DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:
2300/09
CP

From: Commandant of the Marine Corps

Subj: ENTERPRISE INFORMATION TECHNOLOGY SERVICE MANAGEMENT PROBLEM MANAGEMENT PROCESS GUIDE

Ref: (a) MCO 5271.1B

Encl: (1) IRM-2300-09 Enterprise Information Technology Service Management Problem Management Process Guide

1. PURPOSE. The purpose of the Enterprise Information Technology Service Management (ITSM) Problem Management Process Guide is to establish a documented and clear foundation for process implementation and execution across the Marine Corps Information Environment (MCIE). Process implementation and execution at lower levels (e.g., Regional, Local and Programs of Record) must align and adhere to directives and schema documented within this guide. The use of this guide enables USMC Information Technology (IT) activities through promoting standardization of work instructions and operating procedures across a continuum of document specificity.

2. CANCELLATION. N/A.

3. AUTHORITY. The information promulgated in this publication is based upon policy and guidance contained in reference (a).

4. APPLICABILITY. This publication is applicable to the Marine Corps Total Force.

5. SCOPE.

a. Compliance. Compliance with the provisions of this publication is required unless a specific waiver is authorized.

b. Waivers. Waivers to the provisions of this publication will be authorized by the Commanding Officer, Marine Corps Network Operations and Security Center.

6. SPONSOR. The sponsor of this technical publication is HQMC C4 CP.

K. J. NALLY
Brigadier General
U.S. Marine Corps
Director, Command, Control,
Communications and Computers (C4)

DISTRIBUTION: PCN 18623000100

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

Enterprise IT Service Management
Problem Management
Process Guide

Release Date:
April 15, 2013

Document Approval/Major Revision Change History Record

This table is used for initial release and subsequent revisions. Major revisions are indicated by the number to the left of the decimal point while minor revisions are indicated by the number to the right. Major revisions are required when the intent or process is changed rendering the prior version obsolete or when the number of minor releases total twenty (20). Changes to this document shall be recorded, described and approved using the table below:

Release Date (MM/DD/YY)	Release No.	Approvals		Change Description
		Author	Process Owner/Approver	
03/27/2013	0.1			Draft Release
		Printed Name	Printed Name	
4/1/2013	0.2			Updated per process owner review
		Printed Name	Printed Name	
		Printed Name	Printed Name	
		Printed Name	Printed Name	
		Printed Name	Printed Name	
		Printed Name	Printed Name	
		Printed Name	Printed Name	
		Printed Name	Printed Name	
		Printed Name	Printed Name	

Table of Contents

Section	Title	Page
1.0	**Introduction**	**1**
1.1	Purpose	1
1.2	Scope	1
1.3	Process and Document Control	2
2.0	**Process Overview**	**3**
2.1	Purpose, Goals, and Objectives	3
2.2	Relationships with other Processes	3
	2.2.1 Relationships with other Processes	4
2.3	High-Level Process Model	6
	2.3.1 PbM Process Description	7
2.4	Key Concepts	7
	2.4.1 Commander's Critical Information Requirements	7
	2.4.2 Problem and Known Error Status	8
	2.4.3 Proactive Problem Management	8
	2.4.4 Reactive Problem Management	8
	2.4.5 Problem Management Database	8
	2.4.6 Known Error Database (KEDB)	9
	2.4.7 Relationship of Problem with Other Processes	9
	2.4.8 Root Cause Analysis	9
	2.4.9 Known Error	9
	2.4.10 Workarounds	9
	2.4.11 Problem Models	9
	2.4.12 Problem	10
	2.4.13 Incident	10
	2.4.14 Event	10
2.5	Quality Control	10
	2.5.1 Metrics, Measurements and Continual Process Improvement	10
	2.5.2 Critical Success Factors with Key Performance Indicators	10
3.0	**Roles and Responsibilities**	**14**
3.1	Responsibilities	18
4.0	**Sub-Processes**	**21**
4.1	Problem Detection (sub-process 1.0)	21
4.2	Problem Logging (sub-process 2.0)	23
4.3	Problem Categorization (sub-process 3.0)	25
4.4	Problem Prioritization (sub-process 4.0)	25
4.5	Problem Investigation and Diagnosis (sub-process 5.0)	28
4.6	Create Problem Known Error Record (sub-process 6.0) and Problem Resolution (sub-process 7.0)	31
4.7	Problem Closure (sub-process 8.0)	34
4.8	Major Problem Review (sub-process 9.0)	35
APPENDIX A — Acronyms		**37**
APPENDIX B — Glossary		**38**
APPENDIX C — Problem Solving Techniques		**42**
C.1	Brainstorming Session	42
C.2	Ishikawa Diagram	44
C.3	5-Whys	46
C.4	Kepner-Tregoe	47
C.5	Flow Diagrams	47
C.6	Inductive Reasoning	47
C.7	Deductive Reasoning	47

List of Tables

Table	Title	Page
Table 1: Document Design Layers		2
Table 2: PbM Process Activity Descriptions		6
Table 3: Problem Status Designations		8
Table 4: PbM Objectives		11
Table 5: PbM Defined Roles and Responsibilities		15
Table 6: Responsibilities for Enterprise PbM Management Roles for an Enterprise Problem		19
Table 7: Responsibilities for Regional PbM Management Roles for a Regional Problem		20
Table 8: Problem Detection Sub-Process Descriptions		22
Table 9: Problem Logging Sub-Process Descriptions		24
Table 10: Urgency Matrix		26
Table 11: Priority Matrix		26
Table 12: Categorization and Prioritization Sub-Process Descriptions		27
Table 13: Problem Investigation and Diagnosis Sub-Process Descriptions		29
Table 14: Create Know Error Record Sub-process Descriptions		32
Table 15: Create Know Error Record Sub-process Descriptions		34
Table 16: Major Problem Review Sub-process Descriptions		36

List of Figures

Figure	Title	Page
Table 1: Document Design Layers		2
Figure 2: Problem Management Relationships with other E-ITSM Processes		4
Figure 3: High-Level Problem Management Workflow		6
Figure 4: Problem Management Roles		15
Figure 5: Problem Detection Sub-Process		22
Figure 6: Problem Logging Sub-Process		24
Figure 7: Problem Categorization and Prioritization Sub-Processes		27
Figure 8: Problem Investigation and Diagnosis Sub-Process		29
Figure 9: Create Known Error Record and Problem Resolution		32
Figure 10: Problem Closure Sub-Process		34
Figure 11: Major Problem Review Sub-Process		35
Figure 12: Sample Ishikawa Diagram		46

Enterprise Problem Management Process Guide

1.0 INTRODUCTION

1.1 Purpose

The purpose of this process guide is to establish a documented and clear foundation for process implementation and execution across the Marine Corps Information Environment (MCIE). Process implementation and execution at lower levels (e.g., Regional, Local, and Programs of Record) must align and adhere to directives and schema documented within this guide. The use of this guide enables USMC IT activities through promoting standardization of work instructions and operating procedures across a continuum of document specificity as represented in Figure 1.

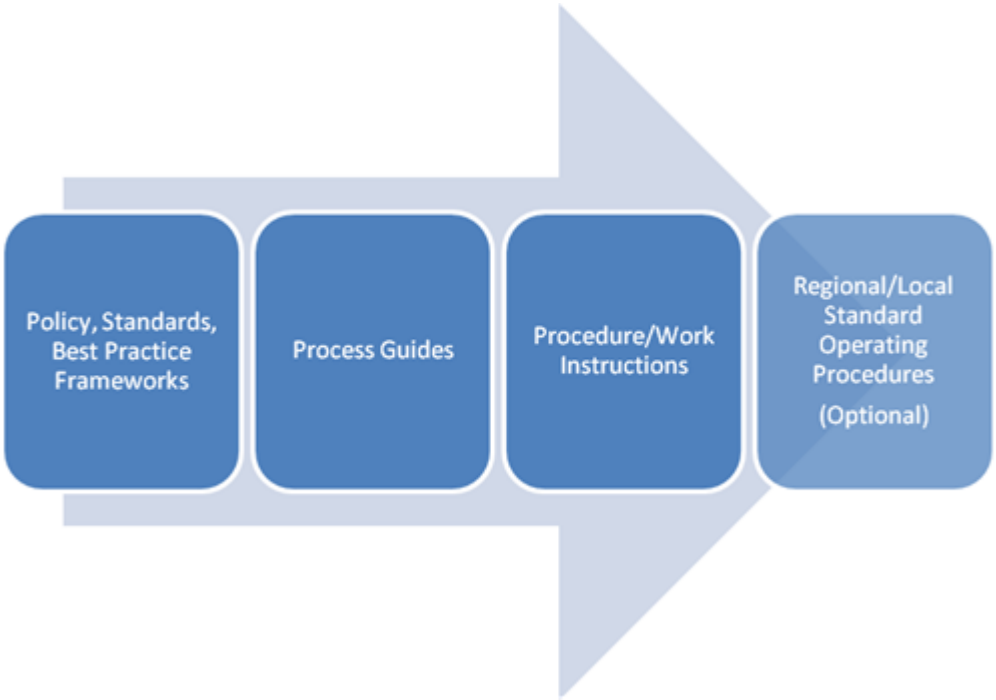

Figure 1: Process Document Continuum

1.2 Scope

The scope of this document covers all services provided in support of the MCIE for both the Secret Internet Protocol Router Network (SIPRNET), and the Non-Secure Internet Protocol Router Network (NIPRNET). Information remains relevant for the global operations and defense of the Marine Corps Enterprise Network (MCEN) as managed by Marine Corps Network Operations and Security Center (MCNOSC) including all Regional Network Operations and Security Centers (RNOSC) and Marine Air Ground Task Force Information Technology Support Center (MITSC) assets and supported Marine Expeditionary Forces (MEF), Supporting Establishments (SE) organizations, and Marine Corps Installation (MCI) commands.

Table 1 depicts the various layers of document design. Each layer has discrete entities, each with their own specific authority when it comes to promulgating documentation. This enterprise process operates at Level B, sub processes such as procedures and work instructions are not included within the scope of this document.

Table 1: Document Design Layers

	ENTITIES	DOCUMENTS GENERATED
LEVEL A	Federal Govt DoD DoN CMC/HQMC	Statutes/Laws DoD Issuances DoN Policies Marine Corps Orders/IRMS
LEVEL B	HQMC C4 MCNOSC MCSC	MCOs IRMs (Process Guides) Directives MARADMINS
LEVEL C	RNOSC MITSC	Regional Procedures Work Instructions
LEVEL D	MCBs POSTS STATIONS	Locally Generated SOP's

1.3 Process and Document Control

This document will be reviewed semi-annually for accuracy by the Process Owner with designated team members. Questions pertaining to the conduct of the process should be directed to the Process Owner. Suggested Changes to the process should be directed to USMC C4 CP in accordance with MCO 5271.1C Information Resource Management (IRM) Standards and Guidelines Program.

2.0 PROCESS OVERVIEW

2.1 Purpose, Goals, and Objectives

The purpose of the Problem Management (PbM) process is to identify problems and their root cause, determine and implement corrective actions that will eliminate possible reoccurrence, and document known errors to include work around solutions for incidents affecting the Marine Corps Information Environment (MCIE) and manage the life cycle of all problems.

The primary goal of Problem Management is to prevent problems and resulting incidents from happening, to eliminate recurring incidents and to minimize the impact of incidents that cannot be prevented. Meeting this goal will result in increased operational productivity and availability of services provided via the MCEN.

The objectives of Problem Management include:

- Decrease reoccurring incidents by utilizing thorough Root Cause Analysis (RCA) to determine permanent solutions for all problems directly and indirectly affecting the services of the MCEN.
- Initiate Requests for Change (RFC) driven by the direct findings of a problem investigation and resolution.
- Decrease service interruptions through the use of proactive analysis utilizing trending and pattern recognition which will locate and relate problems that are occurring in different geographical locations.
- Decrease service restoration times by providing technicians with a Known Error Database (KEDB) that will allow them to take advantage of previously identified solutions and work-arounds.

2.2 Relationships with other Processes

All IT Service Management processes are interrelated. The E-ITSM processes in Figure 2 were selected due to the strength of the relationships and dependencies between them and the degree to which they underpin USMC near-term objectives. While any one of the E-ITSM processes can operate in the presence of an immature process, the efficiency and effectiveness of each is greatly enhanced by the maturity and integration of all E-ITSM processes. Figure 2 depicts key relationships that exist between Problem Management and the other E-ITSM processes.

