1. RACI Matrix

Process Roles / Process Activities	Knowledge Management Process Owner	Knowledge Management Process Manager	Knowledge Management Practitioner (Librarian)	Knowledge Artifact Owner	Knowledge Artifact Consumer	SKMS Tool Administrator	Business/User Stakeholders
4.1 Plan SKMS	A	R,C,I	R	C, I	C	R,C	C
4.2 Implement SKMS	A	R,C,I	C,I	C,I	I	R,C	I
4.3 Control SKMS	A	R,C,I	R,C,I	C,I	I	R,C	I
4.4 Verification & Audit	A	R,C,I	R,C,I	R	I	I	I

Legend

R = Responsible: Executes the task
A = Accountable: Accountable for final result
C = Consulted: Consulted about the task to provide additional information
I = Informed: Needs to be kept up-to-date on activities/tasks

5.2. Procedure Descriptions

4.1	Plan SKMS
Purpose	To ensure knowledge and the KA required by stakeholders is created, managed and made readily available to the target audiences.
Policy Statement	The KM Process Owner ensures that knowledge is readily accessible to the stakeholders that are dependent on that specific knowledge.
Input	• Information Architecture • SKMS (Service Knowledge Management System) Tool inventory including CMS (Configuration Management System) and CMDB (Configuration Management Database) • Knowledge Management Plan • SACM (Service Access Configuration Management) process input based on current scope and scale of CMDB

Procedure Or Work Instruction Steps	• Review the Information Architecture, Tool Inventory and Knowledge Management Plan
	• Define the Data Layer, Information Integration Layer, Knowledge Processing Layer and Presentation Layer are capable of providing knowledge so that:
	  o Content for specific audience and use is available
	  o Format ensures that knowledge can be consumed by intended audience
	  o Changes to source data and information are reflected in knowledge artifact updates in a timely manner
	• Identify key process integration points to ensure that SKMS content is kept accurate and up-to-date. This is accomplished via real-time integration of ITSM process inputs to KM process
	• Establish control mechanisms and verification procedures to ensure knowledge is accurate, relevant and accessible at all times for all audiences
	• Establish feedback mechanisms to ensure that stakeholder concerns, knowledge incidents and gaps are identified and can be addressed

Output	SKMS Plan
Metric	Number of steps completed
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

4.2	Implement SKMS
Purpose	The identified data and information sources and the knowledge transfer capabilities enabling access to the KA are configured and made operational for day to day real-time creation, management and consumption of knowledge across the service lifecycle.
Policy Statement	The KM Process Owner ensures that the tools necessary to create, manage and deliver knowledge are fully implemented.

4.2	**Implement SKMS**
Input	• Information Architecture • SKMS Tool inventory (including CMS and CMDB) • Knowledge Management Plan

Procedure Or Work Instruction Steps	• Execute the SKMS Plan
	• Perform ongoing checks to ensure that stakeholders can search, find, retrieve and consume knowledge as required
	• Review the Information Architecture, Tool Inventory and Knowledge Management Plan
	• Implement the Data Layer, Information Integration Layer, Knowledge Processing Layer and Presentation Layer so they are capable of providing knowledge so that:
	  o Content for specific audience and use is available
	  o Format ensures that knowledge can be consumed by intended audience
	  o Changes to source data and information are reflected in knowledge artifact updates in a timely manner
	• Configure the key process integration points to ensure that SKMS content is kept accurate and up-to-date through real time integration of KM Process inputs to the ITSM Process

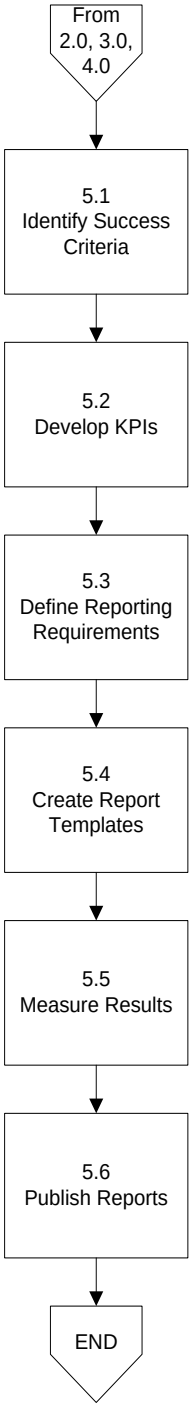
Output	Live SKMS
Metric	Number of steps completed
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

4.3	**Control SKMS**
Purpose	Knowledge and the KA required by stakeholders continues to be relevant, up-to-date and accurate by ensuring that the four layers of the SKMS structure can continue to provide relevant, up-to-date and accurate knowledge for the organization.
Policy Statement	The KM Process Owner ensures that the configuration, integration and use of all tools within the SKMS are managed in a controlled and planned manner.
Input	• Information Architecture • SKMS Tool Inventory including CMS and CMDB • Knowledge Management Plan
Procedure Or Work Instruction Steps	• Review all requests and plans that directly impact data sources, processing tools and presentation tools • Validate changes to any tool within the SKMS for impact on the accuracy and availability of knowledge via the SKMS to the consumers of the knowledge • Approve change to the components within the SKMS • Execute changes as approved
Output	Changes to SKMS structure and/or content
Metric	• Number of successful changes to the SKMS structure or contents

4.3	Control SKMS
	• Number of unsuccessful changes to the SKMS structure or contents
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

4.4	Verification & Audit
Purpose	Changes to the structure/tools that form the SKMS and to the KA contained within the SKMS are reviewed on the basis of scheduled audits as well as whenever changes to the structure/tools or content are made.
Policy Statement	The KM Process Owner ensures that regular reviews in the form of audits and verifications are carried out.
Input	• Information Architecture • SKMS Tool Inventory (including CMS and CMDB) • Knowledge Management Plan • Request For Change's (RFC) and Change Schedule
Procedure Or Work Instruction Steps	• Schedule periodic reviews of the SKMS Tool Inventory to validate accuracy of discovery data • Verify that any changes to the SKMS itself or changes that indirectly impact the SKMS are completed successfully and as planned
Output	• Audit reports • Completed Change review and reports
Metric	• Number of audits completed • Number of unsuccessful changes revealed through auditing
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

6. Activity 5.0 – Management Information & Reporting



6.1. RACI Matrix

Process Activities / Process Roles	Knowledge Management Process Owner	Knowledge Management Process Manager	Knowledge Management Practitioner (Librarian)	Knowledge Artifact Owner	Knowledge Artifact Consumer	SKMS Tool Administrator	Business/User Stakeholders
5.1 Identify Success Criteria	A	R,C	R	C	C	C	C
5.2 Develop KPIs	A	R,C	R	C			
5.3 Define Reporting Requirements	A	R,C	R	C		C	C
5.4 Create Report Templates	A	R,C	R			R,C	
5.5 Measure Results	A	R,C	R	I		C	
5.6 Publish Reports	A	R,C	R	I	I	I	I

Legend

R = Responsible: Executes the task
A = Accountable: Accountable for final result
C = Consulted: Consulted about the task to provide additional information
I = Informed: Needs to be kept up-to-date on activities/tasks

6.2. Procedure Descriptions

5.1	Identify Success Criteria
Purpose	To ensure that the accuracy, relevance, usefulness, timeliness and availability of knowledge is provided to stakeholders in a way that meets their requirements. A set of success criteria that measures the KM process's ability to deliver that knowledge is identified.
Policy Statement	The KM Process Owner ensures that the success criteria (by which the KM process adds value to the organization will be measured) is identified.
Input	• Stakeholder requirements • Process goals and objectives • Process activity descriptions and outputs • Knowledge Management Plan
Procedure Or Work Instruction Steps	Based on the process inputs listed above, define the key success criteria that will form the basis of measurement of the process outcomes
Output	Documented success criteria
Metric	By regular audit, identify number of success criteria that was not accomplished
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

5.2	Develop KPIs
Purpose	To ensure that the KM process is capable of and actually delivers the value required by its stakeholders. A set of Key Performance Indicators (KPIs) will be defined as the basis for measurement of process outcomes compared to process goals, objectives and stakeholder requirements.
Policy Statement	The KM Process Owner ensures that those KPI's (that will best measure the success of the process in meeting stakeholder requirements) are defined and identified.
Input	• Critical Success Factors (CSF's) • Process goals, objectives and activity descriptions • KM process inputs and outputs • Knowledge Management Plan • Stakeholder requirements documentation
Procedure Or Work Instruction Steps	• Based on the inputs listed above, for each critical success factor, identify the most important performance indicators to be measured • Identify process performance KPI's (measuring the importance to the KM consumer) and process management KPI's (measuring the management of the process itself to identify improvements, successes and failures) • Identify the activity metrics that will be used to measure the KPI's • The KPI's should measure compliance, performance, quality and value to ensure that a balanced view of the process is achieved and

5.2	Develop KPIs
	that improvement opportunities are identified in the context of all factors and not just one factor
Output	KPI's listed by type and focus for each Critical Success Factor (CSF)
Metric	Number of KPI's not met
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

5.3	Define Reporting Requirements
Purpose	To ensure that all stakeholders are provided with timely management reports about the KM process and its ability to create management reporting and deliver knowledge to the stakeholders.
Policy Statement	The KM Process Owner ensures that reporting requirements for all stakeholder groups are defined.
Input	• Stakeholder requirements document • Process CSF's and KPI's activity metrics • Target audience for specific reporting content
Procedure Or Work Instruction Steps	• Based on the established measurement framework , identify information and knowledge measurements that are of specific interest to identified stakeholders (e.g. senior management reports vs. line management reports vs. process management reports) • Verify reporting requirements with stakeholders for specific content: i.e. what is being measured, how it is presented, how often, what format is the information in (text, graphic, combination, dashboards etc.) • Reports should link process goals, objectives and targets, CSF's, KPI's and activity metrics • Over time, new and changed requirements will be gathered; what is important or not important today will change over time, necessitating changes in the reporting requirements; update requirements as required and agreed
Output	• Defined reporting criteria and requirements for all stakeholders pertaining to the KM process • KM Management Information Document
Metric	Number of new requirements identified in a specific time period
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

5.4	**Create Report Templates**
Purpose	To ensure that reports can be effectively and efficiently produced for the target audiences.
Policy Statement	The KM Process Owner ensures that report templates for target audiences are created.
Input	• Stakeholder requirements • Defined CSF's, KPI's and activity metrics
Procedure Or Work Instruction Steps	• Using ServiceNow, configure the reporting templates to include all required content for the report and also take into account the desired structure of the report and the delivery mechanism • Validate the report content, structure, look and feel with Stakeholders to ensure the report is meaningful and contains the information required for effective delivery of knowledge as well as good management of the knowledge, its tools and data sources • The template should identify the target audience and specific results of interest to each audience • Additionally the template should contain relevant information about: o CSF linked to process goals o KPI's linked to CSF o Activity metrics used to create KPI measures o Percentage increase/decrease metrics for KPI's o Identified gaps in performance, improvement opportunities and success stories
Output	Completed report templates
Metric	Number of documented possible actions, by classification of action
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

5.5	**Measure Results**
Purpose	To ensure that the actual Knowledge Management results are monitored, tracked and analyzed in order to assure delivery of knowledge to OSI.
Policy Statement	The KM Process Owner ensures KM Process results are measured.
Input	• Stakeholder requirements • Knowledge Management Plan
Procedure Or Work Instruction Steps	• For each of the defined activity metrics and KPI's, collect relevant data about KM process performance • Process, organize or configure the data to create usable information • Analyze information to identify successes and areas for improvement against target measures
Output	• Activity metrics • KPI results

5.5	Measure Results
Metric	Number of audits of activity metrics
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

5.6	Publish Reports
Purpose	To ensure that process performance reports are published and distributed to the appropriate stakeholders.
Policy Statement	The KM Process Owner ensures that reports are published to the appropriate audience in a timely manner.
Input	Process metrics and KPI results
Procedure Or Work Instruction Steps	• Using the designated report template and the approved media/ distribution channel, make the reports available to the target audience • Publication can be in the form of a notification that reports are available with a link to the report site. It could be in the form of a dashboard posted to a website with an alert to the audience that it is now available. Publication can also be in terms of a PowerPoint slide presentation delivered in a meeting as well as in the form of a document containing results pertinent to the audience it is intended for
Output	Published reports
Metric	Number of reports published per media and per audience
Controls	See OSI Governance and Control document in Appendix
Revision History	<Date, Description, Author>

7. Assumptions, Constraints, Risks and Strategy/Procedures

7.1. Assumptions

- OSI and E.K. Associates will own the KM Process Plan
- OSI will provide governance and oversight to process
- ServiceNow will be the main repository of KA
- The Service Desk will be a Single Point Of Contact (SPOC)
- GitHub WIKI will also be utilized for KM
- Service Level Agreements (SLAs) will need to be clearly defined
- Availability Management and Event Management will be established by OSI

7.2. Constraints

- OSI must provide the necessary number of resources to manage the process, capture data, manage data, update data, author KA, etc.
- Lack of a Problem Management process to capture workarounds in a Known Error Database (KEDB) to facilitate faster incident resolutions which saves time and cost
- Lack of proper Change Management process (with owner) would hinder the KM process

7.3. Potential Risks

- Collaboration between Digital Services could become insufficient

7.4. Strategy/Procedures

- The overall strategy for KM and OSI approach to KM is encompassed in the Knowledge Management High-Level ITIL Design Plan (separate document)
- The procedure for updating can be found in this document in section 2.7
- The procedure for purging/archiving can be found in this document in section 2.8
- The procedure for authoring can be found in this document in section 2.3
- The procedure for communication can be found in this document in sections 1.6 and 3.6
- The policy for approval of updating, purging/archiving, authoring and communication of knowledge can be found in the Global Process Policies for KM section of the Knowledge Management ITIL High-Level Design Plan (separate document)
- The procedure for reporting known errors in ServiceNow if known errors are released in production will be covered in the Problem Management ITIL Detailed Design Plan
- The procedures for managing the lifecycle of all problems, including root cause analysis will be covered in the Problem Management ITIL Detailed Design Plan

Appendix A
Knowledge Management High Level Roles & Responsibilities

Knowledge Management Process Owner
The KM Process Owner is accountable for the operational management of the KM Process.

