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

IN REPLY REFER TO:
IRM 2300-04C
C4
14 Nov 17

From: Director, Command, Control, Communications and Computers (C4)

Subj: ENTERPRISE INFORMATION TECHNOLOGY SERVICE MANAGEMENT INCIDENT MANAGEMENT PROCESS GUIDE

Ref: (a) MCO 5271.1B

Encl: (1) IRM-2300-04C

1. PURPOSE. The purpose of the Enterprise Information Technology Service Management (E-ITSM) Incident Management Process Guide is to update the previously defined foundation for process implementation and execution across the Marine Corps Enterprise Network (MCEN). Process implementation and execution at lower levels (e.g., Regional, Local, and Programs of Record) must align with and adhere to directives and schema documented within this guide. 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. IRM-2300-04B

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 Cyberspace Operations Group.

6. SPONSOR. The sponsor of this technical publication is HQMC C4, Network, Plans and Policy Division (CP).

P. G. ANTEKEIER
By direction

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.
DISTRIBUTION: PCN 18623000400

Enterprise IT Service Management
Incident Management
Process Guide

Release Date:
14 November 2017

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	
09/21/2009	0.1			Draft Release
		Printed Name	Printed Name	
11/24/2009	1.0			Initial Release
		Printed Name	Printed Name	
12/03/2009	1.1			Updated as per RFAs post CR
		Printed Name	Printed Name	
06/18/10	2.0			Updated as per CRMs from follow-on Task Order 13, CDRL L0012
		Printed Name	Printed Name	
08/24/10	3.0			Updated as per CRMs from follow-on Task Order 13, CDRL L0012
		Printed Name	Printed Name	
12/17/10	4.0			Updated as per CRMs from follow-on Task Order 13, CDRL L0012
		Printed Name	Printed Name	
02/17/11	5.0			Updated as per CRMs from follow-on Task Order 13, CDRL L0012
		Printed Name	Printed Name	
04/14/11	6.0			Updated as per CRMs from the follow-on E-ITSM Task Order, CDRL L3000
		Printed Name	Printed Name	
3/29/13	7.0			Updated per MCATS tasker to Process Owners for documentation updates
		Printed Name	Printed Name	
8/23/2013	7.1			Updated high level diagrams and sent to MITSCs for review and updated per MITSC feedback
		Printed Name	Printed Name	
04/04/2014	7.2			Updated diagram 2-1 and minor changes
		Printed Name	Printed Name	
04/23/2014	7.3			Adjudicated minor changes from MITSCs (added Problem Management to Investigation and Diagnosis step)
		Printed Name	Printed Name	
08/12/14	7.4			Updated cover page logo and standardized content in section 1 for consistency across the Enterprise.
		Printed Name	Printed Name	
03/24/15	8.0			

		Printed Name	Printed Name	Updated with Process Owner and Regional inputs for current process operation
10/27/15	8.1			Updated KPI Thresholds and Objectives based on feedback from IM Community
		Printed Name	Printed Name	
05/12/16	8.2	Brian LeBar	Brian LeBar	Added additional KPIs for # of incident record transfers and # of reassignments. Included additional measurable metrics as Appendix D. Inserted relationship with Availability Management. Added definition of Transfer and Availability and updated definition of Escalation in Glossary. Added Training section.
		Printed Name	Printed Name	
07/12/17	8.3	Brian LeBar	Brian LeBar	Adjudicated and updated based on comments in CRM
		Printed Name	Printed Name	

Table of Contents

List of Tables

List of Figures

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 Enterprise Network (MCEN). 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 1-1.

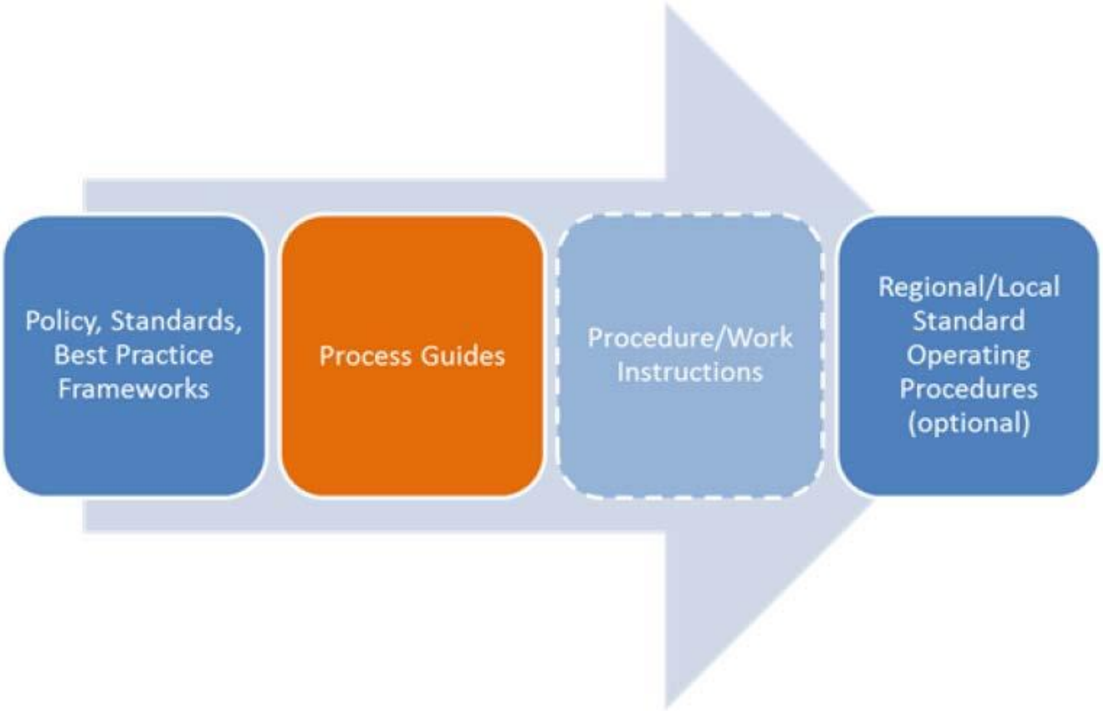

Policy, Standards, Best Practice Frameworks
Process Guides
Procedure/Work Instructions
Regional/Local Standard Operating Procedures (optional)

Figure 1-1 Process Document Continuum

1.2 Scope

The scope of this document covers all services provided in support of the MCEN 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 MCEN as managed by Marine Corps Cyber Operations Group (MCCOG) 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 1-1 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 1-1 Document Design Layers

	ENTITIES	DOCUMENTS GENERATED
LEVEL A	Federal Government Department of Defense (DOD) Department of the Navy (DoN) Marine Corps Headquarters	Statutes/Laws DoD Issuances DoN Policies Marine Corps Orders/IRMS
LEVEL B	MARFORCYBER HQMC C4 Marine Corps System Command (MCSC)	MCOs IRMs (Process Guides) Directives MARADMINS
LEVEL C	Marine Corps Cyberspace Operations Group (MCCOG) MITSC	Regional Procedures Work Instructions
LEVEL D	Marine Corps Bases Marine Corps Posts Marine Corps 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 5271.1 Information Resource Management (IRM) Standards and Guidelines Program.

2.0 PROCESS OVERVIEW

2.1 Purpose, Goals, and Objectives

The purpose of Incident Management (IM) is to ensure that Marine Corps IT users are able to resume their work as quickly as possible following a disruption or degradation to an IT Service, thereby minimizing the adverse impact on the Marine Corps mission. IM is principally a reactive process; its processes provide guidance on investigation, diagnosis, and escalation procedures required to quickly restore services.

Primary objectives of the IM process include:

- Provide a consistent repeatable process to track incidents to ensure:
  - Incidents are properly logged and routed and status is accurately reported
  - Queue of open/unresolved incidents are visible and reported
  - Incidents are completed correctly to ensure that valuable data is available to make informed business decisions
  - Incidents are properly prioritized and handled in the appropriate sequence
  - Resolution provided meets the defined Service Level requirements
- Dynamically assigning service resources to efficiently align IT work against mission objectives via incident prioritization
- Maintaining a constant and accurate link with the Service Desk (SD) function to continually improve the relationship between end users and IT operations

The USMC Service Desk(s), act as a functional component of the IM process, by providing a point of contact for the USMC, enabling the users to quickly and easily interface with IT operations. The Regional Service Desks (RSDs) provide Tier 1 and Tier 2 support for end user services throughout the MCEN. The Service Desk(s) (including the MCEN Enterprise Service Desk (ESD)) allow standard IT issues to be resolved in a centralized, consolidated manner supportive of best practices and Enterprise visibility. Support provided by the USMC Service Desk(s) include desktop application support (e.g., Microsoft Office products, Microsoft Explorer, and Adobe Reader), Windows operating system troubleshooting, and basic print and scanner support. The MCEN ESD in Kansas City serves as the Enterprise Toolset Access Manager and provides support services to the RSDs across the USMC such as training materials, customer services support, user advocacy, quality assurance, reporting, and information management. IM Enterprise Tier 3 support is accomplished through the MCCOG. The MCCOG directs global network operations and defense of the MCEN by providing and facilitating seamless infomation exchange in the support of Marine and Joint Forces (e.g., Enterprise messaging, switches, and routers).

To ensure accurate categorization, prioritization, routing, transfers, data integrity and consistent incident lifecycle processing, the following are USMC Incident Management operational capability goals:

- Field incidents and reports
- Own and manage incident records across the Enterprise
- Coordinate IM actions across all USMC IT organizations
- Monitor status updates, proactively ensuring incidents are resolved or escalated within pre-defined thresholds
- Manage and control queues that are in the supported Area of Responsibility (AoR)
- Ensure IM performance objectives are met
- Manage communications flowing back and forth across the Enterprise
- Support all reported incidents, including fixing technical faults, logging and categorizing incidents and answering queries

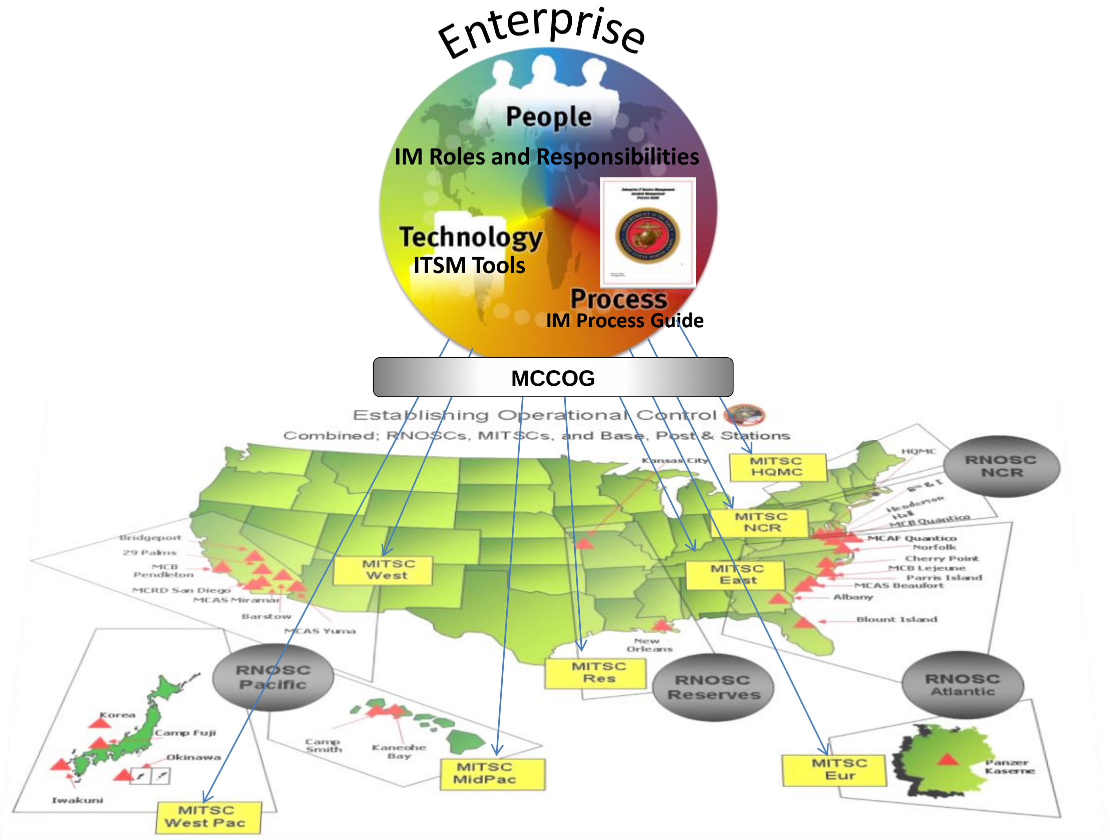


Figure 2-1 Enterprise Incident Management

Figure 2-1 depicts how Enterprise processes, technology, people and standardization support Enterprise Incident Management. Incidents are created, updated, resolved, and closed in the Enterprise Incident Management module of the ITSM tool. When incidents are reported to the Regional Service Desk(s), the Service Desk will log and manage the incident according to the Enterprise Incident Management process. Incidents may be escalated to Tier 2 or Tier 3 support as required for resolution. The entity that creates the incident record is responsible for monitoring and controlling that record through the incident lifecycle.

2.2 Relationships with Other Processes

All IT Service Management processes are interrelated. The processes in Figure 2-2 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 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 developed processes. This figure depicts key relationships between IM and the other processes. This figure is not all-encompassing and the relationships shown can be direct or indirect.

