



**Government of Ontario IT Standard (GO-ITS)**

**GO-ITS Number 38**

**Enterprise Problem Management Process**

**Version 2.0**

**Status: Approved**

Prepared for the Information Technology Standards Council (ITSC) under the delegated authority of the Management Board of Cabinet

## Copyright & Disclaimer

---

Government of Ontario reserves the right to make changes in the information contained in this publication without prior notice. The reader should in all cases consult the Document History to determine whether any such changes have been made.

© 2009 Government of Ontario. All rights reserved.

Other product or brand names are trademarks or registered trademarks of their respective holders. This document contains proprietary information of Government of Ontario, disclosure or reproduction is prohibited without the prior express written permission from Government of Ontario.

## Template Info

---

Template Name	Template #	Template Version	Template Author	Template Completion Date
GO-ITS Template	09.03.26	2.0	Design: PMCoE Boilerplate: TAB/OCCTO	2009-03-26

## Document History (including ITSC and ARB approval dates)

---

Date	Summary
2009-05-12	Updated legacy Standard to replace Portable Guide focus, with enterprise requirements. Based upon ITIL V3
2009-07-08	Updated to reflect IT Standards Council (ITSC) feedback received by June 30, 2009
2009-07-20	Updated to reflect response to ITS feedback received July 14, 2009
2009-08-12	Updated to address ITS feedback received Aug 7, 2009
2009-08-19	Updated to address all ITSC feedback. Endorsed by IT Standards Council
2009-08-27	Approved by Architecture Review Board. Approved version number set to 2.0

## Standard Type

---

Process Standard (Service Management Process)
---

---

## Table of Contents

---

<b>1. FOREWORD</b>	<b>4</b>
<b>2. INTRODUCTION</b>	<b>5</b>
2.1. Background	5
2.2. Purpose	5
2.3. Value to the Business	6
2.4. Basic Concepts	6
2.5. Scope	8
2.6. Applicability Statements	9
2.6.1. Organization	9
2.6.2. Other Applicability	9
2.6.3. Requirements Levels	10
2.6.4. Compliance Requirements	10
<b>3. STANDARDS LIFECYCLE MANAGEMENT</b>	<b>11</b>
3.1. Contact Information	11
3.2. Recommended Versioning and/or Change Management	13
3.3. Publication Details	13
<b>4. TECHNICAL SPECIFICATION</b>	<b>14</b>
4.1. Process Principles	14
4.2. Process Roles and Responsibilities	19
4.2.1. Enterprise Problem Management Process Owner	19
4.2.2. Problem Manager	20
4.2.3. Service Owner	21
4.2.4. Problem Owner	22
4.2.5. Problem Analyst (PA's)	22
4.2.6. Partner Problem Management Liaison	22
4.3. Process Flow	23
4.3.1. Enterprise Problem Management Process Overview	23
4.3.2. Enterprise Problem Management Process Tasks	24
4.4. Linkages to Other Processes	27
4.5. Problem Management Process Quality Control (CSI)	28
4.6. Metrics	28
4.7. Standard Process Parameters	29
<b>5. RELATED STANDARDS</b>	<b>30</b>
5.1. Impacts to Existing Standards	30
5.2. Impacts to Existing Environment	30
<b>6. APPENDICES</b>	<b>31</b>
6.1. Normative References	31
6.2. Informative References	31
6.3. Differentiation: Process, Procedure, Work Instruction	32
<b>7. GLOSSARY</b>	<b>33</b>

# 1. Foreword

---

Government of Ontario Information Technology Standards (GO-ITS) are the official publications on the guidelines, preferred practices, standards and technical reports adopted by the Information Technology Standards Council (ITSC) under delegated authority of the Management Board of Cabinet (MBC).

These publications support the responsibilities of the Ministry of Government Services (MGS) for coordinating standardization of Information & Information Technology (I&IT) in the Government of Ontario.

Publications that set new or revised standards provide enterprise architecture guidance, policy guidance and administrative information for their implementation. In particular, GO-ITS describe where the application of a standard is mandatory and specify any qualifications governing the implementation of standards.

## 2. Introduction

---

### 2.1. Background

An OPS Standard for Problem Management currently exists (GO ITS 38). It was developed several years ago as a high level portable guide, intended as a starting point for local implementations of Problem Management across the OPS. In its current state, it does not provide an enterprise perspective of the process requirement

This process standard was initially part of a portable set of Information Technology Service Management (ITSM) process documentation intended for use as a reference across the OPS. A key objective identified during an OPS ITSM Planning workshop held in December 2003 was to “Define Standard Portable Elements for All ITSM Processes”. As a result, guides were designed to be portable across all IT Clusters as well as any parties in the end-to-end supply chain and to only include the necessary process components that were recommended to be common across the OPS.

A further requirement for an all-encompassing OPS Problem Management standard was predicated by the positioning of all infrastructure service and support within Infrastructure Technology Services (ITS), a new organization within the OPS mandated in 2005 to deliver all infrastructure technology services to the OPS. ITS was created in 2006 to achieve this goal. Establishment of this goal required an update of the requirements for the GO-ITS Standard for Problem Management based on the situation described above.

During February 2009, a series of outages to a major citizen-facing website prompted I & IT Executive Management to re-prioritize the OPS Enterprise ITSM Program (OEIP) Roadmap so that a simplified enterprise Problem Management capability could be developed and made operational by the summer of 2009.

Updates to the existing Go-ITS include:

- Principles, Roles, Responsibilities and the high-level process flow required to support an enterprise Problem Management process
- Incorporation of ITIL V3 (2007) concepts, introduction of a service-based focus on enterprise problem management and the evolution of IT Service Management disciplines within the OPS

This document establishes the enterprise Problem Management Principles, Roles and the associated process model. These standard elements provide a single unified process for enterprise Problem Management within the OPS. Use of this single process and supporting information will enable OPS-wide management and reporting through establishment of common data and associated metrics.

GO-ITS 44 ITSM Terminology Reference Model Portable Guide provides a common information model for key process parameters that require standardization across the OPS to ensure consistency, reliable business intelligence and to support end-to-end cross-jurisdictional service management. GO-ITS 44 will be updated with values defined as part of GO ITS 38. Please refer to:

[http://www.gov.on.ca/MGS/en/IAAndIT/STEL02\\_047295.html](http://www.gov.on.ca/MGS/en/IAAndIT/STEL02_047295.html)

### 2.2. Purpose

The primary objectives of Problem Management are to prevent problems and resulting incidents from happening, to eliminate recurring incidents and to minimize the impact of incidents that cannot be prevented. This leads to increased service availability and quality.<sup>1</sup>

---

<sup>1</sup> Extracted from ITIL V3; Service Operations

## 2.3. Value to the Business

Problem Management works together with Incident Management and Change Management to ensure that IT service availability and quality are increased. When incidents are resolved, information about the resolution is recorded. Over time, this information is used to reduce the resolution time and identify permanent solutions, reducing the number of recurring incidents. This results in less downtime and less disruption to business critical systems.

