

***Enterprise IT Service Management
Incident Management
Process Guide***



***Release Date:
14 April 2011***

Table of Contents

Section	Title	Page
1.0	Introduction	1
1.1	Purpose	1
1.2	Scope	1
1.3	Document and Process Change Procedures	2
2.0	Process Overview	3
2.1	Purpose, Goals, and Objectives	3
2.2	Relationships with other Initial Processes	4
2.3	High-Level Process Model	6
2.3.1	Process Description	9
2.4	Key Concepts	9
2.4.1	Commander's Critical Information Requirements	9
2.4.2	Incident	9
2.4.3	Incident Status	10
2.4.4	Notification	10
2.4.5	Operational Impact	10
2.4.6	Problem	10
2.4.7	Problem Management Database	10
2.4.8	Super-User	11
2.4.9	Incident Ownership	11
2.4.10	Tiered Support	11
2.4.11	Very Important Person	11
2.4.12	Work-Around	12
2.5	Quality Control	12
2.5.1	Metrics, Measurements and Continual Process Improvement	12
2.5.2	Critical Success Factors with Key Performance Indicators	12
3.0	Governance	15
3.1	Roles and Responsibilities	15
3.1.1	Roles	16
3.1.2	Responsibilities	21
3.2	Policies	22
4.0	Sub-Processes	23
4.1	Identification	23
4.2	Logging	24
4.3	Categorization	26
4.4	Prioritization	28
4.5	Request Fulfillment	31
4.6	Major Incident	32
4.7	Diagnosis and Resolution	35
4.8	Resolved?	37
4.9	Escalations and Transfers	38
4.10	Incident Closure	41
Appendix A – Acronyms		43
Appendix B – Glossary		44
Appendix C – Policies		47
Appendix D – IM System Record Attributes		48



List of Tables

Table	Title	Page
Table 1.	IM Process Activity Descriptions	8
Table 2.	Incident Status Designations	10
Table 3.	IM Critical Success Factors with Key Performance Indicators.....	13
Table 4.	IM Defined Roles and Responsibilities	17
Table 5.	Responsibilities for Enterprise IM	22
Table 7.	Operational Categorization Example	27
Table 8.	Urgency Matrix.....	29
Table 9.	Priority Matrix	29
Table 10.	IM Major Incident Sub-Process Descriptions	33
Table 11.	IM Diagnosis & Resolution Sub-Process Descriptions	36
Table 12.	IM Escalations and Transfers Sub-Process Descriptions	40
Table 13.	IM Incident Closure Sub-Process Descriptions.....	42

List of Figures

Figure	Title	Page
Figure 1.	Process Design Pyramid	2
Figure 2.	Enterprise Incident Management Ticket Flow.....	4
Figure 3.	IM Relationship with other Initial Processes	5
Figure 4.	High-Level IM Workflow	7
Figure 5.	IM Roles.....	16
Figure 6.	IM Logging Sub-Process	25
Figure 7.	IM Major Incident Sub-Process.....	33
Figure 8.	IM Diagnosis & Resolution Sub-Process	36
Figure 9.	IM Escalations and Transfers Sub-Process.....	39
Figure 10.	IM Incident Closure Sub-Process	42



Enterprise Incident Management Process Guide

1 1.0 INTRODUCTION

2 1.1 Purpose

3 The purpose of this process guide is to establish a documented and clear foundation for process
4 implementation and execution across the United States Marine Corps (USMC) enterprise.
5 Process implementation and execution at lower levels (e.g., Regional, Local, and Programs of
6 Record) must align and adhere to directives and schema documented within this guide. The
7 active use of this guide ensures USMC IT activities are executed in a uniform manner.

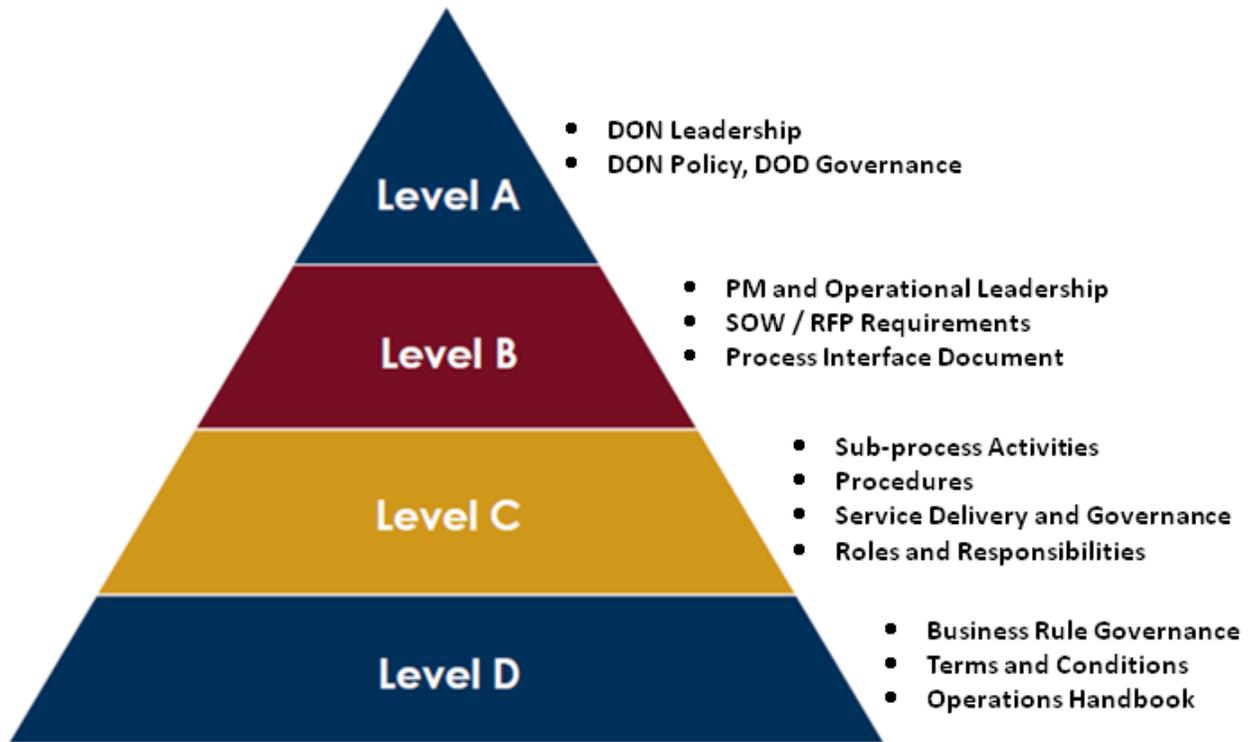
8 1.2 Scope

9 The scope of this document covers Marine Corps Enterprise IT Services (MCEITS) and garrison
10 Secret Internet Protocol Router Network (SIPRNet) related services owned by the USMC while
11 simultaneously providing a foundation for process implementation and execution across the
12 USMC enterprise. Information remains relevant for the global operations and defense of the
13 Marine Corps Enterprise Network (MCEN) as managed by Marine Corps Network Operations
14 and Security Center (MCNOSC) including all Regional Network Operations and Security
15 Centers (RNOSC) and Marine Air Ground Task Force Information Technology Support Center
16 (MITSC) assets and supported Marine Expeditionary Forces (MEF), Supporting Establishments
17 (SE) organizations, and Marine Corps Installation (MCI) commands.

18 This document uses the term “sub-process” to describe process layers that exist beneath the
19 parent process level. This sub-process layer is equivalent to process “Level C” as referenced in
20 the following diagram. Please note that procedures, also associated with Level C, are not
21 included within the scope of this document. The current Procedures and Work Instructions (PWI)
22 can be found at the following location:

23 https://ips.usmc.mil/sites/pg10docr/pm_ccr/E-ITSM/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2fsites%2fpg10docr%2fpm%5fccr%2fE%2dITSM%2fShared%20Documents%2fProcedure%20Work%20Instructions&FolderCTID=&View=%7b575B66E8%2dD286%2d4040%2d980A%2d12D8990F333E%7d
24
25
26





27

28

Figure 1. Process Design Pyramid

29 1.3 Document and Process Change Procedures

30 This document will be reviewed semi-annually for accuracy by the Process Owner with
31 designated team members. Modifications to this document are ultimately governed by the USMC
32 Enterprise Change Management (ChM) process. Please direct any questions or comments
33 concerning this document to the USMC Enterprise Service Desk at 1-800-TBD,
34 Support@usmc.smil.mil, Support@usmc.mil, or eitsm@usmc.mil. For detailed information on
35 process change requests, refer to Section 2.3 of the *Enterprise IT Service Management Change*
36 *Management Process Guide*.

37



38 2.0 PROCESS OVERVIEW

39 2.1 Purpose, Goals, and Objectives

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

45 The goal of IM is to restore normal service operation as quickly as possible in the event of
46 service degradation or interruption, and to minimize the adverse impact of such events on the
47 mission.

