Problem Management Process Training

Before you begin:
This course was prepared for all IT professionals with the goal of promoting awareness of the process. Those taking this course will have varied knowledge of ITIL, Service Operation and Problem Management. As such, this course aims to deliver information that is easily understood and relevant to everyone. We invite your specific questions or comments and encourage you to follow up directly with your manager.

Course Objectives

This course explains the following:

- Difference between Incident Management and Problem Management
- Value of Problem Management to the Enterprise
- Key Definitions and Basic Concepts for Problem Management
- Problem Management Policy
- Roles and Responsibilities
- Key Process Activities of the Problem Management Process
- Using the ServiceNow tool

What is Problem Management and how is it different from Incident Management?

- The objective of Incident Management is to restore the service as quickly as possible while Problem Management deals with solving the underlying cause of one or more incidents; therefore, the emphasis of Problem Management is to resolve the root cause and to find permanent solutions.

- The most common mistake is a tendency to treat a Problem like a "big Incident". The Incident ends when the customer is able to carry on with their job, regardless of whether or not the underlying cause of the Incident has been resolved. Key question to ask is "Can my customer now work?" If the answer is yes, then close the Incident and if appropriate, raise a Problem.

A Case Study and the Value of Problem Management to the Enterprise

Several customers contact the Service Desk to report that they are getting an error message when trying to access a clinical application. With limited time available, the application support team decides to restart the application service on the server which cleared the error message and the customers are able to access the application.

The Incident should now be closed - the customer is now able to work. If a customer encounters this error message again, the Service Desk is aware of this known error and can ask the application support team to apply the workaround to clear the error message. The solution is not perfect, but it has kept the customer working.

At this time, the application support team will raise a Problem record so that the root cause of the error message can be identified.

A common error in this scenario is for the Incident to be left open until the cause of the Incident has been found and resolved and for all the investigation of the underlying error to take place as part of the Incident record. This will negatively impact your Incident statistics even though the customer is quite happy with the workaround he has been given.

The key question to ask yourself is "Can my customer now work?" If the answer is yes, then close the Incident and if appropriate, raise a Problem.

A root cause analysis was conducted and it was determined that the failure was due to a lack of bandwidth at the application server and once its limit was reached, the error occurred and additional users could no longer connect to the application. The server was replaced with more robust hardware and the Service Desk no longer received calls on this error message.

The ability to quickly identify the root cause of underlying issues reduces incidents, avoids outages, lowers cost and improves an IT organization's reputation with the business.

ITIL[ISM]

Are you fighting fires without addressing the root cause?

OIL OIL

Eliminate the root cause with Problem Management

Key Definitions and Basic Concepts

ITIL v3 defines a **Problem** as "the 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.

Basic concepts:

– A *Root Cause* of an incident is the fault in the service component that made the incident occur

– A *workaround* is a way of reducing or eliminating the impact of an incident or problem for which a full resolution is not yet available.

Two major sub processes:

▪ *Reactive problem management* – Analyzing and resolving the causes of incidents.

▪ *Proactive problem management* – Aims to detect and prevent future problems/incidents. Proactive problem management includes the identification of trends or potential weaknesses

Problem Management Policy

Policy

To ensure high availability of UCSF IT Services, all Incidents with a Priority 1 (Critical) or Priority 2 (High) that involve a Major Outage require a Problem Record be opened and the Problem Management process followed.

- Setting the Symptom in an Incident record to "Major Outage" will trigger the Major Incident Review and Problem Management process.

Recommended Guideline

Always open a Problem Record for incidents that continually reoccur, regardless of priority, so that root cause can be determined and a permanent solution put into place.

Roles & Responsibilities

Within the Problem Management process, specific roles and functions have been defined. Each role is responsible for completing specific tasks within the process, *however, all roles contribute to the success of the process.*

The Roles include:

- Problem Manager
- Problem Coordinator
- Technical Expert
- Problem Management Process Committee

Problem Manager

The **Problem Manager** is accountable for the overall Problem Management process across all of IT.

Responsibilities of the Problem Manager include:

- Ensures that the process is defined, documented, maintained, and communicated at an Enterprise level

- Responsible for reviewing monthly metrics and taking action where necessary to enforce process and standards to ensure continued process maturity

- Facilitate Post Major Problem review meetings when required

- Act as an escalation point regarding any Problem Management Process issues

- Drives forward the integration of the Problem Management process with other Service Management processes

- Coordinates and chairs the regularly scheduled Problem Management Process Committee meetings

Problem Coordinator

The **Problem Coordinators** are representatives from each functional group or Problem Category. They are responsible for the operational and managerial tasks required by the problem process flow.