Below are key responsibilities of a KM Process Owner:
- Defining KM Process strategy
- Assisting with KM Process design
- Ensuring that appropriate KM Process documentation is available and current
- Defining appropriate KM policies and standards to be employed throughout the process
- Periodically auditing the KM Process to ensure compliance to policy and standards
- Periodically reviewing the KM Process strategy to ensure that it is appropriate and change strategy as required
- Creating overall architecture for identification, capture and maintenance of knowledge within the organization
- Communicating KM Process information or changes as appropriate to ensure awareness
- Providing KM Process resources to support activities required throughout the service lifecycle
- Ensuring that KM Process staff have the required knowledge and the required technical and business understanding to deliver the KM Process, and understand their role in the KM Process
- Reviewing opportunities for KM Process enhancements and for improving the efficiency and effectiveness of the KM Process
- Addressing issues with the running of the KM Process
- Identifying improvement opportunities for inclusion in the CSI register
- Working with the CSI Manager and KM Process Manager(s) to review and prioritize improvements in the CSI register
- Making improvements to the KM Process
- Sponsoring and ‘change managing’ the KM Process and its metrics
- Acting as an advisor to business and IT personnel on knowledge management matters, including policy decisions on storage, value, worth, etc.

The KM Process Manager
The KM Process Manager’s responsibilities include planning and coordination of all the activities required to carry out, monitor, and report on the KM Process. Depending on the size and scope of the process there can be several KM Process Managers.

Below are the key responsibilities of a KM Process Manager:
- Working with the KM Process Owner to plan and coordinate process activities
- Ensuring all process activities are carried out as required throughout the service lifecycle
- Appointing people to the required roles
- Managing resources assigned to the KM Process
- Working with Service Owners and other Process Managers to ensure the smooth running of services
- Monitoring and reporting on KM Process performance
- Identifying KM Process improvement opportunities for inclusion in the CSI register

- Working with the CSI Manager and KM Process Owner to review and prioritize improvements in the CSI register
- Implementing improvements to the KM Process
- Ensuring that all knowledge items are made accessible to those who need them in an efficient and effective manner
- Planning and managing support for knowledge management tools and processes
- Encouraging people throughout OSI to contribute knowledge to the SKMS

KM Process Practitioner (Librarian)
The KM Process Practitioner (Librarian) is responsible for carrying out one or more KM Process activities. There are usually multiple KM Process Practitioners who may have titles which are more specific to their respective duties.

Below are the key responsibilities of a Process Practitioner:

- Carrying out one or more of the activities of the KM Process
- Understanding how their role contributes to the overall delivery of services and the creation of value for the business (from the KM Process Owner and/or KM Process Manager)
- Working with other stakeholders, such as their manager, co-workers, users and customers, to ensure that their contributions are effective
- Ensuring that their inputs, outputs and interfaces for their activities are correct
- Creating or updating KM records to show that activities have been carried out correctly
- Identifying, controlling and storing any information deemed to be pertinent to the services provided that is not available by other means
- Maintaining controlled knowledge to ensure that it is current, relevant and valid
- Monitoring publicity regarding the knowledge information to ensure the information is not duplicated and is recognized as a central source of information, etc.

Knowledge Artifact Owner (Creator)
The Knowledge Artifact Owner (Creator**)** role can be carried out by many people in the organization. Creation and sharing of knowledge is often written into job descriptions of people in many different roles within IT and the business.

Below are the key accountabilities of a KA Owner (Creator):

- Updates/modifies existing KA and creates new KA
- Identifying delivery mechanisms or media to be used for knowledge
- Formats KA for consumption
- Reviews and tests KA
- Conducts verification and auditing of KA
- Measures results of KA

Appendix B
ITIL Acronyms and Glossary
Acronyms list

ACD Automatic Call Distribution
AM Availability Management
AMIS Availability Management Information System
ASP Application Service Provider
BCM Business Capacity Management
BCM Business Continuity Management
BCP Business Continuity Plan
BIA Business Impact Analysis
BRM Business Relationship Manager
BSI British Standards Institution
BSM Business Service Management
CAB Change Advisory Board
CAB/EC Change Advisory Board/Emergency Committee
CAPEX Capital Expenditure
CCM Component Capacity Management
CFIA Component Failure Impact Analysis
CI Configuration Item
CMDB Configuration Management Database
CMIS Capacity Management Information System
CMM Capability Maturity Model
CMMI Capability Maturity Model Integration
CMS Configuration Management System
COTS Commercial off the Shelf
CSF Critical Success Factor
CSI Continual Service Improvement
CSP Core Service Package
CTI Computer Telephony Integration
DIKW Data–to–Information–to–Knowledge– to–Wisdom
ELS Early Life Support
eSCM–CL eSourcing Capability Model for Client Organizations
eSCM–SP eSourcing Capability Model for Service Providers
FMEA Failure Modes and Effects Analysis
FTA Fault Tree Analysis
IRR Internal Rate of Return
ISG IT Steering Group
ISM Information Security Management
ISMS Information Security Management System ISO International Organization for Standardization ISP Internet Service Provider
IT Information Technology
ITSCM IT Service Continuity Management
ITSM IT Service Management
itSMF IT Service Management Forum
IVR Interactive Voice Response
KEDB Known Error Database
KPI Key Performance Indicator
LOS Line of Service
M_o_R Management of Risk
MTBF Mean Time Between Failures
MTBSI Mean Time Between Service Incidents
MTRS Mean Time to Restore Service
MTTR Mean Time To Repair
NPV Net Present Value
OGC Office of Government Commerce
OLA Operational Level Agreement
OPEX Operational Expenditure
OPSI Office of Public Sector Information
PBA Pattern of Business Activity
PFS Prerequisite for Success
PIR Post-Implementation Review
PSA Projected Service Outage
QA Quality Assurance
QMS Quality Management System
RCA Root Cause Analysis
RFC Request for Change
ROI Return on Investment
RPO Recovery Point Objective
RTO Recovery Time Objective
SAC Service Acceptance Criteria
SACM Service Asset and Configuration Management\
SCD Supplier and Contract Database
SCM Service Capacity Management
SDP Service Design Package
SFA Service Failure Analysis
SIP Service Improvement Plan
SKMS Service Knowledge Management System
SLA Service Level Agreement
SLM Service Level Management
SLP Service Level Package
SLR Service Level Requirement
SMO Service Maintenance Objective
SoC Separation of Concerns
SOP Standard Operating Procedures
SOR Statement of requirements
SPI Service Provider Interface
SPM Service Portfolio Management
SPO Service Provisioning Optimization
SPOF Single Point of Failure
TCO Total Cost of Ownership
TCU Total Cost of Utilization
TO Technical Observation
TOR Terms of Reference
TQM Total Quality Management
UC Underpinning Contract
UP User Profile
VBF Vital Business Function
VOI Value on Investment
WIP Work in Progress

Definitions list

The publication names included in parentheses after the name of a term identify where a reader can find more information about that term. This is either because the term is primarily used by that publication or because additional useful information about that term can be found there. Terms without a publication name associated with them may be used generally by several publications, or may not be defined in any greater detail than can be found in the glossary, i.e. we only point readers to somewhere they can expect to expand on their knowledge or to see a greater context. Terms with multiple publication names are expanded on in multiple publications.

Where the definition of a term includes another term, those related terms are highlighted in a second color. This is designed to help the reader with their understanding by pointing them to additional definitions that are all part of the original term they were interested in. The form 'See also Term X, Term Y' is used at the end of a definition where an important related term is not used with the text of the definition itself.

Acceptance

Formal agreement that an IT Service, Process, Plan, or other Deliverable is complete, accurate, Reliable and meets its specified Requirements. Acceptance is usually preceded by Evaluation or Testing and is often required before proceeding to the next stage of a Project or Process.

Access Management

(Service Operation) The Process responsible for allowing Users to make use of IT Services, data, or other Assets. Access Management helps to protect the Confidentiality, Integrity and Availability of Assets by ensuring that only authorized Users are able to access or modify the Assets. Access Management is sometimes referred to as Rights Management or Identity Management.

Account Manager

(Service Strategy) A Role that is very similar to Business Relationship Manager, but includes more commercial aspects. Most commonly used when dealing with External Customers.

Accounting

(Service Strategy) The Process responsible for identifying actual Costs of delivering IT Services, comparing these with budgeted costs, and managing variance from the Budget.

Accredited

Officially authorized to carry out a Role. For example, an accredited body may be authorized to provide training or to conduct Audits.

Active Monitoring

(Service Operation) Monitoring of a Configuration Item or an IT Service that uses automated regular checks to discover the current status. See also Passive Monitoring.

Activity

A set of actions designed to achieve a particular result. Activities are usually defined as part of Processes or Plans, and are documented in Procedures.

Agreement

A Document that describes a formal understanding between two or more parties. An Agreement is not legally binding unless it forms part of a Contract. See also Service Level Agreement, Operational Level Agreement.

Alert

(Service Operation) A warning that a threshold has been reached, something has changed, or a Failure has occurred. Alerts are often created and managed by System Management tools and are managed by the Event Management Process.

Application

Software that provides Functions that are required by an IT Service. Each Application may be part of more than one IT Service. An Application runs on one or more Servers or Clients. See also Application Management, Application Portfolio.

Application Management

(Service Design) (Service Operation) The Function responsible for managing Applications throughout their Lifecycle.

Application Portfolio

(Service Design) A database or structured Document used to manage Applications throughout their Lifecycle. The Application Portfolio contains key Attributes of all Applications. The Application Portfolio is sometimes implemented as part of the Service Portfolio, or as part of the Configuration Management System.

Application Sizing

(Service Design) The Activity responsible for understanding the Resource Requirements needed to support a new Application, or a major Change to an existing Application. Application Sizing helps to ensure that the IT Service can meet its agreed Service Level Targets for Capacity and Performance.

Architecture

(Service Design) The structure of a System or IT Service, including the Relationships of Components to each other and to the environment they are in. Architecture also includes the Standards and Guidelines that guide the design and evolution of the System.

Assessment

Inspection and analysis to check whether a Standard or set of Guidelines is being followed, that Records are accurate, or that Efficiency and Effectiveness targets are being met. See also Audit.

Asset

(Service Strategy) Any Resource or Capability. Assets of a Service Provider including anything that could contribute to the delivery of a Service. Assets can be one of the following types: Management, Organization, Process, Knowledge, People, Information, Applications, Infrastructure, and Financial Capital.

Asset Management

(Service Transition) Asset Management is the Process responsible for tracking and reporting the value and ownership of financial Assets throughout their Lifecycle. Asset Management is part of an overall Service Asset and Configuration Management Process. See also Asset Register.

Asset Register

(Service Transition) A list of Assets that includes their ownership and value. Asset Management maintains the Asset Register.

Attribute

(Service Transition) A piece of information about a Configuration Item. Examples are: name, location, Version number, and Cost. Attributes of CIs are recorded in the Configuration Management Database (CMDB). See also Relationship.

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. An Audit may be carried out by internal or external groups.