2.2.1 Relationships with other Processes

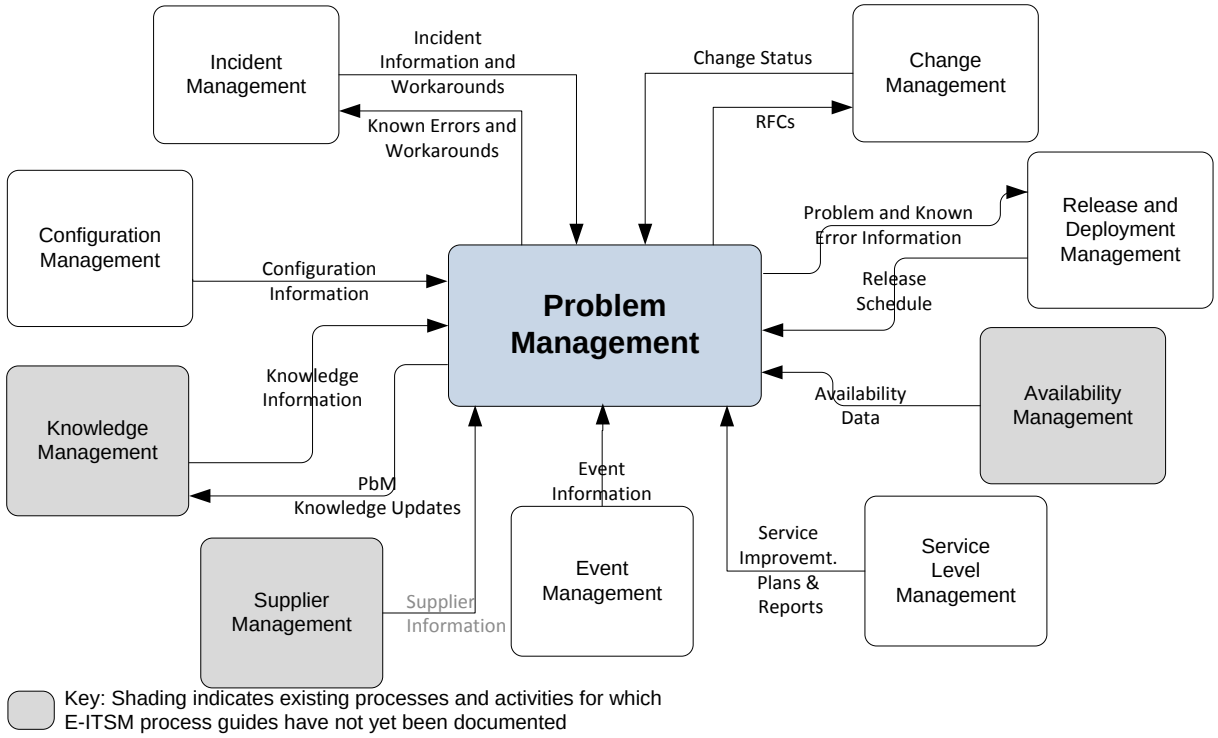

Figure 2: Problem Management Relationships with other E-ITSM Processes

Incident Management (IM)

- Incident Information and Workarounds: Incident data is important input for investigation to determine root cause. Incident information is analyzed over periods of time to identify trends that may indicate previously unidentified problems. Workarounds identified within the Incident Management (IM) process are associated with Known Errors and validated upon successful root cause analysis.
- Known Errors and Workarounds: Known Errors and Workarounds enhance the effectiveness and efficiency of Incident First Call Resolutions.

Change Management (ChM)

- RFCs: Change Requests are submitted to address underlying root causes of problems.
- Change Status: ChM informs PbM of the status of changes implemented so that the Known Error record can be updated and closed upon verification of successful change.

Release and Deployment Management (RDM)

- Problem Information: Provides information about Problems and Known Errors introduced by new releases.
- Identifies preexisting problems and Known Error information received from vendors and implementation teams.

- Coordinates root cause analysis related to new releases and works to establish robust test environment to avoid these issues.
- Release Schedule: Provide notice of Release Schedule and details.

Availability Management

- Availability data: Agreed-to Service Level Targets for IT Infrastructure, Processes, Tools, Roles, etc.

Service Level Management (SLM)

- Service Improvement Plans (SIP) and reports: Bi-directional notification of plans to change services to improve performance. This could be an update to Service Level due to a problem with a service that is changing service levels or notification of an SLM raised SIP so all service plans are coordinated until a regular Continuous Service Improvement function is built.

Event Management (EM)

- Event Information: Event data is important input for providing trend analysis and identification to assist within proactive Problem Management.

Supplier Management (SM)

- Supplier Information: External service providers convey awareness of problems and Incidents that occur within their environment.

Knowledge Management (KM)

- Knowledge Information: Data retrieved form knowledge database needed to perform PbM activities. May consist of existing SLAs, SLRs, OLAs, Operating Level Objectives (OLOs), Underpinning Contract (UCs), and past service reports — historical service information used as input for SLM decisions for a service.
- PbM Knowledge Updates: Updates/edits to knowledge database articles/scripts as it relates to Problem Management. Updated service information and documented changes available to the service stakeholders.

Configuration Management (CfM)

- Configuration Information: Configuration Items (CIs) and relationships are used in trend analysis to identify problems and in investigation to determine root cause.

2.3 High-Level Process Model

The following diagram illustrates the high level process model for Problem Management. See Section 4.0 for complete descriptions of the sub-process activities.

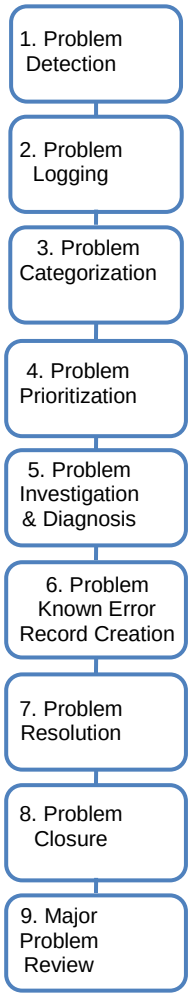

Figure 3: High-Level Problem Management Workflow

Table 2 below contains descriptions of each sub-process. As appropriate, sub-process numbers are hyperlinked to its detailed description in Section 4.0, Sub-Processes.

Table 2: PbM Process Activity Descriptions

Number	Sub-Process	Description
1.0	Problem Detection	Suspicion or detection of an unknown cause of one or more Incidents by the Enterprise Service Desk/Regional and Local Service Desks, resulting in the creation of a Problem Record. May also be the result of analysis of an Incident by a technical support group, automated detection of the infrastructures and applications, notification from a supplier or contractor, or analysis of proactive Problem Management.
2.0	Problem Logging	Problem Record is recorded in the problem tracking tool detailing all relevant information. Problem record will be tracked and updated in Problem tracking tool until closure.

3.0	Problem Categorization	Problem Record is categorized based on the systems, applications or services/segment affected (similar to Incident Management).
4.0	Problem Prioritization	Problem Record is prioritized based on urgency and impact (similar to Incident Management)
5.0	Problem Investigation & Diagnosis	Problem solving techniques (including Known Error Database [KEDB] assistance) are used to identify the root cause of a problem and determine requirements necessary to come to a permanent resolution of the problem.
6.0	Problem Known Error Record Creation	When diagnosis is complete and/or a work-around has been put in place, a problem Known Error Record must be created in the KEDB. This is helpful so that if further incidents or problems arise, service can be restored quicker. This may also be done earlier in the process if it becomes helpful to do so.
7.0	Problem Resolution	As soon as a solution is found to solve a problem it should be applied along with proper safeguards. Some resolutions require a Request for Change (RFC) to be approved and scheduled for release. Resolution of further occurrences of incidents/problems can be assisted by the KEDB.
8.0	Problem Closure	The Problem Record is formally closed after changes have been completed and reviewed and resolution is applied (along with any related Incidents). A full historical description of the related events should now be seen in this record. The status of related Known Errors should be updated with the resolution.
9.0	Major Problem Review	Major problems determined by the priority system are reviewed to identify lessons learned and improve the process as a whole. This will identify; things that were done correctly, things that were not done correctly, how to prevent future recurrence, and third-party responsibility/follow-up actions. This information can be recorded as associated documentation and reviewed with the business customer to enhance satisfaction levels.

2.3.1 PbM Process Description

Problem Management is a life cycle management process geared toward preventing problems from occurring, reducing the impact of unavoidable problems and finding solutions to prevent recurring problems affecting the Marine Corps Information Environment (MCIE) and manage the life cycle of all problems. Problem Management focuses on a problem's root cause and works to resolve the problem in a proactive or reactive manner, as required.

2.4 Key Concepts

The following key concepts are utilized extensively in the Problem Management Process.

2.4.1 Commander's Critical Information Requirements

Commander's Critical Information Requirements (CCIR) are the commander's "need to know immediately" information and response requirements. From MCWP 3-40.2 Information Management, "CCIR are tools for the commander to reduce information gaps generated by uncertainties that he may have concerning his own force, the threat, and/or the environment. They define the information required by the commander to better understand the battle-space, identify risks, and to make sound, timely decisions in order to retain the initiative. CCIR focus the staff on the type and form of quality information required by the commander, thereby reducing information needs to manageable amounts." In the context of Problem Management, CCIRs are a basis for setting problem priority.

All commands are required to produce command specific CCIR guidance with detailed IT service management requirements and are required to adhere to the current CCIR guidance of their superior commands. Common CCIR categories are Enterprise Service Management, Network Defense, Content Management, and MCEN, but others may be applicable based upon the commander's requirements.

2.4.2 Problem and Known Error Status

As a Problem and Known Errors progress through the process, status codes identify the stages of work toward resolution, which is critical for reporting and for continual process improvement. Guidance for the status designations is shown in Table 3.

Table 3: Problem Status Designations

Status	Designation
Rejected	The Problem Process Manager deems not a valid problem record and refuses responsibility for ownership.
Open	The problem has been opened, but has not been accepted by PBM.
Assigned	The Problem Process Manager has accepted this record, and assigned responsibility for action.
Under Investigation	The problem is being addressed.
Pending	This ticket is awaiting input or action by vendor, user, or a decision outside of Problem Management.
Deferred	Because of several possible constraints, Problem Process Manager must postpone based on priority or resources. (This may happen in prioritization and planning, but it can also happen later in the process).
Completed	Problem has been resolved and is awaiting review before being closed.
Under Review	Ticket has been Completed and is waiting to be Closed, or is awaiting Major Problem Review.
Closed	All tasks are complete and Problem/Error is now closed.

2.4.3 Proactive Problem Management

Proactive Problem analysis moves away from the fire-fighting mode of Incident Management by analyzing data in order to identify trends and problems before they cause Incidents. Examples of problem solving techniques are defined in Appendix C.

2.4.4 Reactive Problem Management

Reactive Problem Management is an operational process that identifies existing problems linked to closed/resolved incidents, automated detection of infrastructure errors, supplier notifications, and input from technical support groups. The primary goal of Reactive Problem Management is to ensure the stability of IT Services provided by eliminating systemic problems. Examples of problem solving techniques are defined in Appendix C.

2.4.5 Problem Management Database

The BMC Remedy Problem Management module will serve as the Enterprise solution hosting all Problem Records. These records will contain information pertaining to actual or potential

disruptions of service that are currently being analyzed to determine their root cause as well as the historical records for problems that have been resolved. Support staff who are attempting to resolve incidents may find that similar incidents are related to problems listed in the Problem Management module.

2.4.6 Known Error Database (KEDB)

Problem Management creates, maintains and audits the BMC Remedy KEDB data records. This enterprise solution will be utilized by Service Desks, Field Service Technicians, and other predefined groups across the Marine Corps. Many ITSM processes and functions, particularly the ESD/Regional and Local Service Desks, utilize the KEDB to support operational activities, such as Incident resolution. Standardized documentation guidelines and recommended best practices will be provided by the Process Owner in the form of Standard Operating Procedures and Work Instructions to ensure complete and consistent records.

2.4.7 Relationship of Problem with Other Processes

Incident Management aims to restore service quickly, by whatever means possible including workarounds. Problem Management takes the time to identify the root causes of incidents and what needs to be done to eliminate their cause from the environment. PbM supports IM by capturing work-around and temporary fix information, but does not have responsibility for resolving the Incident. Problem Management coordinates the identification of the Root Cause and works with Change Management to implement a permanent resolution to the Known Error. This permanent resolution is aimed at removing all the associated Incidents and preventing them from recurring.

2.4.8 Root Cause Analysis

Root Cause Analysis (RCA) involves researching the underlying cause(s) of problems. The determination of root cause is used to help determine the course(s) of action that will remove systemic issues from the environment.

2.4.9 Known Error

A Known Error is a problem with a documented work-around and an identified root cause. Known Errors can originate from suppliers and development groups. The Problem Manager updates and reviews Known Errors during Proactive Problem Analysis, Problem Closure, and Major Problem Reviews.

2.4.10 Workarounds

Workarounds are temporary mitigations for incidents that are implemented until the problem is resolved. Workarounds are stored in the KEDB. In some cases a work-around can be used for an extended period if a permanent fix is not available or feasible.

2.4.11 Problem Models

Based on past problem resolution activities and best practices, models can be created. Problem Models are predefined steps that should be taken to handle particular types of problems. Analysis teams, including suppliers, can be determined in advance and resolution windows can be anticipated.

2.4.12 Problem

A Problem is an unknown, underlying cause of one or more incidents. Problem Management is responsible for the further investigation of problems in order to determine and mitigate the root cause.