Responsibilities of the Problem Coordinator include:

- Responsible for the process within their unit, working with the Process Manager to ensure compliance and process maturity

- Oversees the effort of documented Problems within their unit

- Works with necessary support groups in IT to ensure swift resolution of Problems that are owned by their unit

- Analyzes recurring Incidents and identifies Problems

- Acts as training resource within member's functional unit

- Participates in the regularly scheduled Problem Process Committee meetings

Technical Expert

The **Technical Experts** are staff who work on the Problem records to investigate and diagnose them, devise workarounds and work on permanent solutions.

Responsibilities of the Technical Experts include:

- Investigates and resolves Problems under the co-ordination of the Problem Manager and Problem Coordinator

- Ensures problems are managed within their teams, providing workarounds that will resume service and devise permanent solutions.

- Diagnose the underlying root cause of Incidents

- Ensures that work on Problems is accurately recorded in the Problem record

- Ensures that optimal solutions are devised

- Attends Major Incident Reviews and provides accurate and complete Incident details.
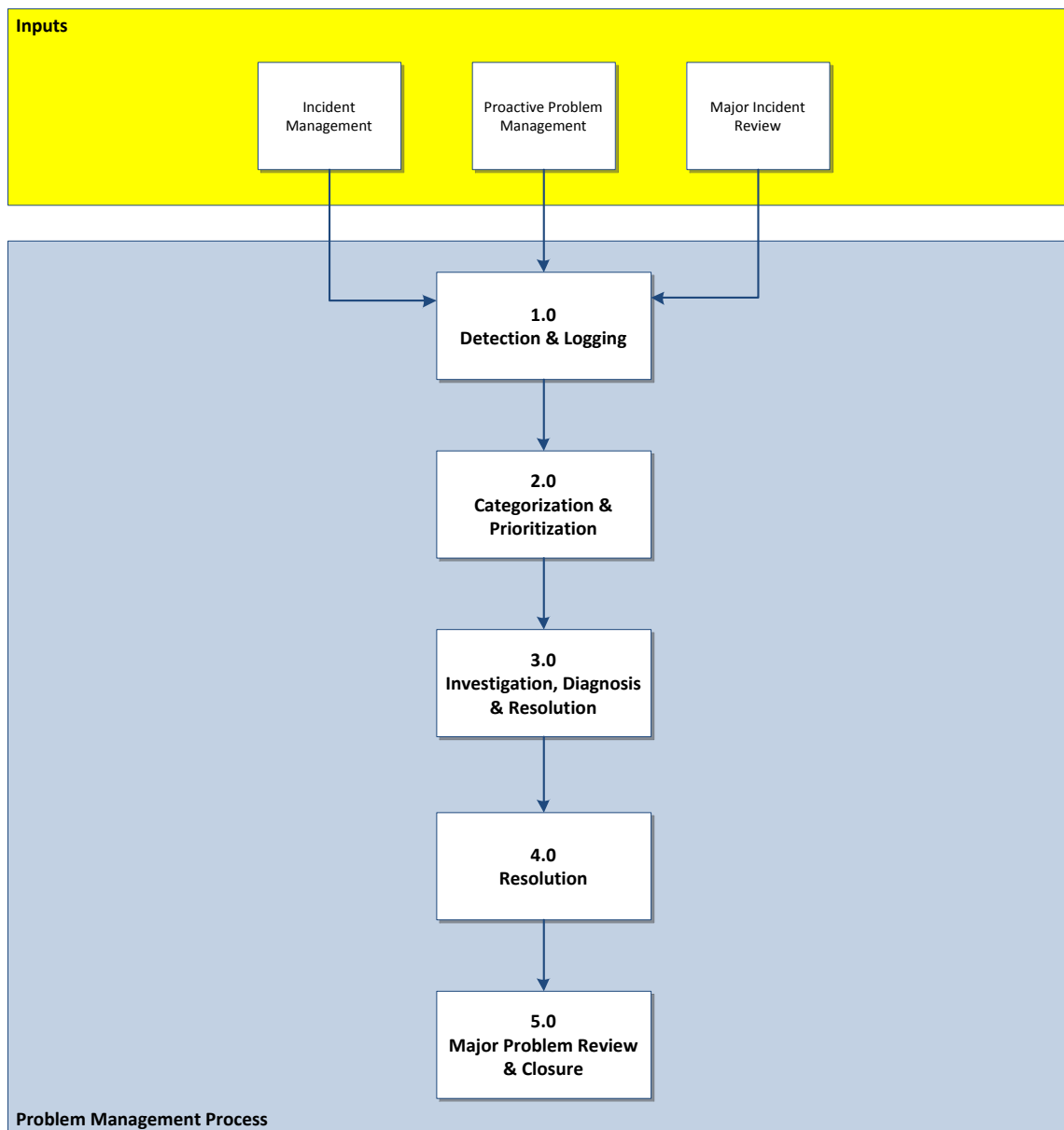
Problem Management Process Committee

The **Problem Management Process Committee** meets regularly and is responsible for reviewing and approving all Problem Management process and tool improvements. Committee members include the Problem Manager and the Problem Coordinators.