Automatic Call Distribution (ACD)

(Service Operation) Use of Information Technology to direct an incoming telephone call to the most appropriate person in the shortest possible time. ACD is sometimes called Automated Call Distribution.

Availability

(Service Design) Ability of a Configuration Item or IT Service to perform its agreed Function when required. Availability is determined by Reliability, Maintainability, Serviceability, Performance, and Security. Availability is usually calculated as a percentage. This calculation is often based on Agreed Service Time and Downtime. It is Best Practice to calculate Availability using measurements of the Business output of the IT Service.

Availability Management

(Service Design) The Process responsible for defining, analyzing, planning, measuring and improving all aspects of the Availability of IT services. Availability Management is responsible for ensuring that all IT Infrastructure, Processes, Tools, Roles, etc. are appropriate for the agreed Service Level Targets for Availability.

Availability Plan

(Service Design) A Plan to ensure that existing and future Availability Requirements for IT Services can be provided Cost Effectively.

Back-out

See Remediation.

Backup

(Service Design) (Service Operation) Copying data to protect against loss of Integrity or Availability of the original.

Balanced Scorecard

(Continual Service Improvement) A management tool developed by Drs Robert Kaplan (Harvard Business School) and David Norton. A Balanced Scorecard enables a Strategy to be broken down into Key Performance Indicators. Performance against the KPIs is used to demonstrate how well the Strategy is being achieved. A Balanced Scorecard has four major areas, each of which has a small number of KPIs. The same four areas are considered at different levels of detail throughout the Organization.

Baseline

(Continual Service Improvement) A Benchmark used as a reference point. For example:

- An ITSM Baseline can be used as a starting point to measure the effect of a Service Improvement Plan
- A Performance Baseline can be used to measure changes in Performance over the lifetime of an IT Service
- A Configuration Management Baseline can be used to enable the IT Infrastructure to be restored to a known Configuration if a Change or Release fails.

Benchmark

(Continual Service Improvement) The recorded state of something at a specific point in time. A Benchmark can be created for a Configuration, a Process, or any other set of data. For example, a benchmark can be used in:

- Continual Service Improvement, to establish the current state for managing improvements
- Capacity Management, to document performance characteristics during normal operations.

See also Benchmarking, Baseline.

Benchmarking

(Continual Service Improvement) Comparing a Benchmark with a Baseline or with Best Practice. The term Benchmarking is also used to mean creating a series of Benchmarks over time, and comparing the results to measure progress or improvement.

Best Practice

Proven Activities or Processes that have been successfully used by multiple Organizations. ITIL is an example of Best Practice.

Brainstorming

(Service Design) A technique that helps a team to generate ideas. Ideas are not reviewed during the Brainstorming session, but at a later stage. Brainstorming is often used by Problem Management to identify possible causes.

Budget

A list of all the money an Organization or Business Unit plans to receive, and plans to pay out, over a specified period of time. See also Budgeting, Planning.

Budgeting

The Activity of predicting and controlling the spending of money. Consists of a periodic negotiation cycle to set future Budgets (usually annual) and the day-to-day monitoring and adjusting of current Budgets.

Build

(Service Transition) The Activity of assembling a number of Configuration Items to create part of an IT Service. The term Build is also used to refer to a Release that is authorized for distribution. For example Server Build or laptop Build.

Business

(Service Strategy) An overall corporate entity or Organization formed of a number of Business Units. In the context of ITSM, the term Business includes public sector and not-for-profit organizations, as well as companies. An IT Service Provider provides IT Services to a Customer within a Business. The IT Service Provider may be part of the same Business as its Customer (Internal Service Provider), or part of another Business (External Service Provider).

Business Capacity Management (BCM) (Service Design) In the context of ITSM, Business Capacity Management is the Activity responsible for understanding future Business Requirements for use in the Capacity Plan.

See also Service Capacity Management.

Business Case

(Service Strategy) Justification for a significant item of expenditure. Includes information about Costs, benefits,

options, issues, Risks, and possible problems. See also Cost Benefit Analysis.

Business Customer

(Service Strategy) A recipient of a product or a Service from the Business. For example, if the Business is a car manufacturer then the Business Customer is someone who buys a car.

Business Impact Analysis (BIA)

(Service Strategy) BIA is the Activity in Business Continuity Management that identifies Vital Business Functions and their dependencies. These dependencies may include Suppliers, people, other Business Processes, IT Services, etc. BIA defines the recovery requirements for IT Services. These requirements include Recovery Time Objectives, Recovery Point Objectives and minimum Service Level Targets for each IT Service.

Business Objective

(Service Strategy) The Objective of a Business Process, or of the Business as a whole. Business Objectives support the Business Vision, provide guidance for the IT Strategy, and are often supported by IT Services.

Business Operations

(Service Strategy) The day-to-day execution, monitoring and management of Business Processes.

Business Perspective

(Continual Service Improvement) An understanding of the Service Provider and IT Services from the point of view of the Business, and an understanding of the Business from the point of view of the Service Provider.

Business Process

A Process that is owned and carried out by the Business. A Business Process contributes to the delivery of a product or Service to a Business Customer. For example, a retailer may have a purchasing Process that helps to deliver Services to its Business Customers. Many Business Processes rely on IT Services.

Business Relationship Management

(Service Strategy) The Process or Function responsible for maintaining a Relationship with the Business. Business Relationship Management usually includes:

- Managing personal Relationships with Business managers
- Providing input to Service Portfolio Management
- Ensuring that the IT Service Provider is satisfying the Business needs of the Customers

This Process has strong links with Service Level Management.

Business Service

An IT Service that directly supports a Business Process, as opposed to an Infrastructure Service, which is used internally by the IT Service Provider and is not usually visible to the Business.

The term Business Service is also used to mean a Service that is delivered to Business Customers by Business Units. For example, delivery of financial services to Customers of a bank, or goods to the Customers of a retail store.

Successful delivery of Business Services often depends on one or more IT Services.

Business Service Management (BSM) (Service Strategy) (Service Design) An approach to the management of IT Services that considers the Business Processes supported and the Business value provided.

This term also means the management of Business Services delivered to Business Customers.

Business Unit

(Service Strategy) A segment of the Business that has its own Plans, Metrics, income and Costs. Each Business Unit owns Assets and uses these to create value for Customers in the form of goods and Services.

Call

(Service Operation) A telephone call to the Service Desk from a User. A Call could result in an Incident or a Service Request being logged.

Call Centre

(Service Operation) An Organization or Business Unit that handles large numbers of incoming and outgoing telephone calls. See also Service Desk.

Call Type

(Service Operation) A Category that is used to distinguish incoming requests to a Service Desk. Common call types are Incident, Service Request and Complaint.

Capability

(Service Strategy) The ability of an Organization, person, Process, Application, Configuration Item or IT Service to carry out an Activity. Capabilities are intangible Assets of an Organization. See also Resource.

Capacity

(Service Design) The maximum Throughput that a Configuration Item or IT Service can deliver whilst meeting agreed Service Level Targets. For some types of CI, Capacity may be the size or volume, for example a disk drive.

Capacity Management

(Service Design) The Process responsible for ensuring that the Capacity of IT Services and the IT Infrastructure is able to deliver agreed Service Level Targets in a Cost Effective and timely manner. Capacity Management considers all Resources required to deliver the IT Service, and plans for short-, medium- and long-term Business Requirements.

Capacity Plan

(Service Design) A Capacity Plan is used to manage the Resources required to deliver IT Services. The Plan contains scenarios for different predictions of Business demand, and costed options to deliver the agreed Service Level Targets.

Capacity Planning

(Service Design) The Activity within Capacity Management responsible for creating a Capacity Plan.

Capital Expenditure (CAPEX)

(Service Strategy) The cost of purchasing something that will become a financial Asset, for example computer equipment and buildings. The value of the Asset is depreciated over multiple accounting periods.

Category

A named group of things that have something in common. Categories are used to group similar things together. For example, Cost Types are used to group similar types of Cost. Incident Categories are used to group similar types of Incident, CI Types are used to group similar types of Configuration Item.

Certification

Issuing a certificate to confirm Compliance to a Standard. Certification includes a formal Audit by an independent and accredited body. The term Certification is also used to mean awarding a certificate to verify that a person has achieved a qualification.

Change

(Service Transition) The addition, modification or removal of anything that could have an effect on IT Services. The Scope should include all IT Services, Configuration Items, Processes, Documentation, etc.

Change Advisory Board (CAB)

(Service Transition) A group of people that advises the Change Manager in the Assessment, prioritization and scheduling of Changes. This board is usually made up of representatives from all areas within the IT Service Provider, representatives from the Business and Third Parties such as Suppliers.

Change Case

(Service Operation) A technique used to predict the impact of proposed Changes. Change Cases use specific scenarios to clarify the scope of proposed Changes and to help with Cost Benefit Analysis. See also Use Case.

Change Management

(Service Transition) The Process responsible for controlling the Lifecycle of all Changes. The primary objective of Change Management is to enable beneficial Changes to be made, with minimum disruption to IT Services.

Change Model

(Service Transition) A repeatable way of dealing with a particular Category of Change. A Change Model defines specific pre-defined steps that will be followed for a change of this Category. Change Models may be very simple, with no requirement for approval (e.g. Password Reset) or may be very complex with many steps that require approval (e.g. major software release). See also Standard Change, Change Advisory Board.

Change Record

(Service Transition) A Record containing the details of a Change. Each Change Record documents the Lifecycle of a single Change. A Change Record is created for every Request for Change that is received, even those that are subsequently rejected. Change Records should reference the Configuration Items that are affected by the Change. Change Records are stored in the Configuration Management System.

Change Schedule

(Service Transition) A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about Changes that have already been implemented.

Charging

(Service Strategy) Requiring payment for IT Services. Charging for IT Services is optional, and many Organizations choose to treat their IT Service Provider as a Cost Centre.

Chronological Analysis

(Service Operation) A technique used to help identify possible causes of Problems. All available data about the Problem is collected and sorted by date and time to provide a detailed timeline. This can make it possible to identify which Events may have been triggered by others.

Classification

The act of assigning a Category to something. Classification is used to ensure consistent management and reporting. CIs, Incidents, Problems, Changes, etc. are usually classified.

Client

A generic term that means a Customer, the Business or a Business Customer. For example, Client Manager may be used as a synonym for Account Manager.

The term client is also used to mean:

- A computer that is used directly by a User, for example a PC, Handheld Computer, or Workstation
- The part of a Client-Server Application that the User directly interfaces with. For example an e-mail Client.

Closed

(Service Operation) The final Status in the Lifecycle of an Incident, Problem, Change, etc. When the Status is Closed, no further action is taken.

Closure

(Service Operation) The act of changing the Status of an Incident, Problem, Change, etc. to Closed.

COBIT

(Continual Service Improvement) Control Objectives for Information and related Technology (COBIT) provides guidance and Best Practice for the management of IT Processes. COBIT is published by the IT Governance Institute. See www.isaca.org for more information.

Commercial Off-The-Shelf (COTS)

(Service Design) Application software or Middleware that can be purchased from a Third Party.

Compliance

Ensuring that a Standard or set of Guidelines is followed, or that proper, consistent accounting or other practices are being employed.

Component

A general term that is used to mean one part of something more complex. For example, a computer System may be a component of an IT Service, an Application may be a Component of a Release Unit. Components that need to be managed should be Configuration Items.

Component Capacity Management

(Service Design) (Continual Service Improvement) The Process responsible for understanding the Capacity, Utilization, and Performance of Configuration Items. Data is collected, recorded and analyzed for use in the Capacity Plan. See also Service Capacity Management.

Component Failure Impact Analysis (CFIA) (Service Design) A technique that helps to identify the impact of CI failure on IT Services. A matrix is created with IT Services on one edge and CIs on the other. This enables the identification of critical CIs (that could cause the failure of multiple IT Services) and of fragile IT Services (that have multiple Single Points of Failure).

Computer Telephony Integration (CTI)

(Service Operation) Computer Telephony Integration (CTI) is a general term covering any kind of integration between computers and telephone Systems. It is most commonly used to refer to Systems where an Application displays detailed screens relating to incoming or outgoing telephone calls. See also Automatic Call Distribution, Interactive Voice Response.

Concurrency

A measure of the number of Users engaged in the same Operation at the same time.

Confidentiality

(Service Design) A security principle that requires that data should only be accessed by authorized people.

Configuration

(Service Transition) 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 is also used to describe the parameter settings for one or more CIs.

Configuration Control

(Service Transition) The Activity responsible for ensuring that adding, modifying or removing a CI is properly managed, for example by submitting a Request for Change or Service Request.