48 Primary objectives of the IM process include:

- 49 • Helping ensure higher availability of IT services by maintaining and improving the
50 ability to appropriately and quickly resolve incidents as they occur
- 51 • Dynamically assigning service resources to efficiently align IT work against mission
52 objectives via incident prioritization
- 53 • Maintaining a constant and accurate link with the Service Desk function to continually
54 improve the relationship between end users and IT operations

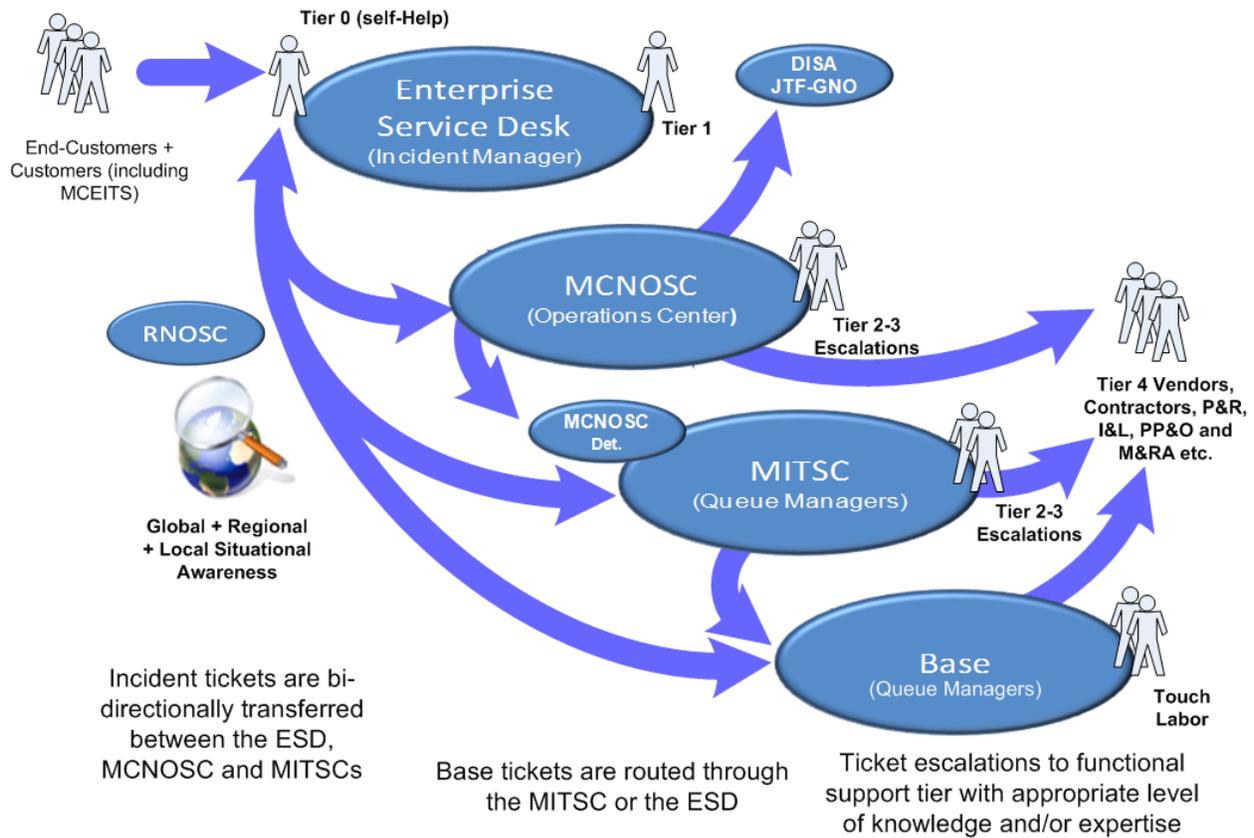
55 The Enterprise Service Desk (ESD), the functional component of the IM process, provides a
56 centralized Single Point of Contact (SPOC) and acts as a “storefront” for the USMC, enabling
57 the Marines to quickly and easily interface with IT operations. The ESD allows standard IT
58 issues to be resolved in a centralized, consolidated manner supportive of best practices and
59 enterprise visibility. Support provided by the ESD includes password resets, desktop application
60 support (e.g., Microsoft Office products, Microsoft Explorer, and Adobe Reader), Windows
61 operating system troubleshooting, and basic print and scanner support.

62 To ensure accurate categorization, prioritization, routing, transfers, data integrity and consistent
63 incident lifecycle processing, the following are ESD operational capability goals:

- 64 • Field incident requests and reports
- 65 • Own and manage incident records across the enterprise
- 66 • Coordinate IM actions across all USMC IT organizations
- 67 • Monitor status updates, proactively ensuring incidents are resolved or escalated within
68 pre-defined thresholds
- 69 • Ensure IM performance objectives are met
- 70 • Manage communications flowing back and forth across the enterprise



- 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



74

75 **Figure 2. Enterprise Incident Management Ticket Flow**

76 Note: While some incidents originate from regional sources (e.g., base/tenant, MITSC, RNOSC,
 77 etc.), they are logged and managed in a common toolset, in a consistent manner that aligns with
 78 the enterprise process, and within the visibility of the ESD. Incidents reported to the ESD that
 79 cannot be resolved by the ESD and appear to be confined to a single Base, must be routed to the
 80 appropriate MITSC. This enables the MITSCs to maintain real-time situational awareness of
 81 incidents that are occurring within their purview. Once USMC processes mature, the ESD will
 82 have the ability to route directly to a Base. Additionally, incidents that have left the ESD and
 83 need to be assigned elsewhere in the USMC organization are assigned back to the ESD to enable
 84 quality control for the incident (ensuring the incident quickly reaches the appropriate destination)
 85 and continual improvement of the transfers and escalations processes at the ESD.

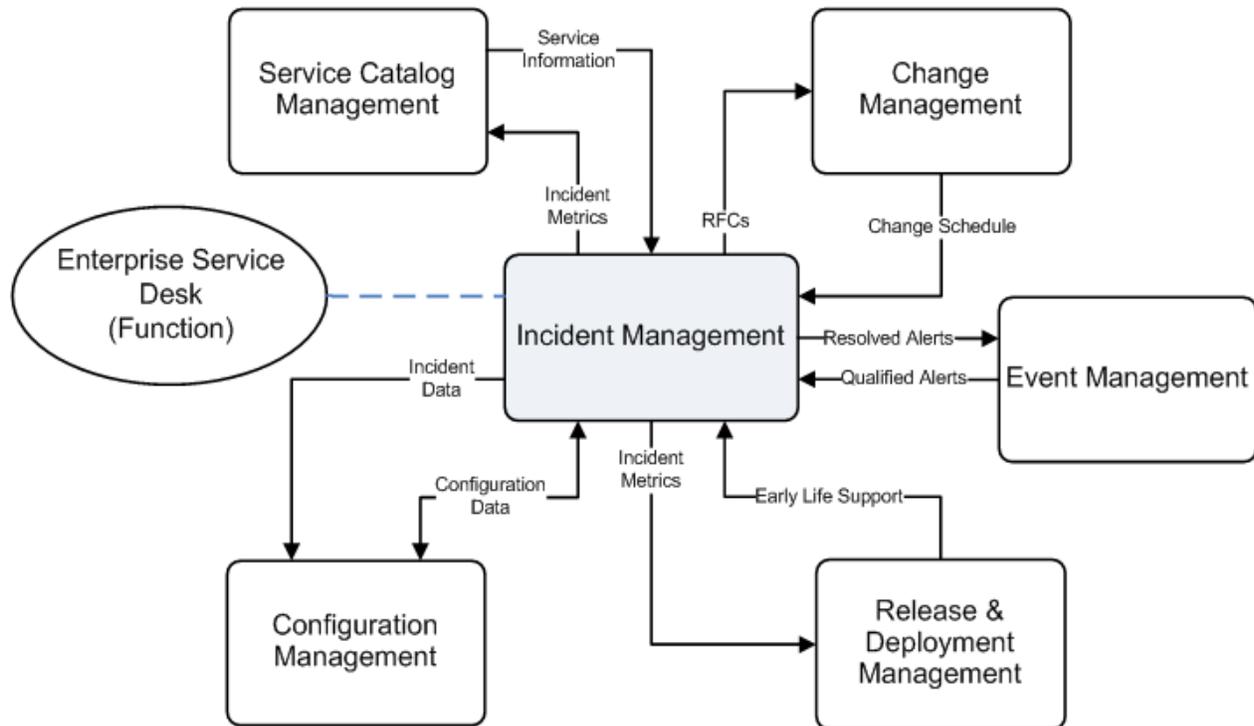
86 **2.2 Relationships with other Initial Processes**

87 All IT Service Management processes are interrelated. The six (6) Initial Processes in Figure 3
 88 were selected due to the strength of the relationships and dependencies between them and the
 89 degree to which they underpin USMC near-term objectives. While any one of the Initial



90 Processes can operate in the presence of an immature process, the efficiency and effectiveness of
 91 each is greatly enhanced by the maturity and integration of all Initial Processes. Figure 3 depicts
 92 key relationships that exist between IM and the other Initial Processes. This figure is not all-
 93 encompassing and the relationships shown can be direct or indirect.

94



95

96

Figure 3. IM Relationship with other Initial Processes

97 The following list describes the IM relationship (input or output) to other Initial Processes, as
 98 depicted in Figure 3:

99 **Service Catalog Management**

100 — Incident Metrics: Incident Management provides metrics regarding the health and
 101 welfare of services present in the IT Service Catalog.

102 — Service Information: The SC will provide service information in support of incident
 103 classification and prioritization.

104 **Change Management**

105 — RFCs: Some incidents will require a Request for Change (RFC) to execute corrective
 106 actions and restore service.

107 — Change Schedule: The Change Schedule is a valuable tool for the Service Desk and
 108 other key incident Management process stakeholders for the purposes of initial



109 diagnosis and troubleshooting. Determining “what changed?” is on the critical path to
110 rapid restoration of service. The Change Schedule can provide quick, valuable insight
111 into this activity.

112 **Event Management**

113 — Qualified Alerts: Events generated via the Event Management process and enabling
114 technologies that meet predefined incident criteria result in incidents to be managed
115 through the incident Management lifecycle.

116 — Resolved Alerts: Resolved Alerts are communicated back to the originating Qualified
117 Alert.

118 **Release and Deployment Management**

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

125 — Incident Metrics: incident metrics associated with releases are critical to continual
126 process improvement.