The following benefits are realized from adopting Problem Management:

### Risk Reduction

- Problem Management reduces incidents leading to more reliable and higher quality I & IT services to business users

### Cost Reduction

- Reduction in the number of incidents leads to a more efficient use of staff time as well as decreased downtime experienced by end-Users

### Service Quality Improvement

- Problem Management helps I & IT organizations to meet customer expectations for I & IT Services and , in turn, client satisfaction objectives
- By understanding existing problems, known errors and corrective actions, the OPS IT Service Desk ability to address incidents at first point of contact is enhanced
- Problem Management generates a cycle of increasing I & IT service quality

### Improved utilization of I & IT staff

- OPS IT Service Desk resources handle calls more efficiently because they have access to a knowledge database of known errors and possible corrective actions
- Consolidating problems, known errors and corrective action information facilitates organizational learning

The opportunity costs of not adopting a formal Problem Management process include the following:

- Business interruptions will result in unsatisfied clients and loss of confidence in the I & IT organization
- Inefficient use of support resources as senior resources spend their efforts on reacting to incidents rather than pro-actively managing the delivery and support of services
- Reduced employee motivation as they repeatedly address incidents with similar characteristics and get the impression that I & IT Senior Management not interested in addressing root cause of service disruption

## 2.4. Basic Concepts

Problem Management is focused on implementing the appropriate corrective actions to address problems that negatively impact IT services to the business. It seeks to implement cost effective, permanent solutions to eliminate the root cause of incidents thereby preventing reoccurrence. This differs from the IT service restoration focus of Incident Management that often uses temporary workarounds to quickly restore service.

.

There are two approaches to Problem Management, proactive and reactive:

- Reactive Problem Management identifies Problems based upon review of multiple events (usually incidents) that exhibit common symptoms or in response to a single incident with significant impact
- Proactive Problem Management identifies Problems by reviewing incident trends and non-incident data to predict that an incident is likely to (re-)occur

The basic steps associated with problem management include:

- Detection of candidate problems via analysis of incident data, problem data, operational data, release notes, knowledge DB and capacity or availability reports
- Logging, classification and prioritization of confirmed problems into the problem management database
- Determination of the root cause of the problems using industry standard techniques such as Kepner-Tregoe, Ishikawa Diagrams, Pain Value Analysis , Brainstorming and Technical Observation Post and Pareto Analysis
- Logging and classification of known errors identified by either root cause analysis or information from other sources
- Determination of alternative corrective actions to resolve the known errors
- Implementation of the appropriate corrective action through Change Management
- Situations will occur where the root cause cannot be determined within the scope of the available resources. At the discretion of the Problem Manager the problem record may be deferred or closed as unresolved.

The term, Known Error, is used in two separate manners:

- Known Error is a state in the Problem lifecycle that represents successful diagnosis and identification of the root cause of a problem. Root causes can take many forms such as technology, procedures and documentation and user knowledge levels. They are targeted for resolution through short-term and/or long-term corrective actions. Examples of other sources of information used to identify Known Errors are:
  - Application variances maintained during Build and Test activities
  - Software release notes
  - Vendors release notes that accompany new products
  - Vendor Patches
  - Online vendor support Web sites
- Known Error, is also used to describe the knowledge record containing details of the fault, symptoms, and any workarounds (also referred to as the Known Error database or KEDB). Sometimes the Known Error and Problem information are consolidated into a single record. Known Error information should be used during Incident diagnosis to facilitate a faster resolution.

The priority of a problem is primarily determined by the impact to the business and the resulting urgency for corrective actions. Urgency is decided by assessment of the likelihood that problem will cause future incidents. Problem prioritization will use an Impact-Urgency matrix similar to Incident Management. Complexity is also considered when ranking problems of a similar Priority since work on highly complex problems may have to await resource availability.

Action may be deferred if not justified by the associated costs and/or impact to the business.

There are significant linkages between Problem Management and Incident Management processes:

- The Incident management process provides incident history information used by problem analysts to identify problems
- Incident Management (and Service Desk agents) use problem and known error information when handling calls and resolving incidents
- The recommended corrective action identified for a known error is initiated by the Problem Owner by raising a Request for Change (RFC) through the ECM process
- Problem records are linked with other records (Incidents and RFCs), though process-enabling technology

Inputs to the Problem Management process include<sup>2</sup>:

- Meaningful Incident records
- Recurring Incident data
- Major Incident data
- Potential Problems (issues brought forward for consideration by customers, staff, senior management)
- Workarounds from different sources / knowledge databases
- Service Availability requirements
- Operational (event) data

Outputs from this process include<sup>3</sup>:

- Infrastructure problems and Known Errors
- Consistent and meaningful Problem and Error records
- RFC's (through ECM) for error removal
- Problem escalation
- Problem records (in knowledge database) linked to Incidents, Known Errors and RFC's
- Trend analysis results
- Meaningful management information
- Incident frequency reduction
- Increased stability for infrastructure elements resulting in improved service

## 2.5. Scope

### In Scope

Problem Management includes the activities required to diagnose the root cause of incidents and to determine the resolution to problems. Implementation of resolution is managed through the Enterprise Change Management (ECM), the control process.

The Problem Management Process Manager will also ensure information about problems and the appropriate workarounds and resolutions are maintained, so that the organization is able to reduce the frequency and impact of incidents over time. This information will be captured in Problem Records and the Known Error Database.

Although Incident and Problem Management are separate processes, they are closely related and will typically use the same enabling technology and identical terminology to identify service categorization, urgency, impact and priority. This will ensure effective communication when dealing with related incidents and problems.

---

<sup>2</sup> Source: Copyright 2003-2007. Ahead Technology Inc.

<sup>3</sup> Source: Copyright 2003-2007 Ahead technology Inc.

IS	IS NOT
Analysis of incident information (break-fix) to determine potential problems.	
Verification that root causes of problems have been accurately determined.	
Maintaining a Known Error Database with information from the root cause analysis of identified problems.	
Development of workarounds for Known Errors (identified by the Problem Management Process) to facilitate Incident resolution until a permanent solution can be implemented.	Activities to address known deficiencies in released applications will be managed outside of Problem Management
Development and testing of corrective actions to permanently resolve problems in order to prevent reoccurrence of incidents	Implementation of the corrective action. This is managed under the Enterprise Change Management (ECM) process.

### Out of Scope

N/A

## **2.6. Applicability Statements**

### **2.6.1. Organization**

Government of Ontario IT Standards and Enterprise Solutions and Services apply (are mandatory) for use by all ministries/clusters and to all former Schedule I and IV provincial government agencies under their present classification (Advisory, Regulatory, Adjudicative, Operational Service, Operational Enterprise, Trust or Crown Foundation) according to the current agency classification system.

Additionally, this applies to any other new or existing agencies designated by Management Board of Cabinet as being subject to such publications, i.e. the GO-ITS publications and enterprise solutions and services - and particularly applies to Advisory, Regulatory, and Adjudicative Agencies (see also procurement link, OPS paragraph). Further included is any agency which, under the terms of its Memorandum of Understanding with its responsible Minister, is required to satisfy the mandatory requirements set out in any of the Management Board of Cabinet Directives (cf. Operational Service, Operational Enterprise, Trust, or Crown Foundation Agencies).