Configuration Item (CI)

(Service Transition) Any Component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the Configuration Management System and is maintained throughout its Lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT Services, hardware, software, buildings, people, and formal documentation such as Process documentation and SLAs.

Configuration Management

(Service Transition) The Process responsible for maintaining information about Configuration Items required to deliver an IT Service, including their Relationships. This information is managed throughout the Lifecycle of the CI. Configuration Management is part of an overall Service Asset and Configuration Management Process.

Configuration Management Database (CMDB)

(Service Transition) A database used to store Configuration Records throughout their Lifecycle. The Configuration Management System maintains one or more CMDBs, and each CMDB stores Attributes of CIs, and Relationships with other CIs.

Configuration Management System (CMS)

(Service Transition) A set of tools and databases that are used to manage an IT Service Provider's Configuration data. The CMS also includes information about Incidents, Problems, Known Errors, Changes and Releases; and it may contain data about employees, Suppliers, locations, Business Units, Customers and Users. The CMS includes tools for collecting, storing, managing, updating, and presenting data about all Configuration Items and their Relationships. The CMS is maintained by Configuration Management and is used by all IT Service Management Processes. See also Configuration Management Database, Service Knowledge Management System.

Continual Service Improvement (CSI) (Continual Service Improvement)

A stage in the Lifecycle of an IT Service and the title of one of the Core ITIL publications. Continual Service Improvement is responsible for managing improvements to IT Service Management Processes and IT Services. The Performance of the IT Service Provider is continually measured and improvements are made to Processes, IT Services and IT Infrastructure in order to increase Efficiency, Effectiveness, and Cost Effectiveness. See also Plan–Do–Check–Act.

Contract

A legally binding Agreement between two or more parties.

Control

A means of managing a Risk, ensuring that a Business Objective is achieved, or ensuring that a Process is followed. Example Controls include Policies, Procedures, Roles, RAID, door locks, etc. A control is sometimes called a Countermeasure or safeguard. Control also means to manage the utilization or behaviour of a Configuration Item, System or IT Service.

Control Objectives for Information and related Technology (COBIT)

See COBIT.

Control perspective

(Service Strategy) An approach to the management of IT Services, Processes, Functions, Assets, etc. There can be several different Control Perspectives on the same IT Service, Process, etc., allowing different individuals or teams to focus on what is important and relevant to their specific Role. Example Control Perspectives include Reactive and Proactive management within IT Operations, or a Lifecycle view for an Application Project team.

Cost

The amount of money spent on a specific Activity, IT Service, or Business Unit. Costs consist of real cost (money), notional cost such as people's time, and Depreciation.

Cost Benefit Analysis

An Activity that analyses and compares the Costs and the benefits involved in one or more alternative courses of action. See also Business Case.

Cost Effectiveness

A measure of the balance between the Effectiveness and Cost of a Service, Process or activity, A Cost Effective Process is one that achieves its Objectives at minimum Cost. See also KPI, Value for Money.

Countermeasure

Can be used to refer to any type of Control. The term Countermeasure is most often used when referring to measures that increase Resilience, Fault Tolerance or Reliability of an IT Service.

Critical Success Factor (CSF)

Something that must happen if a Process, Project, Plan, or IT Service is to succeed. KPIs are used to measure the achievement of each CSF. For example a CSF of 'protect IT Services when making Changes' could be measured by KPIs such as 'percentage reduction of unsuccessful Changes', 'percentage reduction in Changes causing Incidents', etc.

Culture

A set of values that is shared by a group of people, including expectations about how people should behave, their ideas, beliefs, and practices. See also Vision.

Customer

Someone who buys goods or Services. The Customer of an IT Service Provider is the person or group that defines and agrees the Service Level Targets. The term Customers is also sometimes informally used to mean Users, for example 'this is a Customer-focused Organization'.

Dashboard

(Service Operation) A graphical representation of overall IT Service Performance and Availability. Dashboard images may be updated in real-time, and can also be included in management reports and web pages. Dashboards can be used to support Service Level Management, Event Management or Incident Diagnosis.

Definitive Media Library (DML)

(Service Transition) One or more locations in which the definitive and approved versions of all software Configuration Items are securely stored. The DML may also contain associated CIs such as licenses and documentation. The DML is a single logical storage area even if there are multiple locations. All software in the DML is under the control of Change and Release Management and is recorded in the Configuration Management System. Only software from the DML is acceptable for use in a Release.

Deliverable

Something that must be provided to meet a commitment in a Service Level Agreement or a Contract. Deliverable is also used in a more informal way to mean a planned output of any Process.

Demand Management

Activities that understand and influence Customer demand for Services and the provision of Capacity to meet these demands. At a Strategic level Demand Management can involve analysis of Patterns of Business Activity and User Profiles. At a tactical level it can involve use of Differential Charging to encourage Customers to use IT Services at less busy times. See also Capacity Management.

Dependency

The direct or indirect reliance of one Process or Activity on another.

Deployment

(Service Transition) The Activity responsible for movement of new or changed hardware, software, documentation, Process, etc. to the Live Environment. Deployment is part of the Release and Deployment Management Process. See also Rollout.

Design

(Service Design) An Activity or Process that identifies Requirements and then defines a solution that is able to meet these Requirements. See also Service Design.

Detection

(Service Operation) A stage in the Incident Lifecycle. Detection results in the Incident becoming known to the Service Provider. Detection can be automatic, or can be the result of a user logging an Incident.

Development

(Service Design) The Process responsible for creating or modifying an IT Service or Application. Also used to mean the Role or group that carries out Development work.

Development Environment

(Service Design) An Environment used to create or modify IT Services or Applications. Development Environments are not typically subjected to the same degree of control as Test Environments or Live Environments. See also Development.

Diagnosis

(Service Operation) A stage in the Incident and Problem Lifecycles. The purpose of Diagnosis is to identify a Workaround for an Incident or the Root Cause of a Problem.

Diagnostic Script

(Service Operation) A structured set of questions used by Service Desk staff to ensure they ask the correct questions, and to help them Classify, Resolve and assign Incidents.

Diagnostic Scripts may also be made available to Users to help them diagnose and resolve their own Incidents.

Directory Service

(Service Operation) An Application that manages information about IT Infrastructure available on a network, and corresponding User access Rights.

Document

Information in readable form. A Document may be paper or electronic. For example, a Policy statement, Service Level Agreement, Incident Record, diagram of computer room layout. See also Record.

Downtime

(Service Design) (Service Operation) The time when a Configuration Item or IT Service is not available during its Agreed Service Time. The Availability of an IT Service is often calculated from Agreed Service Time and Downtime.

Driver

Something that influences Strategy, Objectives or Requirements. For example, new legislation or the actions of competitors.

Early Life Support

(Service Transition) Support provided for a new or changed IT Service for a period of time after it is released. During Early Life Support the IT Service Provider may review the KPIs, Service Levels and Monitoring Thresholds, and provide additional Resources for Incident and Problem Management.

Economies of scale

(Service Strategy) The reduction in average Cost that is possible from increasing the usage of an IT Service or Asset.

Effectiveness

(Continual Service Improvement) A measure of whether the Objectives of a Process, Service or Activity have been achieved. An Effective Process or activity is one that achieves its agreed Objectives. See also KPI.

Efficiency

(Continual Service Improvement) A measure of whether the right amount of resources has been used to deliver a Process, Service or Activity. An Efficient Process achieves its Objectives with the minimum amount of time, money,

people or other resources. See also KPI.

Emergency Change

(Service Transition) A Change that must be introduced as soon as possible. For example, to resolve a Major Incident or implement a Security patch. The Change Management Process will normally have a specific Procedure for handling Emergency Changes. See also Emergency Change Advisory Board (ECAB).

Emergency Change Advisory Board (ECAB) (Service Transition) A subset of the Change Advisory Board that makes decisions about high-impact Emergency Changes. Membership of the ECAB may be decided at the time a meeting is called, and depends on the nature of the Emergency Change.

Environment

(Service Transition) A subset of the IT Infrastructure that is used for a particular purpose. For Example: Live Environment, Test Environment, Build Environment. It is possible for multiple Environments to share a Configuration Item, for example Test and Live Environments may use different partitions on a single mainframe computer. Also used in the term Physical Environment to mean the accommodation, air conditioning, power system, etc.

Environment is also used as a generic term to mean the external conditions that influence or affect something.

Error

(Service Operation) A design flaw or malfunction that causes a Failure of one or more Configuration Items or IT Services. A mistake made by a person or a faulty Process that affects a CI or IT Service is also an Error.

Escalation

(Service Operation) An Activity that obtains additional Resources when these are needed to meet Service Level Targets or Customer expectations. Escalation may be needed within any IT Service Management Process, but is most commonly associated with Incident Management, Problem Management and the management of Customer complaints. There are two types of Escalation: Functional Escalation and Hierarchic Escalation.

eSourcing Capability Model for Service Providers (eSCM–SP)

(Service Strategy) A framework to help IT Service Providers develop their IT Service Management Capabilities from a Service Sourcing perspective. eSCM–SP was developed by Carnegie Mellon University, US.

Estimation

The use of experience to provide an approximate value for a Metric or Cost. Estimation is also used in Capacity and Availability Management as the cheapest and least accurate Modelling method.

Evaluation

(Service Transition) The Process responsible for assessing a new or Changed IT Service to ensure that Risks have been managed and to help determine whether to proceed with the Change.

Evaluation is also used to mean comparing an actual Outcome with the intended Outcome, or comparing one alternative with another.

Event

(Service Operation) A change of state that has significance for the management of a Configuration Item or IT Service.

The term Event is also used to mean an Alert or notification created by any IT Service, Configuration Item or Monitoring tool. Events typically require IT Operations personnel to take actions, and often lead to Incidents being logged.

Event Management

(Service Operation) The Process responsible for managing Events throughout their Lifecycle. Event Management is one of the main Activities of IT Operations.

Exception Report

A Document containing details of one or more KPIs or other important targets that have exceeded defined Thresholds. Examples include SLA targets being missed or about to be missed, and a Performance Metric indicating a potential Capacity problem.

External Customer

A Customer who works for a different Business to the IT Service Provider. See also External Service Provider.

External Metric

A Metric that is used to measure the delivery of IT Service to a Customer. External Metrics are usually defined in SLAs and reported to Customers. See also Internal Metric.

External Service Provider

(Service Strategy) An IT Service Provider that is part of a different Organization from its Customer. An IT Service Provider may have both Internal Customers and External Customers.

Facilities Management (Service Operation) The Function responsible for managing the physical Environment where the IT Infrastructure is located. Facilities Management includes all aspects of managing the physical Environment, for example power and cooling, building Access Management, and environmental monitoring.

Failure

(Service Operation) Loss of ability to operate to Specification, or to deliver the required output. The term Failure may be used when referring to IT Services, Processes, Activities, Configuration Items, etc. A Failure often causes an Incident.

Fault

See Error.

Fault Tolerance

(Service Design) The ability of an IT Service or Configuration Item to continue to operate correctly after Failure of a Component part. See also Resilience, Countermeasure.

Fault Tree Analysis (FTA)

(Service Design) (Continual Service Improvement) A technique that can be used to determine the chain of events that leads to a Problem. Fault Tree Analysis represents a chain of events using Boolean notation in a diagram.

Financial Management

(Service Strategy) The Function and Processes responsible for managing an IT Service Provider's Budgeting, Accounting and Charging Requirements.

First-line Support

(Service Operation) The first level in a hierarchy of Support Groups involved in the resolution of Incidents. Each level contains more specialist skills, or has more time or other resources. See also Escalation.

Fit for Purpose

An informal term used to describe a Process, Configuration Item, IT Service, etc. that is capable of meeting its objectives or Service Levels. Being Fit for Purpose requires suitable design, implementation, control and maintenance.

Follow the Sun

(Service Operation) A methodology for using Service Desks and Support Groups around the world to provide seamless 24/7 Service. Calls, Incidents, Problems and Service Requests are passed between groups in different time zones.

Fulfilment

Performing Activities to meet a need or Requirement. For example, by providing a new IT Service, or meeting a Service Request.

Function

A team or group of people and the tools they use to carry out one or more Processes or Activities. For example the Service Desk.

The term Function also has two other meanings:

- An intended purpose of a Configuration Item, Person, Team, Process, or IT Service. For example one Function of an e-mail Service may be to store and forward outgoing mails, one Function of a Business Process may be to dispatch goods to Customers.
- To perform the intended purpose correctly, 'The computer is Functioning'.

Functional Escalation

(Service Operation) Transferring an Incident, Problem or Change to a technical team with a higher level of expertise to assist in an Escalation.