2.4.13 Incident

An Incident is an unplanned interruption, degradation or reduction in IT Service quality.

2.4.14 Event

An Event is a change of state that has significance for the management of a Configuration Item or IT Service.

2.5 Quality Control

2.5.1 Metrics, Measurements and Continual Process Improvement

Continual service improvement depends on accurate and timely process measurements and relies upon obtaining, analyzing, and using information that is practical and meaningful to the process at-hand. Measurements of process efficiency and effectiveness enable the USMC to track performance and improve overall end user satisfaction. Process metrics are used as measurements of how well the process is working, whether or not the process is continuing to improve, or where improvements should be made. When evaluating process metrics, the direction of change is more important than the magnitude of the metric.

Effective day-to-day operation and long-term management of the process requires the use of metrics and measurements. Reports need to be defined, executed, and distributed to enable the managing of process-related issues and initiatives. Daily management occurs at the process manager level. Long-term trending analysis and management of significant process activities occurs at the process owner level.

The essential components of any measurement system are Critical Success Factors (CSFs) and Key Performance Indicators (KPIs).

2.5.2 Critical Success Factors with Key Performance Indicators

The effectiveness and performance of processes are measured using metrics-based KPIs which support high level CSFs. The metrics should be monitored and reported upon in order to judge the efficiency and effectiveness of the process and its operation. To the extent possible, metrics should be broken down by service, customer, priority level, etc. and compared with previous reporting periods.

CSFs are defined as process or service-specific objectives that must be achieved if a process (or IT service) is to succeed. KPIs are the metrics used to measure service performance or progress toward stated goals. Not all CSFs will be focused on at the same time.

The following CSFs and KPIs can be used to judge the efficiency and effectiveness of the process. Results of the analysis provide input to improvement programs (i.e., continual service improvement).

Error! Reference source not found. describes the metrics that shall be monitored, measured and analyzed:

Table 4: PbM Objectives

CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Benefits
1	Minimize the impact of Problems.	1	Number and percentage of Problems by age, status, and priority, per reporting period and totals **Method:** 100% Inspection **Calculation:** Total number and percentage of Problem tickets identified by age, status and priority during reporting period/Total number of Problems for each X 100 during same reporting period	Provides ability to analyze and solve Problems so recurring Incidents are not experienced by customers.
		2	Number and percentage of Known Errors by age, status, and priority, per reporting period and totals **Method:** 100% Inspection **Calculation:** Total number and percentage of Known Error identified by age, status and priority during reporting period/Total number of Known Errors for each X 100 during same reporting period	
		3	Number and percentage of Problems with Workarounds **Method:** 100% Inspection **Calculation:** Total number and percentage of Problems coded with Work-arounds/Total number of Problems X 100	
		4	Number and percentage of Problems detected proactively **Method:** 100% Inspection **Calculation:** Total number and percentage of Problem tickets logged proactively by Problem Management team/Total number of Problems logged X 100	

CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Benefits
2	Improve quality of services being delivered.	2	Number and percentage of Known Errors by age, status, and priority, per reporting period and totals. **Method:** 100% Inspection **Calculation:** Total number and percentage of coded by age, status, and priority during reporting period/Total number of Known Errors during reporting period X 100	Provides early visibility and efficient analysis to assure IT services are being delivered.
		4	Number and percentage of Problems detected proactively **Method:** 100% Inspection **Calculation:** Total number and percentage of Problems detected and coded as Proactive/Total number of Problems detected during that period X 100	
		5	Number and percentage of Problems with Known Errors. **Method:** 100% Inspection **Calculation:** Total number and percentage of Problem tickets identified and coded with Known Errors/Total number of Problems logged during the reporting period X 100	
		6	Number of Incidents associated with each Problem. **Method:** 100% Inspection **Calculation:** Total number and Incidents associated with a Problem/Total number of Incident/Problem records X 100	

CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Benefits
3	Resolve Problems and errors efficiently and effectively.	4	Number and percentage of Problems detected proactively **Method:** 100% Inspection **Calculation:** Total number and percentage of Problems proactively detected/Total number of Problems X 100	Establishes problem resolutions in a timely manner so recurring Incidents are not experienced by customers.
		7	Number and percentage of Known Errors with Change Requests. **Method:** 100% Inspection **Calculation:** Total number and percentage of Known Errors with associated Change requests during reporting period X Total number of Known Errors during reporting period/X100	
		8	Number and percentage of Problems with associated Incidents. **Method:** 100% Inspection **Calculation:** Total number and percentage of Problems associated with Incident tickets/Total number of Problems X 100	
		9	Number and percentage of Problems with associated Events **Method:** 100% Inspection **Calculation:** Total number and percentage of Problems associated with Events/Total number of Problems X 100	

3.0 ROLES AND RESPONSIBILITIES

Each process has roles and responsibilities associated with design, development, execution and management of the process. A role within a process is defined as a set of responsibilities.

Ownership (i.e., accountability): The process owner will serve as the authoritative process point of contact for any higher headquarters (DON or DOD) or adjacent organization engagement or coordination. The process owner will provide oversight of the Problem Management process and ensure Problem Management is executed throughout the classified and unclassified MCIE. The Process Owner will coordinate regularly scheduled process review boards to evaluate the business value provided by Problem Management and to discuss recommended enhancements to the process. This team will use this review to evaluate and improve the Critical Success Factors and the Key Performance Indicators that are utilized to measure the success of the Problem Management Process. Process specific metrics will be developed and monitored to ensure that the KPIs are realistic, measurable and relevant to support the Problem Management process.

The process owner will appoint an Enterprise level process manager to support the Problem Management process.

Management (i.e., responsibility) of the Problem Management process may be shared. A single Enterprise PbM Process Manager exists at the MCNOSC and Regional PbM Process Managers are located at the RNOSC or at the MITSCs depending on regional staffing capabilities. The RNOSC is responsible for Situational Awareness (SA) to the Marine Corps Forces G6 in addition to responsibilities outlined in the Marine Corps Information Environment Concept of Employment. There can also be instances where a single person is responsible for multiple roles. Factors such as Area of Responsibility (AOR), size of user base and size of the process support team dictate exactly which roles require a dedicated person(s) and the total number of people performing each role.

The process manager provides direct support to the process owner by daily operational management of the problem management process. Process Managers report deviations in the processes and recommend corrective action to the respective process owner.

The Figure 4 depicts all the *mandatory* roles.

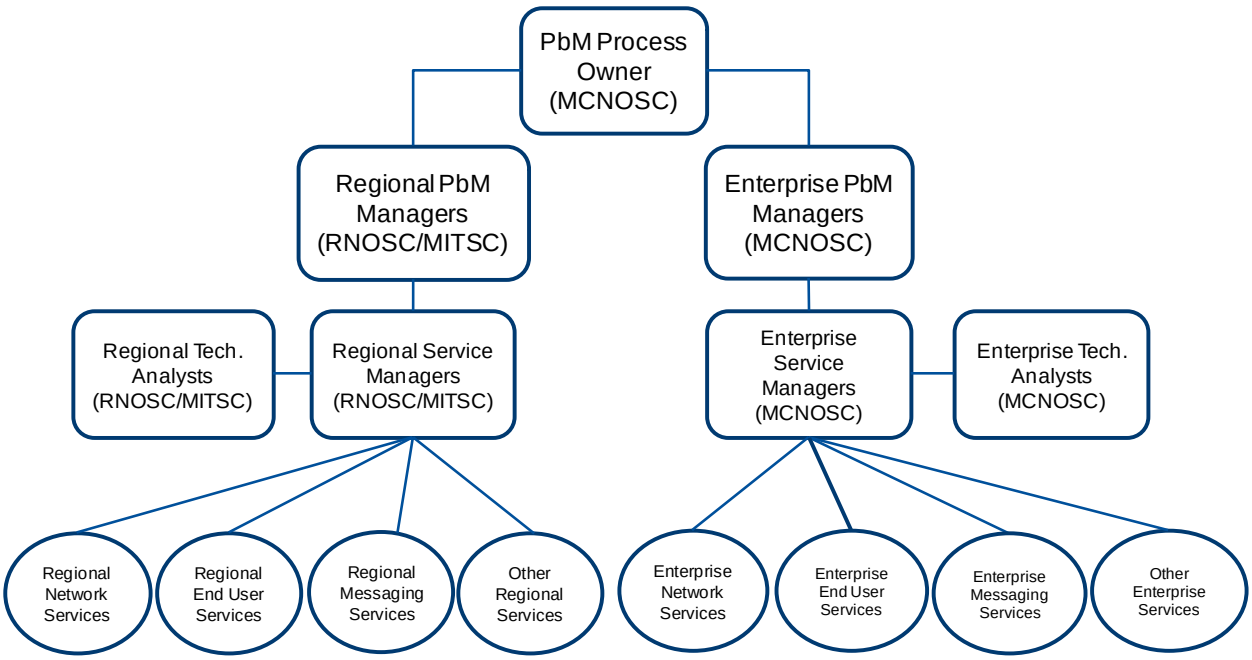

Figure 4: Problem Management Roles

Table 5 describes roles and responsibilities of Problem Management roles:

Table 5: PbM Defined Roles and Responsibilities

Description	Overall Responsibility
Role #1 PbM Process Owner (MCNOSC)	
The Process Owner owns the process and the supporting documentation for the process. The primary functions of the Process Owner are oversight and continuous process improvement. To these ends, the Process Owner oversees the process, ensuring that the process is followed by the organization. When the process isn't being followed or isn't working well, the Process Owner is responsible for identifying and ensuring required actions are taken to correct the situation. In addition, the Process Owner is responsible for the approval of all proposed changes to the process, and development of process improvement plans.	• Reviews and understand all references pertaining to process ownership. • Documents and publicizes the process. • Establishes and communicates the process roles and responsibilities. • Ensures updates to the Process Guide are performed according to the Change Management Process. • Defines the KPIs to evaluate the effectiveness and efficiency of the process. • Reviews KPIs and takes action required resulting from the analysis. • Assist with and being ultimately responsible for the process design. • Ensures the PbM process and tools integrate with other ITSM processes and that requirements for the tools are defined. • Ensure the effectiveness and efficiency of the PbM Process and working practices through continuous improvement. • Reviews any proposed enhancements to the process. • Provides input to the ongoing Service Improvement Plan (SIP). • Addresses any issues with the execution of the process. • Ensures all relevant staff have the required training and are aware of their role in the process. • Ensures that the process, roles, responsibilities and documentation are regularly reviewed and audited. • Interfaces with appropriate organizations to ensure that the process receives the necessary staff resources. • Ensures all stakeholders are sufficiently involved in the PbM

Description	Overall Responsibility
	Process. • Ensures tight linkage between the PbM Process and other related processes. • Ensures organizational adherence to the process.
Role #2 Enterprise PbM Process Manager (MCNOSC)	
The Enterprise PbM Process Manager ensures effective coordination of activities for service quality. The Enterprise PbM Process Manager manages and coordinates all activities necessary to manage all Problems and Known Errors. The Enterprise PbM Process Manager will communicate and coordinate with their regional counterparts (e.g., Regional PbM Process Managers, Service Managers, etc.) when required/beneficial. The Enterprise PbM Process Manager manages the entire Problem Management process life cycle.	• Prioritizes and plans for problems registered. • Communicates with stakeholders, as required. • Informs the Change Manager, if required. • Defers problems, if needed to Regional PbM Process Managers • Decides on investigation of known errors. • Registers Requests for Change or Service Requests to solve known errors. • Conducts problem review and documents lessons learned. • Closes problem tickets and informs stakeholders. • Monitors the problem and known error resolution progress and performs required action. • Periodically performs analysis to see if new problems need to be registered and logged. • Logs problems. • Assigns work to Problem Analytics Group and Regional PbM Process Managers and coordinates root cause analysis. • Registers known errors. • Validates proposed solutions to known errors. • Validates outcome of closed changes and closes known error. • Validates that a problem is solved. • Manages all KEDB input. • Coordinates and conducts Major Problem Reviews.

