CWDS
Problem Management ITIL Detailed Design

Created By:

Project Name:	**CWDS Service Desk Support Services**
Document ID:	**Problem Management Detailed Design**
Version:	**1.1.4**
Issue Date:	**3/2/2018**

Revision History

Date	Version	Description	Author
02-Feb-18	1.0	Problem Management ITIL Detailed Design Plan	Jim McKennan
20-Aug-18	1.1	Updated Appendix D (Problem Analysis Techniques) with additional detail; Updated section 5.0 Problem Investigation and Diagnosis (5.5 Perform Root Cause Analysis procedure)	Jim McKennan
21-Aug-18	1.1.1	Updated section 5.5 referencing the RCA template; Updated Appendix by adding the RCA Template	Jim McKennan
23-Aug-18	1.1.2	Added Problem Coordinator role description	Jim McKennan
1-Oct-18	1.1.3	Changed Process Coordinator role to Process Practitioner, changed N Level Problem Practitioner to N Level Problem Analyst in all RACIs	Jim McKennan
18-Oct-18	1.1.4	Added Service Managers and Development Staff to roles in RACIs and deleted “N Level” designation to Problem Analyst role	Jim McKennan

Approvals

Approver Name	Department/Role	Signature	Date
Reena Vaswani	Service Desk		

Table of Contents

Introduction

The purpose of this document is to provide a detailed view of the **CWDS** Problem Management (PM) process. The document consists of detailed process flows, with procedures and corresponding RACI (Responsible, Accountable, Consulted and Informed) matrix and procedure descriptions.

The procedure descriptions include title, purpose, policy statement, input, procedure or work instruction steps, output, audit/controls and metrics.

The content of this detailed design section is largely beyond the scope of the ITIL® Service Lifecycle books; however, this detailed design builds on the Problem Management High Level Design and is consistent with the best practice guidance of ITIL.

Purpose

The purpose of PM is to manage the lifecycle of all problems from first identification through further investigation, documentation and eventual removal. A problem is the unknown or underlying cause of one or more incidents. PM seeks to minimize the adverse impact of incidents and problems within OSI that are caused by underlying errors within the IT infrastructure (hardware, software, services, etc.). PM will also proactively prevent recurrence of incidents related to these errors. In order to achieve this, PM seeks to get to the root cause of incidents, document and communicate known errors and initiate actions to correct or improve the situation.

The key objectives of the PM process are to:

- Prevent problems and resulting incidents from happening
- Eliminate recurring incidents
- Minimize the impact of incidents that cannot be prevented

Scope

PM includes the activities required to diagnose the root cause of incidents and to determine the resolution to those problems. PM is also responsible for ensuring that the resolution is implemented through the appropriate control procedures, especially the Change Management and Release and Deployment Management processes.

PM will maintain information about problems and the appropriate workarounds and resolutions, so that OSI is able to reduce the number and impact of incidents over time. In this respect, PM has a strong interface with Knowledge Management (KM), and tools such as the Known Error Database (KEDB) will be used.

Although PM and Incident Management (IM) are separate processes, they are closely related and will typically use the same tools, categorization, and priority coding. This will ensure effective communication when dealing with related incidents and problems.

The PM process has both reactive and proactive aspects:

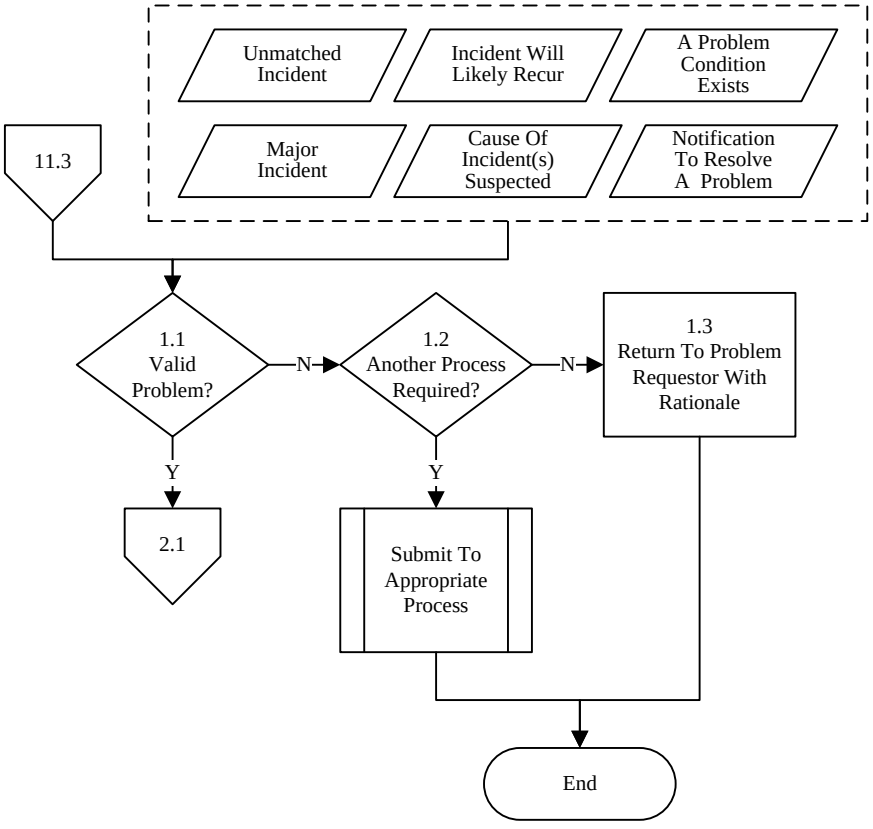
- Reactive PM is concerned with solving problems in response to one or more incidents
- Proactive PM is concerned with identifying and solving problems and known errors before further incidents related to them can occur again
- While reactive PM activities are performed in reaction to specific incident situations, proactive PM activities take place as ongoing activities. These are targeted to improve the overall availability and end user satisfaction with IT services. Examples of proactive PM activities might include conducting periodic scheduled reviews of incident records to find patterns and trends in reported symptoms that may

indicate the presence of underlying errors in the IT infrastructure (see McKennan Method described in Appendix)

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.

Activity 1.0 Problem Detection



RACI (authority) Matrix

The RACI (authority) matrix is a tool used to help understand which parties need to be involved in PM and their level of involvement.

Process Roles Activities Within Process Problem Detection	PM Process Owner Chief of Ops	PM Problem Manager Chief of Dev/Product Owners/Service Managers	Problem Practitioner Sr. Service Desk Analyst	PM Problem Analyst/Development Staff	Service Desk	Service Stakeholder
1.1 Valid Problem?	**A**	**R/C**	**R**			
1.2 Another Process Required?	**A**	**R/C**	**R**			
1.3 Return To Problem Requestor With Rationale	**A**	**R/C**	**R**			

Legend:

R = Responsible: Executes the task

A = Accountable: Accountable for final result

C = Consulted: Consulted about the task to provide additional information

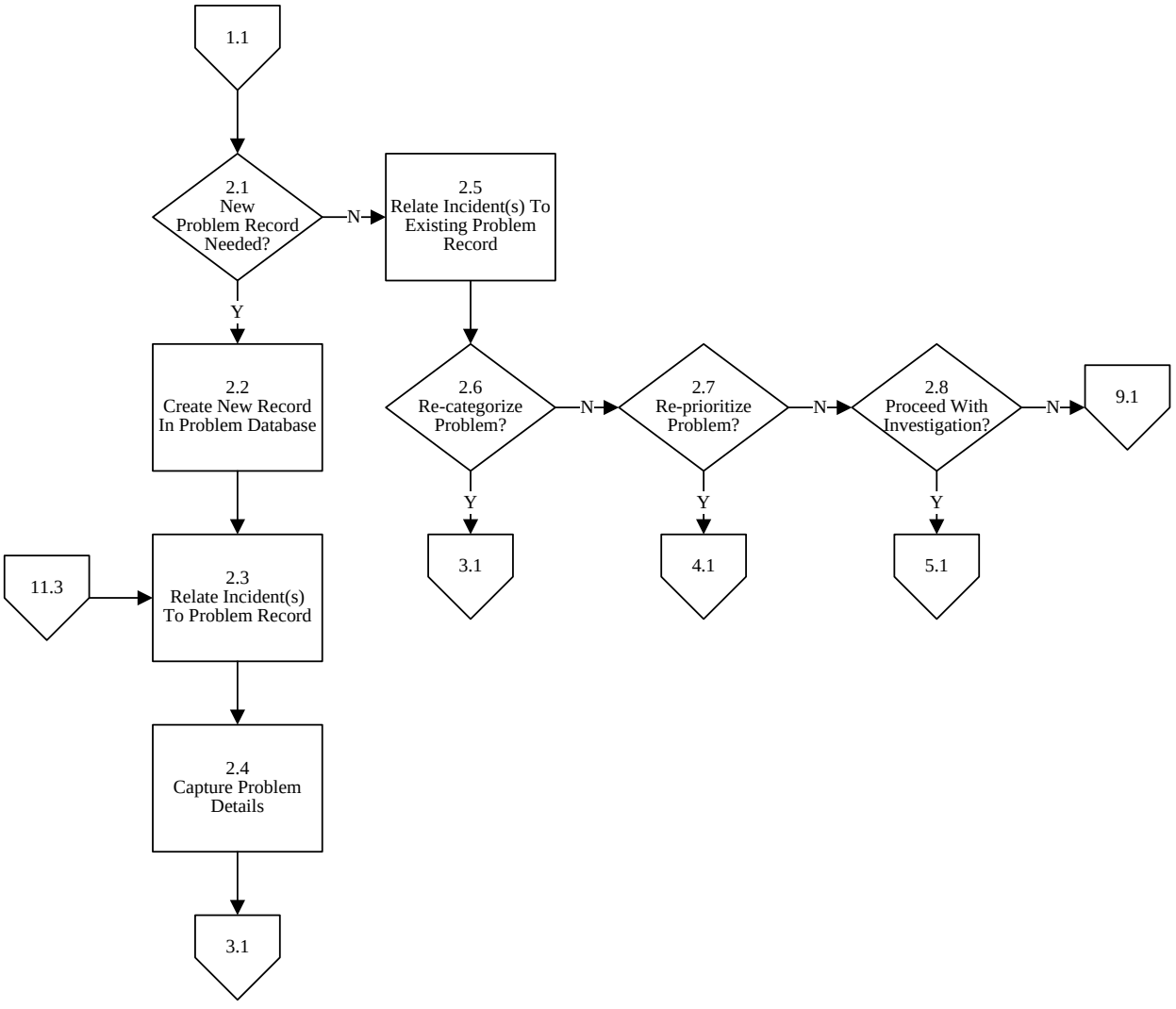
I = Informed: Needs to be kept up-to-date on activities/tasks

1.1	**Valid Problem?**
Purpose	To ensure that when a problem is reported that it's determined to be valid or not.
Policy Statement	When the problem is reported, it is the responsibility of the PM Problem Manager or Problem Practitioner to determine if it is a valid problem and warrants further attention.
Input	Information supporting problem request
Procedure or Work Instruction Steps	Assess the problem request against the criteria that defines a problem. The criteria is located in the Appendices of this document.
Output	Information requesting or denying a problem
Metric	• Number of valid problems • Number of invalid problems
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

1.2	**Another Process Required?**
Purpose	To ensure that any problem request found not to be accepted as a problem is assessed against other processes to determine if they are required.
Policy Statement	When a problem request is determined not to be a problem, it is the responsibility of the PM Problem Manager or Problem Practitioner to determine if any other processes are required.
Input	Information from the problem request
Procedure or Work Instruction Steps	• Consider other processes to evaluate and assess the problem that is reported • If other processes are required, submit to them
Output	Submission to other process
Metric	Number of problem records submitted to other processes
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

1.3	**Return To Problem Requestor With Rationale**
Purpose	To inform the problem requestor that the request is not for a valid problem.
Policy Statement	Upon evaluation of the problem request, if it is not considered to be a valid problem, it is the responsibility of the PM Problem Manager or Problem Practitioner to notify and return the request to the problem requestor with a reason.
Input	Problem request
Procedure or Work Instruction Steps	• Notify the problem requestor of the decision • Return the request to the problem requestor
Output	Returned problem request
Metric	Number of problem requests returned to requestors
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

Activity 2.0 Problem Logging



RACI (authority) Matrix

The RACI (authority) matrix is a tool used to help understand which parties need to be involved in Problem Management and their level of involvement.