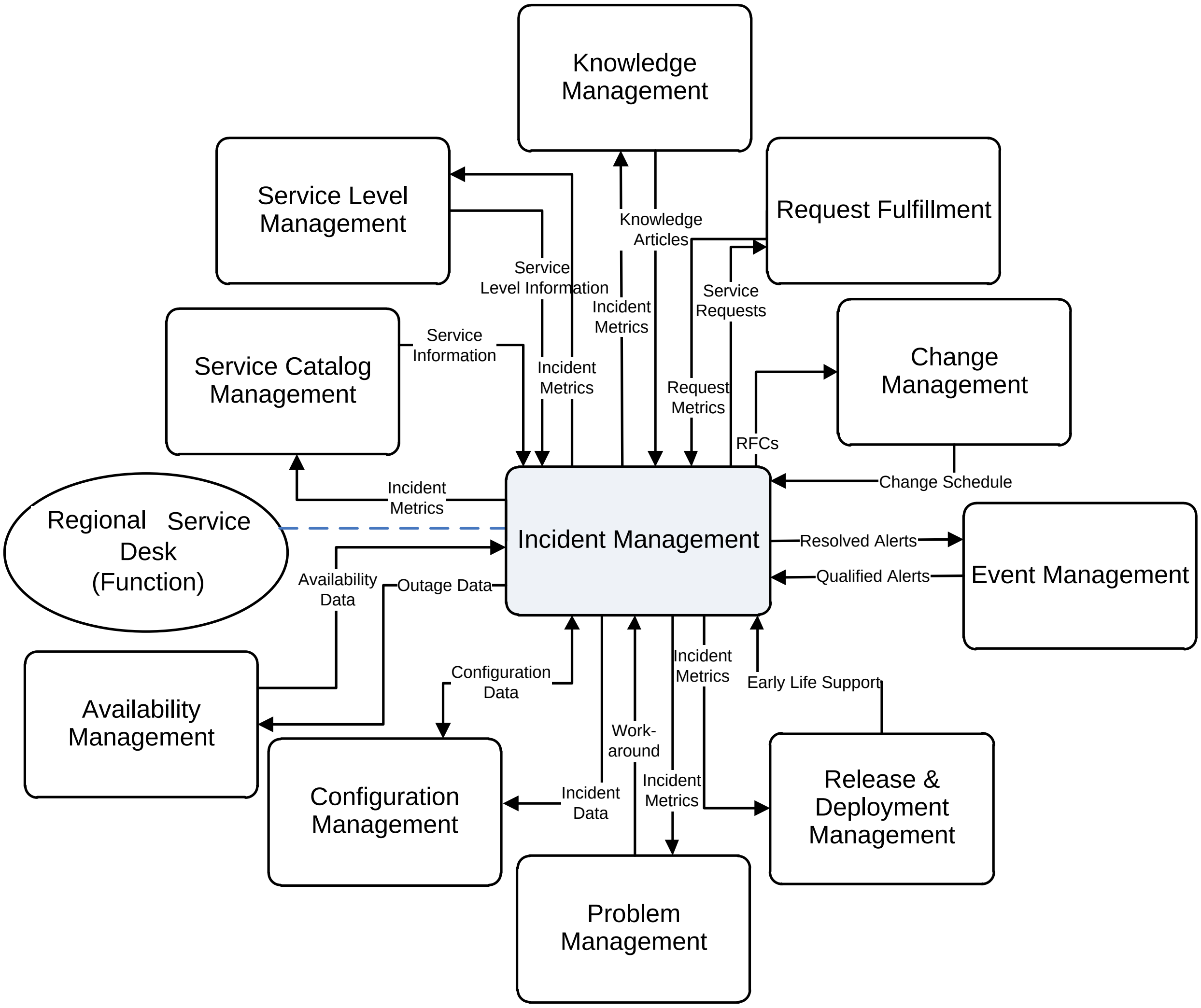


Figure 2-2 IM Relationship with Other Processes

The following list describes the IM relationship (input or output) to other processes, as depicted in Figure 2-2:

Event Management (EM)

- Qualified Alerts: Events generated via the Event Management process and enabling technologies that meet predefined incident criteria result in creation of incidents to be managed through the Incident Management lifecycle.
- Resolved Alerts: Resolved Alerts are communicated back to the originating Qualified Alert.

Service Catalog Management (SCM)

- Incident Metrics: Incident Management provides metrics regarding the health and welfare of services present in the IT Service Catalog.
- Service Information: The SC will provide service information in support of incident classification and prioritization.

Change Management (ChM)

- RFCs: Some incidents will require a Request for Change (RFC) to execute corrective actions and restore service.
- Change Schedule: The Change Schedule is a valuable tool for the Service Desk and other key Incident Management process stakeholders for the purposes of initial diagnosis and troubleshooting. Determining “what changed?” is on the critical path to rapid restoration of service. The Change Schedule can provide quick, valuable insight into this activity.

Configuration Management (CfM)

- Configuration Data: Configuration data, present in the Configuration Management Database (CMDB), provides troubleshooting information to the Service Desk and the Incident Management process for the purposes of troubleshooting, diagnosis, and resolution of incidents.
- Incident Data: incidents are linked to Configuration Items (CIs) in the CMDB. This provides the Service Desk and other interested parties information regarding the disposition of CIs and associated services, systems and applications.

Release and Deployment Management (RDM)

- Early Life Support: Early Life Support is the additional expert service support provided immediately after deployment to ensure service continuity and stakeholder satisfaction. RDM proactively supports deployment activities in the Early Life Support (ELS) process step by providing Incident Management an advanced level of training, documentation, and high-touch support as the new service is introduced into production.

- Incident Metrics: incident metrics associated with releases are critical to continual process improvement.

Request Fulfillment (RqF)

- Service Requests: Calls that originate as incidents may be rerouted to Request Fulfillment if they involve standard, low-risk changes.
- Request Metrics: Request metrics help determine efficiency and effectiveness of handling standard changes and can provide information for service improvement.

Problem Management (PbM)

- Incident Metrics: Incident data is important input for investigation of root cause. Incident metrics are analyzed over periods of time to identify trends that may indicate previously unidentified problems.
- Work-arounds: Work-arounds enhance the effectiveness and efficiency of Incident resolution. Work-arounds are validated upon successful root cause analysis.

Service Level Management (SLM)

- Incident Metrics: Incident management enables SLM to define measurable responses to service disruptions. It also provides reports that enable SLM to review Service Level Agreements (SLAs) objectively and regularly.
- Service Level Information: Incident Management is able to assist in defining where services are at their weakest, so that SLM can define actions as part of the service improvement plan.

Knowledge Management (KM)

- Incident Metrics: All data, metrics, and information useful for Incident Management activities must be properly gathered, stored and assessed.
- Knowledge Articles: Standard methods for addressing incidents are documented in knowledge articles, ensuring efficient and effective resolution of incidents. Careful documentation of steps needed to resolve incidents will result in lower tier analysts being able to provide a greater level of service, quicker resolution of incidents and reducing overall costs.

Availability Management (AvM)

- Input from Incident: Provides information around incidents occurring due to a failure in the IT services or infrastructure components, resulting in unplanned downtime (outage) for Availability analysis. This information is relative to the IT services, software/applications, or infrastructure components affected and, at initial level, includes the start timestamp of the outage and concludes with the timestamp the outage is resolved and IT services, software/applications, or infrastructure components are again available to the users.

- Output to Incident: Provides information to Incident related to planned and unplanned downtime to IT services, software/applications, or infrastructure components for diagnosis and recovery options. For planned downtime, this information is coordinated via Change authority/approval (Forward schedule of Change - FSC), and Release calendars/schedules, and typically regards upgrades, enhancements, refresh, and patches that require a planned downtime to effect. For unplanned downtime, Availability provides diagnosis assistance and recovery options to assist in the Incident investigation. Availability also provides availability data reporting to Incident Management to support investigation of incidents.

2.3 High-Level Process Model

The IM process consists of twelve distinct sub-processes and is integrated with other ITSM Processes (ie. EM process). The following workflow depicted in Figure 2-3 shows these processes and sub-processes that collectively enable and underpin IM. See Section 4.0 for complete descriptions of the sub-process activities.

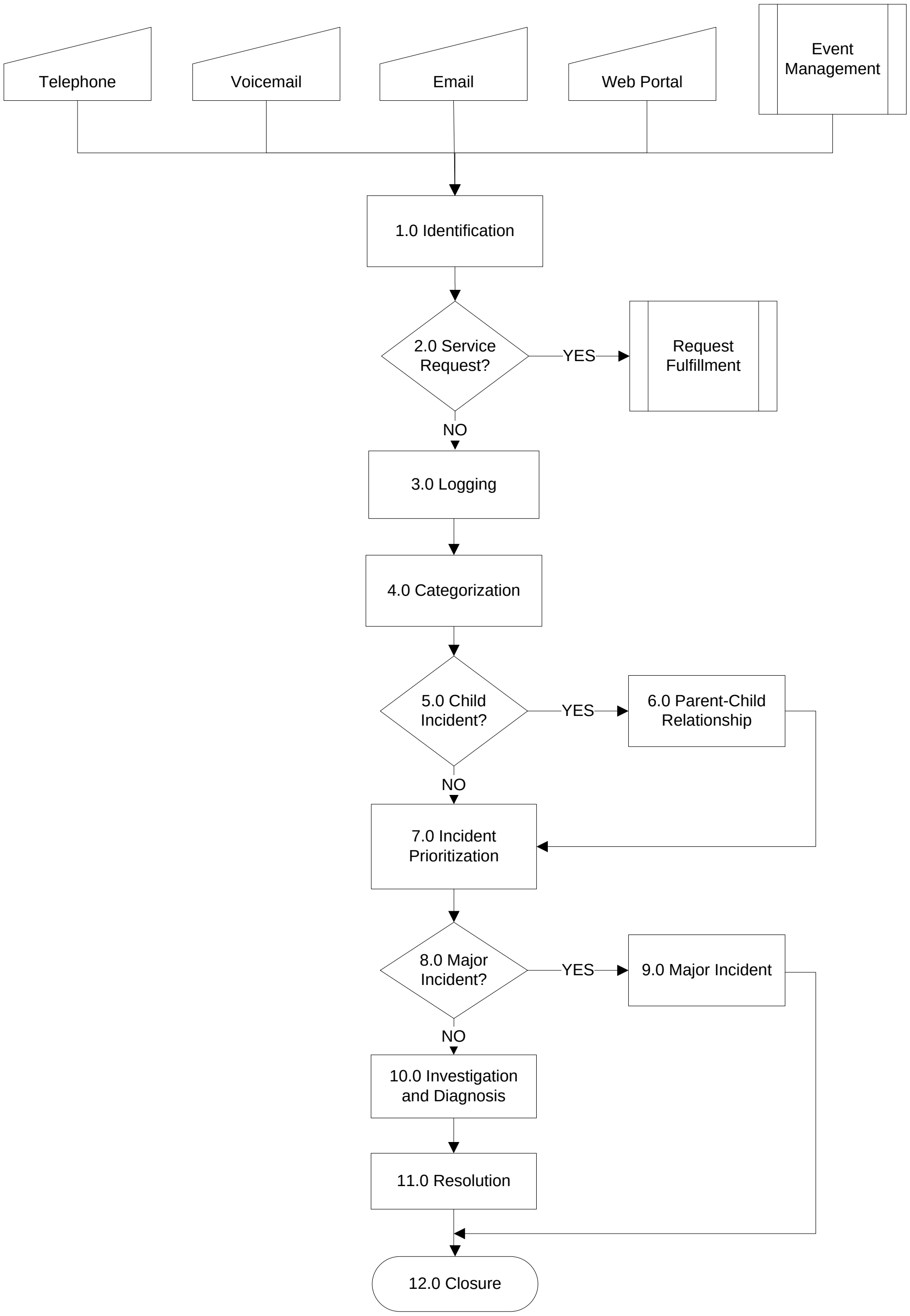


Figure 2-3 High-level IM Workflow

Table 2-1 contains descriptions of each process activity of the Incident Management process. Detailed descriptions are provided in Section 4.0 of this guide.

Table 2-1 IM Process Activity Descriptions

Number	Process Activity	Description
1.0	Identification	Analyst determines the appropriate classification of system (i.e., SIPRNet or NIPRNet) where the record will be logged. Records may be initiated at a user's request or as a result of proactive system monitoring.
2.0	Service Request Decision	Decision point that moves a Request Fulfillment record to its own predefined process for action.
	Request Fulfillment Process	Process responsible for managing the lifecycle of all service requests, as described in the Request Fulfillment Process Guide.
3.0	Logging	Establishes the information relevant to each record entered, including date/time, name and contact information of originator and other significant information to maintain lifecycle accountability for the record. As activities to resolve an incident occur, the record is updated so that a full history is maintained.
4.0	Categorization	Specifies the type of incident being recorded based on generic origin and symptoms. The USMC incident categorization taxonomy employs operational and product categories.
5.0	Child Incident Decision	Decision point that moves the flow of records that have a parent record into this specialized process to ensure related records are handled effectively.
6.0	Parent-Child Relationship	Sub-process responsible for managing related incidents.
7.0	Prioritization	Priority is determined through a combination of urgency and impact and determines how the incident is handled both by the support tools and staff. Factors such as loss of service, rules for VIPs, and other agreed upon requirements are considered in this step.
8.0	Major Incident Decision	Decision point that moves the flow of a record into a special Major Incident procedure for efficiency and timeliness.
9.0	Major Incident	Major incidents typically have a high impact and urgency. Tactical, VIP, timing and service considerations may trigger a Major Incident and these records are identified to ensure escalation and handling through a special sub-process.
10.0	Investigation and Diagnosis	Analyst follows established courses of action to resolve the incident. This step may also involve hierarchical or functional escalation to other support groups or processes.
11.0	Resolution	When a potential resolution has been identified, it is applied and tested. Analyst must ensure that recovery is complete and that service has been fully restored. Analyst updates the record if any changes in categorization are required and reviews or documents procedures for future reference. The user confirms that the incident has been resolved. Analyst determines whether this is a recurring problem and if Problem Management should be involved.
12.0	Closure	Analyst determines user's satisfaction with the handling of the incident. Prior to the incident record closure, the analyst confirms that the incident has been categorized correctly and that adequate work history notes have been completed.The incident is then closed.

2.3.1 Process Description

The primary goal of the IM process is to restore normal service operation as quickly as possible and minimize the adverse impact on operations, thus ensuring that the best possible levels of service quality and availability are maintained. Normal service operation is defined as service operation within Service-Level Agreement(s) (SLA), Memorandum(s) of Understanding (MOU), Memorandum(s) of Agreement (MOA), or other Service Level requirements.

The scope of the IM process includes a standard set of processes, procedures, responsibilities, and metrics utilized by Enterprise NIPRNet and SIPRNet-related services applications, systems and network support teams.

2.4 Key Concepts

The following describe key concepts that are utilized in this IM Process Guide:

2.4.1 Commander's Critical Information Requirements

Commander's Critical Information Requirements (CCIR) is the commander's "need to know immediately" information and response requirements. From Marine Corps Warfighting Publication (MCWP) 3-40.2 Information Management, "CCIR are tools for the commander to reduce information gaps generated by uncertainties that the commander may have concerning their 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 Incident Management, CCIRs are a basis for hierarchical escalations.

All commands are required to produce command specific CCIR guidance with detailed ITSM 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 Incident

An incident is an unplanned interruption or reduction in service quality to an IT service. Incidents can include, but are not limited to, hardware and software errors. Incident records can be reported and manually created using methods such as secure email, a phone call to the Service Desk or a secure web form. Furthermore, incident records can be "auto" generated via input from other systems or processes such as Event Management.

Throughout the lifecycle of an incident, each incident record will be owned and monitored, to include closure, by the support organization that created it. The owner of the incident is responsible for tracking progress, MOU or MOA compliance, keeping stakeholders informed, and incident closure. An incident record can be resolved by a regional support organization that the incident has been assigned or transferred to, however, because the incident record is "owned" by the organization that created it, the creator of the record is responsible for closing it.

2.4.3 Incident Status

An Incident Record passes through a lifecycle on the path to closure. Incident Record status codes identify the stages of the work toward incident resolution, which is critical for reporting and for continual process improvement. Guidance for status designations are shown inTable 2-2.