Description	Overall Responsibility
Role #3 Regional PbM Process Managers (RNOSC/MITSC)	
The Regional PbM Manager manages and coordinates all activities necessary to manage all assigned problems and known errors within their respective region (RNOSC/MITSC). Regional PbM Process Managers will communicate and coordinate with their counterparts when required/beneficial. Regional PbM Process Managers will consult with the Enterprise PbM Process Manager on all regional problems detected and worked on. Regional PbM Process Managers will work through the Service Owners/Managers to coordinate action required in support of the Problem Management process. There will be multiple Regional Process Managers based on regions.	• Prioritizes, coordinates and plans for problems registered by the person in the assigned region and Enterprise PbM Process Manager. • Communicates with stakeholders, when required. • Informs the Change Manager, when required. • Defers problems, if needed, to other Regional PbM Process Managers or Enterprise PbM Process Manager. • Coordinates assignment of Root Cause Analysis through Service Owner/Managers • Decides on investigation of known errors. • Coordinates Requests for Change or Service Requests to solve known errors. • Conducts problem review and documents lessons learned. • Closes problem under management of Regional PbM Process Manager and informs stakeholders. • Monitors the problem and known error resolution progress and performs required action. • Periodically performs analysis to see if new problems need to be logged. • Logs problems. • Coordinates root cause analysis under guidance of Enterprise PbM Process Manager. • Registers known errors in KEDB under guidance of Enterprise PbM Process Manager. • Assigns known error to Problem Analyst Group under guidance of Enterprise PbM Process Manager. • Validates proposed solutions to known errors. • Validates outcome of closed changes and closes known error. • Validates that a problem is solved. • Participates in Major Problem Reviews.
Role #4 Service Managers	
The Service Managers (MCNOSC/MITSC/MCEITS) will represent IT service domain areas (e.g., Network, Messaging, etc.) and be responsible for the oversight of Service Technical Analysts for problems and Incidents assigned.	• Assists as team member of PbM management and IM as necessary to help investigate and find solutions and workarounds. • Supervises and controls workload of service Technical Analysts. • Schedule and assign service work according to priority and maintain an orderly flow of work. • Supervises the training of technicians. • Help technicians diagnose incidents and problems. • Responsible for ESD ticket history and activity input.

Description	Overall Responsibility
Role #5 Technical Analyst	
Technical Analysts are designated by the Enterprise PbM Process Manager in conjunction with the Service Managers, to support the Problem team for root cause analysis and solution development. They use technical knowledge and subject matter expertise to identify Incident trends, identify problems, determine the root cause of problems, and initiate appropriate actions. The group can include, but not limited to, application SMEs, suppliers, architecture SMEs, and other ITSM process managers and analysts. Technical Analysts may also be utilized for Major Problem Reviews.	• Supports the efforts of and is under the management of the Service managers to support Enterprise PbM Process Manager during Investigation and Diagnosis. • Utilizes problem analysis techniques. • Provides effective resolution to the problem in accordance with the service level and DoD/DoN governance. • Identifies the need for a Change Request to resolve the Problem. • Creates workarounds, sometimes in collaboration with other service groups. • Performs problem determination. • Investigates and diagnoses assigned known error tasks for workarounds and/or root cause analysis. • Executes a workaround if applicable, and communicates workarounds to the Service Desk. • Updates Problem Records with the root cause and permanent resolution information. • Updates the closure portion of the PbM record, ensuring the cause code reflects the actual cause of the problem, and all documentation is complete. • Implements a resolution for the Problem unless addressed through a Change. • Responsible for changing, installing and configuring new hardware and software to meet incident resolution or problem fix assigned. • Responsible for testing, repairing and maintaining hardware and software. • Responsible for creating, searching for, modifying, adding additional details, and relating other items to PbM records. • Supports Major Problem Reviews, as requested. • Implements corrective actions and closes known error tasks. • Closes problem tasks as directed by Enterprise or Regional PbM Process Manager(s).

3.1 Responsibilities

Processes may span organizational boundaries; therefore, procedures and work instructions within the process need to be mapped to roles within the process. These roles are then mapped to job functions, IT staff and departments. The process owner is accountable for ensuring process interaction by implementing systems that allow smooth process flow.

The Responsible, Accountable, Support, Consulted, and Informed, (RASCI) model is a method for assigning the type or degree of responsibility that roles (or individuals) have for specific tasks.

Responsible — Completes the process or activity; responsible for action/implementation. The degree of responsibility is determined by the individual with the "A."

Accountable — Approves or disapproves the process or activity. Individual who is ultimately answerable for the task or a decision regarding the task.

Support — Resources allocated to Responsible, and will assist in completing the task.

Consulted — Gives needed input about the process or activity. Prior to final decision or action, these subject matter experts or stakeholders are consulted.

Informed — Needs to be informed after a decision or action is taken. May be required to take action as a result of the outcome. This is a one-way communication.

Table 6 and Table 7 establish process role responsibilities for high-level process activities as they relate to Enterprise and Regional process roles. Process roles transcend organizational boundaries; therefore a role based RASCI chart ensures proper assignment of responsibilities to individuals.

Table 6: Responsibilities for Enterprise PbM Management Roles for an Enterprise Problem

PbM Process Activities	PbM Owner (MCNOSC)	PbM Process Manager (MCNOSC)	Regional PbM Managers (RNOSC/MITSC)	Service Managers	Technical Analysts
Problem Detection	I	AR	S	S	S
Problem Logging	I	AR	S	S	S
Problem Categorization		AR	S	S	S
Problem Prioritization		AR	S	S	S
Problem Investigation and Diagnosis		AR	S	S	S
Problem Known Error Record Creation	I	AR	S	S	S
Problem Resolution	I	AR	S	S	S
Problem Closure	I	AR	S	C	C
Major Problem Review	C	AR	S	S	S

Legend:
Responsible (R) —Completes the process or activity
Accountable (A) — Authority to approve or disapprove the process or activity
Support (S) — Resources allocated to responsible for support
Consulted (C) — Experts who provide input
Informed (I) — Notified of activities

Note: *If Support (S) is assigned, the Consulted (C) is implied.*
Note: *Any department that is designated as Responsible, Accountable, Consulted, or Supportive is not additionally designated as Informed because being designated as Responsible, Accountable, Consulted, or Supportive already implies being in an Informed status.*
Note: *Only one organization can be accountable for each process activity. Enterprise PbM Process Manager is accountable for all process activities.*
Note: *Respective regions will be Responsible for Investigation and Diagnosis, creating Problem Error Control Records and Problem Resolution when assigned by and under the management of the Enterprise PbM Process Manager or Regional PbM Process Manager.*

Table 7: Responsibilities for Regional PbM Management Roles for a Regional Problem

PbM Process Activities	PbM Process Owner (MCNOSC)	PbM Process Manager (MCNOSC)	Regional PbM Managers (RNOSC/MITSC)	Service Managers	Technical Analysts
Problem Detection	I	S	AR	S	S
Problem Logging	I	S	AR	S	S
Problem Categorization		S	AR	S	S
Problem Prioritization		S	AR	S	S
Problem Investigation and Diagnosis		S	AR	S	S
Problem Known Error Record Creation	I	S	AR	S	S
Problem Resolution	I	S	AR	S	S
Problem Closure	I	S	AR	C	C
Major Problem Review	C	S	AR	S	S

4.0 SUB-PROCESSES

The USMC ITSM PbM process consists of seven sub-processes. The following is a description of the Problem Management sub-processes.

4.1 Problem Detection (sub-process 1.0)

The purpose of proactive Problem Management is to find potential problems and errors before they cause incidents. Proactive Problem Management Activity is analytical in nature rather than operational. Proactive analysis relies heavily on accurate, historical data from Incident Management, Change Management, Event Management, and Request Fulfillment. Analysis is performed to identify what types of Incidents and Problems are occurring more frequently. It identifies where similar problems may occur in other places within the infrastructure. It can show that repeated failures have not been adequately resolved and are likely to continue to happen. Analysis results may reveal the need for a problem record to be created or other preventative actions such as training or modifications to business procedures. Problem detection will be done at the MCNOSC, RNOSC, MITSC, and local service desks. At each level, Problem Managers, Service Desk technicians, and Subject Matter Experts, will utilize reports generated from available tools such as Remedy for incidents, and Business Service Management for events, to monitor their Area of Responsibility (AOR).

Why PbM Detection (1.0)?

Ensures problems are detected and action is taken to remove the Problem from the environment.

See Appendix C for Problem Analysis techniques Appendix C.

The following workflow (Figure 5) depicts the Problem Detection sub-process.

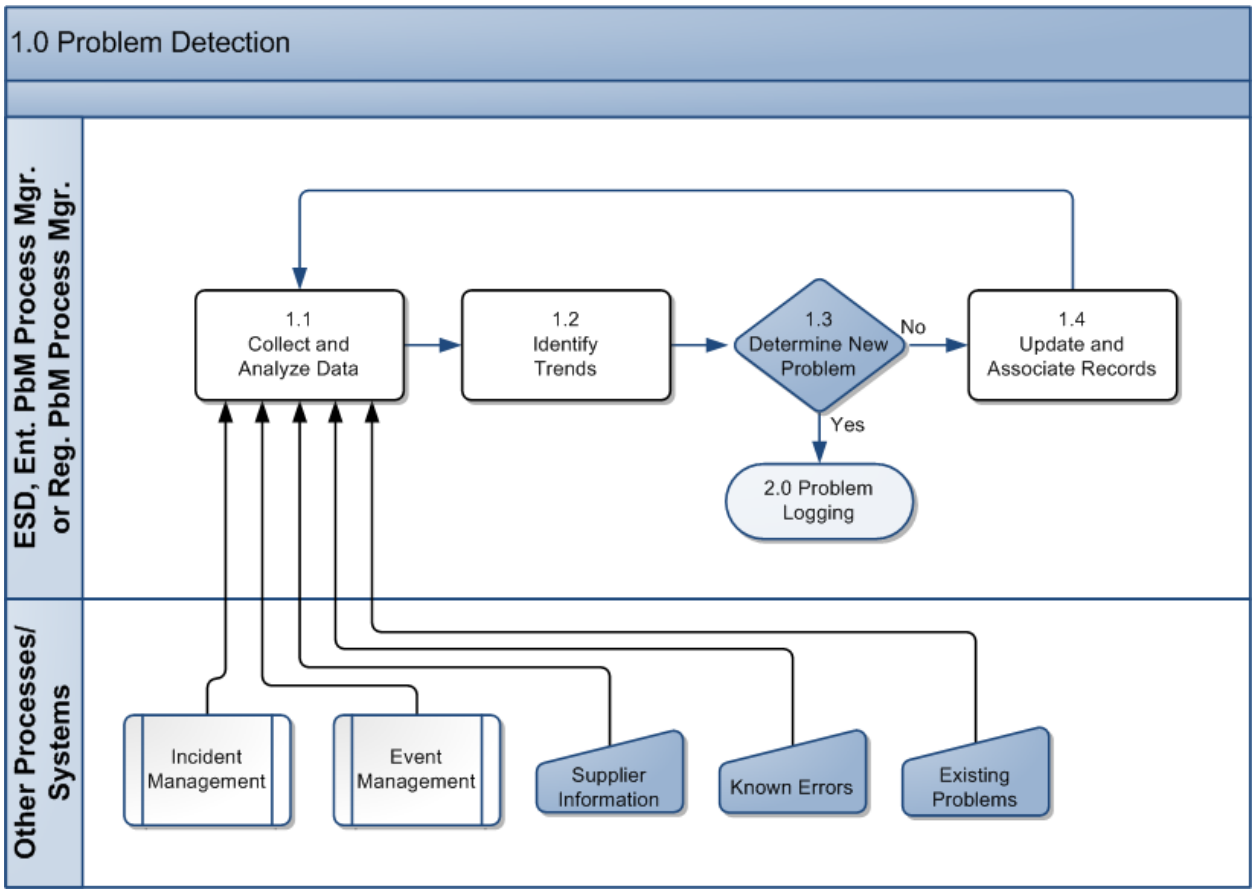

Figure 5: Problem Detection Sub-Process

Table 8 describes the activities in the Problem Detection sub-process.

Table 8: Problem Detection Sub-Process Descriptions

1.0 Problem Detection		
Number	**Process Activity**	**Description**
1.1	Collect and Analyze Data	Definitive data sources are accessed to ensure validity of information used to conduct the analysis. Standard reports provide ongoing views of potential trends which may indicate the presence of a Problem. Ad hoc reporting provides a “drill down” capability to conduct more specific research when indicators and thresholds are triggered.
1.2	Identify Trends	Trend analysis is conducted from various perspectives to identify issues. Analysis of trends related to specific Configuration Items, locations, Services, user profiles, time periods, workgroups, suppliers, and combinations of these attributes.
1.3	Determine New Problem	A problem can be determined by proactively analyzing the incident data for existence of an underlying problem so it can be investigated further. Other detection methods are notification from suppliers; service desk based on incidents;

1.0 Problem Detection		
Number	**Process Activity**	**Description**
		event management triggers; or a technical support groups Yes: Go to 2.0 Problem Logging. No: Continue to Update Problem Records.
1.4	Update and Associate Records	During the analysis, Incident records may be identified that need to be associated with existing Problems. Also, misleading information in the source data may be corrected or enhanced to support future proactive analysis efforts.

4.2 Problem Logging (sub-process 2.0)

Why PbM Logging (2.0)?

Ensures problems are all logged for analysis.

Problems originate via the Service Desk, supplier notifications, or Proactive Problem Management activities. The Enterprise Service Desk/Regional and Local Service Desks may create a Problem based on one or more Incidents where the underlying cause has not been determined. Suppliers may issue bulletins which can be entered as Problems or Known Errors. Based on PbM Work Instructions the ticket will be validated against standard Problem Ticket criteria to ensure that is meets the requirements to be categorized as a Problem. Then all pertinent information must be captured to ensure the Problem can proceed appropriately throughout the life cycle. The Problem record is created in the classified (SIPRNet) or unclassified (NIPRNet) Remedy Action Request System and associated to other Incident or Problem records as reference. USMC, DISA and DoD policies define the criteria for identifying information as classified or unclassified. Specific Work Instructions will dictate the required information that must be included in the initial problem ticket creation.