Process Roles Activities Within Process Problem Logging	PM Process Owner/ Chief of Ops	PM Problem Manager/ Chief of Dev/Product Owners/Service Managers	Problem Practitioner/ Sr. Service Desk Analyst	PM Problem Analyst/Development Staff	Service Desk	Service Stakeholder
2.1 New Problem Record Needed?	**A**		**R**			
2.2 Create New Record In Problem Database	**A**		**R**			**I**
2.3 Relate Incident(s) To Problem Record	**A**		**R**		**I**	
2.4 Capture Problem Details	**A**		**R**		**I**	
2.5 Relate Incident(s) To Existing Problem Record	**A**		**R**		**I**	
2.6 Re-categorize Problem?	**A**		**R**			
2.7 Re-prioritize Problem?	**A**		**R**		**I**	**I**
2.8 Proceed With Investigation?	**A**		**R**			**C**

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

2.1	New Problem Record Needed?
Purpose	To ensure that any problem that has been identified is defined as being new or otherwise.
Policy Statement	When determining if a problem is new, it is the responsibility of the Problem Practitioner to identify if there are current or similar problems open or resolved.
Input	Problem record
Procedure or Work Instruction Steps	• Search ServiceNow to determine if the problem exists or is new • Update the problem record
Output	Updated problem record
Metric	Number of problems identified as new
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

2.2	Create New Record In Problem Database
Purpose	To ensure that any problem identified as new is recorded in the problem database.
Policy Statement	When creating a new record, it is the responsibility of the Problem Practitioner to ensure that all the necessary information is completed.
Input	Problem record
Procedure or Work Instruction Steps	Information to include: • Problem description • User information • Current status
Output	New problem record
Metric	Number of new problem records generated
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

2.3	**Relate Incident(s) To Problem Record**
Purpose	To ensure that any associated incidents are linked to the problem record and any incident data required within the problem record is entered into it.
Policy Statement	When incidents related to the problem are found, it is the responsibility of the Problem Practitioner to relate the incidents to the problem record. This is done by linking the incident records, updating the problem record with the associated incident data or a combination of both.
Input	• Problem record • Incident record(s) • Incident data
Procedure or Work Instruction Steps	Update the problem record with any related incident records and/or incident data
Output	Updated problem record
Metric	Number of problem records with related incident records.
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

2.4	**Capture Problem Details**
Purpose	To ensure that the details are captured when a problem has been identified.
Policy Statement	When a problem has been determined via reactive or proactive means, it is the responsibility of the Problem Practitioner to capture the problem details.
Input	Information supporting problem
Procedure or Work Instruction Steps	• Problem that has been identified based on criteria defined by IT • Analyze trends • Response to multiple incidents or a single major incident • Complete a problem record
Output	Problem record
Metric	Number of problem records made
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

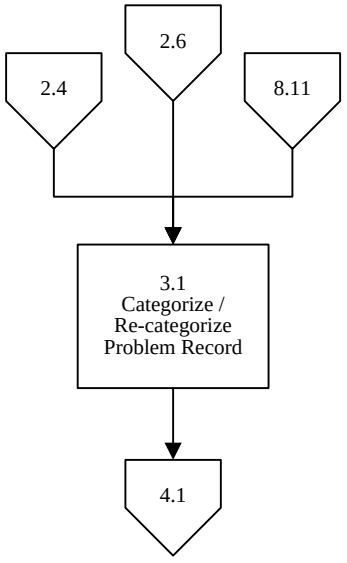
2.5	**Relate Incident(s) To Existing Problem Record**
Purpose	To ensure that if there is an existing problem that the related incident gets associated to it.
Policy Statement	When an existing problem is found, it is the responsibility of the Problem Practitioner to link the existing problem to the current incident(s) in question.
Input	• Problem record • Incident record(s)
Procedure or Work Instruction Steps	• Associate any problem with the existing incident(s) • Update the problem record
Output	Updated problem record
Metric	Number of incidents linked to the existing problem
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

2.6	**Re-categorize Problem?**
Purpose	To determine if a problem record should be re-categorized.
Policy Statement	When a problem is updated, it is the responsibility of the Problem Practitioner to determine if the problem record should be re-categorized.
Input	Categorized problem record
Procedure or Work Instruction Steps	• Determine how to categorize the problem so that it can be assigned to the correct resource • Update the problem record
Output	Decision to re-categorize problem records
Metric	Number of re-categorized problem records
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

2.7	**Re-prioritize Problem?**
Purpose	To determine if a problem record should be reprioritized.
Policy Statement	When an existing problem is discovered, it is the responsibility of the Problem Practitioner to ensure that the priority of the problem is re-evaluated.
Input	Problem record
Procedure or Work Instruction Steps	• Re-evaluate the problem and change the priority if required • Update the problem record
Output	Updated problem record
Metric	Number of problems that have been reprioritized
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

2.8	**Proceed With Investigation?**
Purpose	To determine whether it is important to continue with root cause analysis at this time.
Policy Statement	When a new incident is related to an existing problem, it is the responsibility of the PM Problem Manager or Problem Practitioner to determine if problem analysis should continue at this time.
Input	• Incident record • Problem record
Procedure or Work Instruction Steps	• Gather all the data associated with the problem • Determine if the required resources are available • Determine if there are viable business reasons to continue • Update the problem record
Output	• Updated problem records • Decision to proceed or stop
Metric	Number or percentage of problems that do not proceed beyond the problem logging step
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

Activity 3.0 Problem Categorization



RACI (authority) Matrix

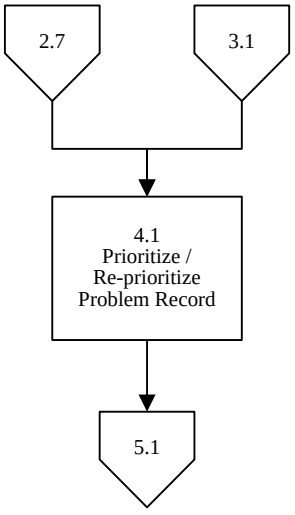
The RACI (authority) matrix is a tool used to help understand which parties need to be involved in Problem Management and their level of involvement.

Process Roles Activities Within Process Problem Categorization	PM Process Owner/ Chief of Ops	PM Problem Manager Chief of Dev/Product Owners/Service Managers	Problem Practitioner/Sr. Service Desk Analyst	PM Problem Analyst/Development Staff	Service Desk	Service Stakeholder
3.1 Categorize/Re-categorize Problem Record	**A**	**R/C**	**R**			

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

3.1	**Categorize/Re-categorize Problem Record**
Purpose	To ensure that all problem records are accurately categorized.
Policy Statement	When a problem is recorded, it is the responsibility of the PM Problem Manager or Problem Practitioner to ensure that it is categorized.
Input	Problem record
Procedure or Work Instruction Steps	• As defined, categorize the problem in order that the problem can be assigned to the correct resource • Update the problem record NOTE: The problem will most likely have the same category as the incident(s) it is associated with.
Output	Categorized problem record
Metric	Number of correctly categorized problem records
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

Activity 4.0 Problem Prioritization



RACI (authority) Matrix

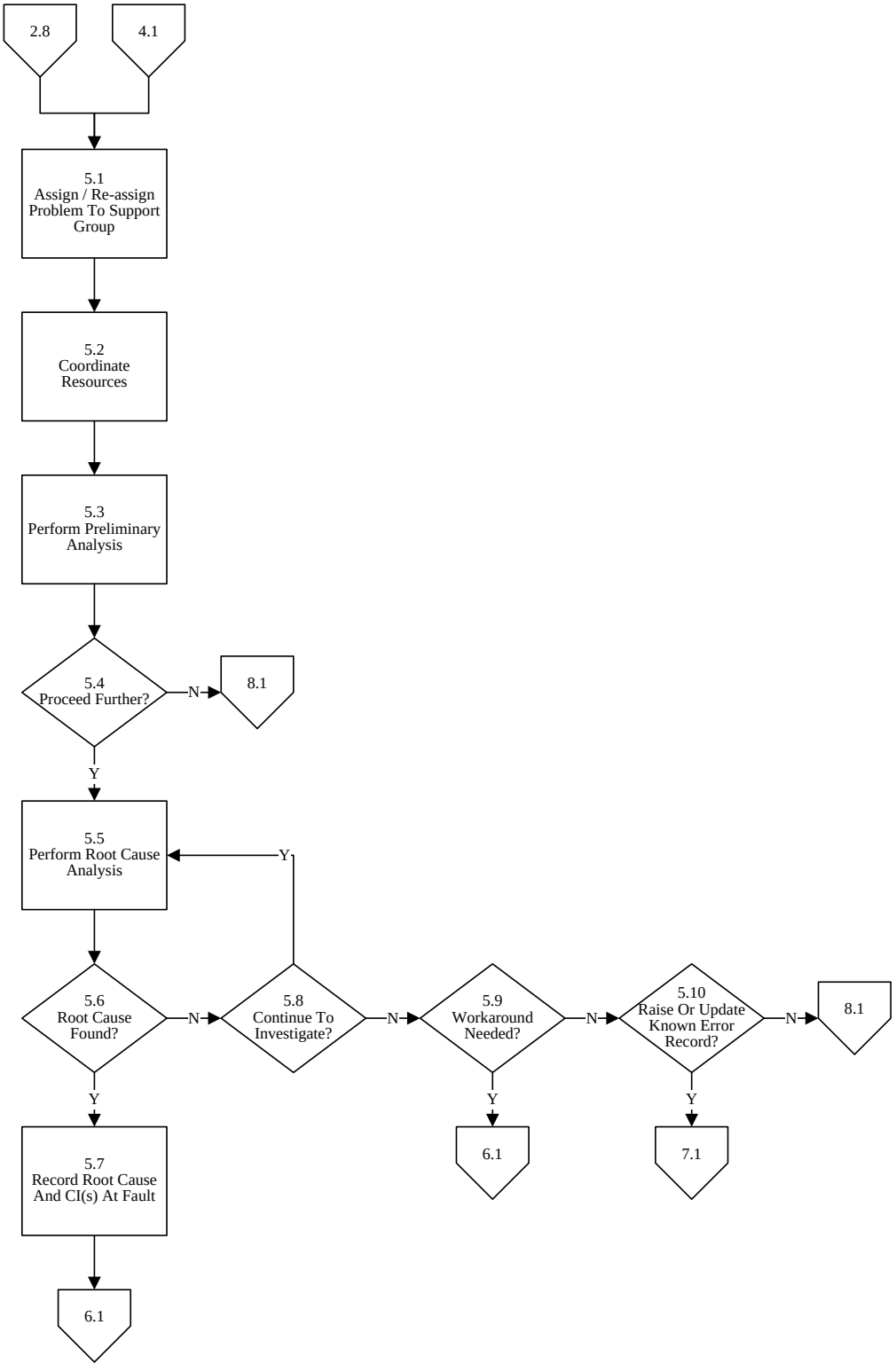
The RACI (authority) matrix is a tool used to help understand which parties need to be involved in Problem Management and their level of involvement.

Process Roles Activities Within Process Problem Prioritization	PM Process Owner/ Chief of Ops	PM Problem Manager Chief of Dev/Product Owners/Service Managers	Problem Practitioner/Sr. Service Desk Analyst	PM Problem Analyst/Development Staff	Service Desk	Service Stakeholder
4.1 Prioritize/Re-prioritize Problem Record	**A**	**R/C**	**R**		**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

4.1	**Prioritize/Re-prioritize Problem Record**
Purpose	To ensure that all problem records are accurately prioritized.
Policy Statement	When a problem is recorded, it is the responsibility of the PM Problem Manager or Problem Practitioner to ensure that it is prioritized.
Input	Problem record
Procedure or Work Instruction Steps	• Assess the problem record based on impact (number of users affected) and urgency (the immediacy of the issue relative to the business) • Define the priority based on the priority model • Update the problem record
Output	Prioritized problem record
Metric	Number of correctly prioritized problem records
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

Activity 5.0 Problem Investigation & Diagnosis



RACI (authority) Matrix

The RACI (authority) matrix is a tool used to help understand which parties need to be involved in Problem Management and their level of involvement.