127 **Configuration Management (CFM)**

128 — Configuration Data: Configuration data, present in the Configuration Management
129 Database (CMDB), provides troubleshooting information to the Service Desk and the
130 incident Management process for the purposes of troubleshooting, diagnosis, and
131 resolution of incidents.

132 — Incident Data: incidents are linked to Configuration Items (CIs) in the CMDB. This
133 provides the Service Desk and other interested parties information regarding the
134 disposition of CIs and associated services, systems and applications.

135 **2.3 High-Level Process Model**

136 The IM process consists of twelve distinct sub-processes and is highly integrated with the
137 Change Management and Configuration Management (CfM) processes. The following workflow
138 depicts these processes and sub-processes that collectively enable and underpin IM. See Section
139 4.0 for complete descriptions of the sub-process activities.



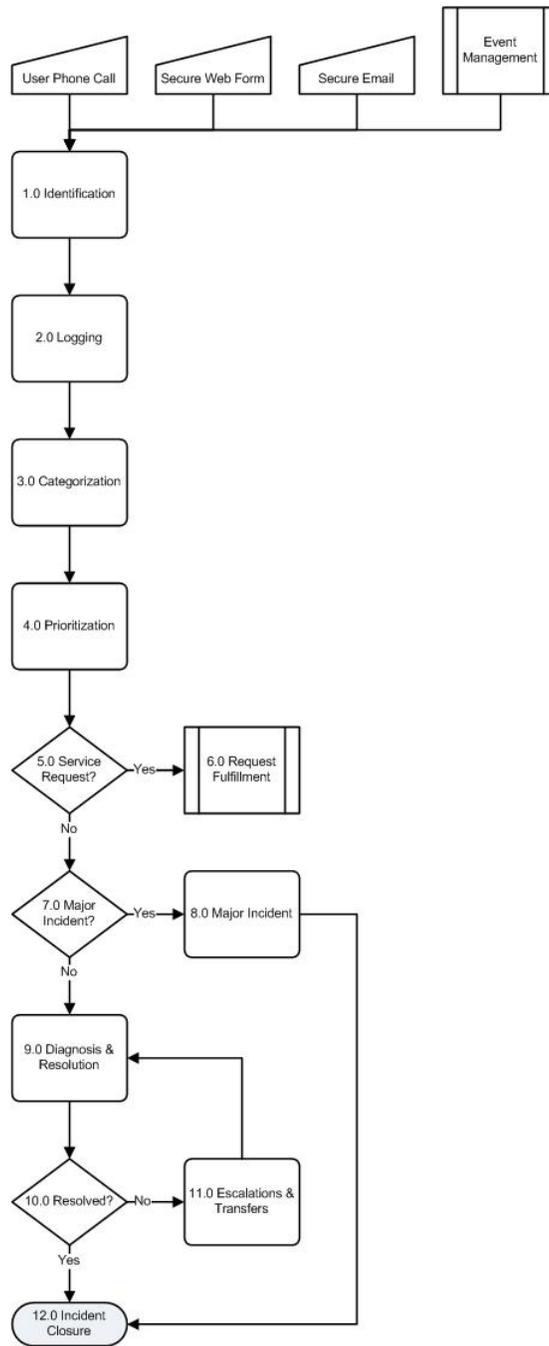


Figure 4. High-Level IM Workflow

140

141



142 Table 1 contains descriptions of each sub-process. As appropriate, sub-process numbers are
143 hyperlinked to its detailed description in Section 4.0, Sub Processes.

144 **Table 1. IM Process Activity Descriptions**

Number	Process Activity	Description
1.0	Identification	Incident identification is the act of learning an incident has occurred. Depending on the nature of the incident, the Analyst must determine whether to log the information in SIPRNet or NIPRNet ticketing system.
2.0	Logging	All incidents must be completely logged and date/time stamped, regardless of whether they are raised through the ESD, email, a web form or automatically detected via an event alert.
3.0	Categorization	This activity identifies the generic origin and symptoms of the incident. (The cause of the incident may or may not be known.) This may not be the final categorization of the incident, but the initial categorization helps determine how to initially handle the incident. The USMC incident categorization taxonomy will utilize both operational categories and product categories.
4.0	Prioritization	Incident priority is defined as the sequence in which incidents are to be worked. Priority is determined based on the impact and the urgency, the speed or time frame, within which resolution is required by the user or the mission. All Incident Managers, Incident Dispatchers, Queue Managers and Watch Officers at all levels of the organization are responsible to ensure priorities are accurately set and make adjustments as appropriate.
5.0	Service Request?	
6.0	Request Fulfillment	This is a standard service with a predefined approval process, low risk, well known and documented. Instead of following the incident process model, the ESD will follow a pre-defined Request Fulfillment process.
7.0	Major Incident?	
8.0	Major Incident	Major incidents have a high impact and high urgency. Tactical, VIP, timing and service considerations may likewise trigger a Major Incident. Incident Managers, Incident Dispatchers, 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.
9.0	Diagnosis & Resolution	This activity assesses incidents and all data associated with the incident in order to identify appropriate responses and actions, and to formulate incident Resolution Plans. When an ESD Analyst receives an incident, they will collect as much information as possible about the incident and utilize all available knowledge databases and support tools to resolve the incident at the 1 st Tier and within agreed time limits.
10.0	Resolved?	
11.0	Escalations & Transfers	Escalations and transfers are the process of routing an incident to the appropriate group for timely resolution. If the incident is not within the scope of the ESD services or capabilities, the incident is transferred to the MCNOSC or appropriate MITSC for resolution. If the incident is within the scope of the ESD services or capabilities, and if the ESD Analyst is unable to resolve the incident, the incident should be Functionally and/or Hierarchically Escalated to the appropriate resolver group or senior officer within the MCNOSC.
12.0	Incident Closure	Incident closure is the act of confirming the resolution with the originator of the incident and closing the incident. If the originator fails to respond or cannot be contacted to close the resolved incident within 7 days via multiple automatic attempts, the resolved record can be automatically closed. Before the incident is closed, the ESD analyst should confirm the incident has been



Number	Process Activity	Description
		categorized correctly and work history notes are complete.

145

146 2.3.1 Process Description

147 The primary goal of the IM process is to restore normal service operation as quickly as possible
 148 and minimize the adverse impact on business operations, thus ensuring that the best possible
 149 levels of service quality and availability are maintained. Normal service operation is defined as
 150 service operation within Service-Level Agreement (SLA) limits. The IM process also handles
 151 Service Requests for standard services supported within the SLAs.

152 The scope of the IM process includes a standard set of processes, procedures, responsibilities,
 153 and metrics utilized by all MCEITS and garrison SIPRNet-related services applications, systems
 154 and network support teams.

155 2.4 Key Concepts

156 The following Key Concepts describe concepts that are utilized extensively in this IM Process
 157 Guide:

158 2.4.1 Commander's Critical Information Requirements

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

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

173 2.4.2 Incident

174 An incident is defined as an unplanned interruption or reduction in service quality to an IT
 175 service. Incidents can include hardware and software errors. Incidents can be created manually
 176 through methods such as secure email, a phone call to the ESD or a secure web form. Incidents
 177 can also be generated from Event Management.



178 2.4.3 Incident Status

179 An Incident Record passes through a lifecycle on the way to closure. Incident Record status
180 codes identify the stages of the work toward incident resolution, which is critical for reporting
181 and for continual process improvement. Depending on the tool implementation and reporting
182 requirements, status codes can have sub-statuses. For example, there may be status/sub-status
183 combinations such as “Pending – Customer info/verification” or “Pending – Vendor
184 equipment/info”. Guidance for the top-level status designations are shown in Table 2.

185 **Table 2. Incident Status Designations**

Status	Designation
Assigned	Incident has been identified, logged and assigned
Pending	Waiting on input from third party (includes RFC)
In-Progress	A resolver group is currently working on resolving the incident
Resolved	Incident has been resolved and is pending acknowledgment
Cancelled	User contacts the ESD and cancels the incident
Closed	Incident record closed (see Closure Codes for additional information)

186

187 2.4.4 Notification

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

194 2.4.5 Operational Impact

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

198 2.4.6 Problem

199 A problem is a cause of one or more incidents. The cause is not usually known at the time a
200 Problem Record is created, and the Problem Management Process is responsible for further
201 investigation.

202 2.4.7 Problem Management Database

203 The Problem Management Database contains information pertaining to actual or potential
204 disruptions of service that are being analyzed to determine their root cause. Individuals who are
205 attempting to resolve incidents may find that similar incidents are listed in the Problem
206 Management Database, which means that Problem Management is aware of the situation and are
207 attempting to find a resolution.



208 **2.4.8 Super-User**

209 With the diversity of needs and geographical spread of USMC, a Super-User is required to
210 facilitate quick resolution of some incidents. A Super-User is a pre-designated person(s)
211 authorized to assume temporary elevated access controls and authorizations for the purpose of
212 resolving high priority incidents or incidents involving VIPs. These elevated rights are granted
213 once the Super-User opens a record with the ESD and is validated as a pre-designated Super-
214 User. The ESD will be responsible for monitoring the resolution of the incident and rescinding
215 the elevated rights once the incident has been resolved or passed along to other processes such as
216 Problem Management or Change Management.

217 **2.4.9 Incident Ownership**

218 Throughout the lifecycle of an incident in IM, the ownership of the incident remains with the
219 ESD at all times. The ESD is responsible for tracking progress, SLA compliance, keeping
220 stakeholders informed and ultimately for incident Closure.

221 **2.4.10 Tiered Support**

222 There are five (5) possible support tiers. Tier 0 is self-help and web options that permit users to
223 resolve their incidents without ESD assistance. The 1st Tier is the ESD. For open records logged
224 into the IM tool, 1st Tier ESD Analysts track all activities/statuses of the incident and are the
225 single point of contact for the customer throughout the lifecycle of the incident.