As new GO-IT standards are approved, they are deemed mandatory on a go-forward basis (Go-forward basis means at the next available project development or procurement opportunity).

When implementing or adopting any Government of Ontario IT standards or IT standards updates, ministries and I&IT Cluster must follow their organization's pre-approved policies and practices for ensuring that adequate change control, change management and risk mitigation mechanisms are in place and employed.

For the purposes of this document, any reference to ministries or the Government includes applicable agencies.

### **2.6.2. Other Applicability**

N/A

### 2.6.3. Requirements Levels

Within this document, certain wording conventions are followed. There are precise requirements and obligations associated with the following terms:

<b>Must</b>	This word, or the terms "REQUIRED" or "SHALL", means that the statement is an absolute mandatory requirement.
<b>Should</b>	This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore the recommendation, but the full implications (e.g., business functionality, security, and cost) must be understood and carefully considered before deciding to ignore the recommendation.

### 2.6.4. Compliance Requirements

Execution of this process at the operational level requires use of procedures, work instructions and enabling technology to automate certain workflow aspects. These elements will be produced by the organization selected by OEIP as the Operational Process Prime. Pending formalization of an ITSM Process Lifecycle Management protocol, the following statements are presented to ensure that these elements are fully compliant with this Standard:

- Procedures must be developed by decomposing each process step from section 4.3 into sub-tasks. These procedures must be submitted to OEIP for certification that they comply with the spirit and intent of the Process Standard.
- Work Instructions must be developed by decomposing all procedural sub-tasks into further sub-tasks. These must be then submitted to OEIP for certification that they comply with the certified process and procedures.
- Functional Requirements must be developed for enabling technology that will be used to automate aspects of the work Instructions and procedures. Functional Requirements must also be submitted to OEIP for certification that they align with the certified procedures.

Any subsequent modifications to the Procedures, Work Instructions or enabling technology must be managed via Enterprise Change Management and will require authorization by OEIP.

Please refer to Appendix 6.3 for a diagrammatic explanation of process, procedure and work instructions.

## 3. Standards Lifecycle Management

---

### 3.1. Contact Information

*This section identifies the OPS organizations and resources involved in the creation and lifecycle management of this process standard:*

#### **Accountable Role Definition**

The individual ultimately accountable for the process of developing this standard. There must be exactly one accountable role identified. The accountable person also signs off as the initial approver of the proposed standard before it is submitted for formal approval to ITSC and ARB. (Note: in the OPS this role is at a CIO/Chief or other senior executive level)

#### **Accountable Role:**

Title: Head, Technology Adoption Branch (OCCTO)  
Ministry: MGS  
Division: OCCTO

#### **Responsible Role Definition**

The organization responsible for the development of this standard, There may be more than one responsible organization identified if it is a partnership/joint effort. (Note: the responsible organization(s) provides the resource(s) to develop the standard)

#### **Responsible Organization:**

Ministry: MGS  
Division: OCCTO  
Branch: Technology Adoption

#### **Support Role Definition**

The support role is the resource(s) to which the responsibility for actually completing the work and developing the standard has been assigned. There may be more than one support role identified. If there is more than one support role identified, the following contact information must be provided for each of them. If there is more than one support role, the first role identified should be that of the editor – the resource responsible for coordinating the overall effort.

#### **Support Role (Editor):**

Ministry: MGS  
Division: OCCTO  
Branch: Technology Adoption  
Section: ITSM  
Job Title: Lead, OPS Enterprise ITSM Program  
Name: Norm Watt  
Phone: 416-327-3542  
Email: norm.watt@ontario.ca

*The above individual will be contacted by the Standards Section once a year, or as required, to discuss and determine potential changes and/or updates to the standard (including version upgrades and/or whether the standard is still relevant and current).*

**2<sup>nd</sup> Support Role (if applicable):**

Section: ITSM  
 Job Title: ITSM Business Consultant  
 Name: Peter Donlevy  
 Phone: (647) 638-8067  
 Email: peter.donlevy@ontario.ca

**3<sup>rd</sup> Support Role (if applicable):**

Section: ITSM  
 Job Title: Enterprise Problem Manager  
 Name: \_\_\_\_\_  
 Phone: \_\_\_\_\_  
 Email: \_\_\_\_\_

**Consulted**

Organization Consulted (Ministry/Cluster)	Division	Branch	Date
N/A			

Committee/Working Group Consulted	Date
ITSM Leads	7 May 2009 13 May 2009
Consultation on this Standard occurred via submissions to IT Standards Council	20 May 2009 17 June 2009 30 June 2009 15 July 2009 19 Aug 2009

**Informed**

*Please indicate who was informed during the development of this standard. Include individuals (by role and organization) and committees, councils and/or working groups.*

*(Note: informed means those who are kept up-to-date on progress, generally characterized by one-way communication such as presentations):*

Organization Informed (Ministry/Cluster)	Division	Branch	Date

Committee/Working Group Informed	Date
SDLC	22 April 2009
ITSM Leads	29 April 2009

### 3.2. Recommended Versioning and/or Change Management

Changes (i.e. all revisions, updates, versioning) to the standard require authorization from the “responsible” organization.

Once a determination has been made by the responsible organization to proceed with changes, the Standards Section, Technology Adoption Branch, OCCTO, will coordinate and provide assistance with respect to the approvals process.

The approval process for changes to standards will be determined based on the degree and impact of the change. The degree and impact of changes fall into one of two categories:

**Minor changes** - requiring communication to stakeholders. No presentations required. No ITSC or ARB approvals required. Changes are noted in the “Document History” section of the standard;

**Major changes** - requiring a presentation to ITSC for approval and ARB for approval (Note: ARB reserves the right to delegate their approval to ITSC)

Below are guidelines for differentiating between minor and major changes:

#### Major:

- represents a major version change to one or more specifications
- impacts procurement
- requires configuration changes to current solutions
- impacts other standards
- responds to legislative, policy or procurement changes

#### Minor:

- represents incremental version changes to one or more specifications
- does not impact procurement (other than informational)
- does not require configuration changes to current solutions
- does not impact other standards
- is not related to legislative, policy, or procurement changes

### 3.3. Publication Details

All approved Government of Ontario IT Standards (GO-ITS) are published on the ITSC Intranet web site. Please indicate below if this standard is also to be published on the public, GO-ITS Internet Site.