Process Roles Activities Within Process Problem Investigation and Diagnosis	PM Process Owner Chief of Ops	PM Problem Manager/Chief of Dev/Product Owners/Service Managers	Problem Practitioner/Sr. Service Desk Analyst	PM Problem Analyst/Development Staff	Service Desk	Service Stakeholder
5.1 Assign/Re-assign Problem To Support Group	**A**	**R/C**	**R**			
5.2 Coordinate Resources	**A**	**R**	**R**			
5.3 Perform Preliminary Analysis	**A**			**R**		
5.4 Proceed Further?	**A**	**R**	**I**	**C/I**		**C**
5.5 Perform Root Cause Analysis	**A**			**R**		**C**
5.6 Root Cause Found?	**A**	**R/C**	**I**	**R**		
5.7 Record Root Cause And CI(s) At Fault	**A**	**I**	**I**	**R**	**I**	
5.8 Continue To Investigate?	**A**	**R**	**I**	**R**	**C**	**C**
5.9 Workaround Needed?	**A**		**I**	**R**		
5.10 Raise Or Update Known Error Record?	**A**	**I**	**R**	**R**	**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

5.1	**Assign/Re-assign Problem To Support Group**
Purpose	To ensure that once a problem has been identified that it is assigned to the correct support group.
Policy Statement	When a problem has been identified, it is the responsibility of the PM Problem Manager or Problem Practitioner to assign it to the support group as defined by the problem data.
Input	Problem record
Procedure or Work Instruction Steps	• Select the appropriate support group and assign the problem to them • Update the problem record
Output	Updated problem record
Metric	Number or percentage of problem records correctly assigned to support groups
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

5.2	**Coordinate Resources**
Purpose	To ensure that all resources assigned to the problem are coordinated.
Policy Statement	When a problem has been assigned, it is the responsibility of the PM Problem Manager or Problem Practitioner to ensure that all the resources are coordinated as efficiently as possible given the priority of the problem against other activities.
Input	Problem record
Procedure or Work Instruction Steps	• Assess the problem • Manage the resources according to the needs of the problem • Coordinate the resources in undertaking a resolution to the problem • Update the problem record
Output	Updated problem record
Metric	Number of problems with appropriate resources assigned
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

5.3	**Perform Preliminary Analysis**
Purpose	To conduct a preliminary analysis of the problem to assess what information has been compiled up to this point.
Policy Statement	When a preliminary analysis is done, it is the responsibility of the Problem Analyst or Problem Practitioner to ensure that all the information pertinent to the necessary groups is available and up-to-date.
Input	Problem record
Procedure or Work Instruction Steps	• Assess the information available and consult with any groups as necessary • Update the problem record
Output	Updated problem record
Metric	Number or percentage of problem records with up-to-date and accurate information to use in preliminary analysis.
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

5.4	**Proceed Further?**
Purpose	To determine after doing the preliminary analysis whether it is practical to continue to do root cause analysis.
Policy Statement	When the preliminary analysis has been achieved, it is the responsibility of the PM Problem Manager to determine the continuation to root cause analysis.
Input	• Preliminary analysis • Problem record
Procedure or Work Instruction Steps	• Determine the ability to reproduce the failure conditions • Gather all the data associated with the problem • Determine if the required resources are available • Determine if there are viable business reasons to continue • Update the problem record
Output	• Updated problem record • Decision to proceed or not
Metric	Number or percentage of problems that do not proceed beyond the preliminary analysis step
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

5.5	**Perform Root Cause Analysis**
Purpose	To ensure that the problem undergoes root cause analysis.
Policy Statement	When proceeding with the problem, it is the responsibility of the Problem Analyst to begin root cause analysis.
Input	Problem record
Procedure or Work Instruction Steps	• Determine the root cause of the problem by utilizing problem analysis techniques in order to get to a permanent solution (see Appendix D for problem analysis techniques) • Fill out Root Cause Analysis template document with details of the analysis (See Appendix F for RCA template) • Update problem record with results
Output	• Updated problem record • Completed RCA report document • Potential root cause
Metric	• Number of problems with a root cause identified • Number of completed RCA reports
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

5.6	**Root Cause Found?**
Purpose	To determine if the root cause has been found.
Policy Statement	When the root cause analysis has been undertaken, it is the responsibility of the PM Problem Manager/Problem Analyst to determine if the failing component has been positively identified and the root cause of the failure has been found.
Input	Problem record
Procedure or Work Instruction Steps	• Determine if the Configuration Item (CI) has been identified as the root cause • Update the problem record
Output	• Updated problem record • Possible root cause
Metric	Number of problems with an identified root cause
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

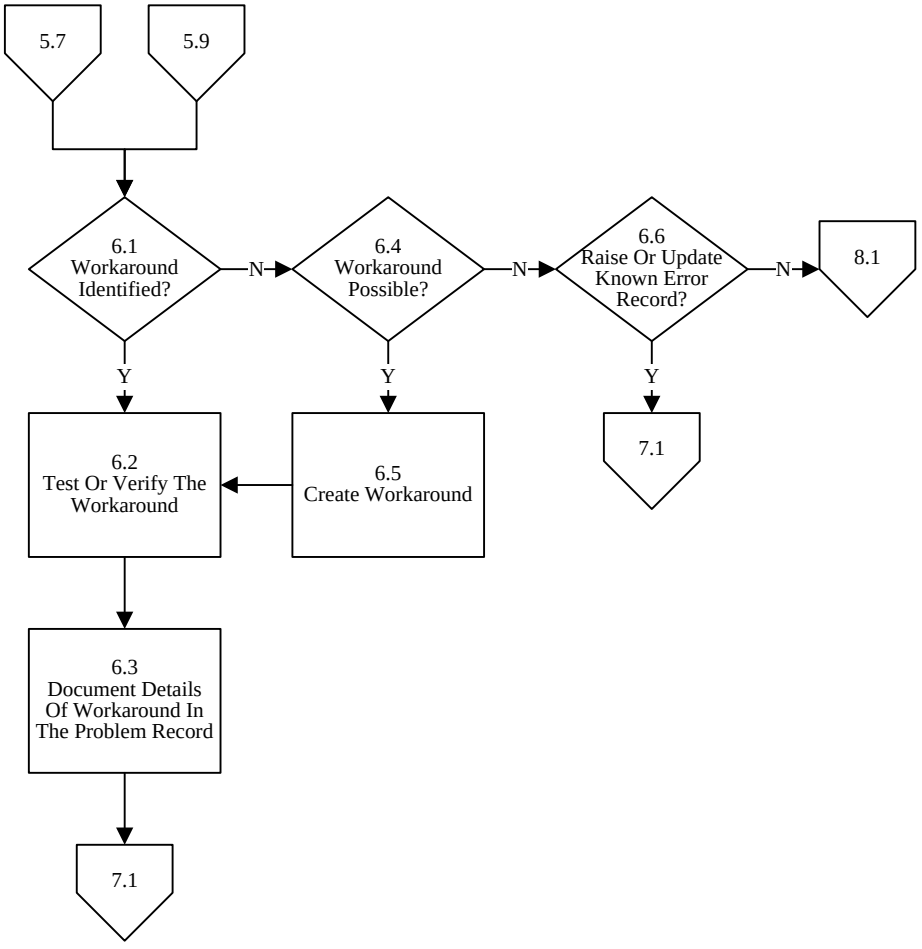
5.7	**Record root cause and CI(s) at fault**
Purpose	To document the root cause and CI(s) at fault once it has been found.
Policy Statement	When the root cause has been found and the CI(s) at fault identified, it is the responsibility of the Problem Analyst or Problem Practitioner to document that information in the problem record and RCA Form.
Input	• Root cause • CI(s) at fault • Problem record • RA Form
Procedure or Work Instruction Steps	• Update the problem record • Update the RCA Form
Output	Updated problem record
Metric	Number of problem records with an identified root cause and CI(s) at fault
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

5.8	**Continue To Investigate?**
Purpose	To determine if a problem should be investigated further.
Policy Statement	When determining if a problem should be investigated further, it is the responsibility of the PM Problem Manager and Problem Analyst to re-evaluate the problem as defined by specified criteria.
Input	Problem record
Procedure or Work Instruction Steps	• Evaluate the problem based on the following criteria: o The ability to reproduce the problem o The viability of the data collected o The resources available o The business reasons o Any new information that has become available o Any new Incidents as a result of problem in its current status • Update the problem record • Update the RCA Form
Output	• Updated problem record • Updated RCA Form
Metric	• Number of problems that have been re-investigated • Number of problems that have been resubmitted through the process
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

5.9	**Workaround Needed?**
Purpose	To determine if a workaround is needed.
Policy Statement	When root cause analysis is complete, it is the responsibility of the Problem Analyst to determine if a workaround needs to be implemented.
Input	Problem record
Procedure or Work Instruction Steps	• Determine if a workaround is needed • Compare the workaround against any other potential workarounds (if available) to determine if one should be utilized
Output	Updated problem record
Metric	Number of problems that have a work around identified
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

5.10	**Raise Or Update Known Error Record?**
Purpose	To determine if a known error needs to be recorded or updated in the known error database.
Policy Statement	When determining if a known error record needs to be created or updated, it is the responsibility of the PM Problem Manager/Problem Analyst to ensure that all the necessary information is completed.
Input	• Problem record • Problem details
Procedure or Work Instruction Steps	Determine if a known error record needs to be created or updated
Output	Decision to create or update a known error record
Metric	Number of known error records created
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

Activity 6.0 Workarounds



RACI (authority) Matrix

The RACI (authority) matrix is a tool used to help understand which parties need to be involved in Problem Management and their level of involvement.

Process Roles Activities Within Process Workarounds	PM Process Owner Chief of OPs	PM Problem Manager Chief of Dev/Product Owners, Service Managers	Problem Practitioner/Sr. Service Desk Analyst	PM Problem Analyst/Development Staff	Service Desk	Service Stakeholder
6.1 Workaround Identified?	**A**	**I**	**I**	**R**		
6.2 Test Or Verify The Workaround	**A**	**I**	**R**	**R**		
6.3 Document Details Of Workaround In The Problem Record	**A**		**R**	**R**		
6.4 Workaround Possible?	**A**			**R**	**C**	
6.5 Create Workaround	**A**	**I**	**I**	**R**		
6.6 Raise Or Update Known Error Record?	**A**		**R/I**	**R**	**C**	

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

6.1	**Workaround Identified?**
Purpose	To determine if there is a viable workaround available.
Policy Statement	When root cause analysis is complete, it is the responsibility of the Problem Analyst to determine if there is a viable workaround available to implement.
Input	Problem record
Procedure or Work Instruction Steps	• If a workaround has been found document the work around in the problem record • Compare the workaround against any other potential workarounds (if available) to determine which should be utilized • Update the problem record
Output	Updated problem record
Metric	Number of problems that have a workaround identified.
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

6.2	**Test Or Verify The Workaround**
Purpose	To test that any workarounds minimize the impact of the problem.
Policy Statement	When a workaround is found to be viable, it is the responsibility of the Problem Analyst or Problem Practitioner to test or verify its use and effectiveness.
Input	• Problem record • Test criteria
Procedure or Work Instruction Steps	• Review workaround(s) to identify they are valid for this problem • Test or verify that there is a minimal impact or is a low risk of using the existing workaround(s) in restoring service for incidents (risk includes business and technology) • Flag workarounds that no longer apply or are invalid so they can be updated or removed • Document results of test/verification in the problem record • Discuss the risks, benefits or impacts of potential workarounds with appropriate individuals or groups (business and technology) • Select best workaround • Record the workaround in the known error record
Output	• Updated problem record • Tested/verified workaround • Documented results of test
Metric	• Number of new workarounds • Number of removed workarounds • Number of updated workarounds
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