226 The 2nd and 3rd Tier Analysts provide functional escalation support and come from organizations
227 such as the MCNOSC, MITSC and MCEITS SIE. The 2nd Tier Analyst Staff consists of
228 personnel with greater (but still generalist) technical skills than the ESD Analyst. The 2nd Tier
229 Analyst has dedicated time to devote to incident diagnosis, and resolution without interference
230 from telephone interruptions. The 3rd Tier Analyst has subject matter expertise and/or the higher
231 level security access required to resolve incidents. This role focuses on complex issues related to
232 operational aspects that cannot be resolved by 1st or 2nd Tiers. This role performs in-depth
233 technical incident investigation, diagnosis and resolution, and provides knowledge and training
234 support to the 1st Tier support group.

235 The 4th Tier is comprised of vendors, contractors or other organizations such as USCYBERCOM,
236 HQMC I&L, HQMC PP&O, and DISA that are outside the influence or governance of the
237 USMC E-ITSM processes.

238 **2.4.11 Very Important Person**

239 Within nearly every organization there are individuals, referred to as a Very Important Person
240 (VIP) who require an enhanced level of response and/or support. VIP is defined across the
241 USMC as “General Officers or their Senior Executive Service (SES) civilian equivalents”. Based
242 upon the total number of VIPs within a particular region, a MITSC is allocated additional
243 manpower resources. This extra touch labor is meant to provide a faster response time (i.e., more
244 stringent SLA) for VIP service requests in the garrison environment. MITSCs are authorized to
245 locally designate other individuals as a VIP; however, services for non-General Officer/SES



246 VIPs are provided at the MITSCs own expense and with an obligation to still meet SLAs for
247 non-VIP users.

248 Given this guidance, and in order to maintain an appropriate level of pre-designated VIPs,
249 MCNOSC, MITSC and Base VIP lists will be subject to regular review. Furthermore, it is at the
250 discretion of the Watch Officer to evaluate tactical, priority, operations tempo and “point in
251 time” factors and, when appropriate, temporarily escalate certain normal users to VIP status.

252 **2.4.12 Work-Around**

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

255 **2.5 Quality Control**

256 **2.5.1 Metrics, Measurements and Continual Process Improvement**

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

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

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

271 **2.5.2 Critical Success Factors with Key Performance Indicators**

272 CSFs are defined as process- or service-specific goals that must be achieved if a process (or IT
273 service) is to succeed. KPIs are the metrics used to measure service performance or progress
274 toward stated goals.

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

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



Table 3. IM Critical Success Factors with 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 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	
		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	
2	Customers are satisfied with Enterprise Service Desk performance	5	Customer Satisfaction Rating Calculation: Customer Satisfaction Surveys	Increased customer satisfaction and utilization of the ESD is encouraged
		6	Average time to answer Calculation: Elapsed time between customer call initiated and customer call answered (Automated Call Distribution)	
		7	Average Response Time Calculation: Average time between customer contact and response from the Enterprise Service Desk back to the customer (this measure will be focused on email/web customer contacts)	



CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Benefits
3	Accurate escalation	8	<p>% of incidents accurately routed by the Enterprise Service Desk on the first attempt</p> <p>Calculation: Escalated incidents not routed back to the Enterprise Service Desk (business process to require that misrouted incidents be sent back to the ESD for further action)</p>	Efficient utilization of IM support operations resources. Reduction in downtime and increase in end user satisfaction.
4	USMC community utilization of the Enterprise Service Desk	9	<p>Trend analysis of ESD contact volume and tickets logged</p> <p>Calculation: Comparison trending of contact volume and total tickets logged over incremental time periods (week, month, quarter, and year).</p>	Efficient utilization of IM support operations resources and realization of ESD goals and objectives

280
281



282 3.0 GOVERNANCE

283 Governance deals with the authority and accountability for directing, controlling and executing
284 IT services. IT governance involves creating the governing principles. This includes:

- 285 • Who makes directing, controlling, and executing decisions
- 286 • How the decisions are made
- 287 • What information is required to make the decisions
- 288 • What decision making mechanisms should be required
- 289 • How exceptions are handled
- 290 • How the governance results should be reviewed and improved

291
292 Enterprises have always strived for effective administration, direction and control. However,
293 there is an increased focus on IT governance because of federal regulations related to privacy,
294 anti-terrorism, security and other factors.

295 IT governance encompasses the organizational structures and IT management processes used to
296 sustain and extend strategies and objectives. Clearly defining roles and responsibilities within
297 each process is a critical activity of IT governance for the USMC. By introducing controlled
298 governance, the level of transparency and accountability within IT operations is improved,
299 thereby reducing risks while linking IT goals with USMC mission accomplishment.

300 3.1 Roles and Responsibilities

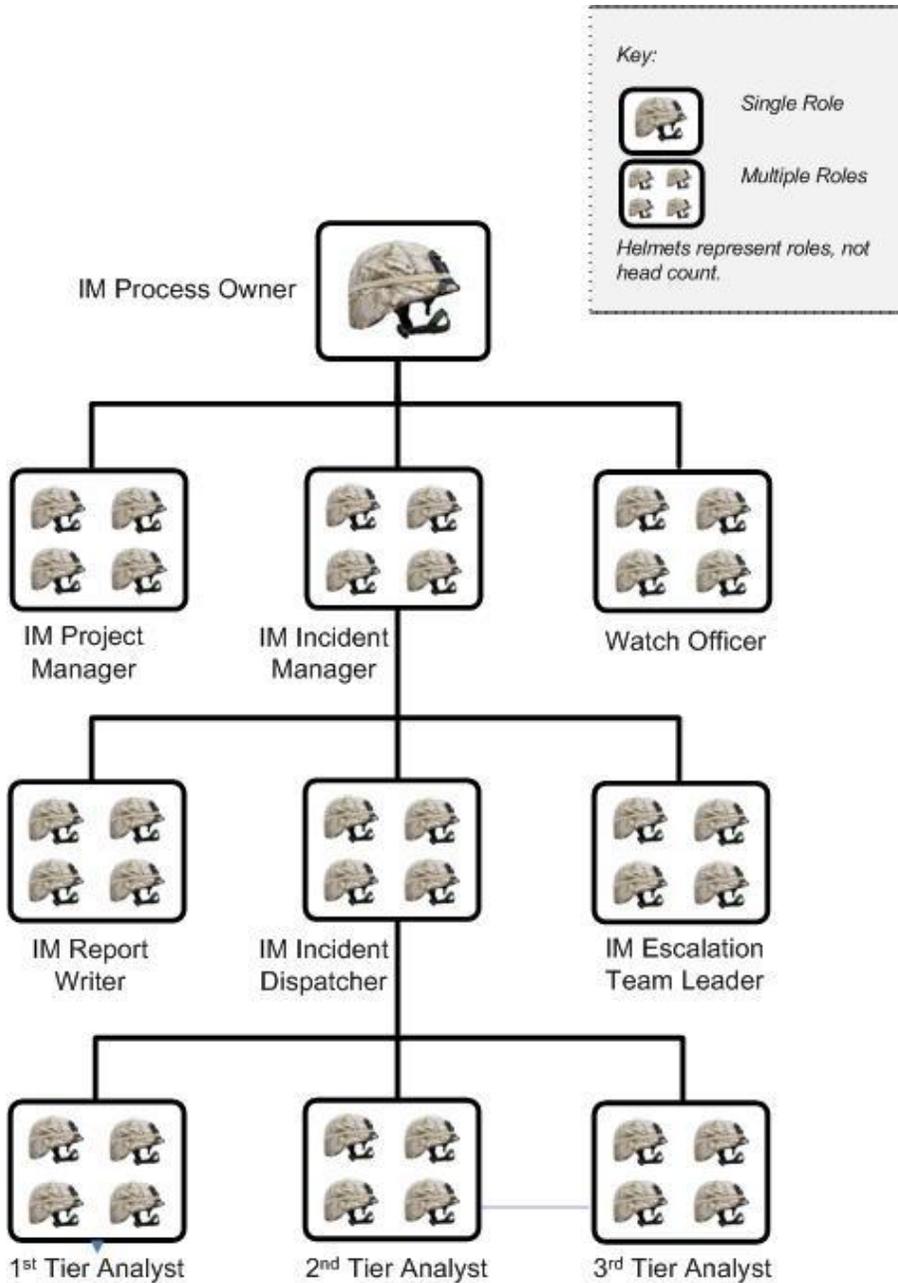
301 Each process has roles and responsibilities associated with design, development, execution and
302 management of the process. A role within a process is defined as a set of responsibilities. Process
303 Managers report process deviations and recommended corrective action to the respective process
304 owner. Authoritative process guide control is under the purview of the Process Owner. The
305 Process Owner for IM will be from the MCNOSC organization.

306 Management (i.e., responsibility) of a process may be shared; generally, a single manager exists
307 at the MCNOSC enterprise and at each MITSC. For certain processes, especially those within
308 Service Design and Service Transition, managers also exist within Marine Corps Systems
309 Command (MARCORSYSCOM) and Programs of Record. Some Service Operation processes
310 (e.g., Event Management) will require managers at the RNOSC. There will be instances where
311 roles are combined or a person is responsible for multiple roles. Factors such as AOR, size of
312 user base and size of the process support team dictate exactly which roles require a dedicated
313 person(s) and the total number of persons performing each role. This process guide defines all
314 *mandatory* roles.



315 **3.1.1 Roles**

316 The following abstract drawing (Figure 5) depicts process roles for the USMC, followed by a
317 description of these roles.