Standard to be published on both the OPS Intranet and the GO-ITS Internet web site (available to the public, vendors etc.)	<b>Yes</b>
--	------------

## 4. Technical Specification

---

### 4.1. Process Principles

Principles are established to ensure that the process identifies the desired outcomes or behaviours related to adoption at an enterprise level. They also serve to provide direction for the development of procedures and (as necessary) work instructions that will ensure consistent execution of the process. The absence of well-defined and well understood principles may result in process execution that is not aligned with the process standard. Mandatory Process Principles for OPS enterprise Problem Management are listed below

**Principle 1:**

**A single Problem Management process that is separate from the Incident Management process shall be used across OPS.**

Rationale:

- There is clear accountability for the Problem Management process;
- There is clear ownership for problem resolution;
- Resources can be focused on identifying the main and contributing root causes of a problem;
- There is a defined review process associated with addressing root causes and corrective actions;
- There is a consistent interface with groups responsible for resolving problems;
- Duplicate problem resolution activities are avoided.

Implications:

- Requires a base level of maturity for Incident Management;
- Sufficient designated resources must be focused on problem management;
- Process linkages with Incident Management must be clear;
- Incident and Problem Management are separately managed processes.

**Principle 2:****Clear criteria shall be established to define what constitutes a Problem and how Problems will be prioritized.**Rationale:

- Protect the Problem Management process to ensure Problem Management resources are effectively focussed on real, not perceived problems
- Ensure that a minimum level of information is captured to allow Problem Analyst to correctly assess and identify the problem for review
- Ensure the most critical Problems are addressed first
- Ensure consistent treatment of reported Incidents

Implications:

- Only the Problem Manager will have the authority to approve and prioritize Problems (by applying said criteria)
- At least one Incident record or Known Error must exist before a Problem Record will be created via reactive Problem Management
- Customer Relationship Management (CRM) and Service Level Management (SLM) functions do not have direct interface with the Problem Management process. They must provide Service Owners with sufficient evidence to warrant a candidate problem being surfaced to the Problem Manager by the Service Owner.
- Incident Management procedures must ensure that information required by Problem Management is captured during incident logging, classification and service restoration activities.
- Incident Management process will need the ability to link similar incidents to an existing problem.

**Principle 3:**

**All problems, known errors and relevant progress and resolution information shall be recorded in a common repository that is linkable to Incident and Change Management records.**

Rationale

- Provides source of reference for Problem Analysts (Knowledge Base)
- A single repository to capture historical knowledge of incidents and problems allows quicker diagnosis and resolution by Service Desk Agents when incidents recur.
- It simplifies problem and known error analysis and reporting.
- It provides a single source of data for integration with other ITSM processes and tools
- Provide source data for Process effectiveness and efficiency measure

Implications

- Enabling technology may require an update based on the above
- A common information model must be used to facilitate linkages between ITSM processes across the OPS.
- All problems/known errors, progress and resolutions must be logged;
- Known errors and related problems must be linked;
- Historical and any new recurring Incidents must be linked to Problems and Known Errors
- The number of recurring Incidents must be captured since this information can influence Problem priority
- Incident Management procedures must be modified to specify that Known Error information will be utilized during Incident diagnosis activities (see process integration section 4.4)

**Principle 4:**

**A Known Error shall be raised as soon as useful knowledge is available, even before a permanent resolution is found**

Rationale

- In some cases the root cause may never be determined. During the course of investigation and diagnosis, more than one Known Error may be identified before completion of root cause analysis. However, it is useful to document workaround and other relevant information for use by Incident Management.
- In other cases such as Vendor issued patches / release notes, or alarms from event monitoring systems a Known Error could be identified without root cause analysis being undertaken.

Implications

- Service Owners must assess vendor information and if applicable to their Service (including all components that enable the service) they must submit a Known Error to the Problem Manager.  
The underlying database needs to be structured to effectively handle different types of data: known errors, workarounds and general information
- Parameters will need to be defined to flag a Problem record as Known Error and also to indicate whether the root cause is known

**Principle 5****Known deficiencies in an implemented Change shall be logged as a Known Error**Rationale

- To ensure that known development and staging defects are documented
- Details of workarounds and / or recommended actions (including “no action required”) can be used by Incident Management to clarify expectations and avoid unnecessary investigation and diagnosis activities
- Knowledge of defects should be factored into Risk-Impact assessments when planning future changes

Implications

- In the absence of a formal Release & Deployment Management Process, the Change Owner must submit a Known Error to Problem Management (which references the RFC #)
- Linkage between Change Management and Problem Management must be defined and adhered to
- Resolution of such deficiencies will NOT be addressed via Problem Management, but via the Service Owner who has consciously accepted and introduced this deficiency. Meanwhile, the KE record is available for Incident Management to close incidents against & link to KE

**Principle 6:****Problem investigation & diagnosis shall employ standard analysis techniques & methodologies leveraging industry best practices**Rationale

- To ensure that effective Problem Management analysis tools & techniques are adopted and consistently applied throughout the enterprise.

Implications

- Resources involved in the Problem Management process require specific training related to Root Cause Analysis techniques.
- This will require identification, documentation and training on standard tools and analysis techniques beyond the guidance in the process and procedure guide
- There is a defined review process associated with addressing root causes and corrective actions;

**Principle 7:****Service Owners must fulfill their roles and responsibilities as defined in this Problem Management process.**Rationale:

- Service Owners are usually assigned as Problem Owners, accountable to manage Problem resolution for owned services.
- Service Owners will typically be accountable for configuration items that are impacted by corrective actions.
- Service Owners may have to secure funding for resolution activities

Implications:

- Service Owners may have to reprioritize existing workload to manage assigned Problems within service objectives.
- Service Owners must ensure that their OLA's and UC's contain explicit language that will require internal and external Service Providers to support OPS Problem Management activities, including analysis and implementation of solutions to eliminate problems.
- Service Owners may have to secure funding from the Service Manager to enable problem resolution (e.g. additional Hardware, new / upgraded software, new solution development).
- Service Owners must be identified for all designated Services

## 4.2. Process Roles and Responsibilities

Each process requires specific roles to undertake defined responsibilities for process design, development, execution and management. An organization may choose to assign more than one role to an individual. Additionally, the responsibilities of one role could be mapped to multiple individuals.

One role is accountable for each process activity. With appropriate consideration of the required skills and managerial capability, this person may delegate certain responsibilities other individuals. However, it is ultimately the job of the person who is accountable to ensure that the “job gets done”.

Regardless of the mapping of responsibilities within an organization, specific roles are necessary for the proper operation & management of the process. This section lists the mandatory roles and responsibilities that must be established to execute the Problem Management process.

Legend: **R**esponsible, **A**ccountable, **C**onsult before, **I**nformed

Process activities	Problem Manager	Problem Analyst	Problem Owner	Partner Liaison	Partner Org	Service Owner
1 - Detect problem	A	R				
2 – Log & classify problem	A	R				
3 – Assign Problem	AR	C	I(R)	I(R)		
4 – Investigate & Diagnose		R	A	R	C	R
5 – Resolve problem			A			R
6 - Close Problem	AR	C				
7 – Review Major Problem	A	R	R	R	R	R
8 - Monitor problems	AR					

### 4.2.1. Enterprise Problem Management Process Owner

The Enterprise ITSM Problem Management Process Owner owns the process and the supporting documentation (typically the associated GO-IT Standard) for the Process being described. This includes accountability for setting Policy and providing leadership and direction for the development, design and integration of the process as it applies to other applicable frameworks and related ITSM processes being used and or adopted in the OPS. The Enterprise Process Owner will be accountable for the overall health and success of the Process and will undertake to achieve this through local Process Owners and Process Mangers throughout the OPS.