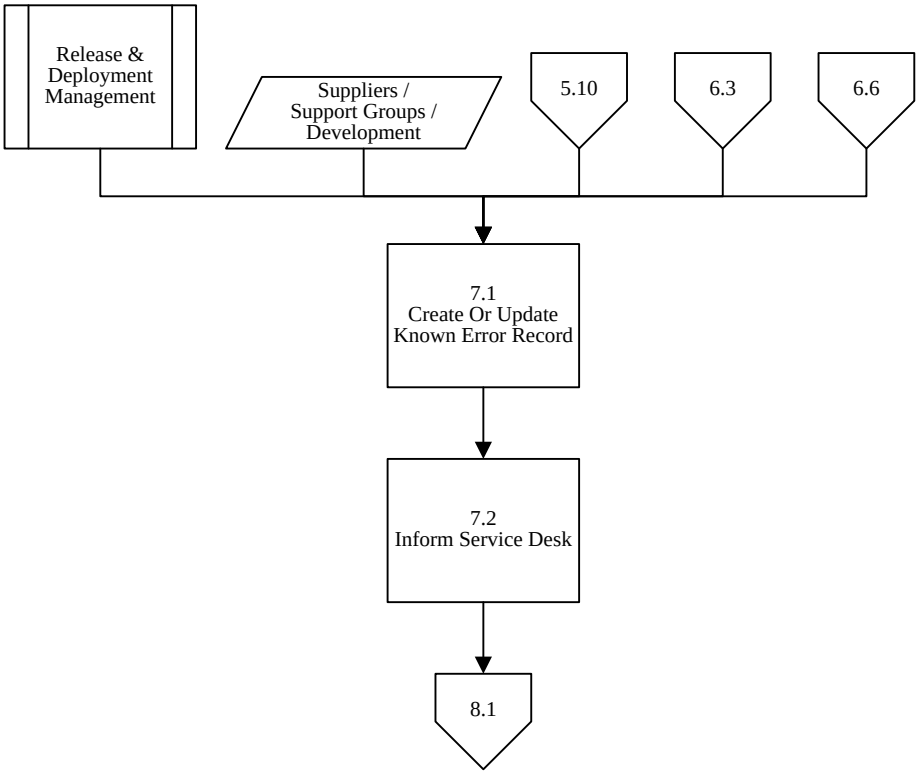
6.3	**Document Details Of Workaround In The Problem Record**
Purpose	To ensure that the workaround is recorded in the problem record.
Policy Statement	When the available workaround has been identified, it is the responsibility of the Problem Practitioner/Problem Analyst to ensure that the problem record is updated with the appropriate information.
Input	• Workaround • Problem record
Procedure or Work Instruction Steps	• Document workaround information in the problem record • Update priority, if necessary
Output	Updated problem record
Metric	• Number of new workarounds • Number of removed workarounds • Number of updated workarounds
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

6.4	**Workaround Possible?**
Purpose	To determine if a new workaround can be created.
Policy Statement	When a workaround has not been identified, it is the responsibility of the Problem Analyst or Problem Practitioner to determine if a new workaround can be created.
Input	• Existing workaround • Problem record • Known error record
Procedure or Work Instruction Steps	• Determine if a new workaround can be created, based on: o Is the required expertise available? o What is the cost? o What is the priority to the business? o Is there time available?
Output	• Decision • Updated problem record
Metric	• Number of times decision is made not to create workaround • Number of times decision is made to create workaround
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

6.5	Create Workaround
Purpose	To ensure that new workarounds are available to provide more time to investigate the problem and devise a permanent solution.
Policy Statement	When a new workaround is required, it is the responsibility of the Problem Analyst to ensure that one is created and available.
Input	• Problem record • Approved workaround
Procedure or Work Instruction Steps	• Identify a workaround to allow restoration of service by Incident Management process, if available • Create workaround • In the process of creating the workaround document all recommended instructions and procedures in the problem record • Initiate the Change Management process, if appropriate • Update the problem record
Output	• Updated problem record • New workaround documented in the problem record • Change record, if appropriate
Metric	• Number of times Change Management was invoked to create a workaround • Number of new workarounds created by Problem Management as opposed to those coming from Incident Management
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

6.6	Raise Or Update Known Error Record?
Purpose	To determine if a known error needs to be recorded or updated in the known error database.
Policy Statement	When determining if a known error record needs to be created or updated, it is the responsibility of the Problem Analyst or Problem Practitioner to ensure that all the necessary information is completed.
Input	• Problem record • Problem details
Procedure or Work Instruction Steps	Determine if a known error record needs to be created or updated
Output	Decision to create or update a known error record
Metric	Number of new or updated known error records
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

Activity 7.0 Raise Known Error Record



RACI (authority) Matrix

The RACI (authority) matrix is a tool used to help understand which parties need to be involved in Problem Management and their level of involvement.

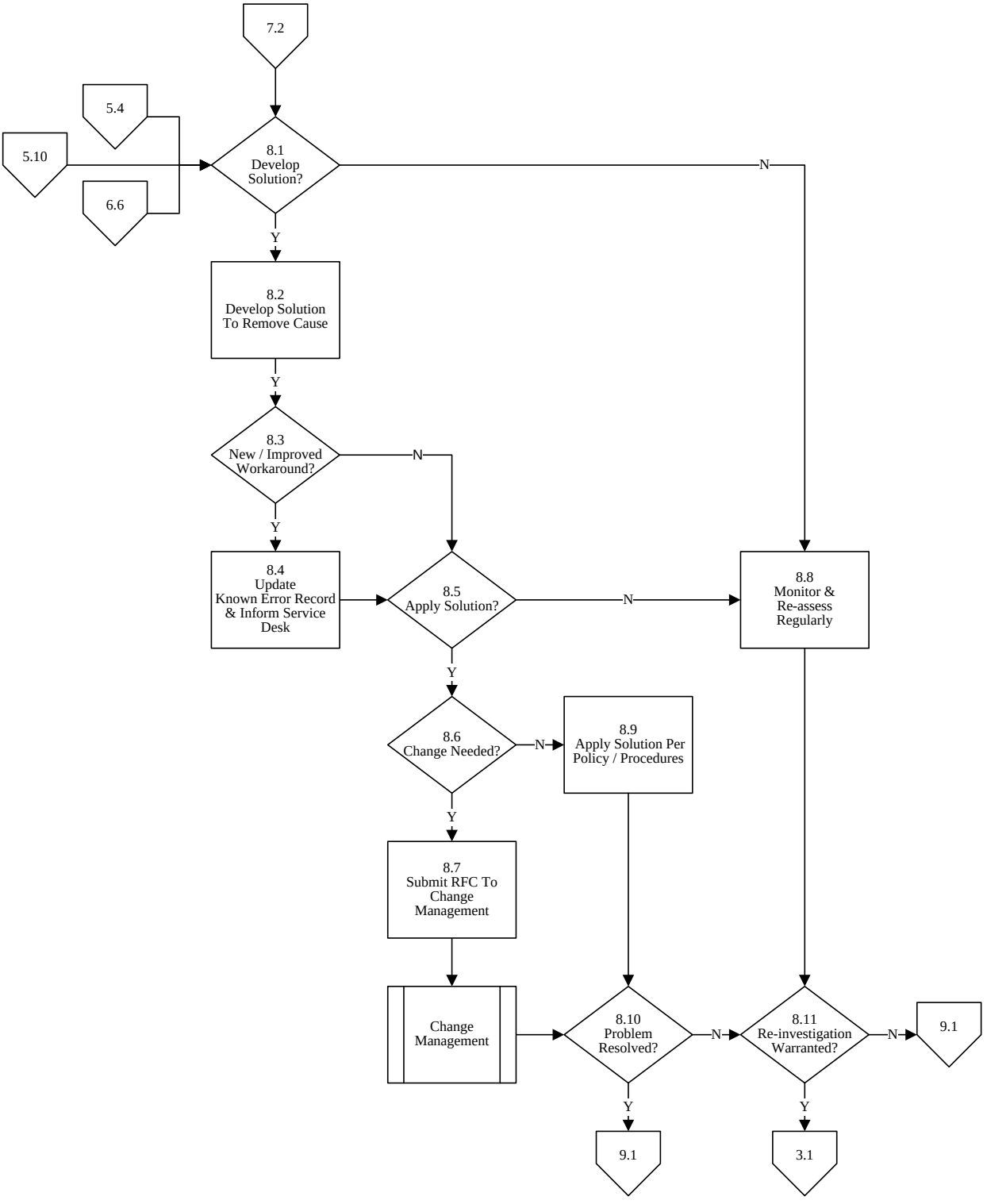
Process Roles Activities Within Process Raise Known Error	PM Process Owner Chief of Ops	PM Problem Manager Chief of Dev/Product Owners/Service Managers	Problem Practitioner/Sr. Service Desk Analyst	PM Problem Analyst/Development Staff	Service Desk	Service Stakeholder
7.1 Create Or Update Known Error Record	**A**	**C/I**	**R**	**R**		
7.2 Inform Service Desk	**A**		**R**	**R**	**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

7.1	**Create Or Update Known Error Record**
Purpose	To ensure that any known error is recorded in the known error database.
Policy Statement	When creating a new known error record, it is the responsibility of the Problem Analyst or Problem Practitioner to ensure that all the necessary information is completed.
Input	• Problem record • Problem details
Procedure or Work Instruction Steps	Create known error record including the following information: • Links to any related problem records and/or information from the problem record • Current status
Output	• Updated problem record • Known error record
Metric	• Number and percentage of known errors recorded in KEDB • Number and percentage of known error records were not linked to problem record and/or did not contain the pertinent information from the problem record it is associated with
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

7.2	**Inform Service Desk**
Purpose	To ensure that the Service Desk is informed of the known error record in the known error database.
Policy Statement	When the known error record has been created or updated, it is the responsibility of the Problem Analyst or Problem Practitioner to ensure that there is communication with the Service Desk.
Input	• Known error record • Known error database
Procedure or Work Instruction Steps	Inform the Service Desk that the known error record is available in the known error database
Output	Communication to Service Desk
Metric	• Number of new or updated known error records • Number or percentage of those that were communicated to the Service Desk
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

Activity 8.0 Problem Resolution



RACI (authority) Matrix

The RACI (authority) matrix is a tool used to help understand which parties need to be involved in Problem Management and their level of involvement.

Process Roles Activities Within Process Problem Resolution	PM Process Owner Chief of Ops	PM Problem Manager Chief of Ops/Product Owners/Service Managers	Problem Practitioner/Sr. Service Desk Analyst	PM Problem Analyst/Development Staff	Service Desk	Service Stakeholder
8.1 Develop Solution?	**A**	**R**	**I**	**R**		
8.2 Develop Solution To Remove Cause	**A**		**I**	**R**		
8.3 New/Improved Workaround?	**A**		**I**	**R**	**C**	
8.4 Update Known Error Record & Inform Service Desk	**A**		**R**	**R**	**I**	
8.5 Apply Solution?	**A**	**C/I**	**I**	**R**		
8.6 Change Needed?	**A**	**R**	**I**	**R**		
8.7 Submit RFC To Change Management	**A**	**R**	**I**			
8.8 Monitor & Re-assess Regularly	**A**	**C/I**	**R**			
8.9 Apply Solution Per Policy/Procedures	**A**		**I**	**R**		
8.10 Problem Resolved?	**A**	**R**	**I**	**R/C**		**C**
8.11 Re-investigation Warranted?	**A**	**R**	**I**	**R/C**		**C**

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

8.1	**Develop Solution?**
Purpose	To determine if a solution should be developed to remove the problem.
Policy Statement	When the resources have been assigned, it is the responsibility of the PM Problem Manager or Problem Analyst to determine if work should be done to find an adequate solution to the problem.
Input	• Problem record • Known error record
Procedure or Work Instruction Steps	• Consult other groups as necessary • Make decision to develop solution • If Yes, go to 8.2 • If No, go to 8.8
Output	• Decision to develop known error solution • Updated known error record • Updated problem record
Metric	• Number of decisions to develop known error solution • Number of updated known error records with new known error solution • Number of updated problem records with new known error solution
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

8.2	**Develop Solution To Remove Cause**
Purpose	To ensure a solution has been found to remove the problem.
Policy Statement	When the resources have been assigned, it is the responsibility of the Problem Analyst to work on finding an adequate solution to the problem.
Input	• Known error record • Problem record • Testing procedures
Procedure or Work Instruction Steps	• Acknowledge the assignment by updating the record status • Assess the information already gathered • Investigate, diagnose and test • Consult other groups as necessary • Update the known error record
Output	Updated known error record
Metric	Number of known error records updated with a resolution
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

8.3	New / Improved Workaround?
Purpose	To determine if a new and/or improved workaround has been identified while finding a solution.
Policy Statement	When the solution has been identified, it is the responsibility of the Problem Analyst to determine if a new and/or improved workaround has been identified and can be implemented.
Input	• Known error record • Problem record
Procedure or Work Instruction Steps	• The assigned group will document all the relevant information of the workaround in the known error record • Evaluate and approve the new workaround in comparison to existing workarounds in the known error database • If Yes go to 8.4 • If No, go to 8.5
Output	• Updated known error record • Updated problem record • Possible workaround
Metric	Number of viable workarounds found
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

8.4	Update Known Error Record & Inform Service Desk
Purpose	To ensure that the Service Desk is informed of any workarounds and the known error database has been updated.
Policy Statement	When the workaround has been identified, it is the responsibility of the Problem Analyst or Problem Practitioner to ensure that there is communication with the Service Desk and the known error database has been updated.
Input	• Known error record • Known error database
Procedure or Work Instruction Steps	• Update the known error database with the workaround information • Inform the Service Desk that the workaround has been identified and is ready for implementation • Update the known error record
Output	• Updated known error record • Updated known error database
Metric	• Number of new or updated known error records • Number or percentage of records that were communicated to the Service Desk
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