Governance

Ensuring that Policies and Strategy are actually implemented, and that required Processes are correctly followed. Governance includes defining Roles and

responsibilities, measuring and reporting, and taking actions to resolve any issues identified.

Guideline

A Document describing Best Practice, which recommends what should be done. Compliance with a guideline is not normally enforced. See also Standard.

Help Desk

(Service Operation) A point of contact for Users to log Incidents. A Help Desk is usually more technically focused than a Service Desk and does not provide a Single Point of Contact for all interaction. The term Help Desk is often used as a synonym for Service Desk.

Hierarchic Escalation

(Service Operation) Informing or involving more senior levels of management to assist in an Escalation.

High Availability

(Service Design) An approach or design that minimizes or hides the effects of Configuration Item Failure on the users of an IT Service. High Availability solutions are designed to achieve an agreed level of Availability and make use of techniques such as Fault Tolerance, Resilience and fast Recovery to reduce the number of Incidents, and the Impact of Incidents.

Identity

(Service Operation) A unique name that is used to identify a User, person or Role. The Identity is used to grant Rights to that User, person, or Roles. Example identities might be the username SmithJ or the Role 'Change manager'.

Immediate Recovery

(Service Design) A Recovery Option that is also known as Hot Standby. Provision is made to recover the IT Service with no loss of Service. Immediate Recovery typically uses Mirroring, Load Balancing and Split Site technologies.

Impact

(Service Operation) (Service Transition) A measure of the effect of an Incident, Problem or Change on Business Processes. Impact is often based on how Service Levels will be affected. Impact and Urgency are used to assign Priority.

Incident

(Service Operation) An unplanned interruption to an IT Service or reduction in the Quality of an IT Service. Failure of a Configuration Item that has not yet affected Service is also an Incident. For example Failure of one disk from a mirror set.

Incident Management

(Service Operation) The Process responsible for managing the Lifecycle of all Incidents. The primary Objective of Incident Management is to return the IT Service to Customers as quickly as possible.

Incident Record

(Service Operation) A Record containing the details of an Incident. Each Incident record documents the Lifecycle of a single Incident.

Indirect Cost

(Service Strategy) A Cost of providing an IT Service, which cannot be allocated in full to a specific customer. For example, the Cost of providing shared Servers or software licences. Also known as Overhead.

Information Security Management (ISM) (Service Design) The Process that ensures the Confidentiality, Integrity and Availability of an Organization's Assets, information, data and IT Services.

Information Security Management usually forms part of an

Organizational approach to Security Management that has a wider scope than the IT Service Provider, and includes handling of paper, building access, phone calls, etc. for the entire Organization.

Information Security Policy

(Service Design) The Policy that governs the Organization's approach to Information Security Management.

Information Technology (IT)

The use of technology for the storage, communication or processing of information. The technology typically includes computers, telecommunications, Applications and other software. The information may include Business data, voice, images, video, etc. Information Technology is often used to support Business Processes through IT Services.

Insourcing

See Internal Sourcing.

Integrity

(Service Design) A security principle that ensures data and Configuration Items are modified only by authorized personnel and Activities. Integrity considers all possible causes of modification, including software and hardware Failure, environmental Events, and human intervention.

Interactive Voice Response (IVR)

(Service Operation) A form of Automatic Call Distribution that accepts User input, such as key presses and spoken commands, to identify the correct destination for incoming Calls.

Intermediate Recovery

(Service Design) A Recovery option that is also known as Warm Standby. Provision is made to recover the IT Service in a period of time between 24 and 72 hours.

Intermediate Recovery typically uses a shared Portable or Fixed Facility that has Computer Systems and Network Components. The hardware and software will need to be configured, and data will need to be restored, as part of the IT Service Continuity Plan.

Internal Metric

A Metric that is used within the IT Service Provider to Monitor the Efficiency, Effectiveness or Cost Effectiveness of the IT Service Provider's internal Processes. Internal Metrics are not normally reported to the Customer of the IT Service. See also External Metric.

Internal Service Provider

(Service Strategy) An IT Service Provider that is part of the same Organization as its Customer. An IT Service Provider may have both Internal Customers and External Customers.

Internal Sourcing

(Service Strategy) Using an Internal Service Provider to manage IT Services.

International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) is the world's largest developer of Standards. ISO is a non-governmental organization that is a network of the national standards institutes of 156 countries. See www.iso.org for further information about ISO.

International Standards Organization

See International Organization for Standardization (ISO).

Internet Service Provider (ISP)

An External Service Provider that provides access to the Internet. Most ISPs also provide other IT Services such as web hosting.

Invocation

(Service Design) Initiation of the steps defined in a plan. For example initiating the IT Service Continuity Plan for one or more IT Services.

Ishikawa Diagram

(Service Operation) (Continual Service Improvement) A technique that helps a team to identify all the possible causes of a Problem. Originally devised by Kaoru Ishikawa, the output of this technique is a diagram that looks like a fishbone.

ISO 9000

A generic term that refers to a number of international Standards and Guidelines for Quality Management Systems. See www.iso.org for more information. See also ISO.

ISO/IEC 20000

ISO Specification and Code of Practice for IT Service Management. ISO/IEC 20000 is aligned with ITIL Best Practice.

ISO/IEC 27001

(Service Design) (Continual Service Improvement) ISO Specification for Information Security Management. The corresponding Code of Practice is ISO/IEC 17799. See also Standard.

IT Infrastructure

All of the hardware, software, networks, facilities, etc. that are required to develop, Test, deliver, Monitor, Control or support IT Services. The term IT Infrastructure includes all of the Information Technology but not the associated people, Processes and documentation.

IT Operations

(Service Operation) Activities carried out by IT Operations Control, including Console Management, Job Scheduling, Backup and Restore, and Print and Output Management. IT Operations is also used as a synonym for Service Operation.

IT Operations Control

(Service Operation) The Function responsible for Monitoring and Control of the IT Services and IT Infrastructure. See also Operations Bridge.

IT Operations Management

(Service Operation) The Function within an IT Service Provider that performs the daily Activities needed to manage IT Services and the supporting IT Infrastructure. IT Operations Management includes IT Operations Control and Facilities Management.

IT Service

A Service provided to one or more Customers by an IT Service Provider. An IT Service is based on the use of Information Technology and supports the Customer's Business Processes. An IT Service is made up from a combination of people, Processes and technology and should be defined in a Service Level Agreement.

IT Service Continuity Management (ITSCM) (Service Design) The Process responsible for managing Risks that could seriously affect IT Services. ITSCM ensures that the IT Service Provider can always provide minimum agreed Service Levels, by reducing the Risk to an acceptable level and Planning for the Recovery of IT Services. ITSCM should be designed to support Business Continuity Management.

IT Service Continuity Plan

(Service Design) A Plan defining the steps required to recover one or more IT Services. The Plan will also identify the triggers for Invocation, people to be involved, communications, etc. The IT Service Continuity Plan should be part of a Business Continuity Plan.

IT Service Management (ITSM)

The implementation and management of Quality IT Services that meet the needs of the Business. IT Service Management are performed by IT Service Providers through an appropriate mix of people, Process and Information Technology. See also Service Management.

IT Service Management Forum (itSMF)

The IT Service Management Forum is an independent Organization dedicated to promoting a professional approach to IT Service Management. The itSMF is a not-for-profit membership Organization with representation in many countries around the world (itSMF Chapters). The itSMF and its membership contribute to the development of ITIL and associated IT Service Management Standards. See www.itsmf.com for more information.

ITIL

A set of Best Practice guidance for IT Service Management. ITIL is owned by the Axelos and consists of a series of publications giving guidance on the provision of Quality IT Services, and on the Processes and facilities needed to support them. See www.itil.co.uk for more information.

Job Description

A document that defines the Roles, responsibilities, skills and knowledge required by a particular person. One Job Description can include multiple Roles, for example the Roles of Configuration Manager and Change Manager may be carried out by one person.

Job Scheduling

(Service Operation) Planning and managing the execution of software tasks that are required as part of an IT Service. Job Scheduling is carried out by IT Operations Management, and is often automated using software tools that run batch or online tasks at specific times of the day, week, month or year.

Kepner & Tregoe Analysis

(Service Operation) (Continual Service Improvement) A structured approach to Problem solving. The Problem is analyzed in terms of what, where, when and extent. Possible causes are identified. The most probable cause is tested. The true cause is verified.

Key Performance Indicator (KPI)

(Service design) (Continual Service Improvement) A Metric that is used to help manage a Process, IT Service or Activity. Many Metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the Process, IT Service or Activity. KPIs should be selected to ensure that Efficiency, Effectiveness, and Cost Effectiveness are all managed. See also Critical Success Factor.

Knowledge Base

(Service Transition) A logical database containing the data used by the Service Knowledge Management System.

Knowledge Management

(Service Transition) The Process responsible for gathering, analyzing, storing and sharing knowledge and information within an Organization. The primary purpose of Knowledge Management is to improve Efficiency by reducing the need to rediscover knowledge. See also Service Knowledge Management System.

Known Error

(Service Operation) A Problem that has a documented Root Cause and a Workaround. Known Errors are created and managed throughout their Lifecycle by Problem Management. Known Errors may also be identified by Development or Suppliers.

Known Error Database (KEDB)

(Service Operation) A database containing all Known Error Records. This database is created by Problem Management and used by Incident and Problem Management. The Known Error Database is part of the Service Knowledge Management System.

Known Error Record

(Service Operation) A Record containing the details of a Known Error. Each Known Error Record documents the Lifecycle of a Known Error, including the Status, Root Cause and Workaround. In some implementations a Known Error is documented using additional fields in a Problem Record.

Lifecycle

The various stages in the life of an IT Service, Configuration Item, Incident, Problem, Change, etc. The Lifecycle defines the Categories for Status and the Status transitions that are permitted. For example:

- The Lifecycle of an Application includes Requirements, Design, Build, Deploy, Operate, Optimize
- The Expanded Incident Lifecycle includes Detect, Respond, Diagnose, Repair, Recover, Restore
- The Lifecycle of a Server may include: Ordered, Received, In Test, Live, Disposed, etc.

Live

(Service Transition) Refers to an IT Service or Configuration Item that is being used to deliver Service to a Customer.

Live Environment

(Service Transition) A controlled Environment containing Live Configuration Items used to deliver IT Services to Customers.

Major Incident

(Service Operation) The highest Category of Impact for an Incident. A Major Incident results in significant disruption to the Business.

Management Information

Information that is used to support decision making by managers. Management Information is often generated automatically by tools supporting the various IT Service Management Processes. Management Information often includes the values of KPIs such as ‘Percentage of Changes leading to Incidents’, or ‘first-time fix rate’.

Management of Risk (M_o_R)

The OGC methodology for managing Risks. M o_R includes all the Activities required to identify and Control the exposure to Risk, which may have an impact on the achievement of an Organization’s Business Objectives. See www.m-o-r.org for more details.

Management System

The framework of Policy, Processes and Functions that ensures an Organization can achieve its Objectives.

Maturity

(Continual Service Improvement) A measure of the Reliability, Efficiency and Effectiveness of a Process, Function, Organization, etc. The most mature Processes and Functions are formally aligned to Business Objectives and Strategy, and are supported by a framework for continual improvement.

Mean Time Between Failures (MTBF)

(Service Design) A Metric for measuring and reporting Reliability. MTBF is the average time that a Configuration Item or IT Service can perform its agreed Function without

interruption. This is measured from when the CI or IT Service starts working, until it next fails.

Mean Time To Repair (MTTR)

The average time taken to repair a Configuration Item or IT Service after a Failure. MTTR is measured from when the CI or IT Service fails until it is repaired. MTTR does not include the time required to Recover or Restore. MTTR is sometimes incorrectly used to mean Mean Time to Restore Service.

Mean Time to Restore Service (MTRS)

The average time taken to restore a Configuration Item or IT Service after a Failure. MTRS is measured from when the CI or IT Service fails until it is fully restored and delivering its normal functionality. See also Mean Time To Repair.

Metric

(Continual Service Improvement) Something that is measured and reported to help manage a Process, IT Service or Activity. See also KPI.

Middleware

(Service Design) Software that connects two or more software Components or Applications. Middleware is usually purchased from a Supplier, rather than developed within the IT Service Provider. See also Off the Shelf.

Model

A representation of a System, Process, IT Service, Configuration Item, etc. that is used to help understand or predict future behavior.

Modelling

A technique that is used to predict the future behavior of a System, Process, IT Service, Configuration Item, etc.

Modelling is commonly used in Financial Management, Capacity Management and Availability Management.