#### Responsibilities

- Ensures that the process is defined, documented, maintained and communicated at an Enterprise level through appropriate vehicles (IT Standards Council / Corporate ARB).
- Undertakes periodic review of all ITSM processes from an Enterprise perspective and ensures that a methodology of Continuous Service Improvement, (including applicable Process-level supporting metrics) is in place to address shortcomings and evolving requirements.
- Ensures that the all Enterprise ITSM processes are considered and managed in an integrated manner, taking into consideration OPS Policies and Directives and factoring in evolving trends in technology and practice.
- Solicits OPS Stakeholders and communities of interest to establish Enterprise ITSM process requirements for consideration by the Enterprise ITSM Program. Coordinate, present and recommend options for the prioritization, development and delivery of these to appropriate governing body.
- Ensure enterprise process requirements are documented and provided to operational support teams to be developed and implemented with enabling technology.

### Segregation of Duties

The role of Enterprise Process Owner is separate and distinct from that of the Problem Manager and the roles shall be separately staffed. The Enterprise PM Process Owner shall reside in OCCTO, while the Enterprise PM Process Manager shall reside in a Cluster designated by ITEL C.

#### **4.2.2. Problem Manager**

The Problem Manager manages execution of the Problem Management process and coordinates all activities required to respond to problems in compliance with SLAs and SLO's. The Problem Manager has the ultimate accountability for resolution of Problems and is the escalation point for problem management activities.

#### Responsibilities

- Develops and maintains operational procedures to execute the enterprise Problem Management process
- Develops and maintains functional requirements for enabling technology and corresponding usage guidelines
- Ensures tight linkage between the enterprise Problem Management and Incident & Change Management at the operational level (including linkages to enabling technology)
- Monitors and reports on various attributes of the Problem Management process and identifies improvement opportunities to the enterprise Process Owner:
  - Process efficiency
  - Process / procedural adherence
  - Process effectiveness (i.e. reduction in number of incidents)
  - service level performance of the Problem Management Process
- Uses matrix management and assistance from Partner Problem Management Liaisons to:
  - ensure that Problem Analysts (from all organizations) are assigned at an appropriate level, with adequate skill levels and training in standard problem management techniques
  - assess the effectiveness of Problem Management activities and identifies need for further training of Problem Analysts
- Manages and co-ordinates all activities necessary to detect problems by ensuring analysis of Incident Management data and other relevant sources of information
- Authorizes the creation of Problem records & prioritizes problem activities
- Assigns problems to the appropriate Problem Owner for analysis and resolution
- Assigns Problem Analyst(s) to support Problem Owners in their activities
- Ensures creation and maintenance of the Known Error Database, including approval of Known Errors
- Monitors assigned Problems and takes appropriate action if activities are not conducted within process performance objectives (PPO).

### 4.2.3. Service Owner

To ensure that services are 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 a specific service within an organization regardless of where the underpinning technology components, processes or professional capabilities reside.

The Service Owner is accountable for:

- Initiation, transition, and support of a particular service
- Continual improvement and the management of change to the service
- Exchanging relevant service information with the Service Level Manager who is the prime customer contact for all service-related performance enquiries and issues

#### Responsibilities

- Provides input in service attributes such as performance, availability etc.
- Represents the service across the organization
- Understands the service (components etc.)
- Point of escalation (notification) for major Incidents
- Represents the service in Change Advisory Board meetings
- Provides input to the Continual Service Improvement (CSI) process
- Participates in internal service review meetings (within IT)
- Works with the CSI Manager to identify and prioritize service improvement
- Assists the enterprise Problem Manager with identification prioritization and resolution of Problems
- Participates in external service review meetings
- Responsible for ensuring that the service entry in the organization's Service Catalogue is accurate and is maintained
- Ensures that service support staff review Vendor and / or Service Provider supplied documentation for components that enable his / her Service (e.g. patch information, s/w release notes, h/w and firmware upgrades) in order to identify and communicate Known Error information to the Problem Manager.
- Participates in negotiating SLAs and OLAs

#### 4.2.4. Problem Owner

The Problem Owner has ultimate responsibility for analysis and resolution of assigned problems. A Service Owner may be assigned as the Problem Owner in many cases, but this is not mandatory. The assigned Problem Owner must possess the appropriate management skills and authority to manage activities across organizational boundaries.

##### Responsibilities

- Ensures required stakeholders are involved in the problem management activities
- Engages required support staff from other organizations via Partner Problem Management Liaisons
- Utilizes a matrix management approach to plan, manage and co-ordinate activities necessary to identify root cause, develop workarounds, preventative actions and long term solutions for assigned problems
- If elimination of the root cause requires modification of an item under configuration change control, he ensures that an RFC with an assigned Change Owner is initiated to manage implementation of the permanent solution via ECM, and informs the Problem Manager upon implementation of the solution.
- Ensures through the Partner Problem Management Liaison that support staff in the organization in question have adequate skill levels and training in problem management techniques
- Requests assistance from Problem Manager after attempted escalation to secure appropriate stakeholder support has proven unsuccessful.

#### 4.2.5. Problem Analyst (PA's)

The Problem Analysts provides skills and knowledge in a particular domain (technical, operational or application). He is also trained in best practice techniques for problem investigation. He will use this expertise to facilitate root cause analysis of assigned problems, and the development of workarounds and / or permanent solutions with the assistance of appropriate SME's.

##### Responsibilities

- Assists Problem Manager in data analysis to identify suspected Problems
- Identifies required participants (SME's) from other organizations to the Problem Owner
- Under the direction of the Problem Owner, requests information from supporting SME's and uses standard problem analysis techniques to facilitate identification and validation of root cause
- In collaboration with SME's and Service Owners:
  - Facilitates development of Workarounds and short term corrective actions for Known Errors
  - Facilitates development and testing of permanent solution
- Records and updates Problem and Known Error records with appropriate information
- Assists Problem Manager in validating that root cause has been eliminated upon implementation of the recommended solution.