8.5	**Apply solution?**
Purpose	To determine if a solution to the problem should be applied.
Policy Statement	When there is a solution to be implemented to remove the problem, it is the responsibility of the Problem Analyst to determine if it will be applied.
Input	• Known error record • Problem record
Procedure or Work Instruction Steps	• Review the policies and procedures applicable to the solution • Make decision about applying the solution • If Yes, go to 8.6 • If No, go to 8.8
Output	Decision to apply solution
Metric	Number of decisions to apply solution
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

8.6	**Change Needed?**
Purpose	To ensure that once the solution has been accepted, it will be determined whether Change Management is required.
Policy Statement	When the solution has been accepted, it is the responsibility of the PM Problem Manager or Problem Analyst to determine if Change Management is required and if the change is necessary.
Input	• Known error record • Accepted solution • Change Management process and procedures
Procedure or Work Instruction Steps	• Determine if changes are required • If Yes, go to 8.7 • If No, go to 8.9 • Update the known error record
Output	• Decision of change needed • Updated known error record
Metric	Number of decisions to submit RFCs to Change Management
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

8.7	**Submit RFC To Change Management**
Purpose	To ensure that any changes which are required as defined are submitted via Request For Change (RFC) to Change Management.
Policy Statement	When changes are required, it is the responsibility of the PM Problem Manager/Problem Analyst to submit an RFC to Change Management.
Input	• Known error record • Accepted solution • Change Management process and procedures
Procedure or Work Instruction Steps	• The assigned group prepares and submits the RFC. (The RFC must include the reference number of the known error record/problem record) • The Change Management group must respond well within the target resolution time. This includes allotting time for the assigned group to make the necessary revisions, and for the solution to be implemented and tested • If not, the assigned group implements the workaround or solution • Update the known error record • Update the problem record
Output	• Updated known error record • Updated problem record
Metric	Number of RFCs submitted to Change Management
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

8.8	**Monitor & Re-assess Regularly**
Purpose	To ensure the problem is monitored and reported on regularly.
Policy Statement	When the status of the known error record has been updated to 'monitoring', it is the responsibility of the Problem Analyst or Problem Practitioner to ensure it is regularly monitored and reported.
Input	• Problem record • Known error record
Procedure or Work Instruction Steps	• Revisit the known error record regularly, based on the potential for re-occurrence (weekly, at minimum) • Report on the conditions that warranted its placement in monitoring (e.g. timing, resources, technology, etc.) • Update known error record • Update problem record
Output	• Updated known error record • Updated problem record
Metric	• Number of known error and problem records where PM Manager and/or Problem Analyst are Watchers • Number of "watched" records that were updated showing a status was reported to the user
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

8.9	**Apply Solution Per Policy / Procedures**
Purpose	To ensure that policies and procedures are followed when applying the solution.
Policy Statement	When the solution is implemented, it is the responsibility of the Problem Analyst to ensure that the policies and procedures are followed as outlined.
Input	• Known error record • Problem record
Procedure or Work Instruction Steps	• Review the policies and procedures applicable to the solution • Follow the policies and procedures when applying the solution • Update the known error record • Update the problem record
Output	• Updated known error record • Updated problem record
Metric	• Number of implemented solutions that followed the policies and procedures • Number of implemented solutions that did not follow the policies and procedures
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

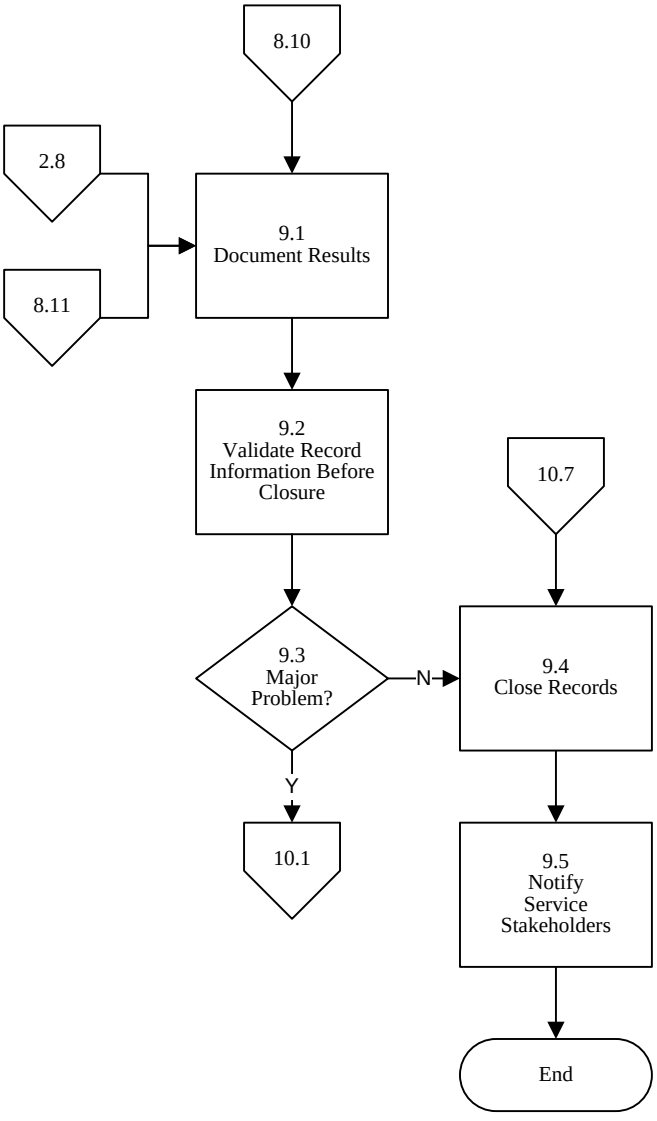
8.10	**Problem Resolved?**
Purpose	To verify that the problem has been resolved.
Policy Statement	When the solution has been applied, it is the responsibility of the PM Problem Manager/Problem Analyst to determine if the solution has resolved the problem.
Input	• Problem record • Known error record
Procedure or Work Instruction Steps	• Test the affected CI in a test environment and in production • Consult with other groups as required • If problem has not been resolved, update the problem record status • If Yes, go to 9.1 • If No, go to 8.11 • Update the known error record • Update the problem record
Output	• Updated known error record • Updated problem record
Metric	• Number of solutions that resolved the problem • Number of solutions that did not resolve the problem • Number or known error and problem records not updated with resolution status
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

8.11	**Re-investigation Warranted?**
Purpose	To determine if a problem should be re-investigated.
Policy Statement	When a solution has been found unacceptable, it is the responsibility of the PM Problem Manager/Problem Analyst to determine if re-investigation is warranted.
Input	• Known error record • Problem record

Procedure or Work Instruction Steps	• The following sample criteria are re-evaluated:
	  o Reproducibility of the failure conditions
	  o Feasibility of sufficient data collection (e.g. error log, information from user)
	  o Resource availability
	  o Business reasons
	• New conditions are also evaluated:
	  o Has new information (external to production support) become available?
	  o Has the number of associated incidents increased the priority?
	  o If the problem needs to be re-investigated, update the known error record status
	• If not, decide if the known error record can be retired, based on the following sample criteria:
	  o The problem may be outside the scope of Incident, Problem or Change Management
	  o The problem investigation may be terminated at the request of the Problem Management Process Manager
	• If Yes, go to 3.1
	• If No, go to 9.1
	• Update the known error record
	• Update the problem record

Output	• Updated known error record • Updated problem record
Metric	Number of problems that have been re-investigated
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

Activity 9.0 Problem Closure



RACI (authority) Matrix

The RACI (authority) matrix is a tool used to help understand which parties need to be involved in Problem Management and their level of involvement.

Process Roles Activities Within Process Problem Closure	PM Process Owner Chief of Ops	PM Problem Manager Chief of Dev/Product Owners/Service Managers	Problem Practitioner/Sr. Service Desk Analyst	PM Problem Analyst/Development Staff	Service Desk	Service Stakeholder
9.1 Document Results	**A**	**R/C**	**R**	**R**		
9.2 Validate Record Information Before Closure	**A**	**C/I**	**R**	**R**		
9.3 Major Problem?	**A**	**R**	**I**	**C**		
9.4 Close Records	**A**	**R/C**	**R**	**R/C**	**I**	**C**
9.5 Notify Service Stakeholders	**A**	**R**	**R**	**R/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

9.1	Document Results
Purpose	To ensure the known error record and problem record contain valid reasons for closure.
Policy Statement	When the known error record and problem record have been closed, it is the responsibility of the PM Problem Manager, Problem Practitioner or Problem Analyst to provide the information required for closure.
Input	• Problem record • Known error record
Procedure or Work Instruction Steps	• Document the reason for closing the problem record and/or known error record. Some reasons may include the following: o The problem investigation may be terminated at the request of the PM Process Manager or requestor if no viable and/or acceptable solution is found o The problem may have been successfully resolved • Update the problem record and/or known error record
Output	• Updated problem record • Updated known error record
Metric	Number of closed problem or known error records without documented results
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

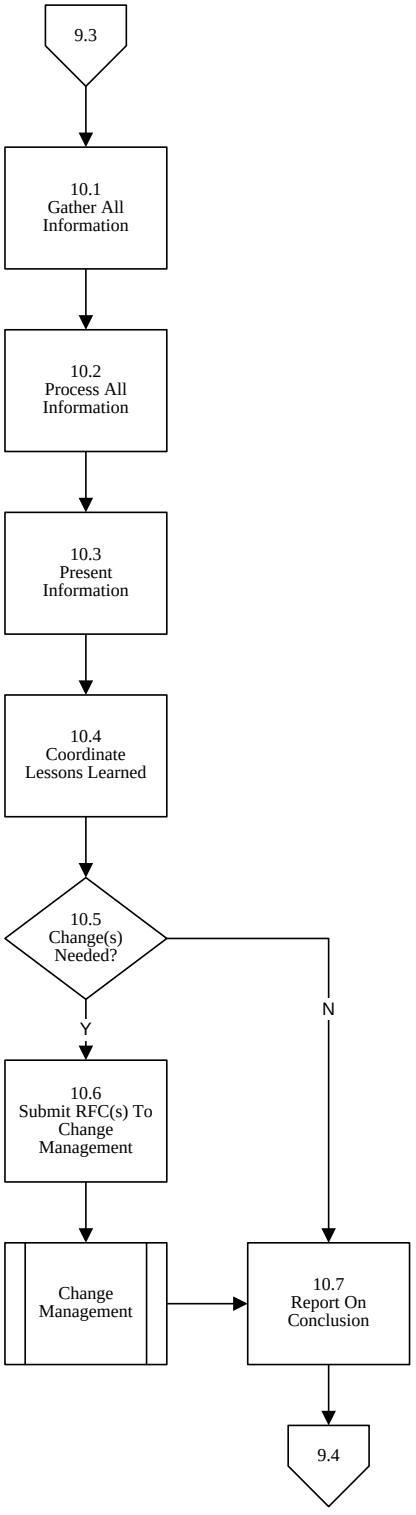
9.2	Validate Record Information Before Closure
Purpose	To ensure that the known error record and problem record information have been validated before being closed.
Policy Statement	When the known error record and problem record are to be closed, it is the responsibility of the Problem Analyst or Problem Practitioner to validate all the necessary information prior to closing the known error record and problem record.
Input	Known error record
Procedure or Work Instruction Steps	• Validate all the known error record information before closing • Validate all the problem record information before closing
Output	• Validated known error information • Validated problem record information
Metric	• Number of invalid known error records found before closure • Number of invalid problem records found before closure
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

9.3	**Major Problem?**
Purpose	To ensure that after a major problem has occurred a decision is made whether to hold a formal major problem review.
Policy Statement	When a major problem has occurred, it is the responsibility of the PM Problem Manager to determine if it warrants a major problem review.
Input	• Known error record • Related problem(s) • Related incident(s) • Information from vendors • Information from Event Management
Procedure or Work Instruction Steps	• Determine if a problem exists and if it is a major problem as defined by the major problem criteria • If Yes, go to 10.1 • If No, go to 9.4 • Update the problem record
Output	• Updated known error record • Updated problem record
Metric	Number of problems undergoing a major problem review
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

9.4	**Close Records**
Purpose	To close known error record and problem record
Policy Statement	When the resolution has been implemented and the Configuration Item (CI) has been recovered to normal working state, it is the responsibility of the PM Problem Manager, Problem Practitioner or Problem Analyst to close the known error record and the problem record.
Input	• Known error record • Problem record
Procedure or Work Instruction Steps	• Update the known error record with the required information to close it • Close the known error record • Update the problem record with the required information to close it • Close the problem record
Output	• Closed known error record • Closed related problem record(s)
Metric	Number of closed problem records
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

9.5	**Notify Service Stakeholders**
Purpose	To ensure that all service stakeholders are notified of the problem status.
Policy Statement	When the problem record and known error record are being closed, it is the responsibility of the PM Problem Manager, Problem Practitioner or Problem Analyst to notify the Service Desk, Incident Management and other stakeholders with the required information.
Input	• Problem record • Known error record • Related incident record(s)
Procedure or Work Instruction Steps	• Communicate information regarding the closed known error record and problem record • Update the known error record • Update the problem record
Output	• Updated known error record • Updated problem record • Communication to stakeholders
Metric	Number of communications to the Service Desk, Incident Management and other stakeholders
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

Activity 10.0 Major Problem Review



RACI (authority) Matrix

The RACI (authority) matrix is a tool used to help understand which parties need to be involved in Problem Management and their level of involvement.