Table 2-2 Incident Status Designations

Status	Designation
New	Incident has been identified and logged
Assigned	Incident has been assigned to a queue
Pending	Waiting on input from third party
In-Progress	The assigned technician is working on resolving the incident
Resolved	Incident has been resolved and is pending acknowledgment
Cancelled	User contacts the Service Desk and cancels the incident
Closed	Incident record closed

2.4.4 Notification

Notification is defined as the activity by which a stakeholder is notified of incidents or when an incident status change occurs. Notifications are required throughout the incident management lifecycle. Notification mechanisms may include: official message, unclassified email, classified email, self-service access, phone call, etc. In addition to other means of notification, notification for incidents that are high risk, high priority, or high visibility will be sent via an official message.

2.4.5 Operational Impact

Operational impact is defined as an outage or incident that has significantly altered, hindered, or impacted current operations/missions as determined by the major command, base, station or deployed force.

2.4.6 Problem Management

A problem is a cause of one or more incidents. The root 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 management database contains information pertaining to actual or potential disruptions of service that are being analyzed to determine their root cause. Individuals who are attempting to resolve incidents may find that similar incidents are listed in the problem management database, which means that Problem Management is aware of the situation and is attempting to find a resolution.

The Known Error Database (KEDB) contains all known error records. Each known error record documents the lifecycle of the error, including the status, root cause, and workaround.

2.4.7 Work-Around

A work-around is a means of reducing or eliminating the impact of an incident or problem for which a resolution is not yet possible.

2.4.8 Tiered Support

There are five support tiers.

- **Tier 0:** Tier 0 is self-help. End users attempt to diagnose their issues and resolve the incident without assistance. **Information Systems Coordinators (ISCs)** serve as a user's first-response for IT support. They do not have system administrative permissions (by default); instead train users, troubleshoot basic issues, liaison with the local Service Desk, perform data calls, and disseminate policy. The ISC also may assist the Responsible Officer with inventory control, and supply management.

- **Tier 1:** Tier 1 analysts are responsible for keeping the user apprised of the status of the incident record, tracking the incident record until verification of user satisfaction, and performing incident record closure. Tier 1 analysts strive for first call resolution using all available capabilities within the MCEN.
- **Tier 2:** Tier 2 provides functional escalation/transfer support. The 2nd Tier analyst's primary focus is diagnosis and resolution. The 2nd Tier Analyst Staff consists of personnel with greater (but still generalist) technical skills or greater system privileges than the Tier 1 Analyst.
- **Tier 3:** Tier 3 is an Enterprise level capability for more complex or specialized escalation support. The Tier 3 analyst has subject matter expertise and/or higher level system access required to resolve incidents. This role focuses on complex issues related to operational aspects that cannot be resolved at Tiers 1 and 2. This role performs in-depth technical incident investigation, diagnosis and resolution, and provides knowledge and training support.
- **Tier 4:** Tier 4 is comprised of vendors, contractors or other organizations such as USCYBERCOM, HQMC I&L, HQMC PP&O, and DISA that are outside the influence or governance of the USMC E-ITSM processes.

2.4.9 Enterprise Very Important Person (eVIP)

Within nearly every organization there are individuals referred to as Enterprise Very Important Persons (eVIPs) who require an enhanced level of response and/or support. eVIP is defined across the USMC as "General Officers or their Senior Executive Service (SES) civilian equivalents." Based upon the total number of eVIPs within a particular region, a MITSC is allocated additional manpower resources. C4 maintains and reviews the eVIP listing.

2.4.9.1 Very Important Person (VIP)

MITSCs are authorized to locally designate other individuals as VIPs; however, services are provided to them at the MITSCs own expense. Furthermore, it is at the discretion of the Watch Officer (WO) to evaluate tactical, priority, operations tempo and "point in time" factors and, when appropriate, temporarily escalate certain normal users to VIP status.

2.5 Quality Control

2.5.1 Metrics, Measurements and Continual Process Improvement

Continual Process Improvement depends on accurate and timely process measurements and relies upon obtaining, analyzing, and using information that is practical and meaningful to the process. Measurements of process efficiency and effectiveness enable the USMC to track performance and improve overall end user satisfaction. Process metrics are used as measures of how well Service Level Targets are being met.

In addition to process metrics, Customer Satisfaction Surveys are a key feedback tool used to measure IM success, satisfaction, and operational validation within the IM process. These surveys are analyzed for future IM improvements and solidify the Continual Service Improvement (CSI) process. Furthermore, they are used as a principal connection between IM performance and customer satisfaction. Customer Satisfaction Surveys are a significant KPI metric captured within Table 2-3.

Effective operation and 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

- **Critical Success Factor (CSF)** – A Critical Success Factor is a metric that represents key operational performance requirements and indicates whether a process or operation is performing successfully from a customer or business perspective.
- **Key Performance Indicator (KPI)** – A KPI is used to measure the achievement of each Critical Success Factor. 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. A KPI should lead to action and be a driver for improvement.
- **Metric** – A metric is a measure for quantitatively or qualitatively assessing, controlling or selecting a person, process, event, or institution along with the procedures to carry out measurements for interpretation. Metrics may be used to help manage an IT process, service, or activity.

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). See Appendix C – for Thresholds and Appendix D – for Common Metrics.

Table 2-3 describes the metrics that shall be monitored, measured and analyzed:

Table 2-3 IM Critical Success Factors and Key Performance Indicators

CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Benefits
1	Incidents are rapidly resolved	1	Average time to resolve incidents by service MTTR (Mean time to Resolve) Calculation: Elapsed time between incident logged and incident placed in Resolved state, sorted by Service	Reduction in downtime and increase in end user satisfaction
		2	Average time to resolve incidents by service and priority Calculation: Elapsed time between incident logged and incident placed in Resolved state, sorted by service (determined by product categorization) and priority	

CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Benefits
		3	Average time to resolve incidents by service and region Calculation: Elapsed time between incident logged and incident placed in Resolved state, sorted by service (determined by product categorization) and region (determined by customer profile)	
		4	Open incident backlog Calculation: Incidents not resolved or closed that have exceeded resolution closure targets by priority	
		5	Incident Assignment Time Calculation: Elapsed time between creation of incident record to assignment to a queue	
2	Users are satisfied with Service Desk and Tier 2 performance	6	Customer Satisfaction Rating Calculation: Customer Satisfaction Survey scores use a weighted scoring mechanism, based on points per question, and is assessed based on the user's responses to the survey questions	Increased customer satisfaction and utilization of the Service Desk is encouraged
		7	Average time to answer Calculation: Elapsed time between customer call initiated and customer call answered (Automated Call Distribution)	
		8	Average Response Time Calculation: Average time between customer contact and response from the Service Desk back to the customer (this measure will be focused on email/web customer contacts)	
3	Accurate escalation	9	% of incidents accurately routed by the Service Desk on the first attempt Calculation: Escalated incidents not routed back to the Service Desk (business process to require that misrouted incidents be sent back to the Service Desk for further action)	Efficient utilization of IM supports operations resources. Reduction in downtime and increase in end user satisfaction.
		10	# of reassignments per Incident Calculation: Incident reassignments to another agent and/or queue.	

2.5.3 Training

Training is a key component of quality control. Incident Management roles within the IM Process require unique training which enforces the responsibilities of the specific role being performed. Prior to analysts being granted access to the ITSM Tool, they are required to complete the required Enterprise training (i.e. CBT).

3.0 ROLES AND RESPONSIBILITIES

The Incident Management Process has roles and responsibilities associated with design, development, execution and management. A role within a process is defined as a set of responsibilities.

Best Practices indicate that process ownership should reside with a single individual to ensure clear accountability. The Process Owner role is critical for the successful design and ongoing management and support of the process. Management (i.e., responsibility) of the IM process may be shared; a single process manager exists at the Enterprise level and Incident Managers will exist at the MITSCs. There will be instances where roles are combined or a person is responsible for multiple roles. Factors such as 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 persons performing each role.

3.1 Roles

The following abstract drawing (Figure 3-1) depicts IM process roles for the USMC, followed by a description of these roles. Table 3-1 describes the roles and responsibilities in more detail.

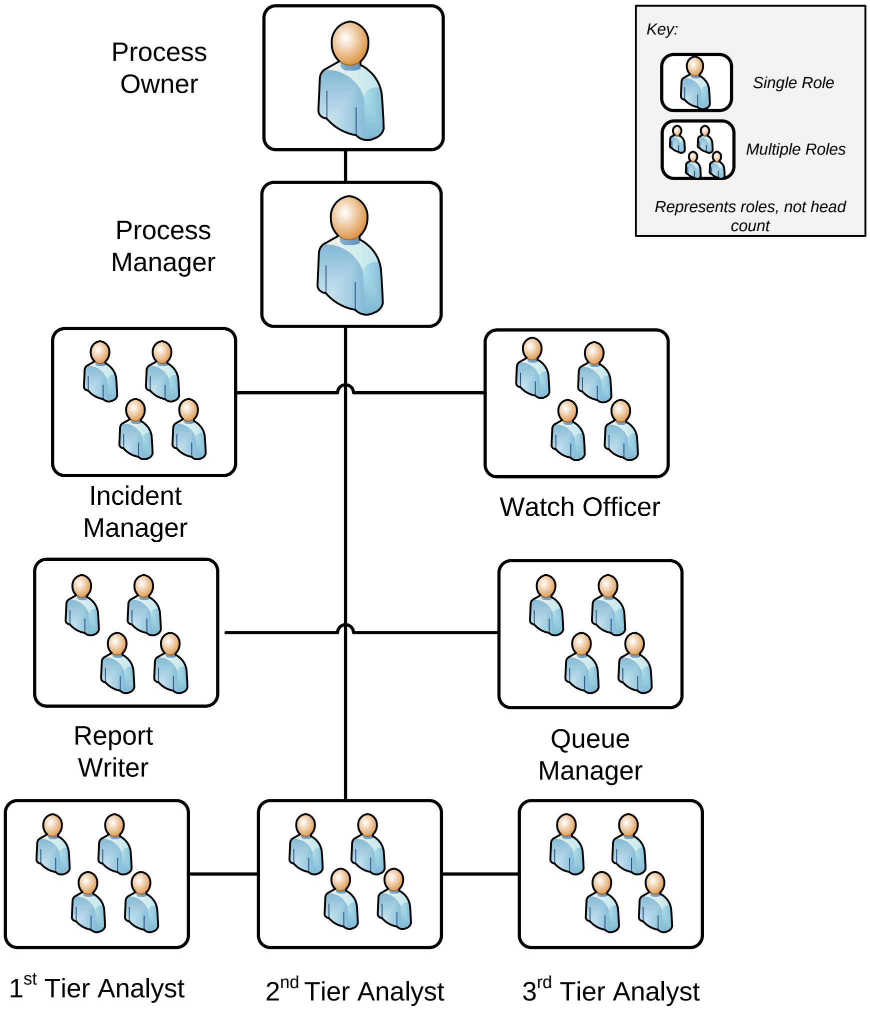


Figure 3-1 Incident Management Roles

Table 3-1 IM Roles and Responsibilities

Description	Overall Responsibility
Role #1 Process Owner	
The Process Owner is accountable for the ongoing value and integrity of the process Owns the process and the supporting documentation for the process. The primary functions of the Process Owner are oversight, continuous process improvement and ensuring that the process is followed by the organization. The Process Owner may choose to delegate specific responsibilities to another individual (ie. IM Process Manager) but remains ultimately accountable for the results of the IM process.	• Responsible for the performance of the process with the authority to make changes and represent management decision. Ensures the process is defined, documented, maintained, and communicated. Establishes and communicates the process roles and responsibilities. Defines Incident Management strategy and the strategic direction for the IM tool/system. • Accountable for organizational awareness and advocacy. Ensures organizational adherence to the process and verifies process compliance. • Monitors and reports on the effectiveness and efficiency of the IM Process at all levels of the Enterprise. Defines, develops, and communicates IM service levels and metrics; works with the metrics team to produce reports. • Ensures IM processes and tools integrate with other ITSM processes and that requirements for the tools are defined. Promotes integration with other processes by participating in other ITSM process initiatives and process reviews. • Manages changes to the process, including reviewing and approving proposed changes and communicating changes to all the participants and affected areas. Decision maker on any proposed enhancements to the process. Initiates and sponsors projects to improve or reengineer the process. • Ensures availability of training, onboarding and orientation, teambuilding exercises, and conflict facilitation.
Role #2 Process Manager	
Responsibilities as delegated by the Process Owner. Ensures effective coordination of activities to restore service. The Incident Process Manager manages and coordinates all activities necessary to respond to, record and resolve incidents by communicating preventive actions and best practices that (potentially) affect the service level. The Process Manager will communicate and coordinate with their counterparts on incidents or the process when required/beneficial.	• Assists Process Owner in developing and maintaining the Incident Management Process and procedures and ensures they are implemented and adhered to at all levels of the Enterprise. • Maintains awareness of USMC and DoD directives. Interfaces with Watch Officer and Queue Managers; Assists the support engineers through the IM process within the support engineering domain. Provides direction and consultation on support staff performance of the IM process, creating and executing action plans when necessary to ensure continuous improvement. • Provides management information on IT service quality and customer satisfaction. • Requests, reviews, and reports on metrics. • Coordinates interfaces between Incident Management and other processes. • Drives the efficiency and effectiveness of the Incident Process. Identifies opportunities to improve the process.
Role #3 Incident Manager(s)	
Ensures effective coordination of activities to restore service within their AoR. The Incident Manager manages and coordinates all activities necessary to respond to, record and resolve incidents by communicating preventive actions and best practices that (potentially) affect the service level. Incident Managers will communicate and coordinate with other Incident Managers, the Process Manager and Process	• Maintains awareness of USMC and DoD directives. Interfaces with Watch Officer and Queue Managers; manages Major Incidents with the assistance of the Watch Officer within AoR. Manages support staff performance of the IM process, creating and executing action plans when necessary to ensure continuous improvement within AoR. • Provides management information on IT service quality and customer satisfaction within AoR. • Requests, reviews, and reports on metrics within AoR. • Coordinates interfaces between Incident Management and other processes within AoR.