Monitor Control Loop

(Service Operation) Monitoring the output of a Task, Process, IT Service or Configuration Item; comparing this output to a predefined Norm; and taking appropriate action based on this comparison.

Monitoring

(Service Operation) Repeated observation of a Configuration Item, IT Service or Process to detect Events and to ensure that the current status is known.

Objective

The defined purpose or aim of a Process, an Activity or an Organization as a whole. Objectives are usually expressed as measurable targets. The term Objective is also informally used to mean a Requirement. See also Outcome.

Off the Shelf

See Commercial Off the Shelf.

Office of Government Commerce (OGC)

OGC owns the ITIL brand (copyright and trademark). OGC is a UK Government department that supports the delivery of the government's procurement agenda through its work in collaborative procurement and in raising levels of procurement skills and capability with departments. It also provides support for complex public sector projects.

Off-shore

(Service Strategy) Provision of Services from a location outside the country where the Customer is based, often in a different continent. This can be the provision of an IT Service, or of supporting Functions such as Service Desk.

Operate

To perform as expected. A Process or Configuration Item is said to Operate if it is delivering the required outputs.

Operate also means to perform one or more Operations. For example, to Operate a computer is to do the day-to- day Operations needed for it to perform as expected.

Operation

(Service Operation) Day-to-day management of an IT Service, System, or other Configuration Item. Operation is also used to mean any pre-defined Activity or Transaction. For example loading a magnetic tape, accepting money at a point of sale, or reading data from a disk drive.

Operational

The lowest of three levels of Planning and delivery (Strategic, Tactical, Operational). Operational Activities

include the day-to-day or short-term Planning or delivery of a Business Process or IT Service Management Process. The term Operational is also a synonym for Live.

Operational Cost

Cost resulting from running the IT Services. Often repeating payments. For example staff costs, hardware maintenance and electricity (also known as 'current expenditure' or 'revenue expenditure'). See also Capital Expenditure.

Operational Expenditure (OPEX)

See Operational Cost.

Operational Level Agreement (OLA)

(Service Design) (Continual Service Improvement) An Agreement between an IT Service Provider and another part of the same Organization. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties. For example there could be an OLA:

- Between the IT Service Provider and a procurement department to obtain hardware in agreed times
- Between the Service Desk and a Support Group to provide Incident Resolution in agreed times.

See also Service Level Agreement.

Operations Bridge

(Service Operation) A physical location where IT Services and IT Infrastructure are monitored and managed.

Operations Control

See IT Operations Control.

Operations Management

See IT Operations Management.

Optimize

Review, Plan and request Changes, in order to obtain the maximum Efficiency and Effectiveness from a Process, Configuration Item, Application, etc.

Organization

A company, legal entity or other institution. Examples of Organizations that are not companies include International Standards Organization or itSMF. The term Organization is sometimes used to refer to any entity that has People, Resources and Budgets. For example a Project or Business Unit.

Outcome

The result of carrying out an Activity; following a Process; delivering an IT Service, etc. The term Outcome is used to refer to intended results, as well as to actual results. See also Objective.

Outsourcing

(Service Strategy) Using an External Service Provider to manage IT Services. See also Service Sourcing.

Overhead

See Indirect cost.

Pain Value Analysis

(Service Operation) A technique used to help identify the Business Impact of one or more Problems. A formula is used to calculate Pain Value based on the number of Users affected, the duration of the Downtime, the Impact on each User, and the cost to the Business (if known).

Partnership

A relationship between two Organizations that involves working closely together for common goals or mutual benefit. The IT Service Provider should have a Partnership with the Business, and with Third Parties who are critical to the delivery of IT Services. See also Value Network.

Passive Monitoring

(Service Operation) Monitoring of a Configuration Item, an IT Service or a Process that relies on an Alert or notification to discover the current status. See also Active Monitoring.

Performance

A measure of what is achieved or delivered by a System, person, team, Process, or IT Service.

Performance Management

(Continual Service Improvement) The Process responsible for day-to-day Capacity Management Activities. These include monitoring, threshold detection, Performance analysis and Tuning, and implementing changes related to Performance and Capacity.

Pilot

(Service Transition) A limited Deployment of an IT Service, a Release or a Process to the Live Environment. A pilot is used to reduce Risk and to gain User feedback and Acceptance. See also Test, Evaluation.

Plan

A detailed proposal that describes the Activities and Resources needed to achieve an Objective. For example a Plan to implement a new IT Service or Process. ISO/IEC 20000 requires a Plan for the management of each IT Service Management Process.

Plan–Do–Check–Act

(Continual Service Improvement) A four-stage cycle for Process management, attributed to Edward Deming. Plan–Do–Check–Act is also called the Deming Cycle.

PLAN: Design or revise Processes that support the IT Services.

DO: Implement the Plan and manage the Processes.

CHECK: Measure the Processes and IT Services, compare with Objectives and produce reports.

ACT: Plan and implement Changes to improve the Processes.

Planned Downtime

(Service Design) Agreed time when an IT Service will not be available. Planned Downtime is often used for maintenance, upgrades and testing. See also Downtime.

Planning

An Activity responsible for creating one or more Plans. For example, Capacity Planning.

Policy

Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of Processes, Standards, Roles, Activities, IT Infrastructure, etc.

Practice

A way of working, or a way in which work must be done. Practices can include Activities, Processes, Functions, Standards and Guidelines. See also Best Practice.

PRINCE2

The standard UK government methodology for Project management. See www.ogc.gov.uk/prince2 for more information.

Priority

(Service Transition) (Service Operation) A Category used to identify the relative importance of an Incident, Problem or Change. Priority is based on Impact and Urgency, and is used to identify required times for actions to be taken. For example the SLA may state that Priority 2 Incidents must be resolved within 12 hours.

Proactive Monitoring

(Service Operation) Monitoring that looks for patterns of Events to predict possible future Failures. See also Reactive Monitoring.

Proactive Problem Management

(Service Operation) Part of the Problem Management Process. The Objective of Proactive Problem Management is to identify Problems that might otherwise be missed. Proactive Problem Management analyses Incident Records, and uses data collected by other IT Service Management Processes to identify trends or significant problems.

Problem

(Service Operation) A cause of one or more Incidents. The cause is not usually known at the time a Problem Record is created, and the Problem Management Process is responsible for further investigation.

Problem Management

(Service Operation) The Process responsible for managing the Lifecycle of all Problems. The primary objectives of

Problem Management are to prevent Incidents from happening, and to minimize the Impact of Incidents that cannot be prevented.

Problem Record

(Service Operation) A Record containing the details of a Problem. Each Problem Record documents the Lifecycle of a single Problem.

Procedure

A Document containing steps that specify how to achieve an Activity. Procedures are defined as part of Processes.

See also Work Instruction.

Process

A structured set of Activities designed to accomplish a specific Objective. A Process takes one or more defined inputs and turns them into defined outputs. A Process may include any of the Roles, responsibilities, tools and management Controls required to reliably deliver the outputs. A Process may define Policies, Standards, Guidelines, Activities, and Work Instructions if they are needed.

Process Control

The Activity of planning and regulating a Process, with the Objective of performing the Process in an Effective, Efficient, and consistent manner.

Process Manager

A Role responsible for Operational management of a Process. The Process Manager's responsibilities include Planning and coordination of all Activities required to carry out, monitor and report on the Process. There may be several Process Managers for one Process, for example regional Change Managers or IT Service Continuity Managers for each data center. The Process Manager Role is often assigned to the person who carries out the Process Owner Role, but the two Roles may be separate in larger organizations.

Process Owner

A Role responsible for ensuring that a Process is Fit for Purpose. The Process Owner's responsibilities include sponsorship, Design, Change Management and continual improvement of the Process and its Metrics. This Role is often assigned to the same person who carries out the Process Manager Role, but the two Roles may be separate in larger Organizations.

Production Environment

See Live Environment.

Program

A number of Projects and Activities that are planned and managed together to achieve an overall set of related Objectives and other Outcomes.

Project

A temporary Organization, with people and other Assets required to achieve an Objective or other Outcome. Each Project has a Lifecycle that typically includes initiation, Planning, execution, Closure, etc. Projects are usually managed using a formal methodology such as PRINCE2.

Qualification

(Service Transition) An Activity that ensures that IT Infrastructure is appropriate, and correctly configured, to support an Application or IT Service. See also Validation.

Quality

The ability of a product, Service, or Process to provide the intended value. For example, a hardware Component can be considered to be of high Quality if it performs as expected and delivers the required Reliability. Process Quality also requires an ability to monitor Effectiveness and Efficiency, and to improve them if necessary. See also Quality Management System.

Quality Assurance (QA)

(Service Transition) The Process responsible for ensuring that the Quality of a product, Service or Process will provide its intended Value.

Quality Management System (QMS) (Continual Service Improvement) The set of Processes responsible for ensuring that all work carried out by an Organization is of a suitable Quality to reliably meet

Business Objectives or Service Levels. See also ISO 9000.

Reactive Monitoring

(Service Operation) Monitoring that takes action in response

to an Event. For example submitting a batch job when the previous job completes, or logging an Incident when an Error occurs. See also Proactive Monitoring.

Record

A Document containing the results or other output from a Process or Activity. Records are evidence of the fact that an activity took place and may be paper or electronic. For example, an Audit report, an Incident Record, or the minutes of a meeting.

Recovery

(Service Design) (Service Operation) Returning a Configuration Item or an IT Service to a working state. Recovery of an IT Service often includes recovering data to a known consistent state. After Recovery, further steps may be needed before the IT Service can be made available to the Users (Restoration).

Recovery Option

(Service Design) A Strategy for responding to an interruption to Service. Commonly used Strategies are Do Nothing, Manual Workaround, Reciprocal Arrangement, Gradual Recovery, Intermediate Recovery, Fast Recovery, and Immediate Recovery. Recovery Options may make use of dedicated facilities, or Third Party facilities shared by multiple Businesses.

Recovery Point Objective (RPO)

(Service Operation) The maximum amount of data that may be lost when Service is restored after an interruption. Recovery Point Objective is expressed as a length of time before the Failure. For example a Recovery Point Objective of one day may be supported by daily Backups, and up to 24 hours of data may be lost. Recovery Point Objectives for each IT Service should be negotiated, agreed and documented, and used as requirements for Service Design and IT Service Continuity Plans.

Recovery Time Objective (RTO)

(Service Operation) The maximum time allowed for recovery of an IT Service following an interruption. The Service Level to be provided may be less than normal Service Level Targets. Recovery Time Objectives for each IT Service should be negotiated, agreed and documented.

See also Business Impact Analysis.

Redundancy

See Fault Tolerance.

The term Redundant also has a generic meaning of obsolete, or no longer needed.

Relationship

A connection or interaction between two people or things. In Business Relationship Management it is the interaction between the IT Service Provider and the Business. In Configuration Management it is a link between two Configuration Items that identifies a dependency or connection between them. For example Applications may be linked to the Servers they run on, IT Services have many links to all the CIs that contribute to them.

Release

(Service Transition) A collection of hardware, software, documentation, Processes or other Components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, tested, and deployed as a single entity.

Release and Deployment Management (Service Transition) The Process responsible for both Release Management and Deployment.

Release Management

(Service Transition) The Process responsible for Planning, scheduling and controlling the movement of Releases to Test and Live Environments. The primary Objective of Release Management is to ensure that the integrity of the Live Environment is protected and that the correct Components are released. Release Management is part of the Release and Deployment Management Process.

Release Process

The name used by ISO/IEC 20000 for the Process group that includes Release Management. This group does not include any other Processes.

Release Process is also used as a synonym for Release Management Process.

Release Record

(Service Transition) A Record in the CMDB that defines the content of a Release. A Release Record has Relationships with all Configuration Items that are affected by the Release.

Reliability

(Service Design) (Continual Service Improvement) A measure of how long a Configuration Item or IT Service can perform its agreed Function without interruption. Usually measured as MTBF or MTBSI. The term Reliability can also be used to state how likely it is that a Process, Function, etc. will deliver its required outputs. See also Availability.

Remediation

(Service Transition) Recovery to a known state after a failed Change or Release.

Repair

(Service Operation) The replacement or correction of a failed Configuration Item.

Request for Change (RFC)

(Service Transition) A formal proposal for a Change to be made. An RFC includes details of the proposed Change, and may be recorded on paper or electronically. The term RFC is often misused to mean a Change Record, or the Change itself.

Request Fulfilment

(Service Operation) The Process responsible for managing the Lifecycle of all Service Requests.

Requirement

(Service Design) A formal statement of what is needed. For example, a Service Level Requirement, a Project Requirement or the required Deliverables for a Process. See also Statement of Requirements.