318

319

Figure 5. IM Roles



Table 4. IM Defined Roles and Responsibilities

Description	Overall Responsibility
Role #1 IM Process Owner	
<p>The Process Owner owns the process and the supporting documentation for the process. The primary functions of the Process Owner are oversight and continuous process improvement. To these ends, the Process Owner oversees the process, ensuring that the process is followed by the organization. When the process isn't being followed or isn't working well, the Process Owner is responsible for identifying and ensuring required actions are taken to correct the situation. In addition, the Process Owner is responsible for the approval of all proposed changes to the process, and development of process improvement plans.</p> <p>May delegate specific responsibilities to another individual within their span of control, but remains ultimately accountable for the results of the IM process.</p>	<ul style="list-style-type: none"> • Reviews effectiveness and efficiency of the IM/Service Request Process at all levels of the enterprise • Establishes Procedures for IM/Service Request and ensures they are implemented and adhered to at all levels of the enterprise • Defines and develops IM/Service Request metric requirements, then works with the metrics team to produce reports • Ensures IM/Service Request processes and tools integrate with other ITSM processes and that requirements for the tools are defined • Responsible for the success or failure of the process with the authority to make changes and represent management decision. This is imperative for processes that are cross-functional, spanning organizational boundaries • Ensures the process is defined, documented, maintained, and communicated at an organizational level • Decision maker on any proposed enhancements to the process • Ensures organizational adherence to the process • Responsible for the requirement and guidelines of the IM/Service Request tool usage • Establishes and communicates the process roles and responsibilities • Provides the strategic direction for the IM/Service Request tool/system • Establishes and communicates the process, service levels, process metrics, and process performance metrics • Responsible for service financial modeling and budget analysis • Monitors and reports on the performance of the process • Identifies and communicates opportunities for process improvement • Initiates and sponsors projects to improve or reengineer the process • Manages changes to the process, including reviewing and approving all proposed changes and communicating changes to all the participants and affected areas • Benchmarks the process performance • Participates in other ITSM process initiatives and process reviews
Role #2 Watch Officer	
<p>The Watch Officer 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.</p>	<ul style="list-style-type: none"> • Reviews effectiveness and efficiency of the IM/Service Request Process at their level of the enterprise • Ensures IM/Service Request 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 at their level • 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



Description	Overall Responsibility
	<p>actions</p> <ul style="list-style-type: none"> • Manages and uses a trouble ticket 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/Service Request process • The Watch Officer also is accountable for the activities and resources required to resolve escalated incidents <ul style="list-style-type: none"> — 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 — 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 #3 IM Incident Manager	
<p>The Incident Manager ensures effective coordination of activities to restore service. 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 their counterparts on incidents or the process</p>	<ul style="list-style-type: none"> • Awareness of USMC and DoD directives • Interfaces with Watch Officer and Queue Managers • Communicates command requirements and directives as it relates to IM to subordinate Incident Managers and Dispatchers • Requests, reviews, and reports on metrics • Provides management information on IT Service Quality and Customer satisfaction • Manages support staff performance of the IM/Service Request



Description	Overall Responsibility
when required/beneficial.	<p>process, creating and executing action plans when necessary to ensure continuous improvement</p> <ul style="list-style-type: none"> • Allocates resources • Detects possible Problems and assigns them to the Problem Management team to establish Problem Records • Assists the support engineers through the IM/Service Request process within the support engineering domain • Analyzes and correlates incoming real-time incidents • Identifies opportunities to improve the process • The Watch Officer also is accountable for the activities and resources required to resolve escalated incidents <ul style="list-style-type: none"> — Performs escalation and prioritization evaluations — Understands the business impact of the escalated incident or Service Call — 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 closes escalation after customer's approval — Uses escalation post-mortem review results to determine follow up actions — Develops, documents and follows up on action plans — Provides data on escalation history and manages requests for information regarding escalations — Ensures that Emergency RFCs required as part of the escalation process are documented — Schedules and facilitates escalation meetings and phone teleconferences — 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 #4 IM Incident Dispatcher	
The Incident Dispatcher ensures effective coordination of activities to restore service with a primary focus on escalations, prioritizations, routing and queue management.	<ul style="list-style-type: none"> • 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/Service Request process, creating and executing action plans when necessary to ensure continuous improvement • Assists the support engineers through the IM/Service Request process within their domain • Identifies opportunities to improve the process
Role #5 IM Escalation Team Leader	
A Senior Technical Expert with experience in project management, working in/with teams and expertise in solving and resolving the most complex of incidents.	<ul style="list-style-type: none"> • Addresses complex issues related to operation aspects that cannot be resolved at lower level support • Investigates, diagnoses, and resolves incidents • Manages/directs an Escalation Team in solving a complex outage • Interfaces with third party vendors as required for incident resolution



Description	Overall Responsibility
Role #6 3rd Tier Analyst	
<p>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.</p>	<ul style="list-style-type: none"> • 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 • Detects potential Problems and informs the Incident Manager • 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 customer/caller regarding quick fixes • Provides knowledge and training to lower level support teams
Role #7 2nd Tier Analyst	
<p>The 2nd Tier Analyst Staff consist of personnel with greater (but still generalist) technical skills than the 1st Tier Analyst. The 2nd Tier Analyst supports incident diagnosis and resolution without interference from telephone interruptions.</p>	<ul style="list-style-type: none"> • 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 Customer/caller regarding quick fixes • Attempts second level incident resolution • 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	
<p>The 1st Tier Analyst interfaces with the Customer as the initial point of contact in the IM process. The 1st Tier owns the incident records he or she generates (i.e., incidents or Service Requests). 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.</p>	<ul style="list-style-type: none"> • Welcomes customers by phone, web, mail, or other authorized means • Authenticates the caller (check information in the Global Address List, confirm location, etc.) • Creates a Service Request or incident record in the Incident/Service Request Control system • Categorizes the record (i.e., Incident or Service Request) • Applies procedures applicable to the customer/caller/categories • Qualifies Service Request/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 help



Description	Overall Responsibility
	desk and other staff/interested parties <ul style="list-style-type: none"> Once a record is reported as resolved, ensures the customer agrees the resolution provided addresses the incident reported. Either closes the record or returns the record to the Incident Manager for further work Informs procedure owners if issues are detected in procedures
Role #9 IM Report Writer	
The IM Report writer is responsible for the design, modification and publishing of all enterprise IM reports as well as ad-hoc reporting, as required by the Incident Manager.	<ul style="list-style-type: none"> 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
Role #10 IM Project Manager	
Responsible for forming and leading project teams that undertake planned and ad hoc projects in support of the USMC IM process implementation and operations	<ul style="list-style-type: none"> Works with Service Transition Team to ensure ESD Analyst staff are properly trained, required documentation has been prepared, and the IM Tool has been correctly updated before ESD assumes the support of a new service Works with service providers to update and optimize the service specific attributes of the categorization taxonomy Leads projects to implement USMC IM processes at the MITSCs and Bases. Provides ongoing support to these MITSCs and Bases Coordinates communications and meetings between the Incident Managers and Incident Dispatchers

321

322 **3.1.2 Responsibilities**

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

327 The Responsible, Accountable, Consulted, Informed, Participant (RACI-P) model is a method
 328 for assigning the type or degree of responsibility that roles (or individuals) have for specific
 329 tasks. Table 5 displays the department level RACI-P model for incidents fielded by the ESD.

330 **Responsible** – Completes the process or activity; responsible for action/implementation. The
 331 degree of responsibility is determined by the individual with the ‘A’.

332 **Accountable** – Approves or disapproves the process or activity. Individual who is ultimately
 333 answerable for the task or a decision regarding the task.

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



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

338 **Participant** –Assists ‘R’ in the execution of the process and/or activity.

339 Table 5 establishes responsibilities for high-level process activities by organization.

340 **Table 5. Responsibilities for Enterprise IM**

IM Process Activities	Enterprise Service Desk	MCNOSC	RNOSC	MCSC	MCCDC	MITSC	Base
Identification	RC	ACP				PC	PC
Logging	RC	ACP					
Categorization	RC	ACP				C	C
Prioritization	RC	ACP	C			C	C
Request Fulfillment	RC	ACP		P		P	P
Major Incident	RC	ACP	C	P	I	P	P
Diagnosis & Resolution	RC	ACP	I			P	P
Escalations & Transfers	RC	ACP	I	P		CP	CP
Incident Closure	RC	ACP					

Legend:
Responsible (R) – Completes the process or activity
Accountable (A) – Authority to approve or disapprove the process or activity
Consulted (C) – Experts who provide input
Informed (I) – Notified of activities
Participant (P) – Assists in execution of process or activity

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

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

341

342 **3.2 Policies**

343 This process requires the following policy for success:

- 344 • Compliance with Governance requirements (see Appendix C for more information)
 - 345 a. FCAPS standard is followed, providing control for daily operations and systems
 - 346 administrative support interacting with DISA and at the RNOSCs
 - 347 b. DIACAP requirements for releases that affect the security posture of the network
 - 348 are followed
 - 349 c. DoD compliance including Common Criteria Certifications