#### 4.2.6. Partner Problem Management Liaison

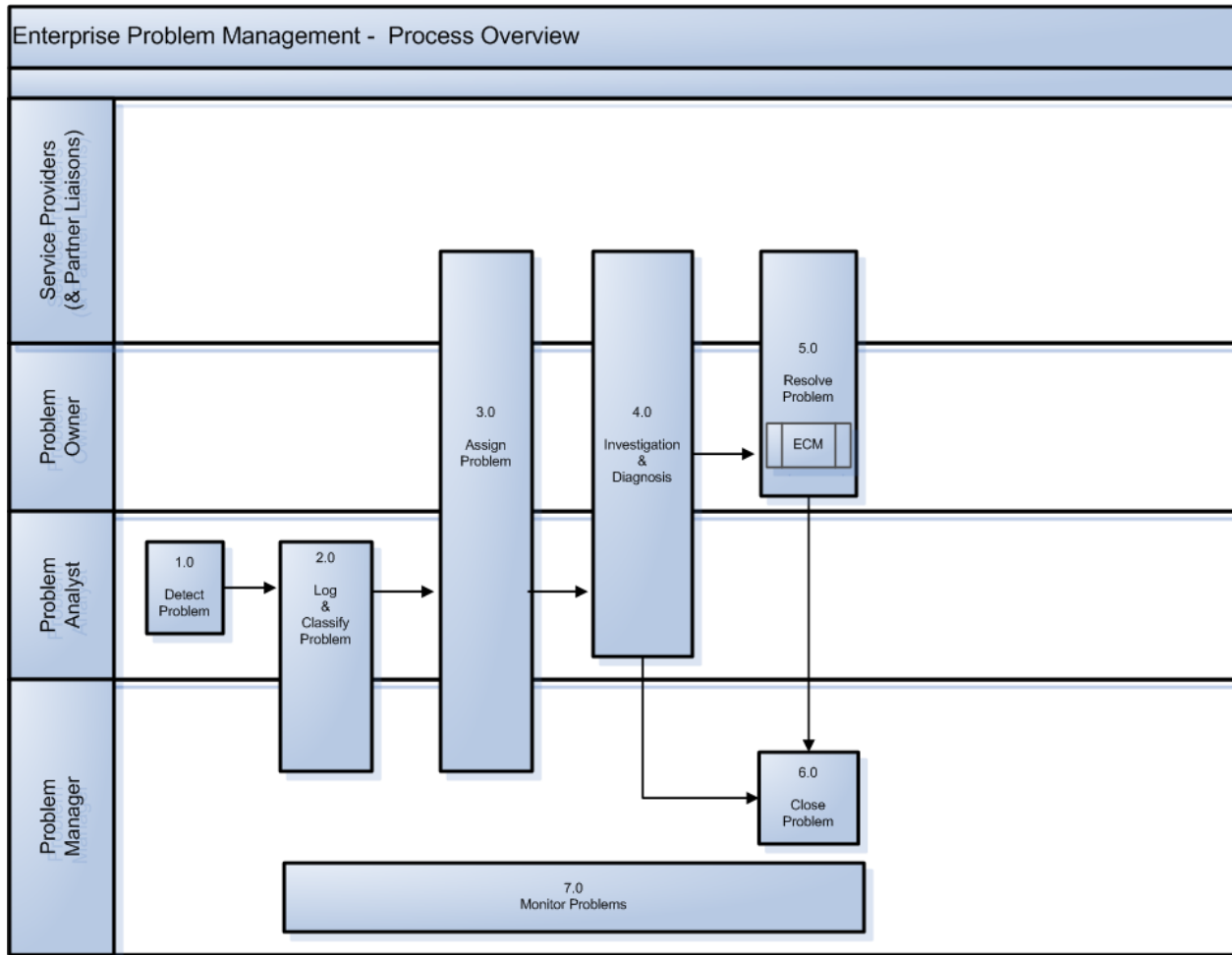
Manages and co-ordinates all activities within their organization necessary to assist in detection of root cause & development of workarounds and permanent solutions.

##### Responsibilities

- Upon request by the Problem Owner, confirms the assignment of required resources with accountable manager within their organization to work on Problem Management activities , including escalation if unable to secure resources
- Monitors and reports on partner Problem Management Process activities and Identifies improvement opportunities to the enterprise Problem Manager

### 4.3. Process Flow

#### 4.3.1. Enterprise Problem Management Process Overview



#### 4.3.2. Enterprise Problem Management Process Tasks

The following table lists the mandatory tasks to be performed during execution of the Problem Management process.

No	Task	Roles	Input, Trigger	Description	Output, Completion Criteria
1.0	Detect Problem	PA-R	Input: Incident data base, incident trend reports, service metrics reports, event data, patterns  Trigger: Release notification, multiple incidents, major/ severe incident	Identify possible Problem areas by analyzing incident data, problem data, operational data, release notes, knowledge DB and capacity or availability reports.	Problem Identified
2.0	Log & Classify Problem	PM-R	Problem Identified	Log a problem record, including all relevant information and links to associated Incident and Change records, CI's)  Classify the problem. Determine the impact and urgency to set the priority of resolution.  If the Problem Analysts cannot support parallel investigation of multiple Problems of the same priority, then the Problem Manager ranks the order in which Problems will be addressed. PM may choose to consult with stakeholders in this activity	Logged, classified and prioritized problem record
3.0	Assign Problem	PM-R PO-I PA-I PL-I	Problem logged	PM assigns problem to Problem Owner. PM assigns Problem Analyst to facilitate analysis of this problem. PA identifies if support is required from other organizations: if so, PM assigns Partner Liaison(s) who obtain SME support, as required, within their organizations	Problem team assembled

No	Task	Roles	Input, Trigger	Description	Output, Completion Criteria
4.0	Investigation & Diagnosis	PO-R PA-R PL-R PM-C	Problem Assigned	<p>PA uses standard problem analysis techniques investigation to diagnose and validate root cause of the problem,</p> <p>Once root cause is found, PA submits a Known Error record (KE) to the PM for acceptance. Once a workaround is developed, PA updates KE so that Incident Management can utilize this information should the incident recur.</p> <p>PA collaborates with SME's and Service Owners to develop and test a permanent solution to eliminate the Known Error.</p> <p>If duration of problem investigation has reached a predetermined threshold, PM consults PO to decide if further investigation is warranted. If he decision is not to proceed, or if a permanent solution cannot be found, the problem is closed as unresolved.</p>	<p>Root cause &amp; permanent solution identified</p> <p>Or ...</p> <p>Investigation threshold exceeded</p>
5.0	Resolve Problem	PO-R	Investigation completed	<p>If permanent solution has been identified, Problem Owner will determine whether sufficient cost-justification exists to proceed with permanent solution.</p> <ul style="list-style-type: none"> <li>▪ If so, PO secures assignment of person who will act as Change Owner, and permanent resolution activities are initiated via Enterprise Change Management.</li> <li>▪ If not, problem will be closed as Deferred.</li> </ul>	<p>Change Owner assigned and ECM process invoked.</p> <p>OR</p> <p>No further action.</p>
6.0	Close Problem	PM-A PA-R PO-I	<p>Indication from ECM that permanent solution has been implemented</p> <p>OR ...</p> <p>Root cause not found</p> <p>OR ...</p> <p>Permanent solution not cost justifiable</p>	<p>The Problem Record is updated to reflect all activities carried out during Problem investigation and resolution.</p> <p>The status of any related Known Error Record should be updated to shown that the resolution has been applied.</p>	

No	Task	Roles	Input, Trigger	Description	Output, Completion Criteria
7.0	Monitor Problem	PM-R		This is an oversight activity by the Problem Manager to proactively monitor progress of problem resolution. Problem Manager decides if escalation is required and communicates status to stakeholders, as required.	