Process Roles Activities Within Process Major Problem Review	PM Process Owner Chief of Ops	PM Problem Manager Chief of Dev/Product Owners/Service Managers	Problem Practitioner/Sr. Service Desk Analyst	PM Problem Analyst/Development Staff	Service Desk	Service Stakeholder
10.1 Gather All Information	**A**	**R**	**R**	**R**		
10.2 Process All Information	**A**	**R**	**I**	**C**		**C**
10.3 Present Information	**A**	**R**	**I**	**I**		**I**
10.4 Coordinate Lessons Learned	**A**	**C**	**R**	**C/I**	**I**	**I**
10.5 Change(s) Needed?	**A**	**R**	**I**	**C**		
10.6 Submit RFC(s) To Change Management	**A**	**R**	**I**	**R/C**	**I**	
10.7 Report On Conclusion	**A**	**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

10.1	Gather All Information
Purpose	To ensure all the information has been compiled for the major problem review.
Policy Statement	When a major problem review has been declared, it is the responsibility of the PM Problem Manager, Problem Analyst or Problem Practitioner to gather all the necessary information for analysis.
Input	• Known error record • Related problem(s) • Related incident(s) • Information from vendors • Information from Event Management
Procedure or Work Instruction Steps	• Gather all the information as it relates to the problem • Update the known error record
Output	• Compiled problem information • Updated known error record
Metric	Number of updated known error records and other pertinent information for discussion at major problem review
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

10.2	Process all information
Purpose	To ensure that all the information that has been gathered is processed.
Policy Statement	When all the information has been gathered, it is the responsibility of the PM Problem Manager to process all the information.
Input	Compiled known error/problem information.
Procedure or Work Instruction Steps	• Analyze all the information gathered • Update the known error record • Update the problem record
Output	• Updated known error records • Updated problem records
Metric	Number of updated known error and problem records
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

10.3	**Present Information**
Purpose	To ensure that the information that has been processed is presented to the appropriate individual/groups.
Policy Statement	When the information on the major problem has been analyzed, it is the responsibility of the PM Problem Manager to present the information to the appropriate individuals/groups.
Input	Compiled and processed known error/problem information.
Procedure or Work Instruction Steps	The presentation should include the following: • Things done right • Things done wrong • What could be done better in the future • How to prevent recurrence • Any vendor responsibilities and associated follow-up actions required • Update known error record
Output	• Presentation of information • Updated known error record
Metric	Number of reports with major problem review information presented to stakeholders
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

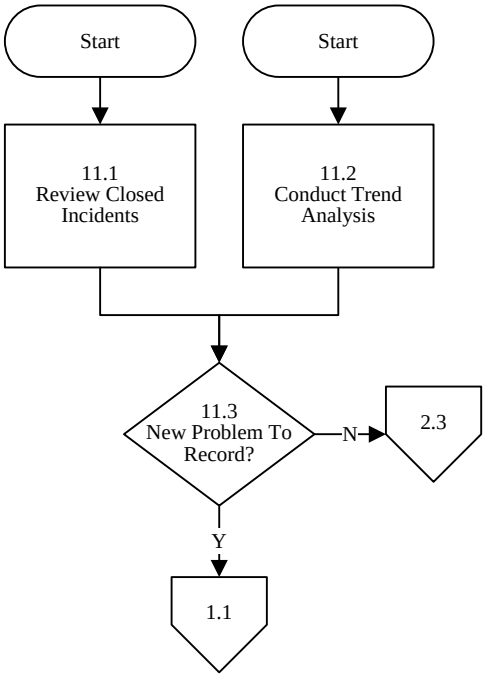
10.4	**Coordinate Lessons Learned**
Purpose	To ensure that any lessons learned are consolidated and documented.
Policy Statement	When the major problem review has occurred, it is the responsibility of the Problem Practitioner to ensure that the lessons learned are documented in procedures, work instructions, diagnostic scripts or known error records.
Input	Compiled and processed known error/problem information
Procedure or Work Instruction Steps	• Consolidated lessons learned and document accordingly • Update the known error record
Output	• Documented lessons learned • Updated known error record
Metric	Number of procedures, work instructions diagnostic scripts and known error records updated with lessons learned from major problem review
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

10.5	Change(s) needed?
Purpose	To determine if, based on any actions as an outcome from lessons learned, changes are required.
Policy Statement	When the lessons learned have actions associated with them, it is the responsibility of the PM Problem Manager to determine if changes are required to be implemented to prevent future major incidents from occurring.
Input	• Information from lessons learned • Known error and related problem record(s)
Procedure or Work Instruction Steps	• Determine if changes are required • If Yes, go to 10.6 • If No, go to 10.7 • Update the known error record
Output	• Decision of change needed • Updated known error record
Metric	Number of changes required as a result of a major problem review
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

10.6	Submit RFC(s) To Change Management
Purpose	To ensure that any changes that are required as defined are submitted via RFCs to Change Management.
Policy Statement	When changes are required following the major problem review, it is the responsibility of the PM Problem Manager or Problem Analyst to submit an RFC to Change Management to prevent future recurrence from happening.
Input	• Lessons learned documentation • Required changes
Procedure or Work Instruction Steps	• Submit RFCs for any changes required as a result of the major problem review • Update the known error record
Output	Submitted RFCs
Metric	Number of RFCs submitted to Change Management
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

10.7	Report On Conclusion
Purpose	To ensure all decisions and changes made from a major problem review are reported accordingly.
Policy Statement	When the major problem review has occurred, it is the responsibility of the PM Problem Manager to report on the conclusion including any changes made to policies, procedures, work instructions, etc.
Input	• All information complied, processed and presented for the major problem review • Decisions from major problem review • Changes made as a result of a major problem review
Procedure or Work Instruction Steps	• Account for the major problem review and lessons learned and report any conclusions as necessary • Update the known error record
Output	• Final reports • Updated known error record
Metric	• Number of final reports with conclusions • Number of updated known error records with conclusions
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

Activity 11.0 Proactive Problem Management



RACI (authority) Matrix

The RACI (authority) matrix is a tool used to help understand which parties need to be involved in Problem Management and their level of involvement.

Process Roles Activities Within Process Proactive Problem Management	PM Process Owner Chief of Ops	PM Problem Manager Chief of Dev/Product Owners/Service Managers	Problem Practitioner/Sr .Service Desk Analyst	PM Problem Analyst/Development Staff	Service Desk	Service Stakeholder
11.1 Review Closed Incidents	**A**	**R**	**R**	**R/C**	**C**	**C**
11.2 Conduct Trend Analysis	**A**	**R**	**R**	**R/C**	**I**	**I**
11.3 New Problem To Record?	**A**	**C**	**R**	**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

11.1	Review Closed Incidents
Purpose	To ensure that closed incidents are reviewed in order to detect new problems or match incidents to existing problems that have not been resolved.
Policy Statement	When closed incidents are being reviewed as part of proactive Problem Management, it is the responsibility of the PM Problem Manager, Problem Analyst or Problem Practitioner to match them to existing problems that have not been resolved.
Input	• Closed incident records • Major incidents • Incidents resolved through a workaround or temporary fix not matched to a problem • Suspected problems (as identified by stakeholders) • Problem candidates • Problem records • Known error records • Problem definition criteria
Procedure or Work Instruction Steps	• Attempt to match open incidents with known error records and/or problem records • Review Incident Management reports, identifying groups of incidents that aren't currently matched to known error records or problem records • Attempt to match all closed incidents not resolved through a permanent fix, temporary fix, or workaround to existing problems • Analyze why Problem Management was able to perform the match and Incident Management was unable to do so • Report on findings as required
Output	• Identified unmatched incidents • Updated incident matching procedures • Incident matching criteria used
Metric	Number of unmatched incidents
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

11.2	Conduct Trend Analysis
Purpose	To ensure the trends as defined in Problem Management are analyzed for potential problems.
Policy Statement	When reports are being generated, it is the responsibility of the PM Problem Manager, Problem Analyst or Problem Practitioner to analyze any trends that are occurring that may lead to problems or incidents.
Input	• Trending information • Trend analysis procedures • Incident records • Problem records • Known error records • Patterns of business activity data • Service level trends
Procedure or Work Instruction Steps	• Compile all the reports that are currently being generated, e.g. capacity reports, availability reports, service level management reports, etc. • Conduct trend analysis using incident data to determine patterns of recurring incidents • Utilize available system monitoring and other tools to perform trend analysis • Look for related symptoms, causes, changes, facts, knowledge articles or other statements that would help determine a relationship between occurrences of incidents • Report on findings as required
Output	• Trend analysis report • Patterns of incident reports • Related incident reports • Most common incident reports
Metric	• Number of problems found as a result of trending • Number of times trend analysis successfully identifies a problem • Number of recurring incidents
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

11.3	New Problem To Record?
Purpose	To determine if a problem record should be created based on the outcomes of trend analysis, incident matching and proactive Problem Management activities.
Policy Statement	When determining if a problem record should be created, it is the responsibility of the Problem Analyst or Problem Practitioner to identify if there are current or similar problems open or resolved.
Input	• Trending information • Unmatched incidents • Closed incident records • Major incidents • Incidents resolved through a workaround or temporary fix not matched to a problem • Suspected problems (as identified by stakeholders) • Problem candidates • Problem records • Known error records • Problem definition criteria
Procedure or Work Instruction Steps	• Go through the problem database to determine if the problem exists or is new • Decide if a new problem record needs to be recorded or if unmatched incidents and trends can be matched to existing problem records • If Yes, go to 1.1 • If No, go to 2.3 NOTE: For additional assistance with proactive PM, see white paper on “The McKennan Method” in Appendix A
Output	Decision about creating a new problem record
Metric	Number of Problems identified as new
Control	See OSI Governance and Control in Appendix
Revision History	<Date, description, author>

Appendix A - The McKennan Method (for Proactive Problem Management)

The McKennan Method was developed in the mid-1990's by Jim McKennan, an IT Service Management Consultant. It is a methodical approach to conducting proactive Problem Management (PM) activities. It is a "three-pronged" approach: investigating the most frequent issues, end users who contact the Service Desk most frequently and departments/locations that contact the Service Desk most frequently.

It begins by proactively examining incident records as a part of data trending analysis. Three reports should be generated. One report will list in descending order the most frequent issues (incidents) reported. A second report will be sorted in descending order by the end users who most frequently report issues to the Service Desk. The third report will be sorted in descending order by the departments or locations that most frequently report issues to the Service Desk.

1. **Most frequent issues (incidents) reported:**

The analysis of the issues report will help determine what SME would be required for Root Cause Analysis (RCA) of those issues. Top Issues should be determined first (this is in preparation for a gathering of minds to complete the Proactive Problem Management process).

Using a "pain value analysis" select the top 5 to 10 issues causing the most pain to the supported business. Based on the category of the problem, choose a SME to be accountable for each RCA investigation. The SME will be given the authority to "deputize" others as appropriate to assist in the RCA investigation. They will also be given to authority to engage Change Management if fixing the issue/problem requires changing a Configuration Item (CI). Once each investigation is complete and the solution applied, each SME will report their results. The SMEs could investigate as many of the 5 to 10 top issues as they are able based on resource and time constraints.

That way the PM Process Manager will know whom to invite to the "kick-off" meeting, which is the gathering of SMEs who will then join the PM Process Manager to facilitate the correct path forward.