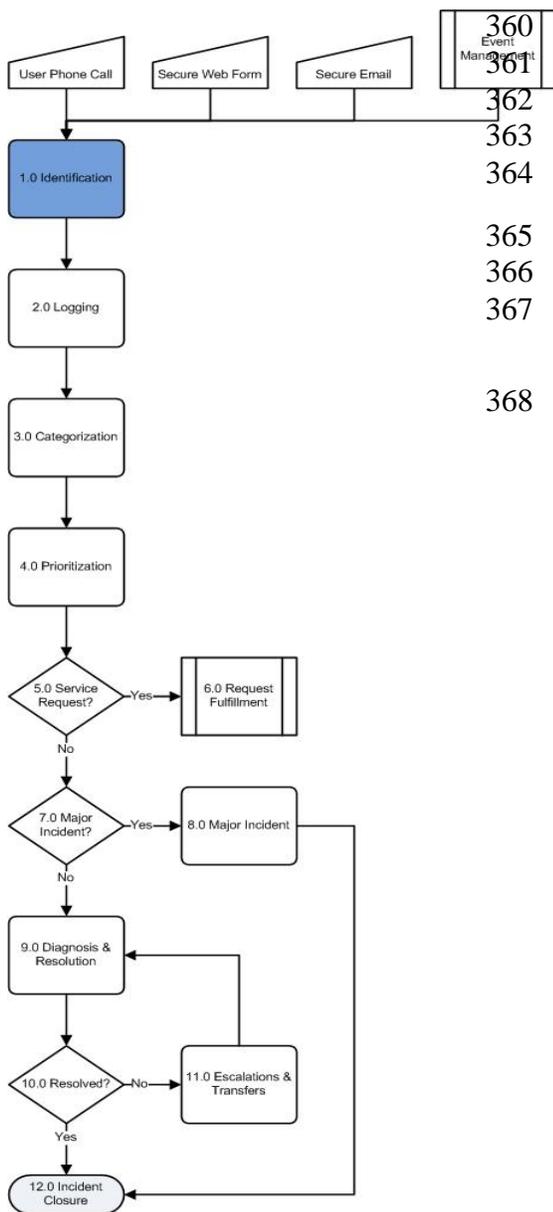
350



351 4.0 SUB-PROCESSES

352 The USMC IM process consists of 12 sub-processes. While every incident will follow each sub-
353 process on some level, not every activity within each sub-process is utilized for every USMC
354 organization or type of incident/request. For example, a standard change request is pre-approved,
355 low risk, occurs frequently, and is low cost. A standard change request is usually unique to a
356 MITSC and will not utilize every process step of Escalations and Transfer. Because requests and
357 incidents vary in the support required in the USMC IM process, examination at the sub-process
358 is required.

359 4.1 Identification



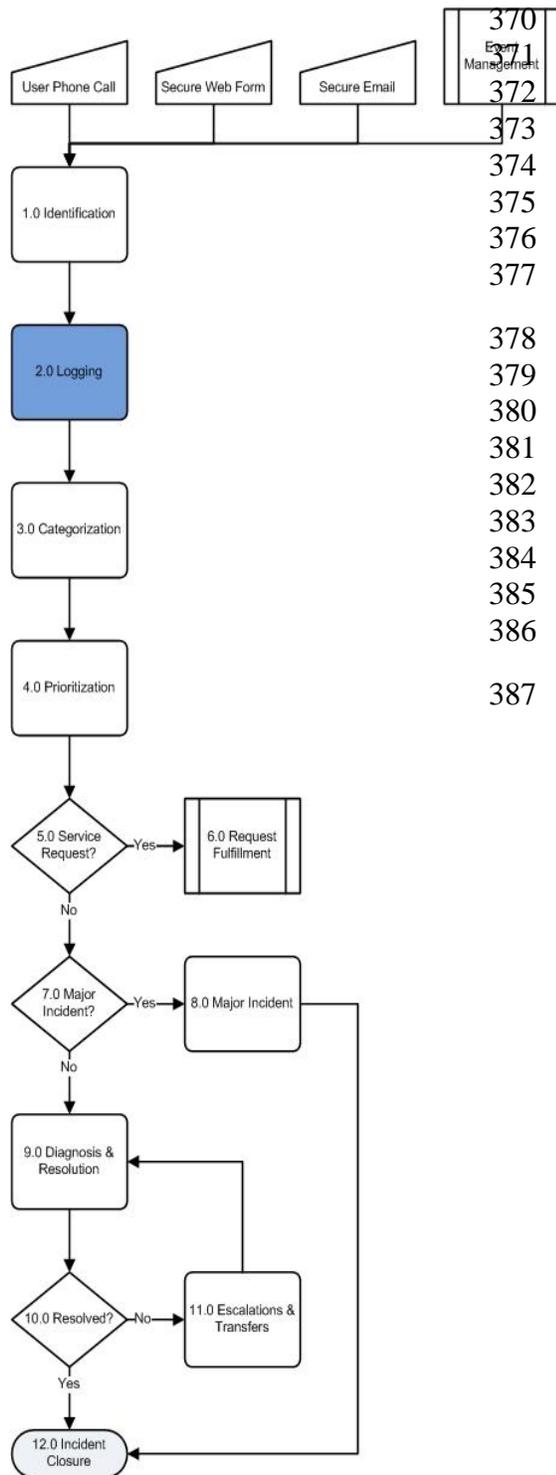
360 Incidents originate via the phone, email, web forms
361 and Event Management. The first step in the IM
362 process is to determine if the incident should be
363 logged in the classified (SIPRNet) or unclassified
364 (NIPRNet) ticketing system.

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

368



369 4.2 Logging



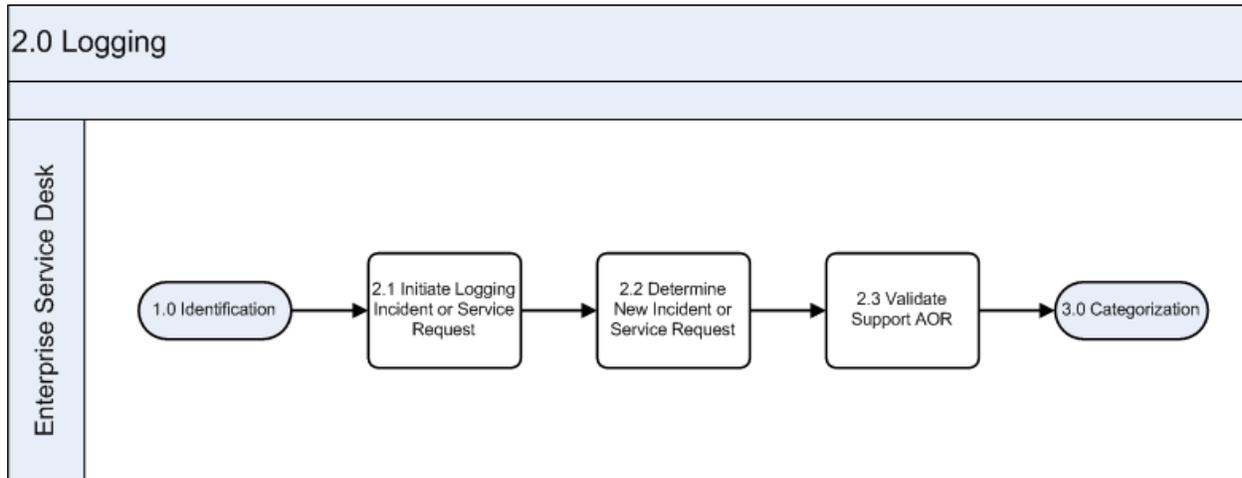
370 For an incident to be managed by the ESD, the
371 incident must be confirmed that the incident meets
372 the USMC IM criteria and is in the AOR of the
373 ESD. The identity of the person reporting the
374 incident must be confirmed. If they are calling on-
375 behalf (proxy) of another person, the proxy must be
376 identified along with the identity information for
377 the person for which they are the proxy.

378 Regardless of the incident's origin, the incident
379 must be manually or automatically date/time
380 stamped and logged into the IM tool to be
381 actionable. If an incident or request is not logged in
382 the IM tool, the incident or request cannot be
383 supported. If a technician is asked to solve an issue,
384 they must open an incident report. Logging is
385 absolutely essential for accurate reporting, tracking
386 and SLM.

387



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



389

390

Figure 6. IM Logging Sub-Process

391 Table 6 describes the Logging sub-process steps as depicted in Figure 6.

392

Table 6. IM Logging Sub-Process Descriptions

2.0 Logging		
Number	Process Activity	Description
2.1	Initiate Logging Incident or Service Request	The Analyst searches for the Customer record, confirms essential information and begins logging the issue.
2.2	Determine New Incident or Service Request	The Analyst searches the Customer records to determine whether the inquiry is regarding an existing Incident or Service Request or if a new Incident or Service Request is required. 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.
2.3	Validate Support AOR	The Analyst further determines if the inquiry is within the MCEN Area of Responsibility (AOR), updates the Customer on the next step in the process and routes the Incident or Service Request accordingly.