The following workflow (Figure 6) depicts the Problem Logging sub-process.

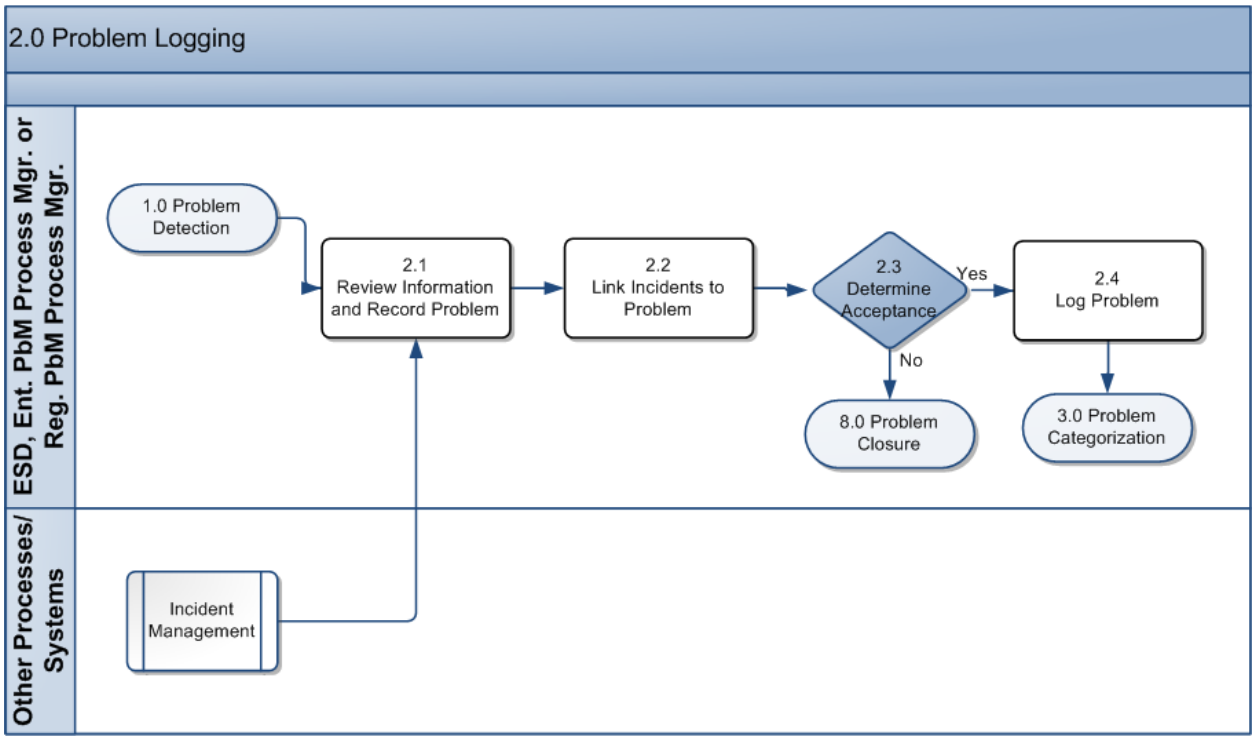

Figure 6: Problem Logging Sub-Process

Table 9 describes the activities in the Problem Logging sub-process.

Table 9: Problem Logging Sub-Process Descriptions

2.0 Problem Logging		
Number	**Process Activity**	**Description**
2.1	Review Information and Record Problem	Ensure sufficient information is captured in the Problem record to support subsequent efforts to analyze and resolve the Problem. Templates and consistent use of standard terms and indicators enhance overall productivity of the process through improved communications.
2.2	Link Incidents to Problem	Incident records and Problem records are associated in the tracking system using links through key identifiers. Associations enable a more thorough analysis during Problem Investigation.
2.3	Determine Acceptance	Ensure that problem has linkages to incident(s). If mistakenly misidentified, then close ticket. If incident(s) cross-referenced, ensure that incident details are included in ticket, then log. Yes: Go to 2.4 Log Problem. No: Cancel Problem and go to 8.0 Problem Closure.
2.4	Log Problem	Log Problem as a Problem ticket in system. Go to 3.0 Problem Categorization.

4.3 Problem Categorization (sub-process 3.0)

Accurate categorization of Problems helps to establish correct routing, enabling a faster time to resolution. Problems are categorized in the same manner as Incidents and use the same criteria. Product categories are leveraged for reporting and routing to functional support groups. One or more product categories will directly align to fields in the tracking system and should ultimately map to IT services to enable metrics and reporting of problems associated with IT services. The Marine Corps product categorization structure contains three tiers designed to quickly and accurately identify technologies, manufacturers, products, versions, and configuration items. Operational categories define the work for a particular problem and related incidents, known errors, or change requests. The Marine Corps operational categorization is also a three-tier structure used to qualify reporting in the system, groups and support staff assignments and to manage the routing of approvals.

Why PbM Categorization (3.0) and Prioritization (4.0)?

Ensures problem tickets are uniformly identified and prioritized based on urgency and impact.

4.4 Problem Prioritization (sub-process 4.0)

Prioritization is consistent with Incident Management. Problem priority determines:

- The type and number of resources necessary to reach the service-level objective for each level of priority (e.g., response, resolution, and updates)
- The criteria used to determine the timing by which technical resources and leadership personnel are engaged to manage the Problem through to resolution and closure

Before a priority determination of a Problem can be reached, the impact and the urgency must be evaluated. Impact plus urgency determines priority. The criteria for determining impact is relative to an organization's echelon, AOR, operations tempo, operational situations and the status of the person(s) impacted. Other relevant aspects of impact to consider include, but are not limited to:

- Number of users affected
- Type of service(s) affected
- Degree to which the service is affected

Urgency is defined as the necessary speed to resolve the Problem and should not be based on the service or the number of users affected. When evaluating urgency consider the user's required time to resolution and the availability of a work-around. Other relevant aspects of urgency to consider include, but are not limited to:

- Operational impact
- VIP status of the impacted user(s)

- Point in time — Is a critical deployment or tactical operation under way that is being impacted? Is a time sensitive business process or operation under way, for example payroll processing?
- Service-level or operating-level targets or objectives
- Risk — Is a combination of the likelihood of a mission disruption occurring and the possible loss that may result from such mission disruption

Table 10 provides general guidance for establishing Problem urgency at the primary echelons, under "normal" operating conditions and involving non-VIP users. The exact required resolution times for echelons, MITSCs, bases, and commands will be determined at the time of implementation.

Table 10: Urgency Matrix

Problem Urgency Matrix	
Level	**Description**
Critical	Immediate resolution is required ○ A work-around (e.g., a temporary, alternative method of achieving the desired action) is not available and the need to achieve the desired action is immediate. -Or- ○ Risk is high that Impact will increase significantly if immediate resolution is not achieved. -Or- ○ The customer billet or mission is such that immediate resolution is required.
High	○ No work-around exists however work can be temporarily shifted to other activities to maintain productivity. -Or- ○ There is plausible risk that Impact will increase if resolution is not achieved.
Medium	○ A work-around exists but productivity is affected. -Or- ○ A system or service is available, but degraded.
Low	○ A work-around exists and/or productivity effect is minimal or nonexistent ○ Routine Work.

By evaluating the impact and urgency, it is possible to assign priority to the Problem, as shown in Table 11.

Table 11: Priority Matrix

URGENCY	IMPACT				
		Extensive / Widespread 9	Significant / Larger 5	Moderate / Limited 3	Minor / Localized 0
Critical 20		Critical 29	Critical 25	High 23	High 20
High 15		Critical 24	High 20	High 18	Medium 15
Medium 10		High 19	Medium 15	Medium 13	Medium 10
Low 0		Low 9	Low 5	Low 3	Low 0

The PbM tool assigns a standard weighting to each combination of urgency and impact just as in Incident Management. The overall priority can be adjusted by increasing or decreasing this weighting without having to modify the actual impact and urgency values. This is the appropriate

method for adjusting the priority as the actual urgency and impact should be accurately reflected in the Problem records.

The following workflow (Figure 7) depicts the Problem Categorization and Prioritization Sub-Processes.

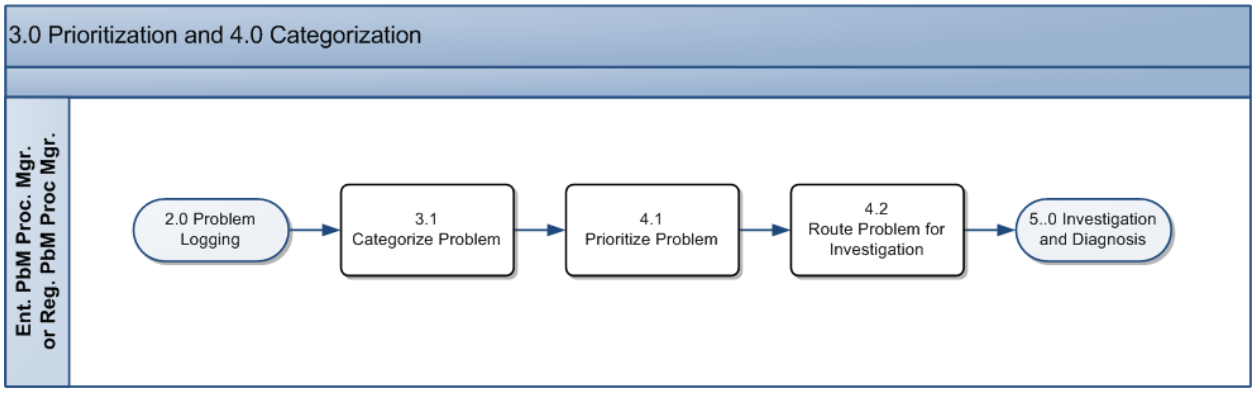

Figure 7: Problem Categorization and Prioritization Sub-Processes

Table 12 describes the activities in the Categorization and Prioritization Sub-Process.

Table 12: Categorization and Prioritization Sub-Process Descriptions

3.0 Problem Categorization and 4.0 Prioritization		
Number	**Process Activity**	**Description**
3.1	Categorize Problem	If there are Incidents associated with the Problem, use the Categorization indicated in the Incident record(s). For Problems with no associated Incidents, follow the guidelines described in the PbM Process Guide Section 3.3.
4.1	Prioritize Problem	If there are Incidents associated with the Problem, use the highest Priority as indicated in the Incident record(s). For Problems with no associated Incidents, follow the guidelines described in the PbM Process Guide Section 3.4.
4.2	Route Problem for Investigation	Based on Problem categorization, the Problem is forwarded to the appropriate Analyst Group for Investigation and Diagnosis (sub-process 5.0).

4.5 Problem Investigation and Diagnosis (sub-process 5.0)

The appropriate level of resources should be allocated based on the impact, urgency and the assigned priority of the Problem. This sub-process includes Root Cause Analysis, creating workarounds, and identification of Known Errors.

Why PbM Investigation and Diagnosis (5.0)?

Ensures Root Cause Analysis is performed and potential workaround is identified and documented.

The KEDB is a database containing all Known Error Records. The data in the database is maintained by Problem Management and used by many different function groups and processes. The purpose of a Known Error Database is to allow storage of previous knowledge of incidents and problems — and how they were overcome — to allow quicker diagnosis and resolution if they reoccur. There will be one Known Error Database utilized across the MCEN, therefore standard data entry rules must be created and adhered to by all parties. Knowledge Management standards are critical to ensure that the data in the KEDB is accurate and reliable.

Workarounds identify measures that can be deployed to temporarily resolve or reduce the impact of Incidents related to problems. They are a temporary means of eliminating or reducing the impact of Incidents related to problems and must be documented in the Problem Record and linked to related Incidents. If a work-around is identified and approved for deployment, this sub-process ensures the work-around is known to be effective.

The techniques (see Appendix E) commonly used for root cause analysis (RCA) include:

- Incident life cycle analysis and Incident trending
- Ishikawa analysis brainstorming sessions
- Pareto analysis (80/20)
- Kepner-Trego Problem Analysis
- Automated modeling tools
- Inductive Reasoning
- Deductive Reasoning

The following workflow (Figure 8) depicts the Problem Investigation and Diagnosis Sub-Process.