Description	Overall Responsibility
Owners on incidents or the process when required/beneficial.	• Analyzes and correlates incoming real-time incidents. Detects possible Problems and assigns them to the Problem Management team to establish Problem Records. • Drives the efficiency and effectiveness of the Incident Process. Identifies opportunities to improve the process
Role #4 Watch Officer (WO)	
Supervises professional employees (military, civilian, and contractor) responsible for the IM Process. The Watch Officer ensures effective coordination of activities to restore service. They are responsible for the execution of their respective portion of the Enterprise IM framework and will communicate and coordinate with their counterparts on incidents or the process itself when required/beneficial.	• Reviews effectiveness and efficiency of the IM Process at their level of the Enterprise • Ensures IM processes and tools integrate with other ITSM processes and that requirements for the tools are defined • Ensures that the process is defined, documented, maintained, and communicated • Establishes and communicates the process roles and responsibilities • Initiates CCIR events • Responsible for the development and execution of the Major Incident Response Plan and the resolution of all Major incidents • Participates in other ITSM process initiatives and process reviews • Keeps superiors advised of unusual situations and potential problem areas and recommends courses of action and/or conclusive actions • Maintains 24x7x365 network operations situational awareness • Analyzes and correlates incoming real-time incidents • Coordinates planned MCEN outages, and MCEN incident response actions • Manages and uses a trouble record reporting system at the appropriate level • Conducts rapid reaction planning for network operations events • Coordinates current operations between operating departments within the echelon and with external agencies • Provides operational support for MCEN users • Maintains contact with other groups and organizations performing related work and coordinates new ideas and developments • Provides direction and guidance to subordinates engaged in the review, design, development, modification, implementation, and the day-to-day sustainment of a myriad of Operations Center related issues • Owns management review process for incidents not resolved through the standard IM process • The Watch Officer also is accountable for the activities and resources required to resolve escalated incidents — Performs escalation and prioritization evaluations — Understands the business impact of the escalated incident or Service Call — Manages the escalation process — Ensures communications regarding escalations are planned and orderly — Coordinates the creation of escalation teams — Conducts checkpoint escalation status review meetings — Conducts escalation post- mortem reviews and closing escalations with the customer's approval — Uses escalation post-mortem review results to determine follow up actions — Ensures escalation communication to the Customer is timely and accurate

Description	Overall Responsibility
	— Develops, documents and follows up on action plans — Provides data on escalation history managing requests for information regarding escalations — Ensures Emergency Requests for Change required as part of the escalation are documented — Schedules and facilitates escalation meetings and phone conferences — Plans work to be accomplished by subordinates, setting priorities and scheduling completion. Assigns work to subordinates based on priorities and selective considerations of the difficulty of assignments and capabilities of employees — Resolves escalation and routing conflicts
Role #5 Queue Manager	
Ensures effective coordination of activities to restore service with a primary focus on escalations, prioritizations, routing and queue management.	• Awareness of USMC and DoD directives • Ensures incidents are accurately transferred to the appropriate AoR and/or escalated to the appropriate functional group • Requests, reviews, and report metric performance • Manages support staff performance of the IM process, creating and executing action plans when necessary to ensure continuous improvement • Assists the support engineers through the IM process within their domain • Identifies opportunities to improve the process
Role #6 3rd Tier Analyst	
The 3rd Tier Analyst is a subject matter expert with the highest security access required to resolve incidents. This role manages and resolves complex issues related to operational aspects that cannot be resolved by Tier 1 or Tier 2 support. This role performs in-depth technical incident investigation, diagnosis, and resolution, providing knowledge and training to 1st Tier support.	• Provides all facets of support concerning CIs in the IT infrastructure • Detects potential problems, alerting the incident Manager (notification to Problem Management) • Interfaces with third party vendors for incident resolution • Incident investigation, diagnosis and resolution where possible • Resource to Resolution Team on escalated incidents • Involved in planning, designing, developing, and implementing CIs • Maintains and updates work-arounds and proactive management of CIs in knowledge database • Resolves incidents • Understands the service level and executes accordingly • Provides technical communication to user regarding quick fixes • Provides knowledge and training to lower level support teams
Role #7 2nd Tier Analyst	
The 2nd Tier Analyst Staff consist of personnel with greater technical skills than the 1st Tier Analyst. The 2nd Tier Analyst supports incident diagnosis and resolution without interference from telephone interruptions.	• Provides all facets of support concerning CIs in the IT infrastructure • Involved in planning, designing, developing and implementing CIs • Maintains and updates work-arounds and proactive management of CIs in knowledge database • Resolves incidents • Understands the service level and executes accordingly • Provides technical communication to user regarding quick fixes • Attempts second level incident resolution to include touch labor personnel such as field services • Uses available resources to resolve incidents (people, tools and processes), engaging the next level of support as needed • Provides knowledge and training to lower level support teams
Role #8 1st Tier Analyst	
Interfaces with the Customer as the initial point of contact in the IM process. The 1st	• Welcomes customers by phone, web, mail, or other authorized means

Description	Overall Responsibility
Tier owns the incident records he or she generates. As the record owner, the 1st Tier Analyst tracks all record activities/statuses remaining the single point of contact for the customer throughout the lifecycle of the record.	• Authenticates the caller (check information in the Global Address List, confirm location, etc.) • Creates an incident record in the Incident system • Categorizes the record • Applies procedures applicable to the customer/caller/categories • Qualifies Incident • Prioritizes the incident record. • Transfers the incident record to the appropriate level of support • Knowledgeable of the service level impacted and executes remediation paths accordingly • Attempts first level incident resolution • Provides technical communication to customer/caller regarding “work-arounds” • Uses available resources to resolve records, engaging the next level of support as needed • Coordinates the transfer of a record between support levels • Communicates the status and completion to the user/external service desk and other staff/interested parties • Once a record is reported as resolved, ensures the customer agrees the resolution provided addresses the incident reported. Closes the record.
Role #9 Report Writer	
Responsible for the design, modification and publishing of all Enterprise IM reports as well as ad-hoc reporting, as required by the Incident Manager.	• The Report Writer role is mainly responsible for producing statistics and reports from the IM System • Designs, develops and produces new reports as well as modifying existing reports • Establishes and maintains automatic reporting capabilities • Establishes and maintains the IM Reporting architecture and user reporting portal • Produces monthly reports for Service Level Management and service analysis • Participates in data gathering and trend analysis

3.2 Responsibilities

Processes may span departmental 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, 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 – Supports the process or activity.

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 3-2 establishes responsibilities for high-level process activities by role.

Table 3-2 Responsibilities for Incident Management

IM Process Activities	Process Owner	Process Manager	Incident Managers	Watch Officer	Queue Manager	Tier 1-3 Analyst	Report Writer
Identification	A	R	R		I	R	I
Logging	A	R	R		I	R	I
Categorization	A	R	R	S	S	R	I
Service Request decision	A			S		R	I
Parent Child relationship decision	A	R	R	S	I	R	I
Prioritization	A	R	R	SC	R	R	I
Major Incident decision	A	R	R	R	I	R	I
Investigation & Diagnosis	A	R	R	I		R	I
Resolution	A	R	R	I		R	I
Incident Closure	A	R	R	I	I	R	I

Legend:
Responsible (R) – Completes the process or activity
Accountable (A) – Authority to approve or disapprove the process or activity
Support(S) – Supports process or activity
Consulted (C) – Experts who provide input
Informed (I) – Notified of activities

Note: Any role that is designated as Responsible, Accountable, Consulted, or Supporting is not additionally designated as Informed because being designated as Responsible, Accountable, Consulted, or Supporting already implies being in an Informed status. A role is designated as Informed only if that role is not designated as having any of the other four responsibilities.

Note: Only one role can be accountable for each process activity.

4.0 SUB-PROCESSES

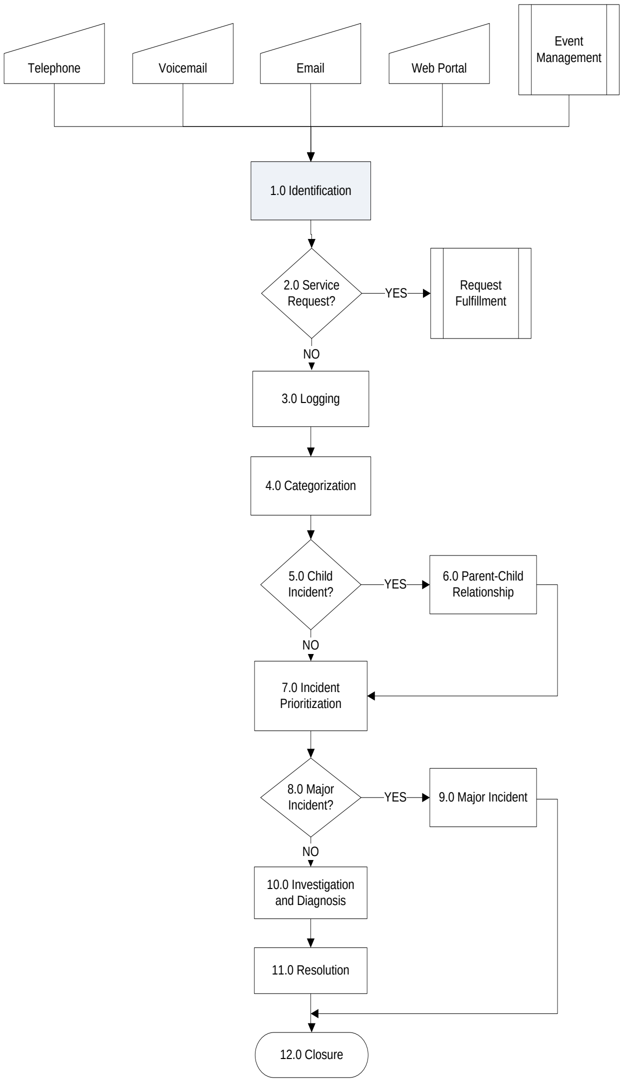
The USMC Enterprise IM process consists of multiple sub-processes. While every incident will follow each sub-process on some level, not every activity within each sub-process is utilized for every USMC organization or type of incident.

The following operational capability requirements are identified to ensure accurate categorization, prioritization, routing, transfers, data integrity and consistent incident lifecycle processing:

- Support all reported user issues, including fixing technical faults, logging and categorizing incidents or events, responding to service requests or answering queries, and coordinating "standard" changes.
- Management of the life cycle of incidents (including; reception, acknowledgement, classification, response, logging, monitoring, tracking, and closure) for all components involved in the provision of IT service.
- Own and manage incident records for AoR, including those reported by users and those discovered within the IT organization.
- Employ remote access tools and processes to allow analysts to conduct troubleshooting and incident resolution without in-person response.
- Consistent and standardized prioritization of incidents.
- Coordinate IM actions across all Marine Corps IT organizations.
- Monitor status updates, proactively ensuring incidents are resolved or escalated within pre-defined thresholds.
- Maintain a Known Error Database (KEDB) and use of Knowledge Management (KM) tools to retain information as it pertains to incident resolution and processing IT requests.

The following steps follow the logical path for reporting and processing Incidents.

4.1 Identification



Incidents enter the process via multiple sources such as: telephone, voicemail, Email, Web Portal or the Event Management sub-process.

For an incident to be managed, it must be confirmed that the incident meets the USMC IM criteria and is in the AoR of entity opening the incident. Once the AoR is validated, then the tracking system that the Incident record must be logged is determined (i.e., the classified (SIPRNet) or unclassified (NIPRNet) system).

USMC, DISA and DoD policies define the criteria for identifying information as classified or unclassified.

The workflow in Figure 4-1 Identification Sub-Process depicts the Identification sub-process.

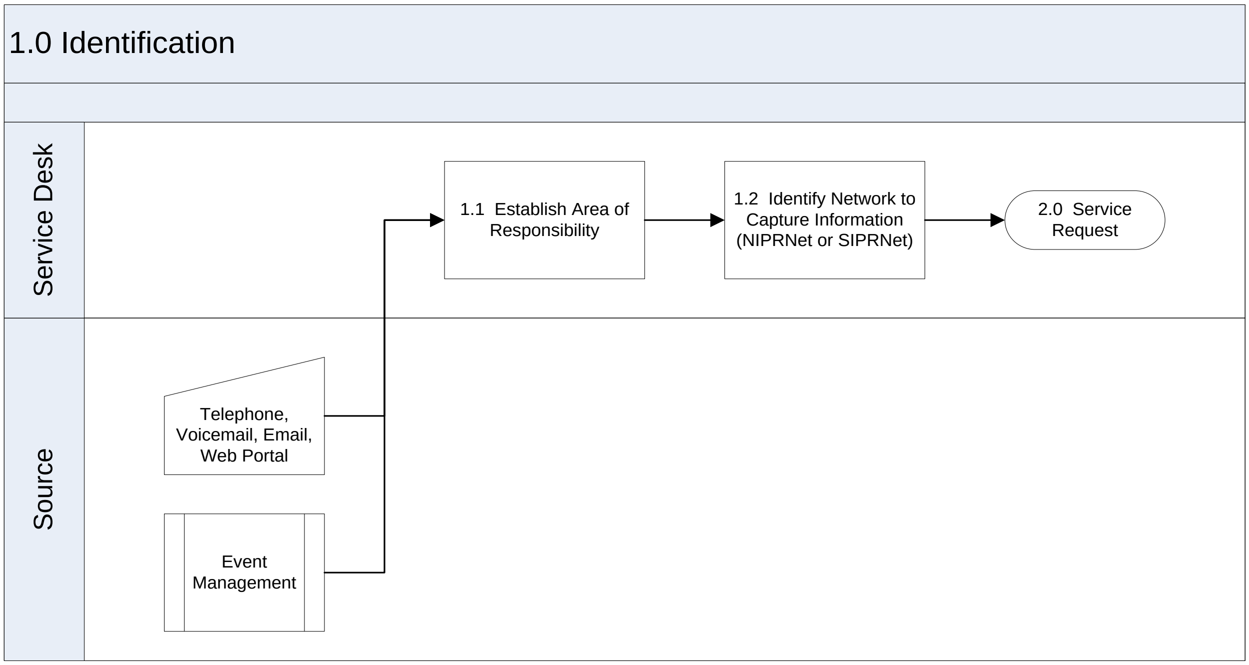

1.0 Identification
Service Desk
Source
1.1 Establish Area of Responsibility
1.2 Identify Network to Capture Information (NIPRNet or SIPRNet)
2.0 Service Request
Telephone, Voicemail, Email, Web Portal
Event Management

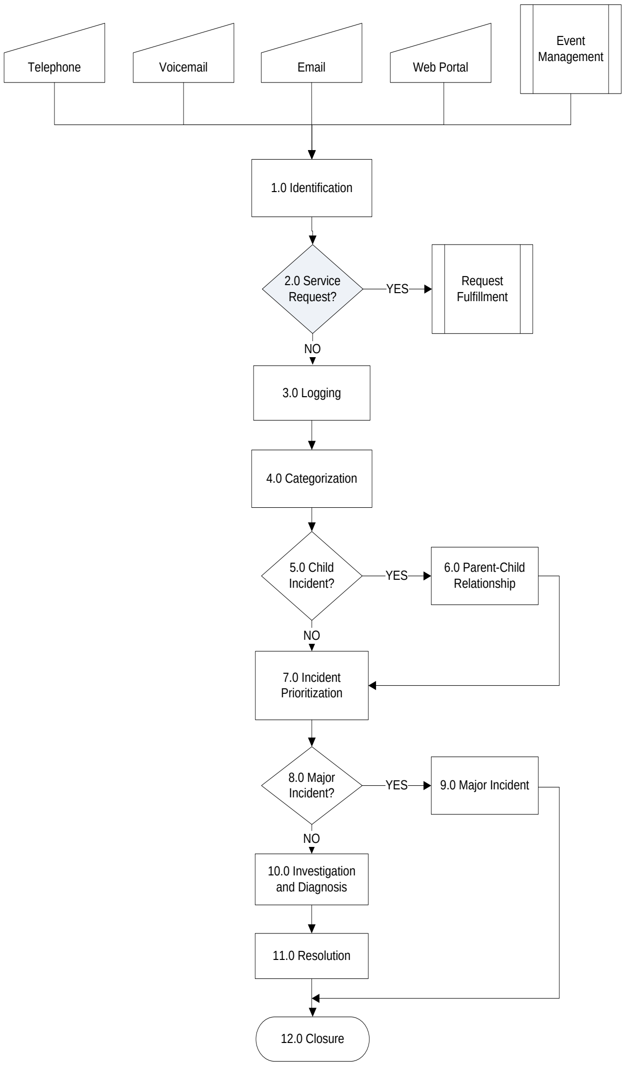
Figure 4-1 Identification Sub-Process

Table 4-1 describes the Identification sub-process steps as depicted in the above figure.