Kick-off Meeting

The kick-off meeting is designed as a mechanism to determine how to assign the work to the appropriate SMEs. The meeting begins by setting out the goals and objectives of this proactive PM initiative. Each person or group that will be assigned RCA duties will be required to formally report the results of their assignments at subsequent meetings.

To begin RCA, the creation of baseline statistics for each issue, end-user and department/location is crucial. The SME should analyze the incident records to establish these baselines as they will be used for later comparison once the investigation results are established. Knowledge Articles (KAs) for most frequent issues will be created. Creating self-help KAs will enrich improved end-user productivity and prevent knowledge loss.

2. **End Users who most frequently contact the Service Desk**

From the reports select the names of the top 5 to 10 end users who contact the Service Desk by location. The Problem Analyst will review and analyze the incident records for specific end user(s). The Problem Analyst will thoroughly review all incidents reported by each individual on the report, so they have a complete understanding of all the issues each user has encountered.

While performing the analysis, the Problem Analyst should look for answers to several important questions:

- Is there a pattern or connection between the issues being reported?
- What do you think is the root cause of these issues?
- What steps did you take to reduce issues for this end-user?
- What other recommendations do you have?

One of the responsibilities of the PM Process Manager is to focus on Customer Satisfaction. They will also document ways to reduce or eliminate contacts for frequently called issues to the Service Desk. This may include training recommendations on how to perform certain tasks or how to use an application, showing the end-users any existing support documentation or how to use any self-help tools or KAs available. This not only will reduce contacts to the Service Desk for frequently called issues but will increase the productivity of the end user, which improves the "customer experience."

With the expertise of the PM Process Manager and more in-depth understanding of the end-user and the problem, the PM Process Manager should be able to reduce contacts to the Service Desk by each end user. Creating a form with the above questions for the Service Desk Analysts to ask during future contacts will help him or her when discussing the results of these contacts at the subsequent root cause team follow up meetings.

The reporting and discussion at the meetings allows sharing of ideas and opens up dialogue with other support teams who may have encountered similar issues and may have formulated better solutions. Track the Service Desk activity of those end users contacted to see if future contacts to the Service Desk by these end users is reduced.

3. Top Departments/Locations/Counties

Thirdly, make sure the Managers of the locations that contact the Service Desk most frequently become aware of the frequency (and reasons) that their employees contact the Service Desk. For example: if a number of users are calling about a certain module of an application, it is possible that those individuals could use more training in that module and that training could be offered. They may not have any idea how many calls from their department go to the Service Desk and might not realize how much lost productivity is represented by all the contacts. Solicit assistance from those Managers to partner with your root cause group by sharing with them your recommendations to reduce the frequency of contacts to the Service Desk. Getting some of those Managers to buy into your efforts may result in developing a better relationship with departments/locations that you support.

Appendix B - Problem Management Roles

Problem Management Process Owner

The Problem Management (PM) Process Owner is accountable for ensuring the Problem Management Process is ready for implementation. The PM Process Owner is also accountable for ensuring that Problem Management is performed according to the agreed and documented standard and meets the aims of the process, purpose and scope.

The PM Process Owner's responsibilities include:

- Defining PM Process strategy
- Assisting with PM Process design
- Ensuring that appropriate PM Process documentation is available and current
- Defining appropriate PM policies and standards to be employed throughout the process
- Periodically auditing the PM Process to ensure compliance to policy and standards
- Designing Problem models and workflows
- Periodically reviewing the PM Process strategy to ensure that it is appropriate and change strategy as required
- Communicating PM Process information or changes as appropriate to ensure awareness
- Providing PM Process resources to support activities required throughout the service lifecycle
- Ensuring that PM Process team members have the required knowledge and the required technical and business understanding to deliver the PM Process, and understand their role in the PM Process
- Reviewing opportunities for PM Process enhancements and for improving the efficiency and effectiveness of the PM Process
- Addressing issues with the operations of the PM Process
- Identifying improvement opportunities for inclusion in the Continual Service Improvement (CSI) register
- Working with the CSI Manager and PM Process Manager(s) to review and prioritize improvements in the CSI register
- Recommending improvements to the PM Process
- Sponsoring and managing any changes to the PM Process and its metrics
- Working with other Process Owners to ensure there is an integrated approach to the design and implementation of Problem Management, Incident Management, Event Management, Access Management and Request Fulfillment

Problem Management Process Manager

The PM Process Manager is accountable for the operational management of the PM Process. There may be multiple PM Process Managers, especially in larger organizations.

The PM Process Manager's responsibilities include:

- Working with the PM 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 and 'deputizing' Subject Matter Experts (SME) relevant to the type of problem to be investigated
- Managing resources assigned to the PM Process
- Working with Service Owners and other Process Managers to ensure the smooth running of services
- Monitoring and reporting on PM Process performance

- Planning and managing support for PM tools (such as ServiceNow)
- Coordinating interfaces between PM and other service management processes
- Liaising with all problem resolution groups to ensure swift resolution of problems within Service Level Agreement (SLA's) targets
- Ownership and maintenance of the Known Error Database (KEDB)
- Gatekeeper for the inclusion of all known errors and management of search algorithms
- Formal closure of all problem records
- Liaising with suppliers/contractors, etc. to ensure third parties fulfill their contractual obligations, especially with regard to resolving problems and providing problem-related information and data
- Driving the efficiency and effectiveness of the PM Process
- Monitoring the effectiveness of PM and making suggestions for improvement
- Managing the work of Problem support staff (1st and 2nd line)
- Managing Major Problems
- Following-up on tasks related to Major Problem Reviews
- Working with the CSI Manager and PM Process Owner to review and prioritize improvements in the CSI register
- Implementing improvements to the PM Process
- Developing and maintaining the PM processes and procedures

Problem Analyst

The Problem Analyst is responsible to perform actual root cause analysis and resolving Problems. Problem Analysts could include support resources who may work in many different areas, but will come together to undertake problem resolution activities under the coordination of the Problem Management Process Manager.

Problem Analyst responsibilities include:

- Reviewing Incident data to analyze assigned Problems
- Reviewing Problems for correct prioritization and classification
- Investigating Problems through root cause and resolution
- Coordinating actions of others as necessary to assist with analysis and resolution for Problems and known errors
- Submitting RFCs to Change Management to resolve Problems
- Monitoring progress on the resolution of known errors
- Carrying out one or more of the activities of the PM Process
- Understanding how their role contributes to the overall delivery of services and the creation of value for the business (from the PM Process Owner and/or PM Process Manager)
- Working with other stakeholders, such as their manager, co-workers, users and customers, to ensure that their contributions are effective
- Creating or updating PM records to show that activities have been carried out correctly
- Recording Problems
- Focusing on customer satisfaction
- Routing Problems to support specialists when needed
- Analyzing for correct prioritization, classification and providing initial support for Problems
- Providing ownership, monitoring and tracking of Problem
- Providing resolution and recovery of Problems
- Monitoring the status and progress towards resolution of assigned Problems

- Keeping users and the Service Desk informed about Problem progress
- Escalating Problems as necessary per established policies.

Problem Practitioner

The Problem Coordinator will assist the PM Process Owner and the PM Process Manager by executing the following tasks:

- Filtering Problem requests
- Making sure problem records are created
- Making sure that problem details are captured and problem records are related to incident records
- Ensuring incident details are added to problem records
- Prioritizing and categorizing problem records
- Creating or updating known error records
- Informing the Service Desk of new known errors or workarounds
- Monitoring problem investigation and diagnosis activities
- Monitoring progress on the resolution of known errors
- Ensuring RFCs are submitted to Change Management as needed
- Regularly monitoring RFCs to ensure they are progressing
- Validating information in problem records and known error records before closing
- Notifying stakeholders with results
- Gathering and processing information for use in Major Problem Reviews
- Participating in proactive Problem Management activities by reviewing closed incidents, conducting trend analysis and opening new problem records from those activities
- Understanding how their role contributes to the overall delivery of services and the creation of value for the business (from the PM Process Owner and/or PM Process Manager)
- Working with other stakeholders, such as their manager, co-workers, users and customers, to ensure that their contributions are effective
- Creating or updating PM records to show that activities have been carried out correctly

Appendix C - Problem Model Template

Problem models document a standard work flow, roles and responsibilities for handling a problem, ensuring that a repeatable and consistent set of actions are always undertaken for each problem type.

Problem Model	<Name of the problem model>
Category	*<Problem Category name>*
Summary	<Provide a purpose and high level description of this problem model.> Hint: Check policies for procedures in the Problem Management Detailed Design Document
Input	<Define any prerequisites needed (information, forms, policies, authorizations, etc.) for the problem to be handled>
Financial Requirements	<If applicable, indicate costs incurred by problem handling activities or if requesters are to be billed for them>
Procedure or Work Instruction Steps	<Describe the standard work steps and activities to handle the problem. Problem models should include the steps to be taken, chronological order of the steps, responsibilities (who does what), timescales or thresholds for completing actions and any escalation procedures> *1. Task 1* *a.Instruction 1* *b.Instruction 2* *c.Instruction (n)…* *2. Task 2* *a.Instruction 1* *b.Instruction 2* *c.Instruction (n)…>*
Output	<List the expected output(s) and/or outcome(s) the user/customer can expect to receive>
Flow Chart	<Provide a graphical flow of the tasks required to handle the problem>
Service Level Objective	<The agreed set of criteria for determining the priority based on business need>
Revision History	<Date, Description, Author>

Appendix D - Problem Analysis Techniques

In this Section, we have highlighted a few techniques that are used in PM when analyzing problems (getting to the root cause). These techniques can be used in combination or individually. They should make it easier and quicker to find the root cause of incidents and problems because of their methodical nature.

1. Chronological analysis

If we are confronted by a problem that is difficult to investigate, it may be confusing to understand exactly what has happened and when. Hence it is very helpful to document all the events that led up to the problem occurring and list them in chronological order. This will provide a timeline of the events. This also makes it possible to see what events may have been triggered by others, or to eliminate any possible causes that are not aligned with the order of the timeline of events.

2. Pain value analysis

Instead of just analyzing the number of incidents or problems of a particular type in a particular time period, a more in-depth analysis is done to determine exactly what level of pain has been caused to the customers by these incident and problems. A formula can be devised to calculate the pain level. Typically this might take into account:

- The number of people affected
- The duration of the downtime caused
- The cost to the customers (if this can be readily calculated or estimated)

By taking all of these factors into account, a much more focused and detailed picture of those incidents and problems that are causing the most pain can be determined. This is especially useful, if there are a number of problems to investigate and due to time constraints or resource constraints you are not able to do all the investigation in a timely manner. It is better to focus on the ones that are causing the most pain. You can also show your customers your list of problem investigations planned and ask them to help you prioritize them by simply asking, ‘which of these is causing you the most pain?’

3. Kepner and Tregoe

Charles Kepner and Benjamin Tregoe developed a useful method to analyze problems. They stated that problem analysis should be a systematic process of problem solving and should take maximum advantage of knowledge and experience. They outlined five phases for problem analysis:

1. Defining the problem
2. Describing the problem with regard to identity, location, time and size
3. Establishing possible causes
4. Testing the most probable cause(s)
5. Verifying the true cause

   Even in situations where only a limited amount of information is available, or time pressure is high, it is worthwhile adopting a structured approach to problem analysis to improve the chances of success. Here is a little more detail about the Kepner & Tregoe method:

Defining the problem: Because the investigation is based on the definition of the problem, this definition has to state precisely which deviations from the agreed service levels have occurred. In practice, problem definition is often a difficult task because of a complicated IT technical infrastructure and non-transparent agreements on service levels (or no agreements at all).

Describing the problem: The following aspects are used to describe the problem:

- **Identity** Which part does not function well? What is the problem?
- **Location** Where does the problem occur?
- **Time** When did the problem start to occur? How frequently has the problem occurred
- **Size** What is the size of the problem? How many parts are affected?

The current situation is determined by answers to these questions. The next step is to investigate which similar parts in a similar environment are functioning properly. This answers the question, 'what *could be* but *is not* showing the same problem.'

It is then possible to search effectively for relevant differences in both situations. Furthermore, past changes, especially recent ones, which could be the cause of these differences, can be identified.

Establishing possible causes: The list of differences and changes mentioned most likely hold the cause of the problem so possible causes can be extracted from this list.

Testing the most probable cause: Each possible cause needs to be assessed to determine whether it could be the cause of all the symptoms of the problem.