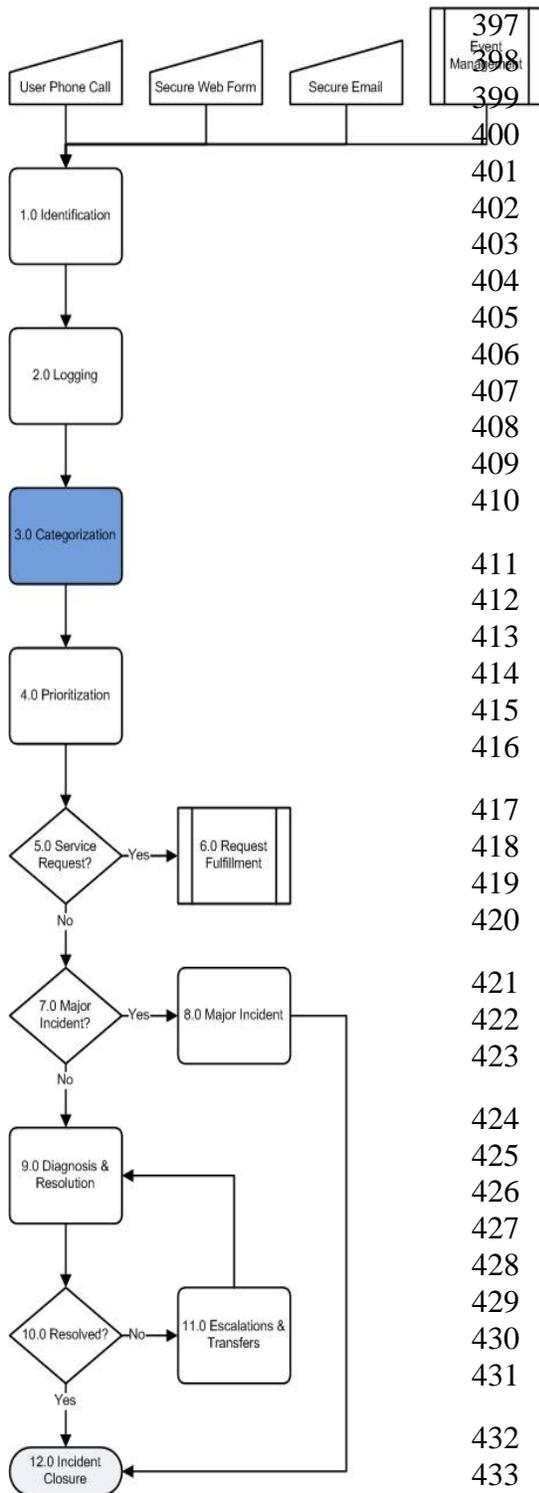
393

394 Consult [Appendix D: IM System Record Attributes](#) for a complete listing of logging attributes.

395



396 **4.3 Categorization**



Accurate categorization of incidents helps to establish correct routing, enabling a faster time to resolution. Additionally, incident analysis based on categorization proactively supports Problem Management. Because incident categorization is a critical input to downstream incident activities as well as other service management processes, it is essential to identify the appropriate level of detail required to meet the business of the organization. The specific categorization taxonomy utilized will depend on the tool selected and desired metrics for reporting. Industry best practices 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 to 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 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 quality 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 7 provides an example of operational categorization.



434

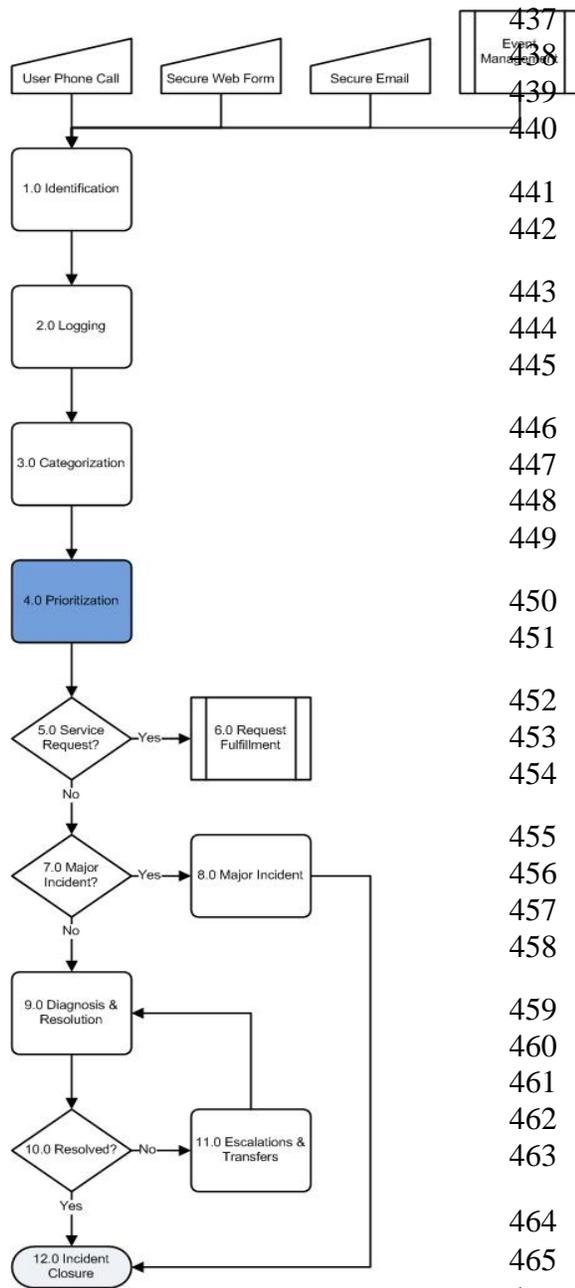
Table 7. Operational Categorization Example

Operational Categorization		
Tier 1	Tier 2	Tier 3
Hardware Action	Move	Same Building
		Different Building
	Add/Install	Approved Hardware
		Unapproved/Non-Standard Hardware
	Change Existing	
	Replace/Swap	Improve Utility or Performance
		Lemon – Previous Issues
	Error/Defect/Repair Physical	Error Message
		No Error Message
	Error/Defect/Repair Logical or Firmware	Error Message
		No Error Message
	Performance/Slowness	
	Decommission	
	User Error	
Training/How-To		
Other	Request New Category	
	Don't Request New Category	

435



436 **4.4 Prioritization**



437 This Prioritization process applies exclusively to
438 incidents. Service requests will be prioritized and
439 handled in accordance with service-level
440 objectives, unique to each service request type.

441 Every incident must be correctly prioritized. The
442 incident priority determines:

443 The type and number of resources necessary to
444 reach the service-level objective for each level of
445 priority (e.g., response, resolution, and updates)

446 The criteria used to determine the timing by which
447 technical resources and leadership personnel are
448 engaged to manage the incident through to
449 resolution and closure

450 The criteria used for Functional and Hierarchical
451 Escalation

452 The level of visibility the event will receive across
453 the organization (to be accomplished via
454 Hierarchical Escalation)

455 Before a priority determination of an incident can
456 be reached, the impact and the urgency must be
457 evaluated. Impact plus urgency determines
458 priority.

459 The criteria for determining impact is relative to
460 an organization’s echelon, AOR, operations
461 tempo, operational situations and the status of the
462 person(s) impacted. Other relevant aspects of
463 impact to consider include, but are not limited:

- 464 • Number of users affected
- 465 • Type of service(s) affected
- 466 • Degree to which the service is affected

467
468 Urgency is defined as the necessary speed to resolve the incident and should not be based on the
469 service or the number of customers affected. When evaluating urgency consider the customer’s
470 required time to resolution and the availability of a work-around. Other relevant aspects of
471 urgency to consider include, but are not limited to:

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



- 474 • Point in time – Is a critical deployment or tactical operation underway that is being
475 impacted by the event? Is a time sensitive business process or operation underway, for
476 example payroll processing
- 477 • Service-level or operating-level targets or objectives
- 478 • Risk - Is a combination of the likelihood of a mission disruption occurring and the
479 possible loss that may result from such mission disruption.

480 Table 8. provides general guidance for establishing incident urgency at the primary echelons,
481 under “normal” operating conditions and involving non-VIP users. The exact required resolution
482 times for echelons, MITSCs, bases, and commands will be determined at the time of
483 implementation.

484 **Table 8. Urgency Matrix**

IM Urgency Matrix	
Level	Description
Critical	Immediate resolution (of an Incident) or fulfillment (of a Service Request) is required <ul style="list-style-type: none"> ○ 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- <ul style="list-style-type: none"> ○ Risk is high that Impact will increase significantly if immediate resolution is not achieved -Or- <ul style="list-style-type: none"> ○ The customer billet or mission is such that immediate resolution or fulfillment is required
High	<ul style="list-style-type: none"> ○ No workaround exists however work can be temporarily shifted to other activities to maintain productivity -Or- <ul style="list-style-type: none"> ○ There is plausible risk that Impact will increase if resolution is not achieved
Medium	<ul style="list-style-type: none"> ○ A workaround exists but productivity is effected -Or- <ul style="list-style-type: none"> ○ A system or service is available, but degraded
Low	<ul style="list-style-type: none"> ○ A workaround exists and/or productivity effect is minimal or non-existent ○ Routine Work

485
486 By evaluating the impact and urgency, it is possible to assign priority to the incident, as shown in
487 Table 9.

488 **Table 9. Priority Matrix**

URGENCY	IMPACT			
		Extensive / Widespread 9	Significant / Larger 5	Moderate / Limited 3
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

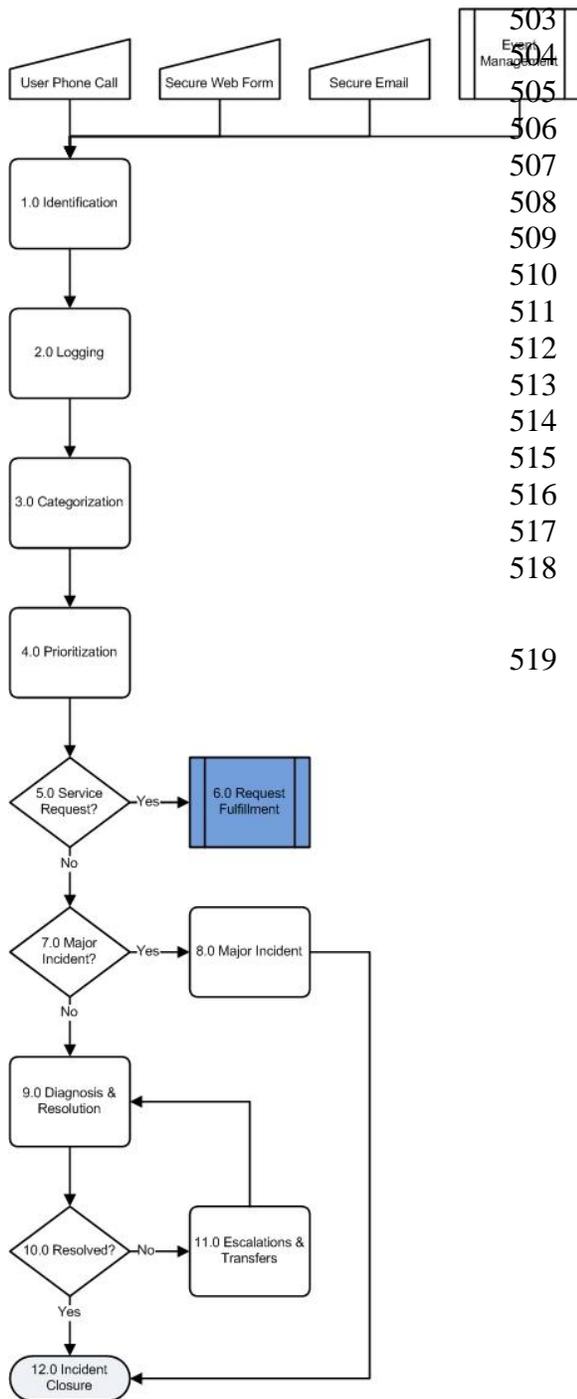
490 The IM tool assigns a standard weighting to each combination of urgency and impact. The
491 overall priority can be adjusted by increasing or decreasing this weighting without having to
492 modify the actual impact and urgency values. This is the appropriate method for adjusting the
493 priority as the actual urgency and impact should be accurately reflected in the incident records.