#### 4.4. Linkages to Other Processes

Process	Linkage
<b>Incident Management</b>	<ul style="list-style-type: none"> <li>• PM requires that Incident Management capture sufficient and accurate information to enable problem identification:               <ul style="list-style-type: none"> <li>○ Proper closure codes</li> <li>○ Proper classification</li> <li>○ Link new Incidents to existing Problems</li> <li>○ Known defective components (based upon event monitoring and component alarms).</li> </ul> </li> <li>• PM makes information available that can benefit Incident resolution activities (eg. Known Errors, workarounds, patterns)</li> <li>• Enabling technology must be able to define relationship between Incidents ,Problem and Known Errors records</li> </ul>
<b>Enterprise Change Management (ECM)</b>	<ul style="list-style-type: none"> <li>• Upon completion of a change driven by problem resolution, the Problem Manager &amp; Problem Owner must be informed so that Problem record can be closed.</li> <li>• Upon identification of known deficiencies at change implementation, Change Management must inform PM, by submitting a Known Error to Problem Management.</li> <li>• Enabling technology must be able to define relationship between Problems and Change records</li> </ul>
<b>Configuration Management</b>	<ul style="list-style-type: none"> <li>• <i>A portable guide was developed as an OPS Standard in 2004. This portable guide will be updated to reflect Enterprise requirements in the near future. At that time it will be linked to Problem Management which will provide information so that a CI can be designated as defective</i></li> </ul>
<b>Release and Deployment Management</b>	<ul style="list-style-type: none"> <li>• <i>Once this Process is developed, Release (not ECM) will submit known defects to PM for creation of Known Errors</i></li> </ul>
<b>Service Level Management</b>	<ul style="list-style-type: none"> <li>• <i>Although not yet a formal OPS Process, this process receives information about problems and their status for discussion with the customer at service review meetings.</i></li> </ul>

## 4.5. Problem Management Process Quality Control (CSI)

In parallel to the execution of the Problem Management process, there are activities related to the management of the process to control quality as well as to ensure that the process is both effective and efficient.

**Monitoring** of the service delivered by the Problem Management team is performed regularly by the Problem Manager. This allows the Problem Manager to answer any questions about service quality and customer satisfaction as well as ensure that the Problem Management process is not running into resource or ownership issues. The Problem Manager is responsible to take corrective actions if bottlenecks are identified in the process.

**Reporting** involves measuring the process via metrics and recording how well it behaves in relation to the objectives or targets specified in the metrics. Metrics provides the Problem Management personnel with feedback on the process. They also provide the Problem Management Process Owner with the necessary information to review overall process health and to undertake continual service improvement techniques.

**Evaluating** the process involves regular reviews of the performance of the process and identification of possible improvements or actions to address performance gaps. Every process is only as good as its last improvement; hence, the feedback loop of continuous improvement is inherent in every process.

## 4.6. Metrics

Metrics are intended to provide a useful measurement of a process effectiveness and efficiency. Metrics are also required for strategic decision support. The following need careful consideration:

- Reporting metrics will be readily measurable (preferably automated collection and presentation of data)
- Metrics will to be chosen to reflect process activity (how much work is done?), process quality (how well was it done?) and process operation (to review and plan job on hand).
- The Enterprise Problem Management Process Owner is accountable for the definition and capture of an appropriate suite of metrics to determine the overall health of the Enterprise Problem Management process.

The following metrics must be used to assess process performance, opportunities for service improvements and also for strategic decision support.

### Workload:

- The total number of problems recorded in the period
- Number of Problems and Known Errors in a period broken down by status, Service, Impact, Category and Closure condition code.

### Process Effectiveness:

Determination of Problem Management effectiveness requires metrics input and analysis across a number of processes: Incident Management, Service Level Management and Problem Management. The following represent the initial suite of Problem Management-related metrics that must be provided by these processes.

- Number of recurring incidents (per service) (IM) (trend decreasing is positive)
- Number of Incidents (IM) (trend should decrease)

- Number of Incidents resolved via workarounds from Known Errors (IM)
- Number of problems that reoccur (PM)
- % of SLA targets achieved (SLM)
- % service Availability (SLM)
- Number of open known errors and status of associated change requests
- Number of deferred corrective actions (PM)
- Number of Incidents linked to problem records (PM)

Process Efficiency: metrics are used analyze the performance of the process in order to determine areas for improving (e.g. *Increase in average time to resolve problems may indicate need for more training or tools*)

- The percentage accuracy of the KEDB (from audits of the database)
- The average effort of handling a problem
- The number and percentage of problems that exceeded their target resolution times
- The backlog of outstanding problems and the trend (static, reducing or increasing?)
- Volume and percentage of problems processed per period with no resolution
- Average time to find root cause
- Average time to identify permanent solution

#### **4.7. Standard Process Parameters**

For an enterprise process to be effective, parameters used for the classification, categorization, prioritization and closure of problems must be consistently used across OPS. Special attention must be given to parameters related to consistency of reporting. This is particularly important for the provision of reliable business intelligence.

Please refer to the Classification Model section of the GO-ITS 44 ITSM Terminology Reference Model Portable Guide for standard process parameters and allowable values for Problem Management.

Please refer to the State Model section of the GO-ITS 44 ITSM Terminology Reference Model Portable Guide for standard status/state parameters and their definitions for Problem Management.

## 5. Related Standards

---

### 5.1. Impacts to Existing Standards

Identify any Standards that reference or are referenced by this Standard and describe the impact.

GO-IT Standard	Impact	Recommended Action
Incident Management	This standard is being updated in parallel and will reflect process linkages described above.	
TRM	This standard is being updated in parallel and will reflect revised terminology and values for e*PM and related processes.	
ECM	This standard is being updated in parallel and will reflect process linkages described above.	