Verifying the true cause: The remaining possible causes have to be verified as being the source of the problem. This can only be done by proving this in one way or another, for example, by implementing a change or replacing a part. Address the possible causes that can be verified quickly and simply first.

4. Brainstorming

It can often be valuable to gather the relevant subject-matter experts and other stakeholders to 'brainstorm' the problem to capture ideas on what the potential cause may be and potential actions to resolve the problem. Be sure to documents all the discussions and ideas for later reference.

It should start with a facilitator, perhaps the Problem Management Process Owner or Problem Manager, with a flip chart and markers. The session begins with the facilitator stating the guidelines for the session. The main rule is that during the time when everyone is calling out ideas no one else is permitted to comment about the relative value of anyone's idea. When an idea is criticized it may shut down the person who was criticized so they will no longer contribute to the discussion and it may shut down others before they ever participate, thus losing valuable ideas.

The facilitator will jot down each idea and with initials of the person who contributed the idea. They will then leave some space below what was written for later use. Then the next idea is written in the same manner. Writing quickly is essential so that it doesn't slow down the flow of ideas. Every idea should be written no matter how good or bad the idea may seem.

This flow of ideas will continue until there are long pauses between ideas. At that point the facilitator will shift to the next phase of the session. They will go back to the first idea on the first page of the flip chart and ask the contributor to explain in more detail the essence of their idea. The clarification comments are then written on the extra space below the original entry. Now is the time for others to weigh in on the value of the idea. The ideas that are not considered relevant to the cause of the problem are lined out and the team moves on to the next idea. Once the exercise is completed there will usually only be a few of the ideas that are still relevant. This narrows down the possible causes to a more manageable number so further analysis can take place to hopefully, winnow the list to a single or several causes. Then closer scrutiny of the final list can be advanced by utilizing another method such as Kepner and Tregoe methodology.

5. **5-Whys**

This simple but effective method is helpful as a way to get to the root cause of a problem. It works by starting out with a description of what event took place and asking ‘why did this happen?’ The resulting answer is given, followed by another round of ‘why did this happen?’ Usually by the fifth iteration, a true root cause will have been found.

6. **Fault isolation**

This approach involves re-executing the transactions or events that led to a problem in a careful stepwise fashion, one Configuration Item (CI) at a time until the CI at fault is identified. The re-execution effort moves to the first CI encountered at the start of the transaction or event, which is then checked for correct operation. The effort then moves to the next CI in the chain of events, which in turn is checked, then the next CI and then the next until the fault is encountered. If the fault cannot be recreated, a variation of this technique can be tried that involves interrogating the healthy state of the CIs involved with the transaction or event. For example, if one CI is deemed to be at fault, all other CIs in the transaction or event path from source to destination are probed for health.

7. **Affinity mapping**

This technique can be used to organize large amounts of data (ideas, opinions, issues) into groupings based on common characteristics. It is typically performed in a brainstorming session with SMEs. Key concepts such as potential solutions are written on individual cards and stuck to a wall or whiteboard. The cards should be moved so that they are grouped by similar traits. A ‘header’ should be developed for each group for future identification. Each of the cards under the header should be examined for potential of a root cause that may underlie all of them.

8. **Hypothesis testing**

This method can be used to generate a list of possible root causes based on educated guessing and then determining whether each hypothesis is true or false. Educated guesses may relate to relationships between variables or potential root causes of a problem. Using information gathered from incidents and other operational information, a team is assembled to brainstorm a list of potential causes that may be underlying the incidents being studied. Each cause is then converted into testable statements or hypotheses and are assigned to one or more support staff. Further data should then be gathered as needed for each assigned statement and an appropriate analysis is performed to accept or reject each hypothesis.

9. **Technical observation post**

In some cases, problems may be linked to incidents that occur intermittently for unknown reasons. This approach consists of a prearranged gathering of technical support staff brought together to focus on a specific problem. Its purpose is to monitor events, real-time as they occur, with the specific aim of identifying the specific situation and possible causes for the problem. Video cameras may also be utilized for this method as well.

10. Ishikawa diagrams

Ishikawa diagrams, 'tree' diagram or 'fishbone' diagrams, can help in identifying where something may be going wrong or be improved. Such a diagram is typically the outcome of a brainstorming session where problem solvers can offer suggestions. The main goal is represented by the trunk or backbone of the diagram, and primary factors are represented as branches or fish bones. Secondary factors are then added and so on. Creating the diagram stimulates discussion and often leads to increased understanding of a complex problem.

After the brainstorming has ended the diagram must be interpreted. This could be done by ranking the top causes on experience and available data. Once the top causes are selected, each one will be investigated further according to its rank and priority, perhaps by using the Kepner & Tregoe method.

See below for examples of Ishikawa diagrams.

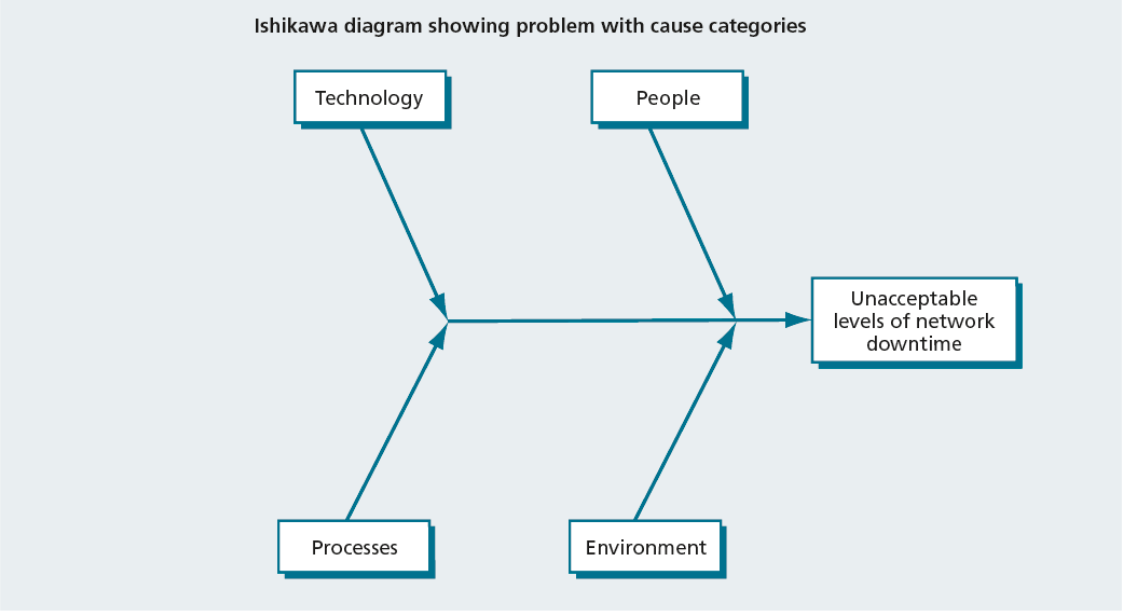


Figure D.1 Sample of starting an Ishikawa diagram

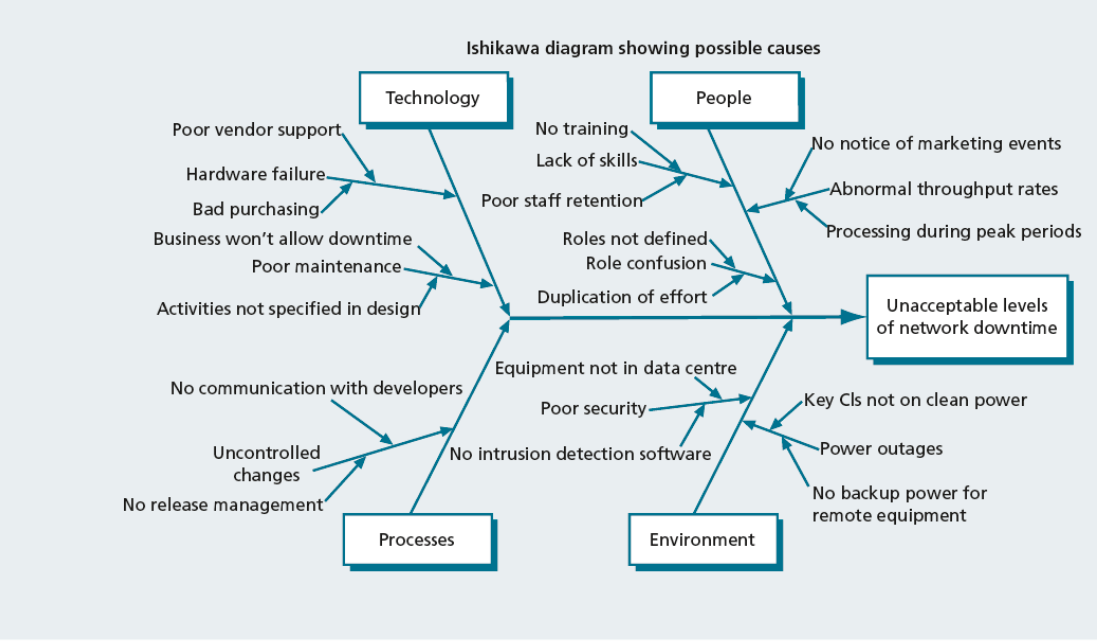


Figure D.2 Sample of a completed Ishikawa diagram

These diagrams are from the ITIL Service Operation v3 2011 edition.

Appendix E - 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.***

Appendix F - 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 behavior 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 licenses. 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 behavior 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 behavior. 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 G - Guidelines for invoking Problem Management

The rules for invoking Problem Management can vary and are at the discretion of OSI. The activities described would be executed by the OSI staff member that the incident is assigned to. *Some general situations where it may be desired to invoke Problem Management might include situations where:*

- Incident Management cannot match an incident to existing problems and known errors.
- Trend analysis of logged incidents reveals an underlying problem exists (from proactive Problem Management reviews)
- A major incident has occurred where Problem Management activities need to be undertaken to identify the root cause. (A major incident is the highest category of impact for an incident. A major incident results in significant disruption to the business. It is, therefore, an incident with the greatest impact and urgency. Special procedures, with shorter timescales and greater urgency for major incidents are outlined in the Incident Management ITIL Detailed Design plan. But if the cause of the incident needs to be investigated at the same time, then Problem Management would be involved as well. However, the Incident Manager must ensure that service restoration, by Incident Management, and underlying cause, by Problem Management are kept separate)
- Major incident reviews which are trying to prevent the recurrence of any major incident can provide identification of an underlying cause or underlying error. Problem management would likely participate in these reviews. When causes or errors are identified during these reviews, Problem Management would initiate the appropriate corrective action. If changing a Configuration Item is necessary to correct the underlying error, Problem Management would fill out a RFC and submit it to the Change Management process. Change Management would assess and evaluate the change, and if approved, would authorize Release and Deployment Management to build, test and deploy the release to correct the error.
- Other IT functions identify that a problem condition exists
- The Service Desk may have resolved an incident but has not determined a definitive cause and suspects that the incident is likely to recur
- Analysis of an incident by a support group which reveals that an underlying problem exists, or is likely to exist
- A notification from a (third-party) supplier that a problem exists and has to be resolved
- A single incident occurs that has Special Circumstances. (Special Circumstances are purposely not defined so that we can be flexible in its meaning so that Problem Management can be invoked whenever it is deemed necessary. It is then up to the Problem Management Process Owner to decide if a root cause investigation needs to be initiated)
- Multiple Incidents have occurred that may indicate they are all related to a single technical fault. (These are usually discovered through proactive Problem Management activities such as trending analysis of historical incident records).

Appendix H – Root Cause Analysis/Outage Report

Root Cause Analysis/Outage Report	
Incident Record Details: [Completed by PM Practitioner]	
Incident #:	
Problem #:	
Incident Date/Time:	
Business Impact Duration:	
RCA Completed By:	
Lead Problem Analyst(s):	
Target Resolution Date (Estimated date of Problem Closure)	
Date Completed:	
Problem Summary (What Happened?): [Completed by PM Practitioner]	
Business Impacted Summary: [Completed by PM Practitioner]	
Work Around (If Any): [Completed by PM Process Analyst]	
Known Error: [Completed by PM Process Analyst]	
Root Cause Summary: [Completed by PM Process Analyst]	
Troubleshooting: [Completed by PM Process Analyst]	
Remediation Plans: [Completed by PM Process Analyst]	
Additional Data (add any other data)	
Sign off by Signatures	
Steve Trimble (PM Process Owner): TBD (PM Process Manager):	