Table 4-1 Identification Sub-process Descriptions

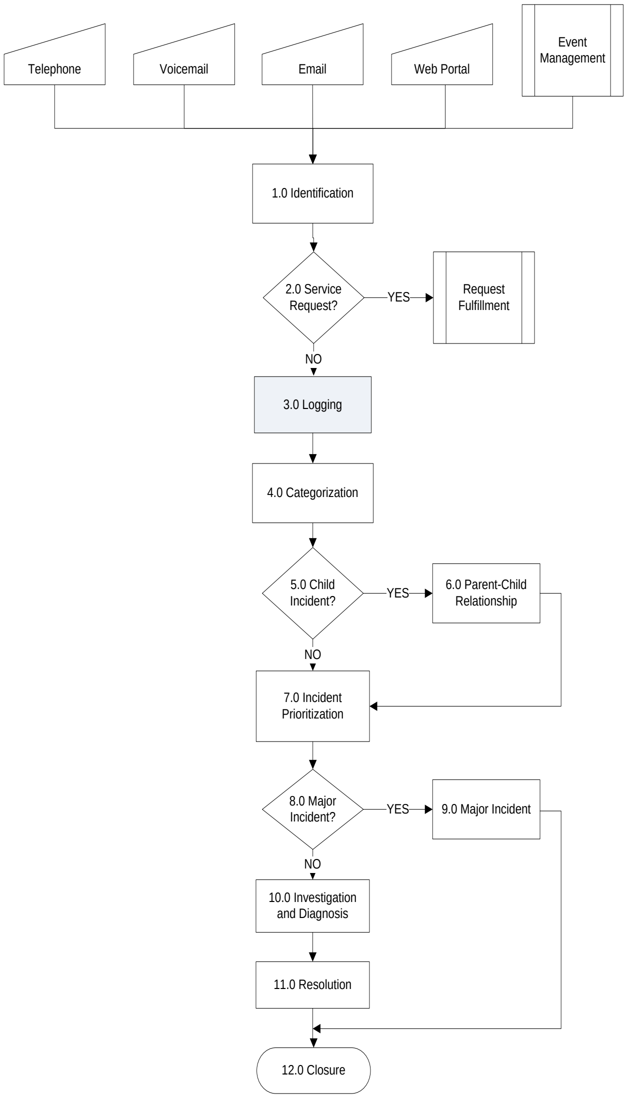
Identification		
Number	**Process Activity**	**Description**
	Initial Entry (Event Management or other means of communication)	Mode of entry into the IM procedure
1.1	Establish Area of Responsibility	The Analyst determines from questioning customer if the incident will fall within their AoR.
1.2	Identify Network to Capture Information (NIPRNet or SIPRNet)	Once AoR is established then the Analyst identifies what Network the incident will be assigned for logging all needed information concerning the incident or request.

4.2 Service Request



The term "Service Request" is used as a generic description for a large portion of requests that are received. Many of these are actually small changes – low risk, frequently occurring, low cost, etc. These requests are routed to the Request Fulfillment process, rather than being allowed to congest and obstruct the normal Incident Management process.

4.3 Logging



The next procedure must collect vital information concerning the incident and the person reporting the incident. If the user is not already in the system, the analyst must collect the required information and add the user to the system. If they are calling on behalf (proxy) of another person, the proxy must be identified along with the identity information for the person for whom they are the proxy.

Specific detailed information about the incident to include its origin is collected and this record must be date/time stamped.

The following workflow shown in Figure 4-2 depicts the Logging sub-process.

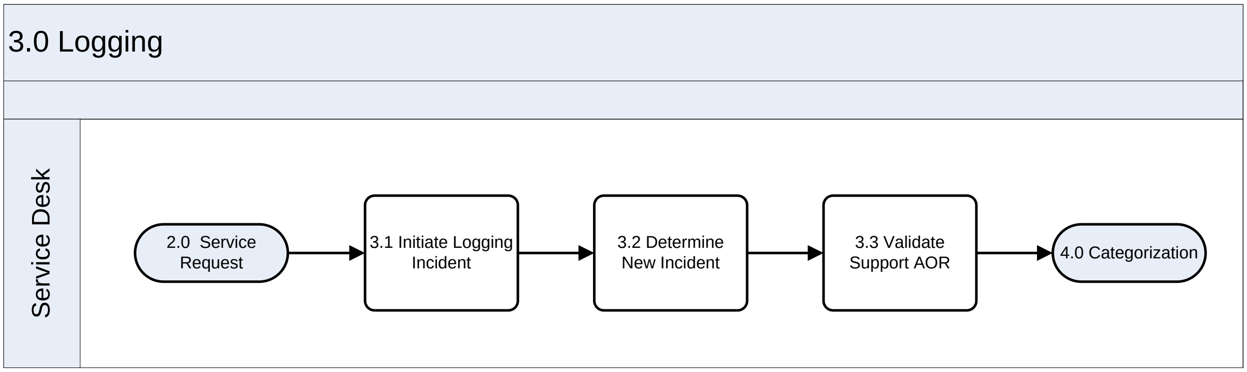


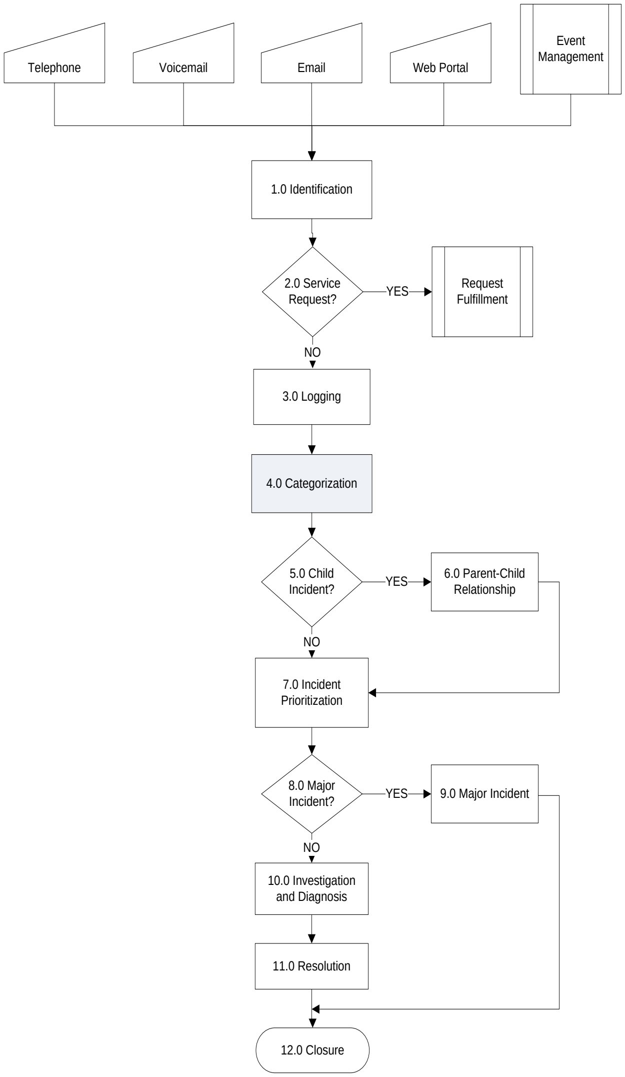
Figure 4-2 Logging Sub-Process

Table 4-2 describes the Logging sub-process steps as depicted in the figure above.

Table 4-2 Logging Sub-process Descriptions

Logging		
Number	**Process Activity**	**Description**
3.1	Log contact Information	The Analyst creates or updates the Customer record and confirms essential information to begin logging the issue.
3.2	Log details of Incident in IM Tool to be actionable	The Analyst searches the Customer records to determine whether the inquiry is regarding an existing or new incident. If an existing incident, open the existing incident record and update according to incident recording procedures. If not an existing incident, initiate a new incident record.
3.3	Validate Support AoR	The Analyst validates support needed for incident.

4.4 Categorization



Accurate categorization of incidents helps to establish correct routing, enabling a faster time to resolution. It is a best practice to utilize operational categories and product categories that link to Service Catalog.

Product categories are frequently leveraged for reporting and routing to functional support groups. One or more product categories will directly align to fields in the CMDB and should ultimately map IT services to enable metrics and reporting of incidents 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 (see Table 4-3 for an example) define the work for a particular incident, problem, known error, change request, or task.

The Marine Corps operational categorization is also a three-tier structure used to support reporting in the system, to qualify groups and support staff assignments and to manage the routing of approvals. The categorization structure contains items that represent symptoms or events associated with incidents or problems, such as applications not working correctly and network performance.

Table 4-3 Operational Categorization Example

Operational Categorization		
Tier 1	**Tier 2**	**Tier 3**
Server Management	Hardware	Add
		Configure
		Degraded performance
		Hardware Failure
		Move
		Rack
		Remove
		Replace
Server Management	Hosted Applications	Account Create
		Account Delete
		Account Disable
		Account Information Update
		Account Logical Move
		Account Unlock
		Archive/Backup
		Configure

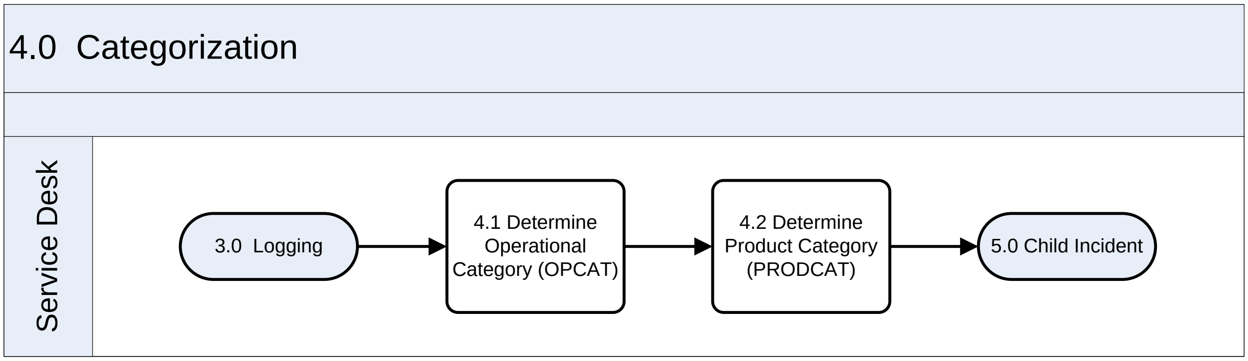

4.0 Categorization
Service Desk
3.0 Logging
4.1 Determine Operational Category (OPCAT)
4.2 Determine Product Category (PRODCAT)
5.0 Child Incident

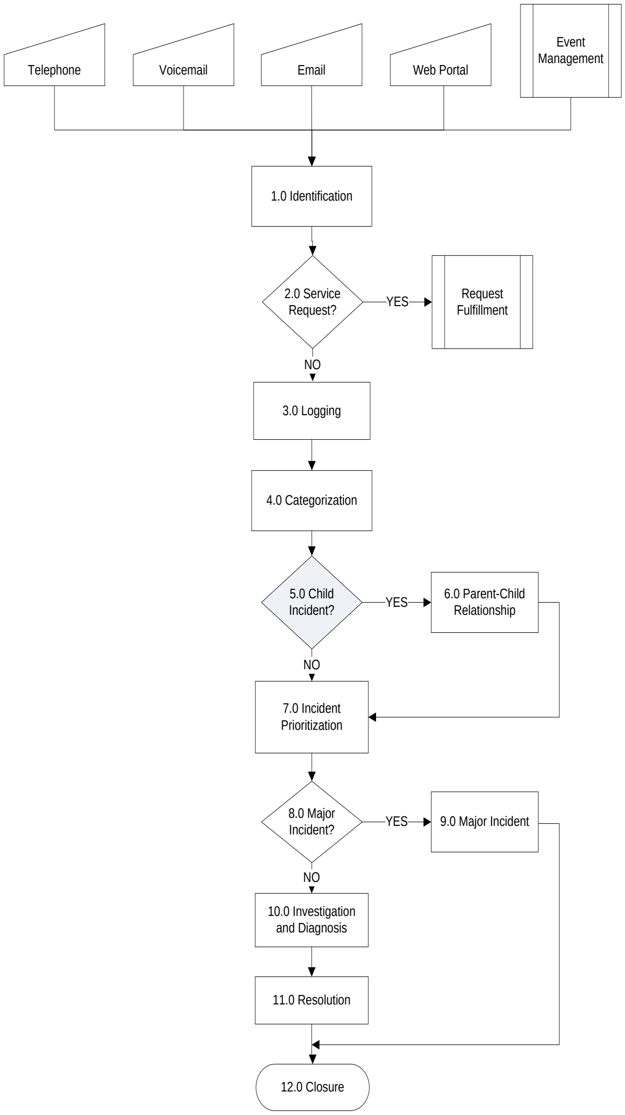
Figure 4-3 Categorization Sub-Process

Table 4-4 describes the categorization procedure steps as depicted in the above figure.

Table 4-4 Categorization Sub-process Descriptions

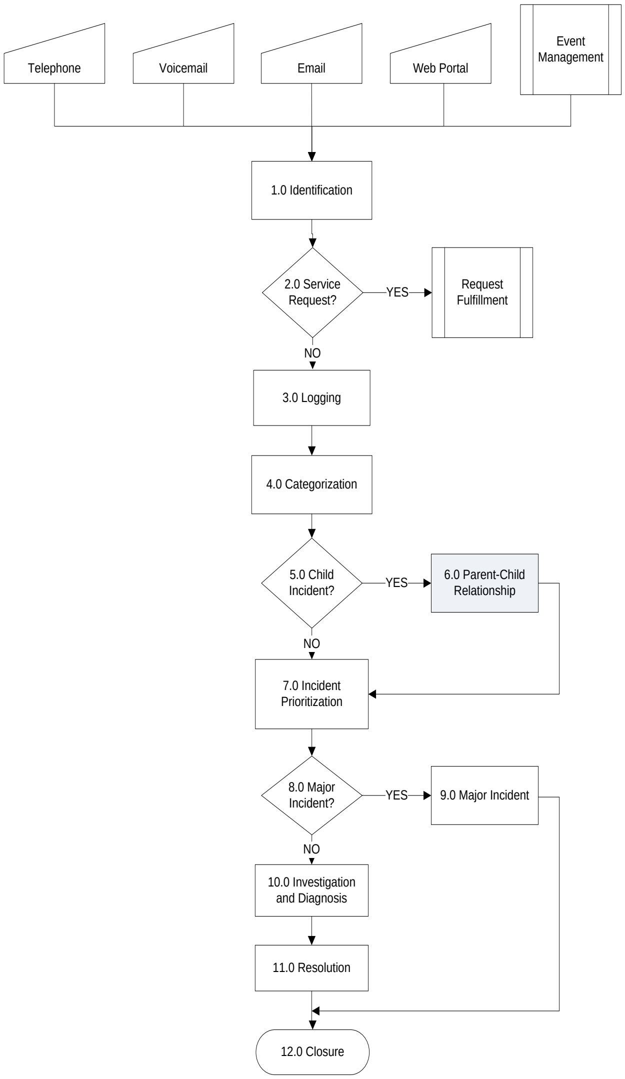
Categorization		
Number	**Process Activity**	**Description**
4.1	Determine Operational Category (OPCAT)	The Analyst selects the operational category from the drop down menus.
4.2	Determine Product Category (PRODCAT)	The Analyst selects the product category from the drop down menus.