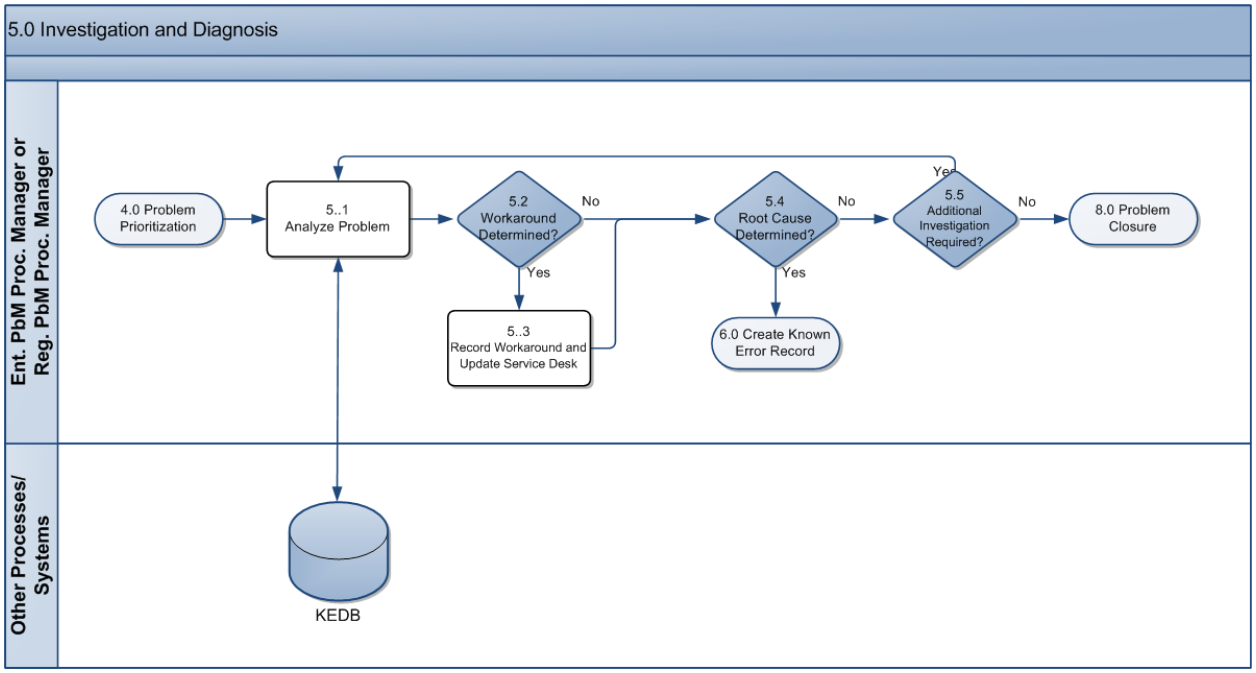

Figure 8: Problem Investigation and Diagnosis Sub-Process

Table 13 describes the activities in the Investigation and Diagnosis sub-process.

Table 13: Problem Investigation and Diagnosis Sub-Process Descriptions

5.0 Problem Investigation and Diagnosis		
Number	**Process Activity**	**Description**
5.1	Analyze Problem	Assemble the appropriate team of resources (e.g., Analyst Group, Service Manager, etc.) and conduct analysis to identify a work-around (as identified in work instructions) and root cause. Access and review Known Error Database (KEDB) for analysis of like Problems. Determine which method of root cause analysis is best based on the nature of the Problem and/or associated Incidents. Refer to Appendix E for examples of industry best-practices Root Cause Analysis techniques (Appendix E).
5.2	Work-around Identified?	During analysis new workarounds may be identified that reduce or eliminate the impact associated Incidents have on the business. Even if Incident Management had identified a work-around to restore normal service operation, it is possible that a better work-around may be identified by the analysis team. Yes: Go to Record Work-around Information and inform the Service Desk. No: Go to Root Caused Determined?
5.3	Record Work-around and Update Service Desk	If there are unresolved Incidents associated with this Problem and the analysis in PbM determines there is a work-around, then update the Problem Database and inform the

5.0 Problem Investigation and Diagnosis		
Number	**Process Activity**	**Description**
		Service Desk.
5.4	Root Caused Determined?	An investigation should be conducted to try to diagnose the root cause of the problem by Regional or Enterprise Problem Manager. As soon as the diagnosis is complete, and particularly where a work-around has been found (even though it may not yet be a permanent resolution), a Known Error Record must be created. Yes: Go to 6.0 Create Known Error Record. No: Go to 5.5 Additional Investigation Required?
5.5	Additional Investigation Required?	There may be specified time periods for Problem resolution for different Services, as documented in Service Level Agreements, Operational Level Agreements, or Underpinning Contracts. Based on Problem urgency and SLA requirements, the Problem Manager must continuously monitor the progress of Problem resolution. Often, an organization establishes limits on the amount of resource applied to particular types of Problem resolution. At the point where the amount of resource being expended exceeds the business value derived from resolving a Problem, work on resolution should cease. This is clearly an Enterprise PbM Process Management decision and should be considered as part of each Problem's life cycle. Yes: Go to 5.1 Analyze Problem. No: Go to 8.0 Problem Closure (sub-process 6.0).

4.6 Create Problem Known Error Record (sub-process 6.0) and Problem Resolution (sub-process 7.0)

When analysis identifies a root cause, a Known Error Record is created that documents the diagnosis and details the underlying root cause. Available approved workarounds are also linked to the Known Error. Known Errors are made available to the Service Desk and other stakeholders via the Known Error Data Base (KEBD). Known Error information is valuable during Incident Management as there may be recurring Incidents related to a Known Error. Having quick access to Known Errors and valid workarounds saves considerable time and effort when resolving Incidents and can contribute to further investigation of related Problems. As Known Errors are detected and documented, further analysis is conducted to outline options for resolving the error(s). After evaluating the various resolution options, a Change Request is submitted to correct the error. Not all Known Errors require changes to be made in the infrastructure. In some cases, the resolution may be increased training or updated procedures. The implementation of the resolution is monitored and tracked and constant communication is established with other E-ITSM processes involved in the change. Once implemented, the resolution is verified and documented in the Problem and Known Error records.

Why PbM Known Error Record (6.0) and Resolution (7.0)?

Known Error Record reduces time spent troubleshooting and captures similar problems for a consolidated effort. Problem Resolution ensures that corrective actions are taken to remove the problem from the

As in the Investigation and Diagnostic task, IT Management must monitor the amount of time and resource allocated to the resolution. There may be Service Level Agreements or Operational Level Agreements that must be met. To contain support costs, organizations often define thresholds to limit investment in Problem resolution.

Once the resolution has been verified as complete, the Problem/Known Error proceeds to Closure.

The following workflow (Figure 9) depicts the Create Known Error Record and Problem Resolution sub-process.

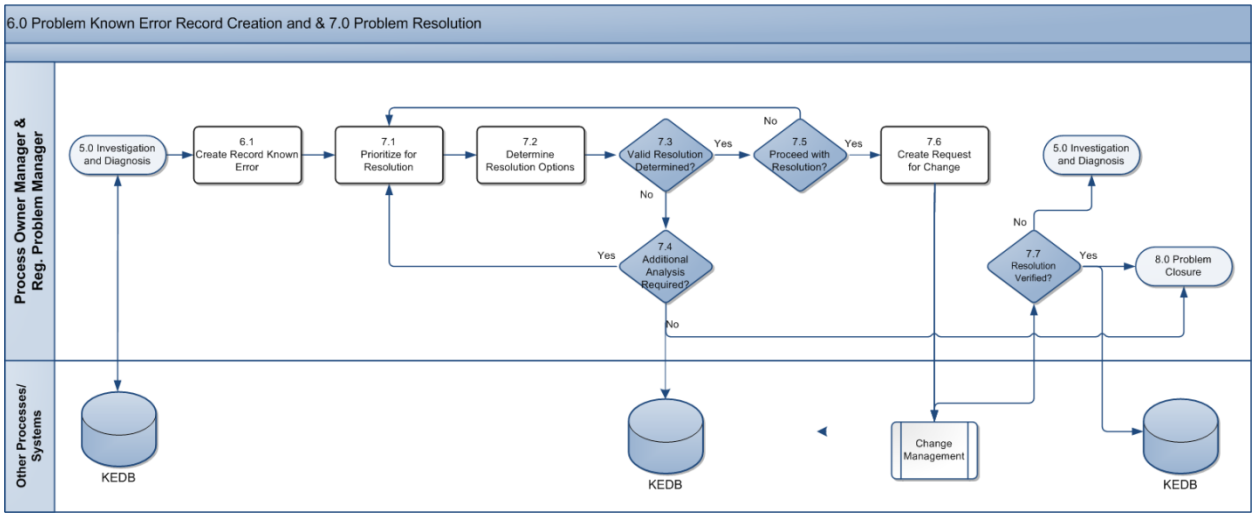

Figure 9: Create Known Error Record and Problem Resolution

Table 14 describes the activities in the Create Known Error Record and Problem Resolution sub-process.

Table 14: Create Know Error Record Sub-process Descriptions

6.0 Create Known Error Record and 7.0 Problem Resolution		
Number	**Process Activity**	**Description**
6.1	Create Known Error Record	A Known Error Record must be raised and placed in the Known Error Database so that if further incidents or problems arise, they can be identified and the service restored more quickly.
7.1	Prioritize for Resolution	Based on urgency and impact, establish a priority for which Problem Records are researched for resolution. Policies are needed as guidance for the amount of time and resource to invest in subsequent tasks. For business reasons, it may make sense to not resolve the Known Errors and continue to use a work-around to minimize impact of Incidents that may occur related to the Known Error. Problems may return to this task (7.4 “Additional Analysis Needed?”) to allow for additional analysis or coordination of new Known Errors with the existing backlog. A “No” decision for 7.5 “Proceed with Resolution” calls re-evaluation of the priority and target date.
7.2	Determine Resolution Options	Evaluate different approaches to resolving the Problem Record. Quantify the cost-benefit of each option to determine which is the best solution.
7.3	Valid Resolution Determined?	Is a resolution option identified? Yes: Go to 7.5 Proceed with Resolution? No: Go to 7.4 Additional Analysis Required?
7.4	Additional Analysis Required?	If a resolution option is not identified, IT Management decides whether to continue expending resource on analysis. Once an established threshold is reached, a business decision must be made whether to continue or re-allocate resources to other activities. Yes: Go to 7.1 Prioritize for Resolution. No: Update KEDB and Go to 8.0 Problem Closure.

6.0 Create Known Error Record and 7.0 Problem Resolution		
Number	**Process Activity**	**Description**
7.5	Proceed with Resolution?	Yes: Go to 7.6 Create Request for Change. No: Go to 7.7 Reprioritize Problem? If business decisions dictate that the recommended resolution not be implemented, this Problem will be reprioritized or closed in conjunction with current business priorities.
7.6	Create Request for Change	RFC raised for approval and implementation of problem resolution via solution or work-around. Following guidance from the Change Management process, submit a Change Request for the preferred resolution option.
7.7	Reprioritize Problem?	Yes: Go to 7.1 Prioritize for Resolution for new assessment of priority and target date. No: Go to 8.0 Problem Closure.
7.8	Resolution Verified?	After submission of a Change Request, monitor progress until notified that the Change has been released into the desired environment (Production, QA, etc.) Verify that the root cause of associated Problems has been eradicated and no Incident occurs when related test cases are run. This task may rely on results produced by the Service Validation and Testing process to ensure proper testing based on best practices. Within that process, ample functional testing is performed along with appropriate regression testing and end-user testing. The KEDB should be used to help resolve quickly any further occurrences of the incidents/problems that occur. Yes: Go to 8.0 Problem Closure. No: Go to 5.0 Investigation and Diagnosis.

4.7 Problem Closure (sub-process 8.0)

The Problem Records are audited for completeness and accuracy. The Problem Manager closes the Problem/Known Error record and any related Problem/Known Error records. If there are any remaining associated Incidents, this will be communicated to the appropriate Incident Management personnel or Service Desk.

The following workflow (Figure 10) depicts the Problem Closure sub-process.

Why PbM Closure (8.0)?

Ensures all problem tickets are closed and properly reviewed for Continual Service Improvement.

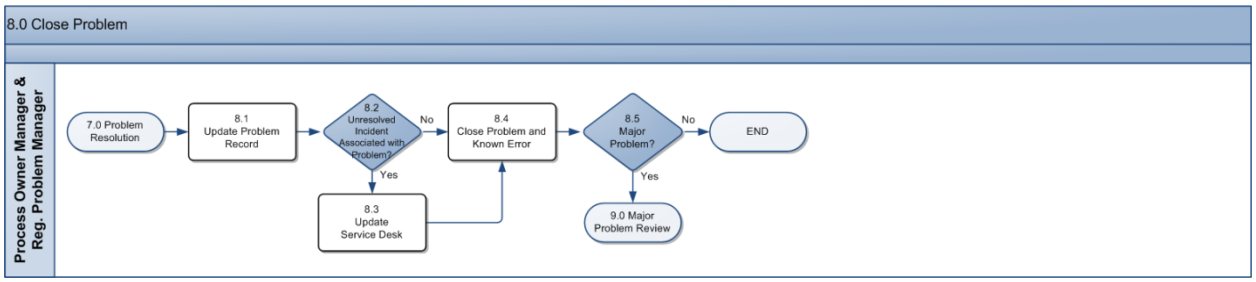

Figure 10: Problem Closure Sub-Process

Table 15 describes the activities in the Problem Closure sub-process.