Resilience

(Service Design) The ability of a Configuration Item or IT Service to resist failure or to recover quickly following a Failure. For example an armored cable will resist failure when put under stress. See also Fault Tolerance.

Resolution

(Service Operation) Action taken to repair the Root Cause of an Incident or Problem, or to implement a Workaround. In ISO/IEC 20000, Resolution Processes is the Process group that includes Incident and Problem Management.

Resource

(Service Strategy) A generic term that includes IT Infrastructure, people, money or anything else that might help to deliver an IT Service. Resources are considered to be Assets of an Organization. See also Capability, Service Asset.

Response Time

A measure of the time taken to complete an Operation or Transaction. Used in Capacity Management as a measure of IT Infrastructure Performance, and in Incident Management as a measure of the time taken to answer the phone, or to start Diagnosis.

Responsiveness

A measurement of the time taken to respond to something. This could be Response Time of a Transaction, or the speed with which an IT Service Provider responds to an Incident or Request for Change, etc.

Restoration of Service

See Restore.

Restore

(Service Operation) Taking action to return an IT Service to the Users after Repair and Recovery from an Incident. This is the primary Objective of Incident Management.

Retire

(Service Transition) Permanent removal of an IT Service, or other Configuration Item, from the Live Environment. Retired is a stage in the Lifecycle of many Configuration Items.

Review

An evaluation of a Change, Problem, Process, Project, etc. Reviews are typically carried out at predefined points in the Lifecycle, and especially after Closure. The purpose of a Review is to ensure that all Deliverables have been provided, and to identify opportunities for improvement.

Rights

(Service Operation) Entitlements, or permissions, granted to a User or Role. For example the Right to modify particular data, or to authorize a Change.

Risk

A possible event that could cause harm or loss, or affect the ability to achieve Objectives. A Risk is measured by the probability of a Threat, the Vulnerability of the Asset to that Threat, and the Impact it would have if it occurred.

Risk Assessment

The initial steps of Risk Management. Analyzing the value of Assets to the business, identifying Threats to those Assets, and evaluating how vulnerable each Asset is to those Threats. Risk Assessment can be quantitative (based on numerical data) or qualitative.

Risk Management

The Process responsible for identifying, assessing and controlling Risks. See also Risk Assessment.

Role

A set of responsibilities, Activities and authorities granted to a person or team. A Role is defined in a Process. One person or team may have multiple Roles; for example, the Roles of Configuration Manager and Change Manager may be carried out by a single person.

Rollout

(Service Transition) See Deployment.

Most often used to refer to complex or phased Deployments or Deployments to multiple locations.

Root Cause

(Service Operation) The underlying or original cause of an Incident or Problem.

Root Cause Analysis (RCA)

(Service Operation) An Activity that identifies the Root Cause of an Incident or Problem. RCA typically concentrates on IT Infrastructure failures. See also Service Failure Analysis.

Scalability

The ability of an IT Service, Process, Configuration Item, etc. to perform its agreed Function when the Workload or Scope changes.

Scope

The boundary, or extent, to which a Process, Procedure, Certification, Contract, etc. applies. For example the Scope of Change Management may include all Live IT Services and related Configuration Items, the Scope of an ISO/IEC 20000 Certificate may include all IT Services delivered out of a named data center.

Second-line Support

(Service Operation) The second level in a hierarchy

of Support Groups involved in the resolution of Incidents and investigation of Problems. Each level contains more specialist skills, or has more time or other resources.

Security

See Information Security Management.

Security Management

See Information Security Management.

Security Policy

See Information Security Policy.

Server

(Service Operation) A computer that is connected to a network and provides software Functions that are used by other Computers.

Service

A means of delivering value to Customers by facilitating Outcomes Customers want to achieve without the ownership of specific Costs and Risks.

Service Asset

Any Capability or Resource of a Service Provider. See also

Asset.

Service Asset and Configuration Management (SACM)

(Service Transition) The Process responsible for both Configuration Management and Asset Management.

Service Capacity Management (SCM) (Service Design) (Continual Service Improvement) The Activity responsible for understanding the Performance and Capacity of IT Services. The Resources used by each IT Service and the pattern of usage over time are collected, recorded, and analyzed for use in the Capacity Plan. See also Business Capacity Management, Component Capacity Management.

Service Catalog

(Service Design) A database or structured Document with information about all Live IT Services, including those available for Deployment. The Service Catalogue is the only part of the Service Portfolio published to Customers, and is used to support the sale and delivery of IT Services. The Service Catalogue includes information about deliverables, prices, contact points, ordering and request Processes.

Service Continuity Management

See IT Service Continuity Management.

Service Culture

A Customer-oriented Culture. The major Objectives of a Service Culture are Customer satisfaction and helping Customers to achieve their Business Objectives.

Service Design

(Service Design) A stage in the Lifecycle of an IT Service. Service Design includes a number of Processes and Functions and is the title of one of the Core ITIL publications. See also Design.

Service Desk

(Service Operation) The Single Point of Contact between the Service Provider and the Users. A typical Service Desk manages Incidents and Service Requests, and also handles communication with the Users.

Service Failure Analysis (SFA)

(Service Design) An Activity that identifies underlying causes of one or more IT Service interruptions. SFA identifies opportunities to improve the IT Service Provider's Processes and tools, and not just the IT Infrastructure. SFA is a time-constrained, project-like activity, rather than an ongoing process of analysis. See also Root Cause Analysis.

Service Hours

(Service Design) (Continual Service Improvement) An agreed time period when a particular IT Service should be Available. For example, 'Monday–Friday 08:00 to 17:00 except public holidays'. Service Hours should be defined in a Service Level Agreement.

Service Improvement Plan (SIP) (Continual Service Improvement) A formal Plan to implement improvements to a Process or IT Service.

Service Knowledge Management System (SKMS)

(Service Transition) A set of tools and databases that are used to manage knowledge and information. The SKMS includes the Configuration Management System, as well as other tools and databases. The SKMS stores, manages, updates, and presents all information that an IT Service Provider needs to manage the full Lifecycle of IT Services.

Service Level

Measured and reported achievement against one or more Service Level Targets. The term Service Level is sometimes used informally to mean Service Level Target.

Service Level Agreement (SLA)

(Service Design) (Continual Service Improvement) An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple customers. See also Operational Level Agreement.

Service Level Management (SLM)

(Service Design) (Continual Service Improvement) The Process responsible for negotiating Service Level Agreements, and ensuring that these are met. SLM is responsible for ensuring that all IT Service Management Processes, Operational Level Agreements, and Underpinning Contracts, are appropriate for the agreed Service Level Targets. SLM monitors and reports on Service Levels, and holds regular Customer reviews.

Service Level Requirement (SLR)

(Service Design) (Continual Service Improvement)

A Customer Requirement for an aspect of an IT Service. SLRs are based on Business Objectives and are used to negotiate agreed Service Level Targets.

Service Level Target

(Service Design) (Continual Service Improvement) A commitment that is documented in a Service Level Agreement. Service Level Targets are based on Service Level Requirements, and are needed to ensure that the IT Service design is Fit for Purpose. Service Level Targets should be SMART, and are usually based on KPIs.

Service Maintenance Objective

(Service Operation) The expected time that a Configuration Item will be unavailable due to planned maintenance Activity.

Service Management

Service Management is a set of specialized organizational capabilities for providing value to customers in the form of services.

Service Management Lifecycle

An approach to IT Service Management that emphasizes the importance of coordination and Control across the various Functions, Processes, and Systems necessary to manage the full Lifecycle of IT Services. The Service Management Lifecycle approach considers the Strategy, Design, Transition, Operation and Continuous Improvement of IT Services.

Service Manager

A manager who is responsible for managing the end-to- end Lifecycle of one or more IT Services. The term Service Manager is also used to mean any manager within the IT Service Provider. It is most commonly used to refer to a Business Relationship Manager, a Process Manager, an Account Manager or a senior manager with responsibility for IT Services overall.

Service Operation

(Service Operation) A stage in the Lifecycle of an IT Service. Service Operation includes a number of Processes and Functions and is the title of one of the Core ITIL publications. See also Operation.

Service Portfolio

(Service Strategy) The complete set of Services that are managed by a Service Provider. The Service Portfolio is used to manage the entire Lifecycle of all Services, and includes three Categories: Service Pipeline (proposed or in Development); Service Catalogue (Live or available for Deployment); and Retired Services. See also Service Portfolio Management.

Service Portfolio Management (SPM) (Service Strategy) The Process responsible for managing the Service Portfolio. Service Portfolio Management considers Services in terms of the Business value that they provide.

Service Provider

(Service Strategy) An Organization supplying Services to one or more Internal Customers or External Customers. Service Provider is often used as an abbreviation for IT Service Provider.

Service Reporting

(Continual Service Improvement) The Process responsible for producing and delivering reports of achievement and trends against Service Levels. Service Reporting should agree the format, content and frequency of reports with Customers.

Service Request

(Service Operation) A request from a User for information, or advice, or for a Standard Change or for Access to an IT Service. For example to reset a password, or to provide standard IT Services for a new User. Service Requests are usually handled by a Service Desk, and do not require an RFC to be submitted. See also Request Fulfilment.

Service Strategy

(Service Strategy) The title of one of the Core ITIL publications. Service Strategy establishes an overall Strategy for IT Services and for IT Service Management.

Service Transition

(Service Transition) A stage in the Lifecycle of an IT Service. Service Transition includes a number of Processes and Functions and is the title of one of the Core ITIL publications. See also Transition.

Shift

(Service Operation) A group or team of people who carry out a specific Role for a fixed period of time. For example there could be four shifts of IT Operations Control personnel to support an IT Service that is used 24 hours a day.

Single Point of Contact

(Service Operation) Providing a single consistent way to communicate with an Organization or Business Unit. For example, a Single Point of Contact for an IT Service Provider is usually called a Service Desk.

Single Point of Failure (SPOF)

(Service Design) Any Configuration Item that can cause an Incident when it fails, and for which a Countermeasure has not been implemented. A SPOF may be a person, or a step in a Process or Activity, as well as a Component of the IT Infrastructure. See also Failure.

Specification

A formal definition of Requirements. A Specification may be used to define technical or Operational Requirements, and may be internal or external. Many public Standards consist of a Code of Practice and a Specification. The Specification defines the Standard against which an Organization can be audited.

Stakeholder

All people who have an interest in an Organization, Project, IT Service, etc. Stakeholders may be interested in the Activities, targets, Resources, or Deliverables.

Stakeholders may include Customers, Partners, employees, shareholders, owners, etc.

Standard

A mandatory Requirement. Examples include ISO/IEC 20000 (an international Standard), an internal security standard for UNIX configuration, or a government standard for how financial Records should be maintained. The term Standard is also used to refer to a Code of Practice or Specification published by a Standards Organization such as ISO or BSI. See also Guideline.

Standard Change

(Service Transition) A pre-approved Change that is low Risk, relatively common and follows a Procedure or Work Instruction. For example, password reset or provision of standard equipment to a new employee. RFCs are not required to implement a Standard Change, and they are logged and tracked using a different mechanism, such as a Service Request. See also Change Model.Standard Operating Procedures (SOP) (Service Operation) Procedures used by IT Operations Management.

Standby

(Service Design) Used to refer to Resources that are not required to deliver the Live IT Services, but are available to support IT Service Continuity Plans. For example a Standby data center may be maintained to support Hot Standby, Warm Standby or Cold Standby arrangements.

Statement of requirements (SOR)

(Service Design) A Document containing all Requirements for a product purchase, or a new or changed IT Service.

Status

The name of a required field in many types of Record. It shows the current stage in the Lifecycle of the associated Configuration Item, Incident, Problem, etc.

Storage Management

(Service Operation) The Process responsible for managing the storage and maintenance of data throughout its Lifecycle.

Strategic

(Service Strategy) The highest of three levels of Planning and delivery (Strategic, Tactical, Operational). Strategic Activities include Objective setting and long-term planning to achieve the overall Vision.

Strategy

(Service Strategy) A Strategic Plan designed to achieve defined Objectives.

Super User

(Service Operation) A User who helps other Users, and assists in communication with the Service Desk or other parts of the IT Service Provider. Super Users typically provide support for minor Incidents and training.

Supplier

(Service Strategy) (Service Design) A Third Party responsible for supplying goods or Services that are required to deliver IT Services. Examples of suppliers include commodity hardware and software vendors, network and telecom providers, and outsourcing Organizations. See also Underpinning Contract, Supply Chain.

Supplier Management

(Service Design) The Process responsible for ensuring that all Contracts with Suppliers support the needs of the Business, and that all Suppliers meet their contractual commitments.