4.5 Child Incident



At this point in the process, a decision needs to be made whether the incident that is being reported should be related to a parent incident, or another record. If an incident has already been reported for the same issue, a parent-child relationship needs to be formed. This allows for incidents to be grouped appropriately for ease of reporting and communication.

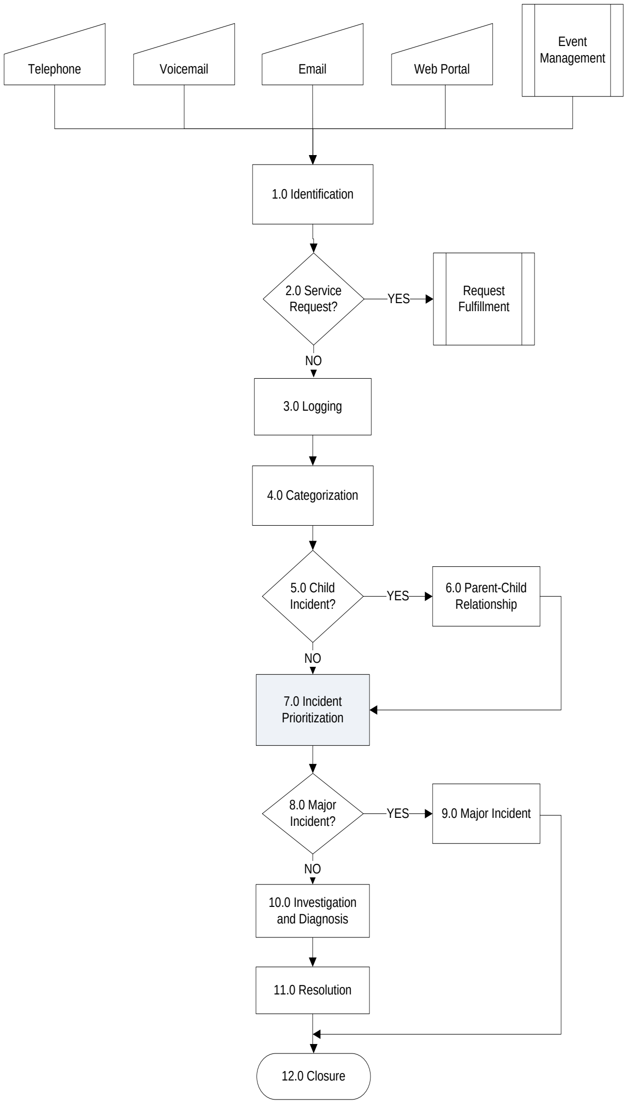
4.6 Parent-Child Relationship



When an incident needs to be related to an incident that has already been reported by a different user, a parent-child relationship is created. When a parent incident is created, child incidents can be related to the parent incident and the associated information will apply to the child incidents. Once the parent is closed, the child incidents will be closed as well.

Other relationships can be made as well, such as relating an incident to a change, an incident to a problem or an incident to a Configuration Item (CI).

4.7 Prioritization



Every incident must be correctly prioritized. Impact and urgency determine priority.

Impact is determined by:

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

Urgency is determined by:

- The user’s required time to resolution
- The availability of a work-around
- User’s VIP status
- Risk

Table 4-5 and Table 4-6 provide general guidance for establishing incident impact and 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.

Impact is the portion of the USMC as a whole that is affected by this incident. Determine the impact by applying the criteria below.

Table 4-5 Impact Matrix

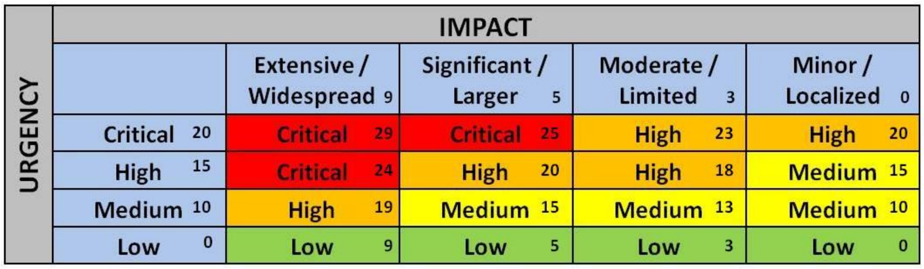
IM Impact Matrix	
Level	**Description**
Extensive/Widespread	Multiple Bases/Posts/Sites are impacted -Or- A Mission Assurance Category MAC I system or service is impacted -Or- A MAC II system or Service is down or significantly degraded > 50% -Or- WO discretion. Guidance: Capabilities vital to mission effectiveness or operational readiness of deployed or contingency forces are impacted
Significant/Large	An entire base/post/site is impacted -Or- A MAC II system or service is degraded <50% -Or- A MAC III service is down or significantly degraded > 50% -Or- WO discretion. Capabilities important to the support of mission effectiveness or operational readiness of deployed or contingency forces are impacted
Moderate/Limited	Multiple End Users are impacted -Or- A MAC III service is degraded <50%
Minor/Localized	An individual End User is impacted

Table 4-6 Urgency Matrix

IM Urgency Matrix	
Level	**Description**
Critical	Immediate resolution (of an Incident) or fulfillment (of a Service Request) is required ○ A workaround (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 or fulfillment is required
High	○ No workaround 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 workaround exists but productivity is effected -or- ○ A system or service is available, but degraded
Low	○ A workaround exists and/or productivity effect is minimal or non-existent ○ Routine work

By evaluating the impact and urgency, it is possible to assign priority to the incident, as shown in Table 4-7.

Table 4-7 Priority Matrix



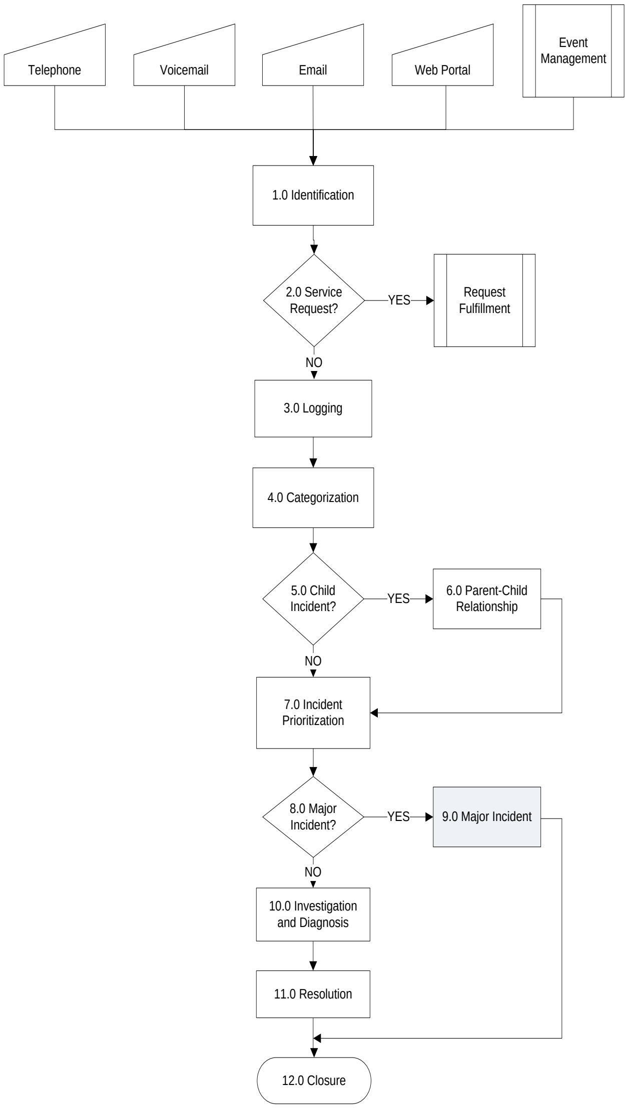
URGENCY	IMPACT				
		Extensive / Widespread 9	Significant / Larger 5	Moderate / Limited 3	Minor / Localized 0
	Critical 20	Critical 29	Critical 25	High 23	High 20
	High 15	Critical 24	High 20	High 18	Medium 15
	Medium 10	High 19	Medium 15	Medium 13	Medium 10
	Low 0	Low 9	Low 5	Low 3	Low 0

The IM tool assigns a standard weighting to each combination of urgency and impact. 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 incident records.

Given the multitude of variables inherent to USMC operations that can affect impact, different echelons or commands can have unique impact and urgency criteria that will be established at the time of implementation. It is the responsibility of Queue Managers and Watch Officers to analyze and correlate incoming real-time incidents to ensure priorities are accurately set and to make adjustments when appropriate.

4.8 Major Incident

Major Incidents have a high impact and/or a high urgency. Tactical, VIP, timing and service considerations may trigger a Major Incident. Incident Managers, Queue Managers and Watch Officers at all levels of the organization are responsible for analyzing and correlating incoming real-time incidents to identify and escalate Major Incidents as quickly as possible. Once a Major Incident has been declared, the Watch Officer is assigned the incident and is responsible for the Major Incident resolution. Every organization implementing Incident Management should have a Major Incident Response Plan based on the model depicted below, that includes escalation, notifications (communications), and response actions that will be followed in the event of a Major Incident.



The following workflow Figure 4-4 depicts the Major Incident sub-process.

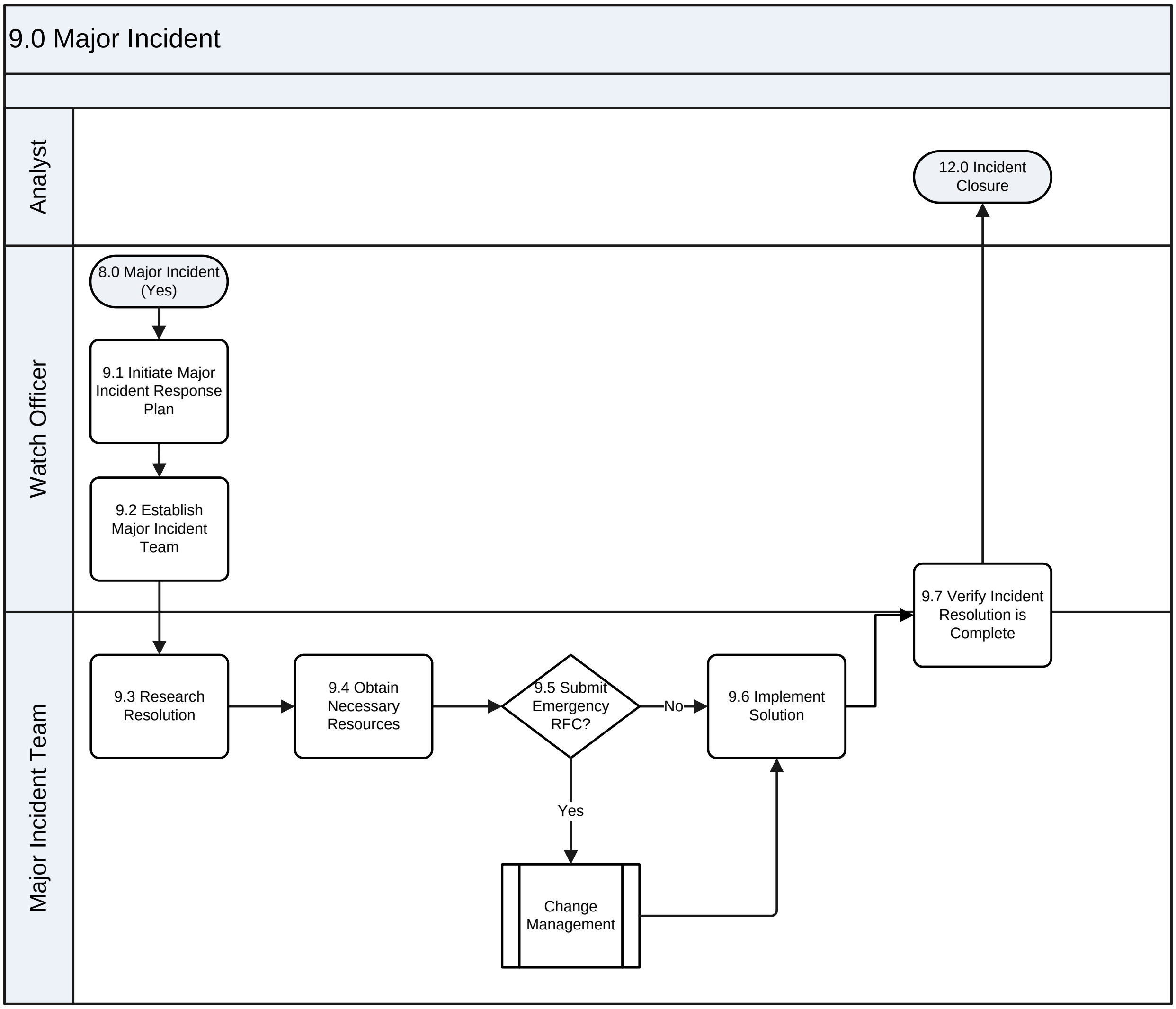

9.0 Major Incident
Analyst
Watch Officer
Major Incident Team
12.0 Incident Closure
8.0 Major Incident (Yes)
9.1 Initiate Major Incident Response Plan
9.2 Establish Major Incident Team
9.7 Verify Incident Resolution is Complete
9.3 Research Resolution
9.4 Obtain Necessary Resources
9.5 Submit Emergency RFC?
No
9.6 Implement Solution
Yes
Change Management

Figure 4-4 Major Incident Sub-Process

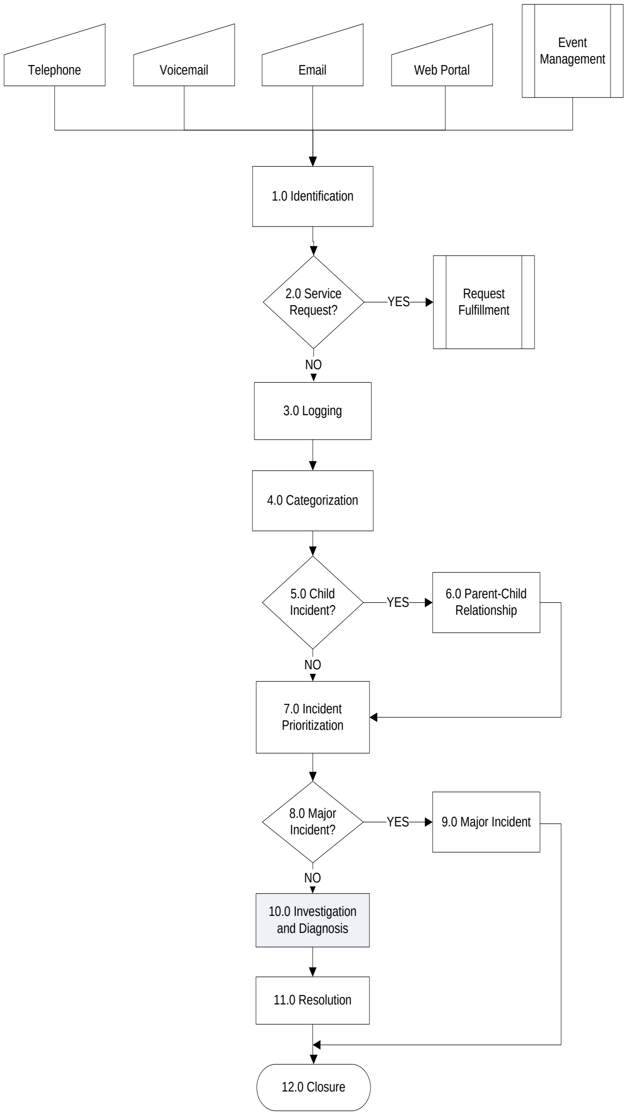
Table 4-8 describes the Major Incident sub-process steps as depicted in the above figure.