Responsibilities of the Process Committee members include:

- Review/approval of all Problem Management process improvements

- Review/approval of all Problem Management tool enhancement requests

Key Process Activities of Problem Management

Inputs

- Incident Management
- Proactive Problem Management
- Major Incident Review

1.0 Detection & Logging

2.0 Categorization & Prioritization

3.0 Investigation, Diagnosis & Resolution

4.0 Resolution

5.0 Major Problem Review & Closure

Problem Management Process

High Level Problem Management Process

Inputs that trigger the Problem Process

There are several inputs that can trigger the Problem Management process. They include:

- Incident Management Process – A Problem record should be opened when Incidents are resolved with a **Workaround** but the **Root Cause** is never addressed. These Problems can be opened by the Service Desk or the Service Provider Group after Incident trend analysis is done.

- Major Incident Process – A Problem record should be opened for all Major Outages. These Problems are triggered automatically when the **Major Incident Process** is followed.

- Proactive Problem Management – Problem records can be opened before an Incident occurs. An example of this is when Data Center monitoring tools send alerts that a drive is reaching capacity and service is at risk. A Proactive Problem record can be opened to replace the drive or purge old data before an Incident occurs.

Activity 1: Detection and Logging

1. Detect a Problem
   - Detecting a problem is much more subjective and qualitative in its nature than Incident Management, which is more objective and quantifiable.
   - There is no clear objective indicator to begin the Problem Management (PM) process. If there is a desire to find the root cause of an occurrence or a need to ask the basic question "Why?", you should move into the PM process.
   - "Why?" could be generated from one incident, recurring incidents (trending analysis) or even no incidents; however, *all critical and high Incidents that are categorized as a major outage are required to trigger the PM process*.

2. Log the Problem in ServiceNow
   - Problem logging is critical as all the necessary information from the Incidents has to be captured while creating the problem.
   - Create a problem from the Incidents (if applicable), maintaining the link to the Incidents.
   - Avoid duplicates by searching for similar Problems before the creation of a new Problem.
   - For High or Critical Incidents where the symptom is Major Outage, the Problem is automatically created.

3. Assign the Problem to the appropriate Support Group.
   - The Problem Coordinator of the functional unit where the Support Group resides should monitor the Problem to ensure a Technical Expert takes ownership of the Problem.

Activity 2: Categorization and Prioritization

1. Categorize the Problem
   – Problem categorization is essential to avoid ambiguities and makes it simpler to search incidents and associated problem records.
   – Proper categorization allows you to tie to a supported service for easy reporting.

2. Prioritize the Problem
   – Determine impact and urgency to determine the priority
   – Problem prioritization helps technical staff to identify critical problems that need to be addressed

Activity 3: Investigation and Diagnosis

1. Collect problem history by investigating related Incidents.
   – The Service Desk is an excellent resource and can help gather the history.
2. Identify symptoms and root cause.
   – Perform problem analysis, diagnosis and solving techniques to facilitate finding the root cause.
3. Suggest and document a workaround, and change the Problem to a known error.
   – The Service Desk browsing through these known error records/workarounds helps in lowering Incidents resolution time.
4. Identify a permanent solution to resolve the Problem.

Activity 4: Resolution

1. Implement the solution
   - Submit a Request for Change (RFC) and follow the Change Management Process to implement the solution.
   - Decide whether the implemented Change has successfully resolved the Problem
   - Update the Problem record and ensure it includes:
     - A documented Solution
   - Notify the Service Desk

Activity 5: Major Problem Review and Closure

1. When a Major Problem occurs, a Major Problem Review must be held to examine:
   - Things that were done correctly and incorrectly
   - Items that can be improved in the future
   - How to prevent reoccurrence
   - Whether follow-up actions are required

2. No review is required for minor problems

3. Post review, update the Problem with <u>Lessons Learned</u>.

4. Close the Problem record.

Note: All UCSF Problem Management documentation including Quick Reference Cards detailing using ServiceNow to create and manage Problem records and completing the Major Incident Review tab on the Incident form can be found at http://it.ucsf.edu/pages/problem-management