Table 15: Create Know Error Record Sub-process Descriptions

8.0 Problem Closure		
Number	**Process Activity**	**Description**
8.1	Update Problem Record	Any remaining documentation that needs to be captured in the Problem record is entered into the tracking tool. Also, any inconsistencies in associations to Incidents and/or Events are corrected.
8.2	Unresolved Incident Associated w/Problem?	Yes: Go to Update Service Desk. No: Go to Close Problem and Known Error.
8.3	Notify Service Desk	A communication is distributed to the appropriate Incident manager(s) or Service Desk Manager to inform them of the resolved Known Errors and to identify those unresolved associated incidents. Then the unresolved incidents are reviewed by Problem Management and the process returns to 2.1 Review Information and Record Problem. This new problem will then go back through the PbM Cycle for resolution. And the appropriate Incident manager(s) are notified of the new PbM Ticket created.
8.4	Close Problem and Known Error	Update the status of the Problem and Known Error to indicate they are closed.
8.5	Major Problem?	Was this a Major Problem based on approved criteria? Yes: Go to 9.0 Major Problem Review. No: End Process.

4.8 Major Problem Review (sub-process 9.0)

A Major Problem is any priority one problem (the severity or impact was high). The scope of the review will include process, actions of staff as well as tools, and the environment.

Why PbM Review (9.0)?

Ensures that high impact incidents are analyzed and process flaws are corrected.

Major Problem Reviews will be initiated within 5 business days (on a weekly basis) after the Problem is closed. Only problems considered major based on approved criteria are subject to this review process. The Problem Manager determines which review team is appropriate and initiates the review. The team's purpose is to determine how the Known Error was initially introduced into the environment, assess what went well and what did not go well across the Problem life cycle. This review is used to address shortfalls that led to the problem and identify needs to prevent further incidents. The goal is to find shortcomings and address any changes to processes, SOPs, training, supplier relationships, and/or governance to avoid future Incidents and Problems. A formal Major Problem Report is the output of the Major Problem Review Team. The general criteria include:

- What did we do right?
- What did we get wrong?
- How can we improve for the future?
- How do we prevent a recurrence?
- Were any third parties involved?
- What are follow-up Actions?

The following workflow (Figure 11) depicts the Major Problem Review sub-process.

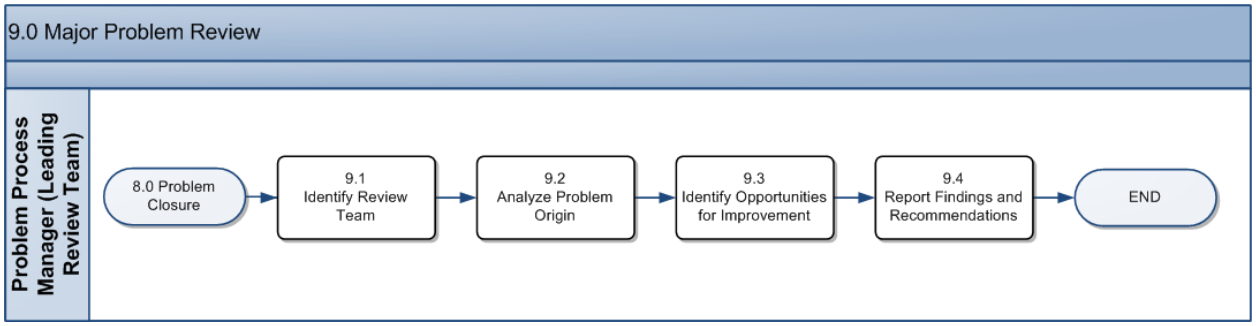

Figure 11: Major Problem Review Sub-Process

Table 16 describes the activities in the Major Problem Review sub-process.

Table 16: Major Problem Review Sub-process Descriptions

9.0 Major Problem Review		
9.0	**Process Activity**	**Description**
9.1	Identify Review Team	The Enterprise Problem Process Manager determines the composition of the review team and schedules the review sessions. It is recommended that the review team for Major Problem Review be a different group than the team that originally assessed the Problem.
9.2	Analyze Problem Origin	Reviews for Major Problems have a different purpose than analysis to determine root cause. However, many of the same root cause analysis techniques may be applied. There will be different problem statements and potential causes which require brainstorming or analysis. For example, instead of analyzing what might be the cause of a failure in the infrastructure, the analysis focuses on how the failure was introduced into the environment. Instead of thinking about which part of the infrastructure is failing, the focus is on how the failed component passed all quality checks and verifications. The Major Problem Review also examines the methods and procedures used for root cause analysis.
9.3	Identify Opportunities for Improvement	Analysis continues until all possibilities are analyzed. The findings are reviewed and improvement recommendations are selected for documentation.
9.4	Report Findings and Recommendations	The Major Problem Review Report is produced and distributed to all stakeholders. Included in the distribution may be the Service Owner, Service Manager, Process Owner, all Regional Problem Managers, and Service Level Managers.

APPENDIX A — ACRONYMS

The official list of E-ITSM acronyms can be found on the Enterprise Information Technology Service Management site (https://eis.usmc.mil/sites/irm/ITSM/default.aspx). The link to the document is referenced below:

https://eis.usmc.mil/sites/irm/ITSM/Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Firm%2FITSM%2FDocuments%2FE%2DITSM%20Acronym%20List&FolderCTID=0x0120001918760B7D35A5478C0474985E3ACBCD&View={9CD820B3-EF85-4D2C-BD0C-A255AEE9E40D}

APPENDIX B — GLOSSARY

Term	Definition
Asset Management	Asset Management is the process responsible for tracking and reporting the financial value and ownership of assets throughout their life cycle.
Back-out Plan	A Back-out Plan is developed in the Release planning phase. This plan provides a recovery plan to return to the original configuration or process if the release fails to achieve the planned outcome.
Backup	Backup is copying data to protect against loss of integrity or availability of the original data.
Change Schedule	A Change Schedule is a document that lists all approved changes and their planned implementation dates.
Configuration Control	Configuration Control is a sub-process of Configuration Management. Configuration Control is a set of processes and approval stages required to change a CI attribute. Configuration Control encompasses the oversight to ensure that a CI is changed through the Change Management process.
Configuration Identification	A sub-process of Configuration Management, Configuration Identification is the selection, identification, and labeling of the configuration structures and CIs including their respective technical owner and the relationships between them. CIs become the manageable unit that is planned for release into a configuration controlled environment. The CIs consist of hardware, software, services, and documentation.
Configuration Item	A Configuration Item (CI) is 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 (CMS) and is maintained throughout its life cycle 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.
CI Type	CI Type is a category used to Classify CIs. The CI Type identifies the required attributes and relationships for a configuration record. Common CI Types include: server, document, user, etc.
Configuration Management Database	A Configuration Management Database (CMDB) is a database used to store configuration records throughout their life cycle. The Configuration Management System (CMS) maintains one or more CMDBs and each CMDB stores attributes of CIs and relationships with other CIs.
Configuration Management Plan	Document defining how configuration management will be implemented (including policies and procedures) for a particular acquisition or program. (Source: MIL HDBK-61A)
Configuration Management System	A Configuration Management System (CMS) is a set of tools and databases used to manage an IT service provider's configuration data. The CMS also includes information about incidents, problems, known errors, changes, and releases and may contain data about employees, suppliers, locations, units, customers and users. The CMS includes tools for collecting, storing, managing, updating and presenting data about all CIs and their relationships. The CMS is maintained by Configuration Management and is used by all IT Service Management processes.
Deployment	Deployment is 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.
Deployment Readiness Test	A Deployment Readiness Test is conducted to ensure that the deployment processes, procedures, and systems can deploy, install, commission, and decommission the release package and resultant new or changed service in the production/deployment environment.
Deployment Verification Test	A Deployment Verification Test is conducted to ensure the service capability has been correctly deployed for each target deployment group or environment.

Term	Definition
Early Life Support	Early Life Support (ELS) involves Technical Management or IT Operations providing support for a new or changed IT service for a period of time after it is released. During ELS, the IT service provider may review the KPIs, service levels, and monitoring thresholds and provide additional resources for incident management and problem management (when implemented).
EM System	The EM System (EMS) is composed of tools which monitor CIs and provide event notifications. It is a combination of software and hardware which provides a means of delivering a message to a set of recipients. The EMS often requires real-time interaction, escalation, and scheduling.
Environment	Environment is a subset of the IT infrastructure used for a particular purpose (e.g., live environment, test environment or build environment). It is possible for multiple environments to share a CI (e.g., test and live environments may use different partitions on a single mainframe computer). In the term physical environment, environment can be defined as the accommodation, air conditioning, power system, etc. Environment can be used as a generic term defined as the external conditions that influence or affect something.
Error	An Error is a design flaw or malfunction that causes a failure of one or more CI 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	Escalation is an activity that obtains additional resources when needed to meet service-level targets or customer expectations.
Event	An Event is a piece of data that provides information about one or more system resources. Most events are benign. Some events show a change of state which has significance for the management of a CI or IT service. The term 'event' is also used to define an alert or notification created by any IT service, CI, or monitoring tool. Events typically require IT operations personnel to take actions and often lead to incidents being logged.
Event Correlation	Event correlation involves associating multiple related events. Often, multiple events are generated as a result of the same infrastructure fault. Events need correlation to prevent duplication of effort in resolving the original fault.
Exit and Entry Criteria (Pass/Fail)	These are criteria (defined well in advance and accepted by the stakeholders) defined at authorized points in the Release and Deployment Process to set expectations of acceptable/unacceptable results.
Fault	Fault is the deviation from *normal* operation of a CI or a series of CIs. A fault is a design flaw or malfunction that causes a failure of one or more CIs or IT services. Fault is also referred to as an error.
Governance	Governance is the process of ensuring 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.
Incident	An Incident is an unplanned interruption, degradation or reduction in IT Service quality.
Key Performance Indicator	A Key Performance Indicator (KPI) is a metric 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 are selected to ensure that efficiency, effectiveness, and cost-effectiveness are all managed.
Known Error	A Known Error is a problem that has a documented root cause and a work-around. Known errors are created and managed throughout their life cycle by Problem Management. Known errors may also be identified by SIE or suppliers.
Known Error Database (KEDB)	A database containing all Known Error Records. This database is created by Problem Management and used by Incident and Problem Management.
Major Problem	A Major Problem is any problem where the severity or impact was such that the Enterprise Problem Process Manager decides to review the entire series of activities.
Monitoring	Monitoring is the process of repeated observation of a CI, IT service, or process to detect events and to ensure that the current status is known.

Term	Definition
Notification	Notification is a communication that provides information.
Problem	A problem is defined as 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. The problem record in Service Manager documents the entire life cycle of a single problem.
Process	A Process is 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 needed.
Quality Assurance	Quality Assurance (QA) is the process responsible for ensuring the quality of a product and also ensuring it will provide its intended value.
Role	A Role refers to a set of connected behaviors or actions that are performed by a person, team, or group in a specific context.
Severity	Severity refers to the level or degree of intensity.
Root Cause Analysis	An Activity that identifies the Root Cause of an Incident or Problem. RCA typically concentrates on IT Infrastructure failures.
Service Design Package	A Service Design Package (SDP) is composed of document(s) defining all aspects of an IT service and its requirements through each stage of its life cycle. An SDP is produced for each new IT service, major change, or IT service retirement.
Service Improvement Plan	A Service Improvement Plan (SIP) is a formal plan to implement improvements to a process or IT service.
Service Knowledge Management System	A Service Knowledge Management System (SKMS) is a set of tools and databases used to manage knowledge and information. The SKMS includes the Configuration Management System (CMS) 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 life cycle of IT services.
Service Level Agreement	A Service-Level Agreement (SLA) is 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.
Service Validation and Testing	Service Validation and Testing is the process responsible for validation and testing of a new or changed IT service. Service Validation and Testing ensures an IT service matches the design specification and will meet the needs of the business. Service Validation and Testing during release conducts testing in the pre-production System Integration Environment (SIE) and during deployment in the pilot production environment.
Single Point of Contact	A Single Point of Contact (SPOC) is an agreement used to assign a single, consistent way to communicate within an organization or unit. For example, the Service Desk will be the SPOC for a service provider.
Snapshot	A Snapshot is the baseline as captured by a discovery tool. A snapshot can also be called a benchmark.
Test	A Test is an activity that verifies that a CI, IT service, or process meets its specification or agreed requirements.
Test Environment	A Test Environment is a controlled environment used to test CIs, builds, IT services, and processes.
Throttling	Some events do not need to be acted on until they have occurred a number of times within a given time period. This is called Throttling. Once a repeated event has reached its limit for repetition, forward that event to be acted upon.
User Acceptance Testing	User Acceptance Testing is a testing activity conducted by the user intended to verify a CI, IT service, or process meets a specification. It is also used to validate whether agreed requirements have been met.

Term	Definition
Work-around	Work-arounds for problems are documented in known error records and are intended to reduce or eliminate the impact of an incident or problem for which a full resolution is not yet available. Work-arounds for incidents that do not have associated problem records are documented in the incident record.
Work Instruction	The Work Instruction is a document containing detailed instructions that specify exactly what steps are followed 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.