Supply Chain

(Service Strategy) The Activities in a Value Chain carried out by Suppliers. A Supply Chain typically involves multiple Suppliers, each adding value to the product or Service. See also Value Network.

Support Group

(Service Operation) A group of people with technical skills. Support Groups provide the Technical Support needed by all of the IT Service Management Processes. See also Technical Management.

System

A number of related things that work together to achieve an overall Objective. For example:

- A computer System, including hardware, software and Applications
- A management System, including multiple Processes that are planned and managed together. For example, a Quality Management System
- A Database Management System or Operating System that includes many software modules that are designed to perform a set of related Functions.

System Management

The part of IT Service Management that focuses on the management of IT Infrastructure rather than Process.

Tactical

The middle of three levels of Planning and delivery (Strategic, Tactical, Operational). Tactical Activities include the medium-term Plans required to achieve specific Objectives, typically over a period of weeks to months.

Technical Management

(Service Operation) The Function responsible for providing technical skills in support of IT Services and management of the IT Infrastructure. Technical Management defines the Roles of Support Groups, as well as the tools, Processes and Procedures required.

Technical Observation

(Continual Service Improvement) A technique used in Service Improvement, Problem investigation and Availability Management. Technical support staff meet to monitor the behaviour and Performance of an IT Service and make recommendations for improvement.

Technical Support

See Technical Management.

Test

(Service Transition) An Activity that verifies that a Configuration Item, IT Service, Process, etc. meets its Specification or agreed Requirements.

Test Environment

(Service Transition) A controlled Environment used to Test Configuration Items, Builds, IT Services, Processes, etc.

Third Party

A person, group, or Business that is not part of the Service Level Agreement for an IT Service, but is required to ensure successful delivery of that IT Service. For example, a software Supplier, a hardware maintenance company, or a facilities department. Requirements for Third Parties are typically specified in Underpinning Contracts or Operational Level Agreements.

Third-line Support

(Service Operation) The third level in a hierarchy of Support Groups involved in the resolution of Incidents and investigation of Problems. Each level contains more specialist skills, or has more time or other resources.

Threat

Anything that might exploit a Vulnerability. Any potential cause of an Incident can be considered to be a Threat. For example a fire is a Threat that could exploit the Vulnerability of flammable floor coverings. This term is commonly used in Information Security Management and IT Service Continuity Management, but also applies to other areas such as Problem and Availability Management.

Threshold

The value of a Metric that should cause an Alert to be generated, or management action to be taken. For example 'Priority 1 Incident not solved within four hours', 'more than five soft disk errors in an hour', or 'more than 10 failed changes in a month'.

Throughput

(Service Design) A measure of the number of Transactions, or other Operations, performed in a fixed time. For example, 5,000 e-mails sent per hour, or 200 disk I/Os per second.

Total Quality Management (TQM) (Continual Service Improvement) A methodology for managing continual Improvement by using a Quality Management System. TQM establishes a Culture involving all people in the Organization in a Process of continual monitoring and improvement.

Transaction

A discrete Function performed by an IT Service. For example transferring money from one bank account to another. A single Transaction may involve numerous additions, deletions and modifications of data. Either all of these complete successfully or none of them is carried out.

Transition

(Service Transition) A change in state, corresponding to a movement of an IT Service or other Configuration Item from one Lifecycle status to the next.

Trend Analysis

(Continual Service Improvement) Analysis of data to identify time-related patterns. Trend Analysis is used in Problem Management to identify common Failures or fragile Configuration Items, and in Capacity Management as a Modelling tool to predict future behaviour. It is also used as a management tool for identifying deficiencies in IT Service Management Processes.

Tuning

The activity responsible for planning changes to make the most efficient use of Resources. Tuning is part of Performance Management, which also includes Performance monitoring and implementation of the required Changes.

Underpinning Contract (UC)

(Service Design) A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.

Unit Cost

(Service Strategy) The Cost to the IT Service Provider of providing a single Component of an IT Service. For example the Cost of a single desktop PC, or of a single Transaction.

Urgency

(Service Transition) (Service Design) A measure of how long it will be until an Incident, Problem or Change has a significant Impact on the Business. For example a high Impact Incident may have low Urgency, if the Impact will not affect the Business until the end of the financial year. Impact and Urgency are used to assign Priority.

Usability

(Service Design) The ease with which an Application, product, or IT Service can be used. Usability Requirements are often included in a Statement of Requirements.

Use Case

(Service Design) A technique used to define required functionality and Objectives, and to design Tests. Use Cases define realistic scenarios that describe interactions between Users and an IT Service or other System. See also Change Case.

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.

User Profile (UP)

(Service Strategy) A pattern of User demand for IT Services. Each User Profile includes one or more Patterns of Business Activity.

Utility

(Service Strategy) Functionality offered by a Product or Service to meet a particular need. Utility is often summarized as 'what it does'.

Validation

(Service Transition) An Activity that ensures a new or changed IT Service, Process, Plan, or other Deliverable meets the needs of the Business. Validation ensures that Business Requirements are met even though these may have changed since the original design. See also Verification, Acceptance, and Qualification.

Value for Money

An informal measure of Cost Effectiveness. Value for Money is often based on a comparison with the Cost of alternatives. See also Cost Benefit Analysis.

Value Network

(Service Strategy) A complex set of relationships between two or more groups or Organizations. Value is generated through exchange of knowledge, information, goods or Services. See also Partnership.

Variance

The difference between a planned value and the actual measured value. Commonly used in Financial Management, Capacity Management and Service Level Management, but could apply in any area where Plans are in place.

Verification

(Service Transition) An Activity that ensures a new or changed IT Service, Process, Plan, or other Deliverable is complete, accurate, reliable and matches its design specification. See also Validation, Acceptance.

Version

(Service Transition) A Version is used to identify a specific Baseline of a Configuration Item. Versions typically use a naming convention that enables the sequence or date of each Baseline to be identified. For example Payroll Application Version 3 contains updated functionality from Version 2.

Vision

A description of what the Organization intends to become in the future. A Vision is created by senior management and is used to help influence Culture and Strategic Planning.

Vital Business Function (VBF)

(Service Design) A Function of a Business Process that is critical to the success of the Business. Vital Business Functions are an important consideration of Business Continuity Management, IT Service Continuity Management and Availability Management.

Work in Progress (WIP)

A Status that means Activities have started but are not yet complete. It is commonly used as a Status for Incidents, Problems, Changes, etc.

Work Instruction

A Document containing detailed instructions that specify exactly what steps to follow to carry out an Activity.

A Work Instruction contains much more detail than a Procedure and is only created if very detailed instructions are needed.

Workaround

(Service Operation) Reducing or eliminating the Impact of an Incident or Problem for which a full Resolution is not yet available. For example by restarting a failed Configuration Item. Workarounds for Problems are documented in Known Error Records. Workarounds for Incidents that do not have associated Problem Records are documented in the Incident Record.

Workload

The Resources required to deliver an identifiable part of an IT Service. Workloads may be categorized by Users, groups of Users, or Functions within the IT Service. This is used to assist in analyzing and managing the Capacity, Performance and Utilization of Configuration Items and IT Services. The term Workload is sometimes used as a synonym for throughput.

Appendix C
OSI Governance and Control

Key ITIL/Service Management Roles for Function, Process and ITSM Control and Governance:

NOTE: The accountabilities and responsibilities of all these roles below are all excerpted from the ITIL publications Service Strategy, Service Design and Service Operation.

The roles described below are intended as overview and can be added to the existing responsibilities of more specific roles defined earlier in this document and/or other documents.

To ensure that we have proper control and governance of our processes, services and functions we suggest that the State CWDS organization appoints the following roles:

Director of Service Management or **Director of SMO (Service Management Office)** or **Director of ITSM (IT Service Management)**

This role will be responsible for all of our ITSM processes and/or to establish a Service Management Office (SMO). *It is a key role in the overall governance of ITSM and is often the missing piece in the success of ITSM.*

The Director's responsibilities would include:

- Takes overall responsibility for the successful implementation and operation of OSI's ITSM (ITIL) processes
- Proposes, initiates and manages any ITSM service improvement initiatives
- Works with individual Service Owners, Process Owners and Process Managers to identify issues, performance levels and potential improvements
- Manages resources between the ITSM processes and functions
- Takes responsibility for overseeing ITSM staff development and training

Process Owner: The Process Owner is accountable to ensure that the process is fit for its purpose. (This person can also take on the role of Process Manager in smaller organizations). The Process Owner makes sure that: the process is executed/performed according to the agreed and documented standards of the process; it meets the aims of the process definition, in part, by holding people accountable for their behavior related to the execution of the process. The owner's responsibilities include sponsorship, design, change management and continual improvement of the process and its metrics. *This role and the other process roles are a significant factor in the ability to "control" processes to make sure processes operate efficiently and effectively.*

The person chosen to be a Process Owner must be at a senior level at OSI to have the level of credibility and authority to inspire others (Process Managers and Process Practitioners).This allows the execution of the process correctly, even though those people may not report to the Process Owner.

The Process Owner's responsibilities would include:

- Ensuring that the ongoing service delivery and support meet agreed customer requirements
- Defining 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 appropriate and change the strategy as required
- Communicating process information or changes as appropriate to ensure awareness
- Providing process resources to support activities required throughout the service lifecycle
- Ensuring that OSI Staff 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
- Working with the CSI Manager and Process Manager to review and prioritize improvements in the CSI register
- Making improvements to the process
- Sponsoring and 'change managing' the process and its metrics

The **Process Manager** is accountable for the operational management of the process. The Process Manager's responsibilities include planning and coordination of all the activities required to carry out, monitor, and report on the process.

The Process Manager's responsibilities would include:

- Working with the Process Owner to plan and coordinate 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 prioritize improvements in the CSI register
- Making improvements to the process implementation

A **Process Practitioner** is responsible for carrying out one or more process activities. There are usually multiple Process Practitioners who may have titles which are more specific to their respective processes.

The responsibilities of the Process Practitioner would include:

- Carrying out one or more of the activities of a process
- Understanding how their role contributes to the overall delivery of services and the creation of value for the business (from the Process Owner and/or Process Manager)
- Working with other stakeholders, such as their Manager, co-workers, users and customers, to ensure that their contributions are effective
- Ensuring that their inputs, outputs and interfaces for their activities are correct

- Creating or updating records to show that activities have been carried out correctly (This important step should be audited and reviewed by the Process Owner and/or Process Manager for compliance to the process policies, objectives and procedures)

The next critical role is the **Service Owner**.
This is another key role in the overall governance of ITSM and is often the missing piece in the success of ITSM.

To ensure that each service is managed with a business focus, the definition of a single point of accountability is absolutely essential to provide the level of attention and focus required for its delivery.

The Service Owner is accountable for the delivery of a specific IT service (e.g. Communications, Applications). The Service Owner is responsible to the customer for the initiation, transition (change management), ongoing maintenance and support of a particular service. They are then accountable to the Director of Service Management, for the delivery of the service. Therefore, the Service Owner will also be a stakeholder in all the processes which enable or support the service that they own. The Service Owner's accountability for a specific service within OSI is independent of where the underpinning technology components, processes, or professional capabilities reside.

The Service Owner's responsibilities would include:

- Ensure that the ongoing service delivery and support meet agreed customer requirements
- Working with the Business Relationship Management process to understand and translate customer requirements into activities or service components that will ensure that OSI can meet those requirements
- Ensuring consistent and appropriate communication with customers for service-related inquiries and issues
- Assisting in assessing the impact of new services or changes to existing services
- Identifying opportunities for service improvements, discussing these with the customer and submitting RFC's as appropriate
- Interfacing with the appropriate Process Owners throughout the service lifecycle
- Soliciting required data, statistics and reports for analysis and to facilitate effective service monitoring and performance
- Providing input in service attributes such as performance, availability, etc.
- Representing the service across the organization
- Understanding the Service and Service components
- Serving as the point of escalation (notification) for major incidents relating to the service
- Representing the service in CAB meetings
- Participating in internal service review meetings (within IT)
- Participating in external service review meetings (with the business)
- Ensuring that the Service Entry in the Service Catalog is up to date and is maintained
- Participating in helping to negotiate SLAs and OLAs relating to the service
- Identifying improvement opportunities for inclusion in the CSI register
- Working with the CSI Manager to review and prioritize improvements in the CSI register
- Making improvements to the service

The Service Owner is responsible for continual improvement and the management of change affecting the Service(s) they own.

When all the parties assigned to these roles take their roles seriously, are trained properly and get support from management that reinforces the importance of these roles we can better manage and deliver services to our customers and users more successfully. ***And this builds governance into what we do.***