### 5.2. Impacts to Existing Environment

Impacted Infrastructure	Impact	Recommended Action
Not Applicable		

## **6. Appendices**

---

### **6.1. Normative References**

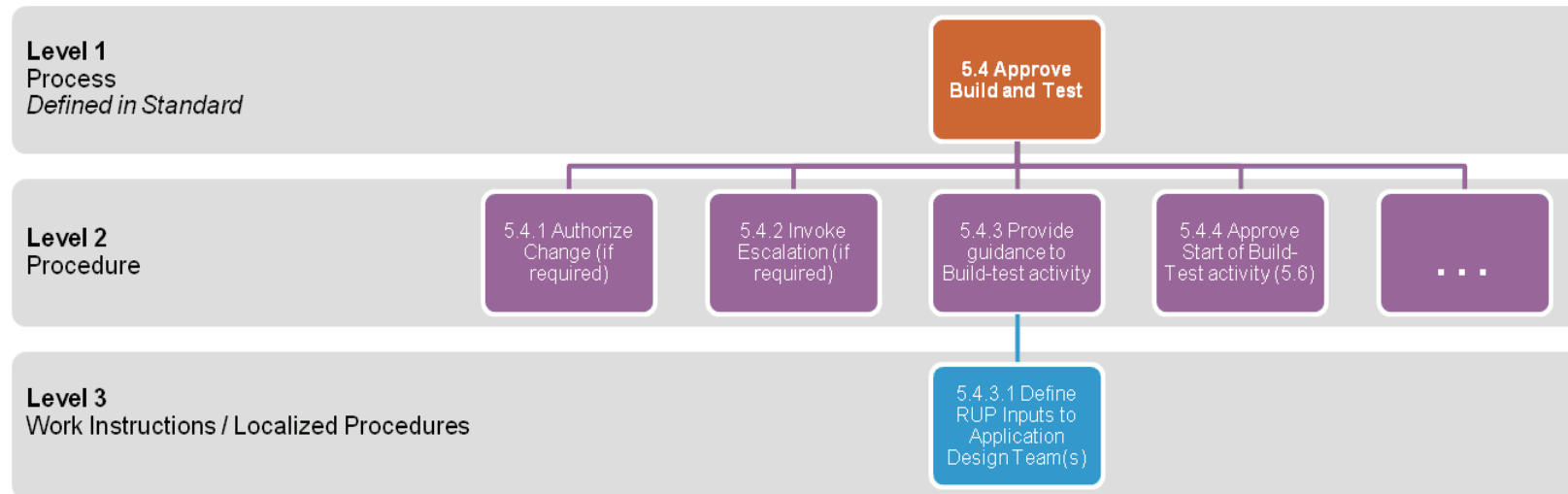
Enterprise Problem Manager will determine if Procedures are a normative or informative reference and how they will be managed / evolved.

### **6.2. Informative References**

Not applicable.

### 6.3. Differentiation: Process, Procedure, Work Instruction

Note: The following diagram depicts three levels of task descriptions that are often confused with one another:



- Level 1 Tasks are defined in a Process. They specify what action must be taken and who is involved.
- Level 2 tasks are defined in Procedures which decompose each level 1 task into more granular operational tasks, and additionally, prescribe how the activity should be performed.
- Level 3 tasks represent Work instructions: they are further decomposition of procedure-level tasks which typically are defined to address any unique local requirements when performing a procedural task.

## 7. Glossary

Term	Description
Complexity	The degree of problem analyst involvement required to isolated the root cause
ECM	The Enterprise Change Management Process. OPS GO-IT Standard 38
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	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.
External Service Provider ???	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.
Functional Escalation	Transferring an Incident, Problem or Change to a technical team with a higher level of expertise to assist in an Escalation.
Hierarchical Escalation	Informing or involving more senior levels of management to assist in an Escalation.
Impact	A measure of the effect of an Incident, Problem or Change on Business Processes. Impact is often based on how Service Levels will be affected. Impact and Urgency are used to assign Priority.
Incident	An unplanned interruption to an IT Service or reduction in the Quality of an IT Service. Failure of a Configuration Item that has not yet affected Service is also an Incident. For example Failure of one disk from a mirror set.
Incident Management	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	A Record containing the details of an Incident. Each Incident record documents the Lifecycle of a single Incident.
Internal Service Provider	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.
Ishikawa Diagram	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.
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.
Kepner & Tregoe Analysis	A structured approach to Problem solving. The Problem is analysed in terms of what, where, when and extent. Possible causes are identified. The most probable cause is tested. The true cause is verified.

Term	Description
Known Error (KE)	A KE has 2 distinct meanings: - The lifecycle state of a Problem that has successfully identified the Root Cause -. Known Error is also used to describe the records that document root cause details and available workarounds. Known Errors may also be identified by Development or Suppliers.
Known Error database	A database containing all Known Error Records. This database is created by Problem Management and used by Incident and Problem Management.
KE Record	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.
Operational Level Agreement (OLA)	An Agreement between an IT Service Owner and another IT Service Owner within the same Organization. The other Service Owner provides services that support delivery of IT services to Service Owner A's customers. The OLA defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA. The OLA defines the goods or Services to be provided and the responsibilities of both parties. For example there could be an OLA: <ul style="list-style-type: none"> <li>Between the IT Service Provider and a procurement department to obtain hardware in agreed times</li> <li>Between the Service Desk and a Support Group to provide Incident Resolution in agreed times.</li> </ul>
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 centre.
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.
Process Service Level Objective (PSLO)	A service level objective for a specific process task or metric. e.g.: <ul style="list-style-type: none"> <li>Problem resolution will complete within x weeks, based upon problem classification.</li> <li>70% of incidents will be linked to Problems</li> </ul>
Proactive Problem Management	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	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	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	A Record containing the details of a Problem. Each Problem Record documents the Lifecycle of a single Problem.

Term	Description
Reactive Problem Management	Reactive Problem Management involves the identification of Problems based upon investigation of Incident data, operational event data, and information provided by Service Desk and Service Owners.
Release	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.
RFC	Request For Change
Root Cause	The underlying or original cause of an Incident or Problem.
Root Cause Analysis (RCA)	An Activity that identifies the Root Cause of an Incident or Problem.
Service	ITIL defines Service as "a means of delivering value to customers by facilitating specific outcomes customers want to achieve without the ownership of specific costs and risks". GO-ITS 56.1 defines services within the OPS as functionality that can be directly consumed by an end-user. Relationships and obligations between Service Owners and Customers are documented in SLA's. (see <i>Support Service</i> )
Service Desk	The Single Point of Contact between the Service Provider and the Users. A typical Service Desk manages Incidents and Service Requests, and also handles communication with the Users.
Service Failure Analysis (SFA)	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 Level Agreement (SLA)	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 and Underpinning Contract)
Service Level Manager	Is the liaison between the business (customer) and IT. He ensures that agreed level of service is provided for current IT services, corrective action is taken if not, and that future IT services are delivered to agreed achievable targets
Service Owner	Member of a Service Provider organization, accountable for delivery of a specific service
Service Manager	A manager who is responsible for managing the end-to-end Lifecycle of one or more IT Services.
Service Provider	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. Where there are several Service Providers that enable an overarching service, they are sometimes called Supply Chain (or Service Chain) Partners
Support Service	Are internal services that support a 'consumable' Service. Support Services are typically not visible to end-users. Relationships and obligations between Service Support Owners and their Customer (Service Owners) are documented in OLA's and UC's. (see <i>Service</i> )
Trend Analysis	Analysis of data to identify time-related patterns. Trend Analysis is used in Problem Management to identify common Failures or fragile Configuration Items, and in Capacity Management as a Modelling tool to predict future behaviour. It is also used as a management tool for identifying deficiencies in IT Service Management Processes.

<b>Term</b>	<b>Description</b>
Underpinning Contract (UC)	Contract between an OPS IT Service Provider and an external Third Party IT Service Provider. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The UC defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA and also specifies the required behaviour to comply with OPS ITSM Standards.
Urgency	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.
Workaround	Reducing or eliminating the Impact of an Incident or Problem for which a full Resolution is not yet available. For example by restarting a failed Configuration Item. Workarounds for Problems are documented in Known Error Records. Workarounds for Incidents that do not have associated Problem Records are documented in the Incident Record.