APPENDIX C — PROBLEM SOLVING TECHNIQUES

Technique	Description
Brainstorming Session	This is a focused group effort, comprising specialist groups to identify and think of all factors that may have an effect or identify a Problem.
Ishikawa Diagram	Also referred to as a cause-and-effect diagram, tree diagram, or fishbone diagram. This technique displays the factors that affect a particular quality characteristic, outcome or Problem.
5-Whys	This is a question-asking method used to explore the cause/effect relationships underlying a particular Problem.
Kepner-Tregoe	Guides the search for causes of a Problem. This technique is often referred to as the “Is-Is Not Diagram.” By isolating the Who, What, When, Where and How regarding an event, it narrows investigation to factors that have an impact.
Flow Diagrams	Flow diagrams are used to illustrate the workflow of specific processes or data flows.
Inductive Reasoning	Form a predicted conclusion by observing past regularities and resemblances.
Deductive Reasoning	Form a conclusion based upon patterns of common sense.

C.1 Brainstorming Session

There are four basic rules in brainstorming. These are intended to reduce the social inhibitions that occur in groups and therefore stimulate the generation of new ideas. The expected result is a dynamic synergy that will dramatically increase the creativity of the group.

- **Focus on quantity:** This rule is a means of enhancing divergent production, aiming to facilitate problem solving through the maxim, quantity breeds quality. The assumption is that the greater the number of ideas generated, the greater the chance of producing a radical and effective solution.
- **No criticism:** It is often emphasized that in group brainstorming, criticism should be put 'on hold'. Instead of immediately stating what might be wrong with an idea, the participants focus on extending or adding to it, reserving criticism for a later 'critical stage' of the process. By suspending judgment, one creates a supportive atmosphere where participants feel free to generate unusual ideas.
- **Unusual ideas are welcome:** To get a good and long list of ideas, unusual ideas are welcomed. They may open new ways of thinking and provide better solutions than regular ideas. They can be generated by looking from another perspective or setting aside assumptions.
- **Combine and improve** ideas: Good ideas can be combined to form a single very good idea, as suggested by the slogan "1+1=3.” This approach is assumed to lead to better and more complete ideas than merely generating new ideas alone. It is believed to stimulate the building of ideas by a process of association.

Set the problem: One of the most important things to do before a session is to define the Problem. The Problem must be clear, not too big, and captured in a definite question such as “What service for mobile phones is not available now, but needed?” If the Problem is too big, the chairman should divide it into smaller components, each with its own question. Some Problems are multi-dimensional and non-quantified, for example “What are the aspects involved in being a

successful entrepreneur?" Finding solutions for this kind of problem can be done with morphological analysis (problem-solving).

Create a background memo: The background memo is the invitation and informational letter for the participants, containing the session name, Problem, time, date, and place. The Problem is described in the form of a question, and some example ideas are given. The ideas are solutions to the Problem, and used when the session slows down or goes off-track. The memo is sent to the participants at least two days in advance, so that they can think about the Problem beforehand.

Select participants: The chairman composes the brainstorming panel, consisting of the participants and an idea collector. Ten or fewer group members are generally more productive than larger groups. Many variations are possible but the following composition is suggested.

- Several core members of the project who have proved themselves.
- Several guests from outside the project, with affinity to the problem.
- One idea collector who records the suggested ideas.

Create a list of lead questions: During the brainstorm session the creativity may decrease. At this moment, the chairman should stimulate creativity by suggesting a lead question to answer, such as Can we combine these ideas? Or How about a view from another perspective? It is advised to prepare a list of such leads before the session begins.

Session conduct: The chairman leads the brainstorming session and ensures that the basic rules are followed. The activities of a typical session are:

- A warm-up session, to expose novice participants to the criticism-free environment. A simple problem is brainstormed, for example, what should be the next corporate Christmas present? Or what can be improved in Microsoft Windows?
- The chairman presents the problem and gives a further explanation if needed.
- The chairman asks the brainstorming panel for their ideas.
- If no ideas are coming out, the chairman suggests a lead to encourage creativity.
- Every participant presents his or her idea, and the idea collector records them.
- If more than one participant has ideas, the chairman lets the most associated idea be presented first. This selection can be done by looking at the body language of the participants, or just by asking for the most associated idea.
- The participants try to elaborate on the idea, to improve the quality.
- When time is up, the chairman organizes the ideas based on the topic goal and encourages discussion. Additional ideas may be generated.
- Ideas are categorized.
- The whole list is reviewed to ensure that everyone understands the ideas. Duplicate ideas and obviously infeasible solutions are removed.

- The chairman thanks all participants and gives each a token of appreciation.

The process:

- Participants who have an idea but no possibility to present it are encouraged to write down their idea and present it later.
- The idea collector should number the ideas, so that the chairperson can use the number to encourage quantitative idea generation, for example: We have 44 ideas now, let's get it to 50!
- The idea collector should repeat the idea in the words he or she has written it, to confirm that it expresses the meaning intended by the originator.
- When more participants are having ideas, the one with the most associated idea should have priority. This to encourage elaboration on previous ideas.
- During the brainstorming session the attendance of managers and superiors is strongly discouraged, as it may inhibit and reduce the effect of the four basic rules, especially the generation of unusual ideas.

C.2 Ishikawa Diagram

The Ishikawa diagram, also referred to as a cause-and-effect diagram, tree diagram, or fishbone diagram, displays the factors that affect a particular quality characteristic, outcome, or Problem. The diagram is named after its developer, Kaoru Ishikawa (1915-1989), a leader in Japanese quality control.

An Ishikawa diagram is typically the result of a brainstorming session in which members of a group offer ideas on how to improve a product, process or service. The main goal is represented by the trunk of the diagram, and primary factors are represented as branches. Secondary factors are then added as stems, and so on. Creating the diagram stimulates discussion and often leads to increased understanding of a complex Problem. Japanese Circle members often post Ishikawa diagrams in a display area where they are accessible to managers and other groups. In the United States, Ishikawa diagrams are included in presentations by plant personnel to management or Customers.

Step 1 — Identify and clearly define the Problem to be analyzed

- Decide on the Problem to be examined. Problems are stated as particular quality characteristics, Problems resulting from work, etc.
- Use Operational Definitions. Develop an Operational Definition of the Problem to ensure that it is clearly understood.

Step 2 — Draw the SPINE and create the Problem box.

- Draw a horizontal arrow pointing to the right. This is the spine.
- To the right of the arrow, write a brief description of the effect or outcome which results from the process. EXAMPLE: Low Network Availability
- Draw a box around the description of the effect.

Step 3 — Identify the main CAUSES contributing to the problem being studied.

- These are the labels for the major branches of your diagram and become categories under which to list the many causes related to those categories.
- Establish the main causes, or categories, under which other possible causes will be listed. Use category labels that make sense for the diagram you are creating. Here are some commonly used categories:
    - Methods, materials, machinery, and people
    - People, Process, Technology
    - Environment — a potentially significant category
- Write the main categories your team has selected to the left of the effect box, some above the spine and some below it.
- Draw a box around each category label and use a diagonal line to form a branch connecting the box to the spine.

Step 4 — For each major branch, identify other specific factors which may be the CAUSES of the problem

- Identify as many causes or factors as possible and attach them as sub branches of the major branches.
- Fill in detail for each cause. If a minor cause applies to more than one major cause, list it under both.

Step 5 — Identify increasingly detailed levels of causes and continue organizing them under related causes or categories.

- Accomplish this by asking a series of why questions.

  Note: OFTEN the Five Whys are implemented in conjunction with the Ishikawa diagram.

Step 6 — Analyze the diagram.

- Analysis helps identify causes that warrant further investigation.
- Look at the "balance" of your diagram, checking for comparable levels of detail for most of the categories.
- A thick cluster of items in one area may indicate a need for further study.
- A main category having only a few specific causes may indicate a need for further identification of causes.
- If several major branches have only a few sub branches, try to combine them under a single category.

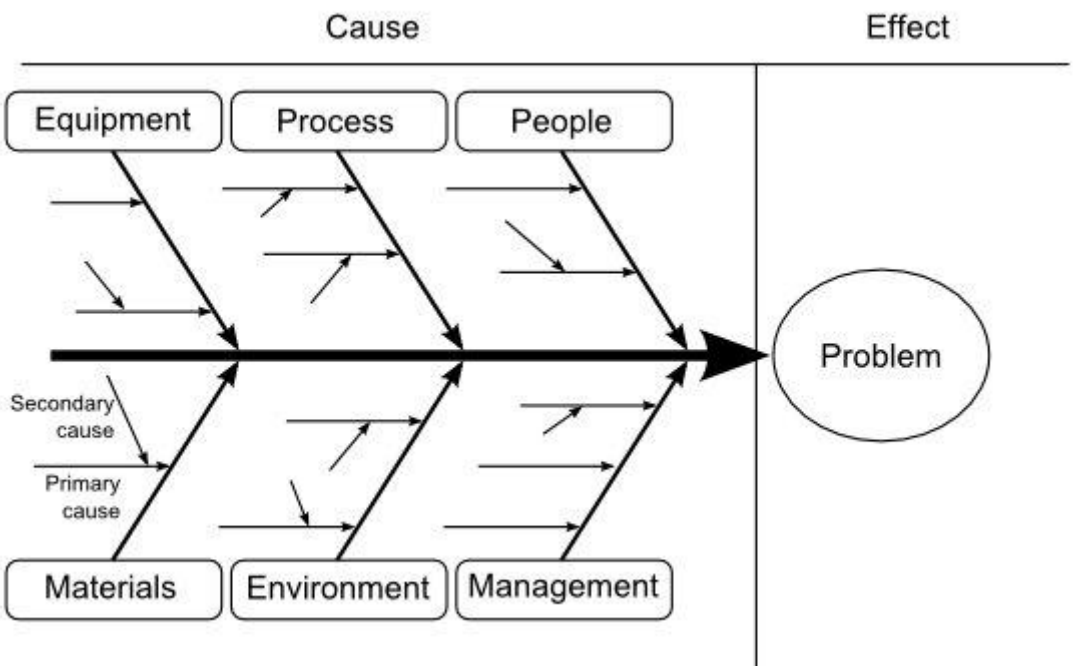

Figure 12: Sample Ishikawa Diagram
Source: Creatingtalent.com

C.3 5-Whys

The 5-Whys is a question-asking method used to explore the cause/effect relationships underlying a particular Problem. Ultimately, the goal of applying the 5-Whys method is to determine the Root Cause of an Error or Problem.

The following example demonstrates the basic process:

My car will not start. (the Problem)

1. **Why?** The battery is dead. (first why)
2. **Why?** The alternator is not functioning. (second why)
3. **Why?** The alternator belt has broken. (third why)
4. **Why?** The alternator belt was well beyond its useful service life and has never been replaced. (fourth why)
5. **Why?** I have not been maintaining my car according to the recommended service schedule. (fifth why, root cause)

The questioning for this example could be taken further to a sixth, seventh, or even greater level. This would be legitimate, as the "five" in 5 Whys is not gospel; rather, it is postulated that five iterations of asking why is generally sufficient to get to a Root Cause. The real key is to encourage the troubleshooter to avoid assumptions and logic traps and instead to trace the chain

of causality in direct increments from the effect through any layers of abstraction to a Root Cause that still has some connection to the original Problem.

C.4 Kepner-Tregoe

The technique of Kepner-Tregoe guides the search for causes of a Problem. This technique is often referred to as the "Is-Is Not Diagram." By isolating the Who, What, When, Where, and How regarding an event, it narrows investigation to factors that have an impact.

Further information on the Kepner-Tregoe methodology is found at http://www.kepner-tregoe.com and in *The New Rational Manager*.[1]

C.5 Flow Diagrams

Flow diagrams are used to illustrate the workflow of specific processes or data flow. Use basic flow chart symbols to document the flow and the connectors between points. This will help illustrate any weak points, or identify troubled areas. When specific points are identified, these points can be looked at in greater detail and verified against current changes in the infrastructure. This technique is usually combined with the Ishikawa Diagram for troubleshooting specific areas.

C.6 Inductive Reasoning

Inductive reasoning works the opposite of Deductive reasoning. We move from specific observations to broader generalizations and theories. Informally, we sometimes call this a "bottom up" In inductive reasoning, we begin with specific observations and measures, begin to detect patterns and regularities, formulate some tentative hypotheses that we can explore, and finally end up developing some general conclusions or theories.

C.7 Deductive Reasoning

Deductive reasoning works from the more general to the more specific. Sometimes this is informally called a "top-down" approach. We begin with thinking up a *theory* about the root cause of our problem. We then narrow that down into more specific *hypotheses* that we can test. We narrow down even further when we collect *observations* to address the hypotheses. This ultimately leads us to be able to test the hypotheses with specific data — a *confirmation* (or not) of our original theories.

[1] Kepner, Charles Higgins; Tregoe, Benjamin B. (1997). *The New Rational Manager*. Princeton Research Press. ISBN: 0971562717.