Table 4-8 Major Incident Sub-process Descriptions

Major Incident		
Number	**Process Activity**	**Description**
9.1	Initiate Major Incident Response Plan	The Watch Officer will initiate all required CCIRs, Hierarchical Escalations, IT operations communications, and all other activities detailed in the Major Incident Response Plan.
9.2	Establish Major Incident Response Team	Establish a team of Tier 2-4 analysts that have the appropriate subject matter expertise or resources.
9.3	Research Resolution	Execute the necessary diagnostics and analysis to determine the root cause or a work-around.
9.4	Obtain Necessary Resources	Obtain necessary resources to resolve the incident.

Major Incident		
Number	**Process Activity**	**Description**
9.5	Submit Emergency RFC?	Is Emergency RFC Required? If so, submit through Change Management Process.
9.6	Implement Solution	Apply remediation.
9.7	Verify Incident Resolution is Complete	Execute necessary procedures to confirm the incident has been resolved.

4.9 Investigation and Diagnosis



After the incident has been identified, logged, categorized, and prioritized, the Analyst records as much information as possible about the incident. Utilizing technical articles, remote control capabilities, user manuals, operations manuals and any other available capabilities, the Analyst attempts to resolve the incident on the first call. If the incident cannot be resolved, the Analyst should follow the escalation/transfer procedures.

Functional Escalation is the process of routing an incident to a technical team with a higher level of permission, knowledge, or expertise. Hierarchical Escalation requires communications to a superior commanding operating officer to affect the resolution of the incident. It is primarily utilized in circumstances that warrant the intervention and/or notification of senior staff and/or superior commands. Depending on the point of origin, this communication will be in the form of a CCIR, phone call, SIPRNet email, NIPRNet email or any other official form of communication.

Transfers are similar to escalations and involve routing an incident to a different AoR.

The following workflow Figure 4-5 depicts the Investigation and Diagnosis sub-process.

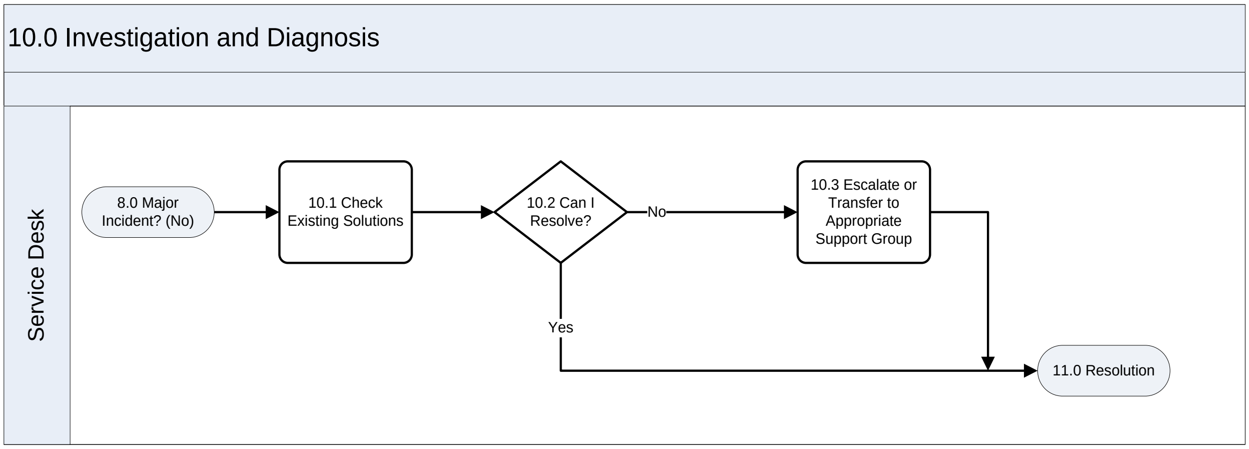

10.0 Investigation and Diagnosis
Service Desk
8.0 Major Incident? (No)
10.1 Check Existing Solutions
10.2 Can I Resolve?
No
10.3 Escalate or Transfer to Appropriate Support Group
Yes
11.0 Resolution

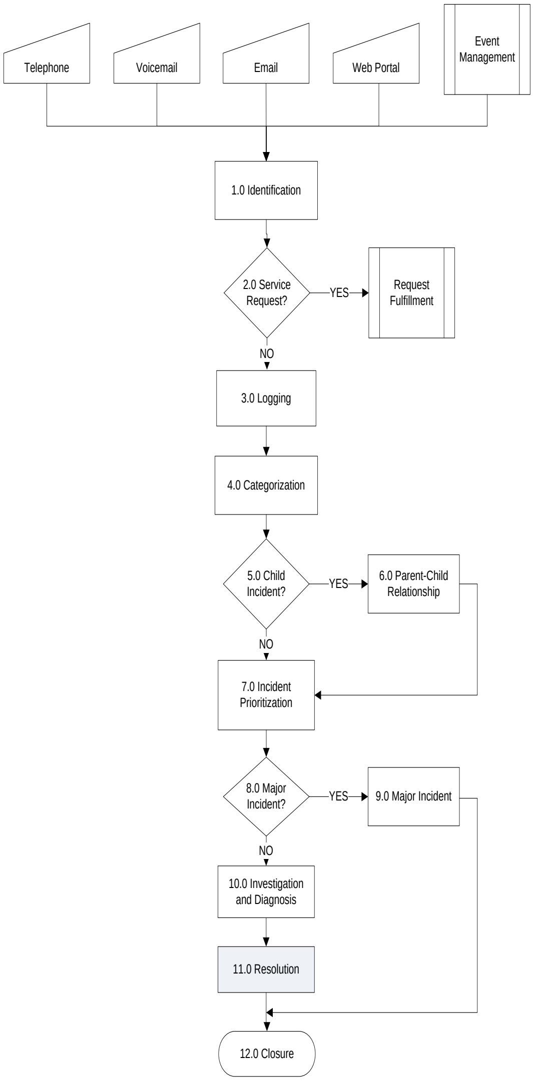
Figure 4-5 Investigation and Diagnosis Sub-Process

Table 4-9 describes the Investigation and Diagnosis sub-process steps as depicted in the figure above.

Table 4-9 Investigation and Diagnosis Sub-process Descriptions

Investigation and Diagnosis		
Number	**Process Activity**	**Description**
10.1	Check Existing Solutions	Perform the following actions to ensure there are no existing solutions: • Determine whether the incident matches any Known Errors or existing work-arounds • Search Incident and Problem Records • Search Technical Articles • Consult Operational and User Documentation • Check Recent Changes or Releases
10.2	Can I resolve?	If able, move to Resolution sub-process.
10.3	Escalate or Transfer to Appropriate Support Group	If not, consult Escalation/Transfer Procedures to determine where to escalate/transfer the incident. If you identify a trend (ie. 10 users have reported the same incident) a problem record should be recommended and the incident(s) may need to be escalated/transferred to Problem Management for review and potential Problem Record creation. Incident management does not have the responsibility of creating problem records.

4.10 Resolution



After the Investigation and Diagnosis step has been completed, the incident is then resolved; meaning service is restored to the customer. After the incident is resolved, then the status of the incident record is set to “resolved” and the Analyst proceeds to the Closure step.

If the implemented solution does not resolve the incident, it goes back to Investigation and Diagnosis and then escalate/transfer. If the implemented solution is a work around, e.g. rebooting the server, but no Reason for Outage (RFO) is determined, then a Problem record needs to be considered.

The following workflow Figure 4-6 depicts the Resolution sub-process.

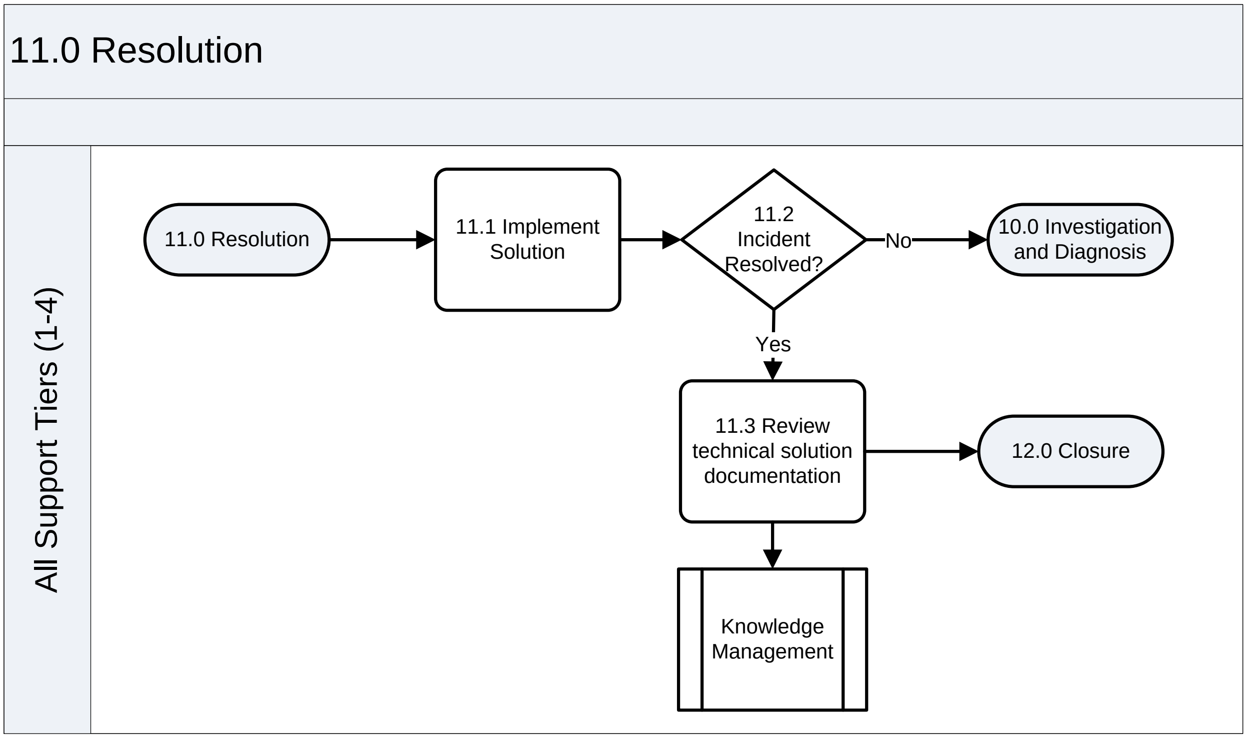


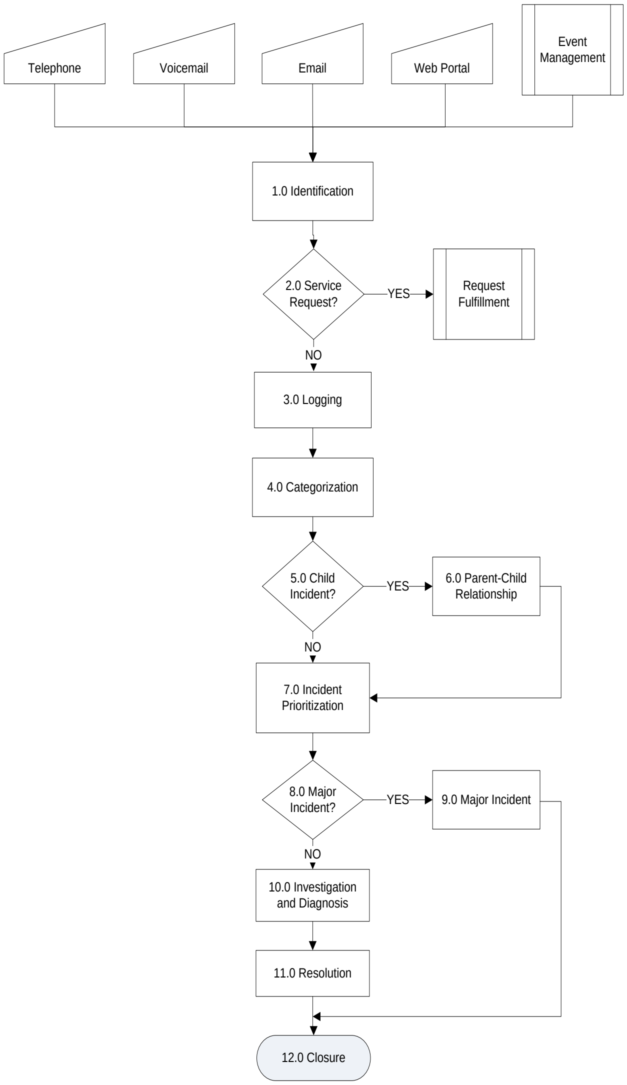
Figure 4-6 Resolution Sub-Process

Table 4-10 describes the Resolution sub-process steps as depicted in the above figure.

Table 4-10 Resolutions Sub-process Descriptions

Escalations & Transfers		
Number	**Process Activity**	**Description**
11.1	Implement Solution	Apply proposed solution steps as determined during Investigation and Diagnosis sub-process.
11.2	Incident Resolved	Determine if incident is resolved.
10.0	Return to Investigation and Diagnosis	If the incident is not resolved, it must be returned to the Investigation and Diagnosis sub-process (step 10.3), including escalation and/or transfer to the appropriate support group.
11.3	Review technical solution documentation	Verification, rewrite, or creation of technical documentation will occur within the Knowledge Management Process.

4.11 Closure



Closure is the final sub-process of the IM lifecycle. Each incident will be closed by the support group that opened it once the user confirms that the incident has been resolved. An incident record can be manually closed by an analyst which has been granted those permissions. Furthermore, an incident record will be automatically closed after seven business days transpire without any response from the user to three automated emails. Once an incident record has been closed, an automated customer satisfaction survey will be sent to the user.

The following workflow Figure 4-7 depicts the Closure sub-process.

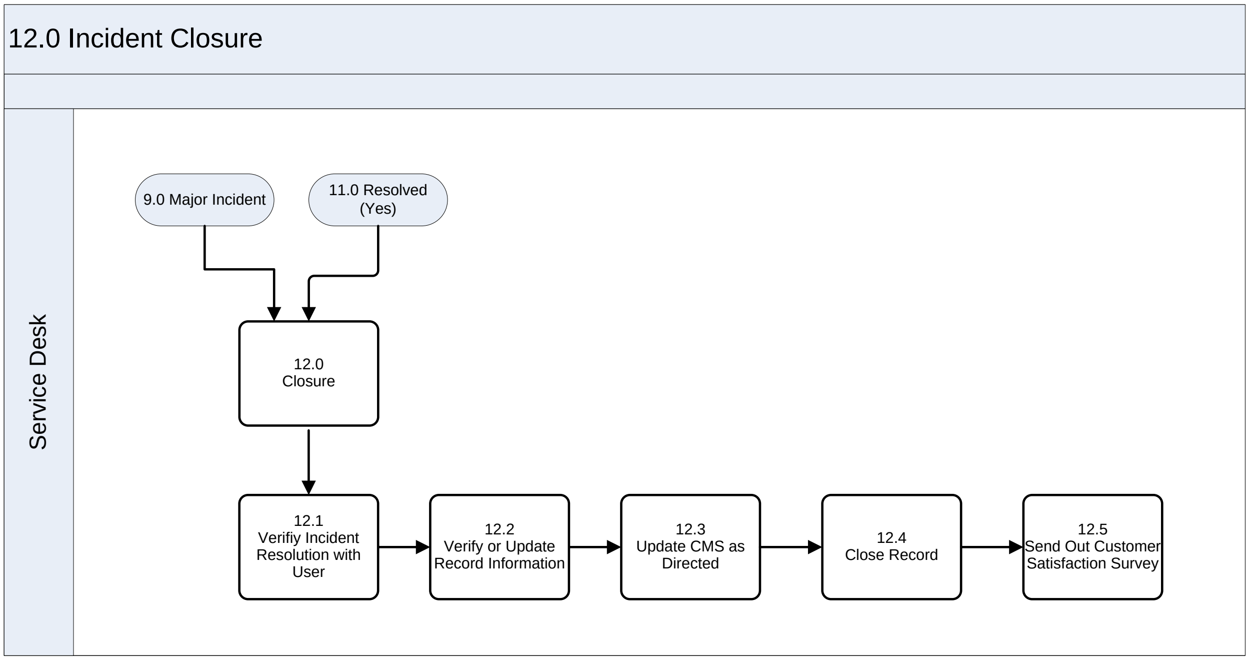

12.0 Incident Closure
Service Desk
9.0 Major Incident
11.0 Resolved (Yes)
12.0 Closure
12.1 Verifiy Incident Resolution with User
12.2 Verify or Update Record Information
12.3 Update CMS as Directed
12.4 Close Record
12.5 Send Out Customer Satisfaction Survey

Figure 4-7 Closure Sub-Process

Table 4-11 describes the Closure sub-process steps depicted in the figure above.

Table 4-11 Closure Sub-process Descriptions

Incident Closure		
Number	**Process Activity**	**Description**
12.1	Verify Incident Resolution with User	Contact user to ensure that resolution is complete and service is restored.
12.2	Verify or Update Record Information	Ensure the applied solution, escalation, transfer and activity information is documented accurately in the record.
12.3	Update CMS as Directed	Update the CMS as directed, usually in the case of standard, pre-approved changes. Major modifications to the CMS require the involvement of Configuration Management.
12.4	Close Record	Set incident record status to "Closed".
12.5	Send Out User Satisfaction Survey	This is an automatic function of the tool.

Appendix A – ACRONYMS

The official list of E-ITSM acronyms is located here.

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 lifecycle.
Availability	The percentage of the total time the IT service, software/application, or infrastructure component functionality is operationally available to the user. This metric applies Mean Time To Repair, Mean Time to Restore Service, and Mean Time Between Service Incidents values from Incident Management records. Unavailability: The IT service, software/application, or infrastructure component functionality is operationally unavailable to the user. This is typically acknowledged as an outage, and is recognized when service/system responses are not being sent by the service/system provider or being received by the service/system requester.
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 lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT services, hardware, software, buildings, people and formal documentation such as process documentation and SLAs.
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 lifecycle. 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.

Term	Definition
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.
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 comprised 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	Escalations occur when an IM record is assigned to another support tier within the same AOR (versus an IM record transfer which assigns the IM record outside of the AOR). 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.
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.

Term	Definition
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 lifecycle by Problem Management. Known errors may also be identified by SIE or suppliers.
Mission Assurance Category	Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categorie.
Mission Assurance Category I	Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.
Mission Assurance Category II	Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.
Mission Assurance Category III	Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.
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.
Notification	Notification is a communication that provides information.
Pilot	A Pilot is a limited deployment of an IT service, a release, or a process to the live environment. A pilot is used to reduce risk and to gain user feedback and acceptance.
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.
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 lifecycle. 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 lifecycle of IT services.

Term	Definition
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 Systems 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.
Transfer	Transfers occur when an IM record is assigned to another support tier outside of the existing AOR (versus an IM record Escalation which assigns the IM record to another support tier within the same AOR).
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.
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 – THRESHOLDS AND OBJECTIVES

CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Threshold	Objective
1	Incidents are rapidly resolved	1	Incident Resolution Time by service	Priority (Critical) <= 8hrs Priority (High) <= 48hrs Priority (Medium) <= 96hrs Priority (Low) <= 168hrs	Priority (Critical) <= 4hrs Priority (High) <= 24hrs Priority (Medium) <= 48hrs Priority (Low) <= 72hrs
		2	Incident Resolution Time by service and priority	Priority (Critical) <= 8hrs Priority (High) <= 48hrs Priority (Medium) <= 96hrs Priority (Low) <= 168hrs	Priority (Critical) <= 4hrs Priority (High) <= 24hrs Priority (Medium) <= 48hrs Priority (Low) <= 72hrs
		3	Incident Resolution Time by service and region	Priority (Critical) <= 8hrs Priority (High) <= 48hrs Priority (Medium) <= 96hrs Priority (Low) <= 168hrs	Priority (Critical) <= 4hrs Priority (High) <= 24hrs Priority (Medium) <= 48hrs Priority (Low) <= 72hrs
		4	Open incident backlog	Priority (Critical) = 0 Priority (High) <= 2 Priority (Medium) <= 5 Priority (Low) <= 10	Priority (Critical) = 0 Priority (High) = 0 Priority (Medium) = 0 Priority (Low) = 0
		5	Incident Assignment Time	Priority (Critical) <= 10min Priority (High) <= 30min Priority (Medium) <= 4hrs Priority (Low) <= 8hrs	Priority (Critical) <= 5min Priority (High) <= 15min Priority (Medium) <= 3hrs Priority (Low) <= 6hrs
2	Users are satisfied with Service Desk and Tier 2 performance	6	Customer Satisfaction Rating	80%	90%
		7	Average time to answer	Phone <= 10sec Email <= 8hrs Web <= 8hrs	Phone <= 5sec Email <= 1hr Web <= 1hr

CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Threshold	Objective
		8	Average Response Time	Priority (Critical) <= 1.5hrs Priority (High) <= 8hrs Priority (Medium) <= 12hrs Priority (Low) <= 16hrs	Priority (Critical) <= 10min Priority (High) <= 4hrs Priority (Medium) <= 6hrs Priority (Low) <= 8hrs
3	Accurate escalation	9	% of incidents accurately routed by the Service Desk on the first attempt	Priority (Critical) <= 50% Priority (High) <= 50% Priority (Medium) <= 50% Priority (Low) <= 50%	Priority (Critical) <= 100% Priority (High) <= 95% Priority (Medium) <= 95% Priority (Low) <= 95%
		10	# of reassignments per Incident	Priority (Critical) <= 10 Priority (High) <= 10 Priority (Medium) <= 10 Priority (Low) <= 10	Priority (Critical) <= 5 Priority (High) <= 5 Priority (Medium) <= 5 Priority (Low) <= 5

Appendix D – COMMON METRICS

Critical Success Factor	Key Performance Indicator	Definition (Explanation)	4 Vectors (Quantity, Quality, Timeliness, Compliance)
Incident service quality	Number of Critical and High incidents (total and by category)	Number of Critical and High incidents.	Quantity
	Number of Incidents per Priority (Impact and Urgency)	Number of incidents opened by priority (displayed as impact and urgency). This type of reporting will assist with manpower estimates by recording workload history. These estimates will only be accurate if we know that every time a user makes contact with IT, a record is created. This high level report can be used by upper management as it provides a snapshot for the reporting period.	Quantity
	Number of incidents incorrectly categorized	Number of incidents that were not categorized correctly on initial assignment. This could indicate the need for additional training.	Quality, Compliance
	Number of incidents incorrectly escalated/assigned	Number of incidents that were not escalated/assigned correctly. Example - incident records that have been reassigned to a higher tier but could have been handled at a lower tier.	Quality, Compliance
	Number of incidents reopened (system)	Number of incidents reopened after being closed (using the “Reopen” button in the IM module). Could be a result of closing the incident record without verifying resolution with the user.	Quality, Compliance
	Number of incidents reopened (administrator)	Number of incidents reopened after being closed. Administrator changes the status in a closed record.	Quality, Compliance
	Number of incidents canceled	Number of incidents canceled. Possible reason: Record is not an incident (ie. Service Request, Release, etc).	Quality, Compliance
	Number of incidents at each Status (e.g., Assigned, In Progress, Pending, etc)	Number of incidents broken down by the number at each stage of the IM process (e.g. Assigned, In Progress, Pending, etc.).	Quantity
	Number of Incidents by Time of Day	Breakdown of number of incidents by time of day. This report is useful in identifying times of the day/week when the volume of incidents is the highest and/or lowest. May be useful in assisting with determining staffing levels and performing workload projection analyses for Incident Management staffing. This proactive planning ensures adequate staffing and helps in the achievement of benchmarks for incident resolution times.	Quantity

Critical Success Factor	Key Performance Indicator	Definition (Explanation)	4 Vectors (Quantity, Quality, Timeliness, Compliance)
Customer Satisfaction	Number of User surveys sent / Number of User surveys responded to	Provides ratio (%) of surveys sent versus number of surveys responded to.	Quantity
	Average User survey score (total and by question category)	Average score (%) of all user surveys sent during reporting period (avg of all surverys and avg by question category).	Quality, Timeliness, Compliance
	Number of Incidents per user (top ten per user)	Top 10 users who reported the most incidents during the reporting period. It lists the sum of incidents by user name. For both submitter and user/customer.	Quantity
	Average queue time waiting for Incident response	Average amount of time a record is in a queue befor the user is contacted. This could be used to determine the amount of time before responding to a incident record submitted via email (ISC submitting a record "on behalf of").	Timeliness, Compliance
Resolving Incidents within established service times	Number of incidents logged	Number of incidents logged during reporting period.	Quantity
	Number/Percentage/Average of Incidents Resolved by Service Desk, Tier 2, Tier 3 & Tier 4	Number and percentage of incidents being resolved at each support tier. Can be used for resource planning purposes.	Quantity
	Average time to restore service for Priority 1, 2, 3 and 4 incidents (hours)	Average time (hours) to restore service (resolve the incident) for each priority incident (1, 2, 3 and 4). Also known as Mean Time To Repair (MTTR).	Quality, Timeliness
Quickly resolve incidents	Incidents reopen rate	Number of incidents reopened (after closed or resolved status) divided by total number of incidents.	Quality, Compliance
	Average time to resolve Priority 1, 2, 3 and 4 incidents (hours)	Average time (hours) to restore service (resolve the incident) for each priority incident (1, 2, 3 and 4). Also known as Mean Time To Repair (MTTR).	Timeliness, Compliance
	Number of incidents at each Status (e.g., Assigned, In Progress, Pending, etc)	Number of incidents broken down by the number at each stage of the IM process (e.g., Assigned, In Progress, Pending, etc.).	Quantity
	Number and percentage of incidents resolved remotely, without the need for a visit	Number and percentage of incidents resolved without the need for escalation to RDM or field service support.	Quantity
	Number and Percentage of Incidents Resolved at First Call	Number and percentage of incidents resolved during first call. Analysts should attempt, when possible, to resolve incidents on the first call by utilizing technical articles, remote control capabilities, user manuals, operations manuals and any other available capabilities.	Quantity, Quality

Critical Success Factor	Key Performance Indicator	Definition (Explanation)	4 Vectors (Quantity, Quality, Timeliness, Compliance)
Maintain IT service quality	Number of incidents in backlog for each IT service (i.e. Network services, Application services, etc)	Backlog - any records out of standards (resolution times).	Quantity, Quality, Timeliness, Compliance
	Number of incidents in Backlog	Detailed analysis of the number of incidents in the backlog. Can be used to ensure proper workload distribution and planning so that incidents are handled in a timely manner. It can also be used to compare the effectiveness of various groups.	Quantity, Quality, Timeliness, Compliance
	Incident resolution rate	Percentage (Number of incidents resolved divided by total number of incidents opened)	Quality, Compliance
	Number and percentage of major incidents for each IT service (i.e. Network services, Application services, etc) (Major = Critical and High priorities)	Number and percentage of major incidents (Critical and High priorities) for each IT service (i.e. Network services, Application services, etc)	Quantity
	User incident impact rate	Determines the impact of incidents upon users by dividing the total number of incidents with user impact by the total number of incidents reported. Incidents noticeabley and measurably impacted users, such as making services unavailable, damaging business files users depend upon, and so on, you would have a 15/20 (75%) user incident impact rate. Tells the successfulness at keeping incidents from impacting the users and can point to where stronger contols are necessary, where systems need to be adjusted, etc.	Quality, Compliance

APPENDIX E - REFERENCES

In meeting and achieving this process guidance, the following directives and documentation should be referenced to ensure compliance and support for the implementation of the IM process.

- Defense Enterprise Service Management Framework, (DESMF) version 3, Jun 2016
- ITIL® Service Strategy, Office of Government Commerce, TSO: 2011
- ITIL® Service Design, Office of Government Commerce, TSO: 2011
- ITIL® Service Transition, Office of Government Commerce, TSO: 2011
- ITIL® Service Operations, Office of Government Commerce, TSO: 2011
- ITIL® Continual Service Improvement, Office of Government Commerce, TSO: 2011
- Joint Publication 3-12 Cyberspace Operations, Feb 2013
- Marine Corps Commander's Readiness Handbook, May, 2014
- Marine Corps Strategy for Assured C2, March 2017
- MCO 5320.21, Information Technology Portfolio Management