494 Given the multitude of variables inherent to USMC operations that can affect impact, different
495 echelons or commands can have unique impact and urgency criteria that will be established at
496 the time of implementation. It is the responsibility of all Incident Managers, Incident
497 Dispatchers, Queue Managers and Watch Officers at all levels of the organization, to analyze and
498 correlate incoming real-time incidents to ensure priorities are accurately set and to make
499 adjustments when appropriate. In instances where there is prioritization contention that cannot be
500 resolved, the matter is escalated to the Incident Manager or Watch Officer for resolution.

501



502 4.5 Request Fulfillment

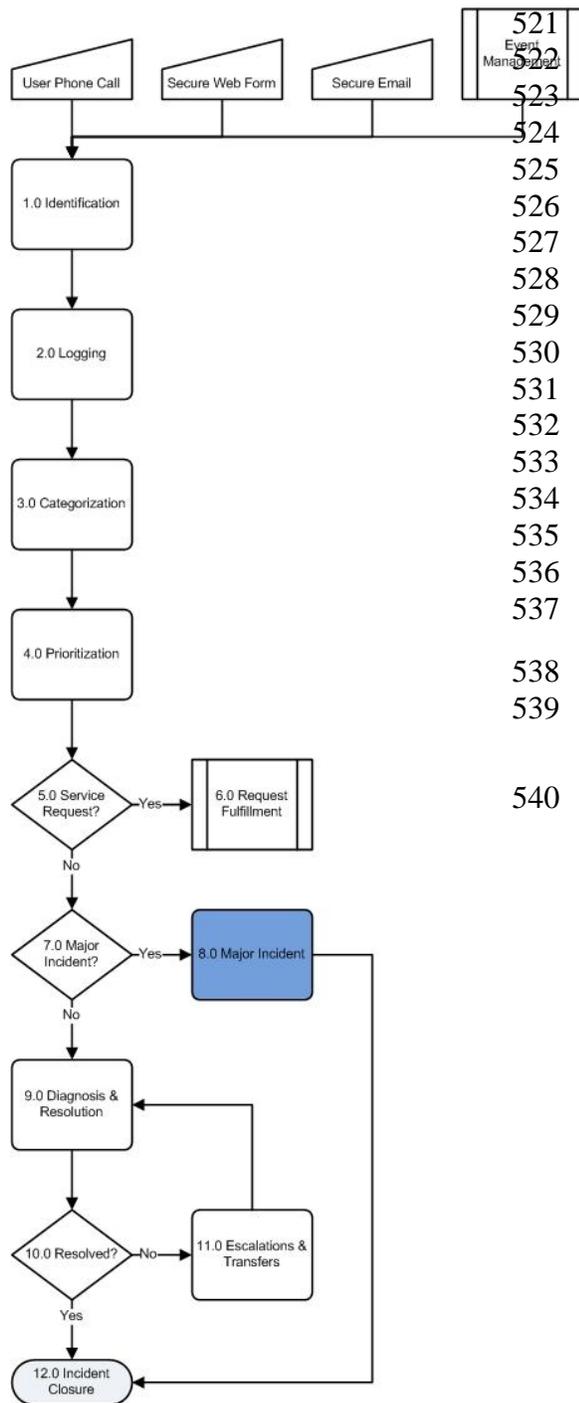


The term “Service Request” is used as a generic description for a large portion of requests that are received by the ESD. Many of these are actually small changes – low risk, frequently occurring, low cost, etc. (e.g., a request to change a password, a request to install an additional software application onto a particular workstation, or a simple “Move-Add-Change” request to relocate some items of desktop equipment) – but their scale and frequent, low-risk nature means that they are better handled by a separate process, rather than being allowed to congest and obstruct the normal Incident and Change Management processes. As with all incidents, Request Fulfillment incidents are categorized and prioritized.

519



520 4.6 Major Incident

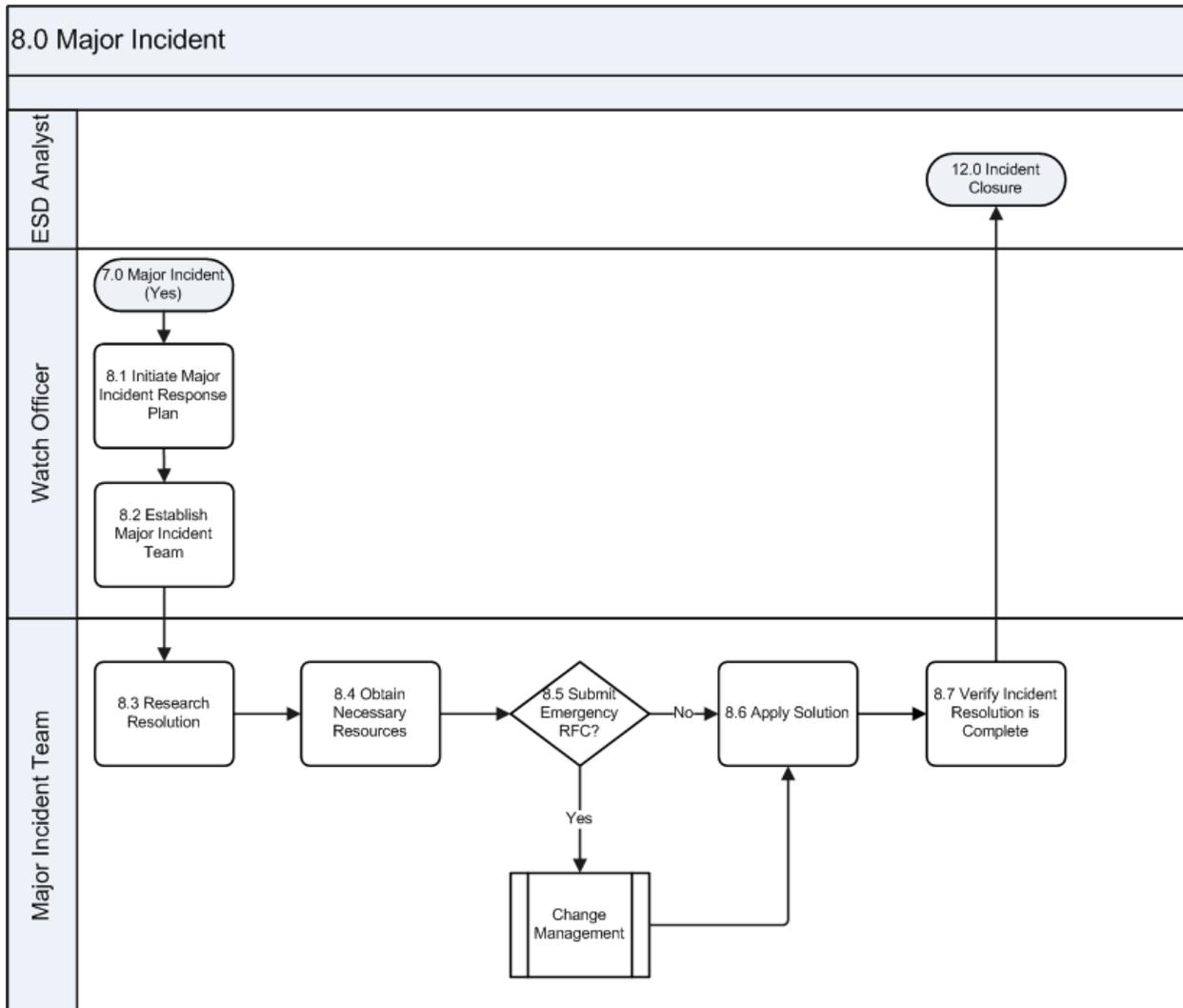


Major Incidents have a high impact and/or a high urgency. Tactical, VIP, timing and service considerations may likewise trigger a Major Incident. Incident Managers, incident Dispatchers, Queue Managers and Watch Officers at all levels of the organization are responsible for analyzing and correlating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

538 The following workflow (Figure 7) depicts the
539 Major Incident sub-process.

540





541

542

Figure 7. IM Major Incident Sub-Process

543

Table 10 describes the Major Incident sub-process steps as depicted in Figure 7.

544

Table 10. IM Major Incident Sub-Process Descriptions

8.0 Major Incident		
Number	Process Activity	Description
8.1	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.
8.2	Establish Major Incident Team	Establish a team of Tier 2-4 analysts that have the appropriate subject matter expertise or resources.
8.3	Research Resolution	Execute the necessary diagnostics and analysis to determine the root cause or a work-around.
8.4	Obtain Necessary Resources	Obtain necessary resources to solve the problem.



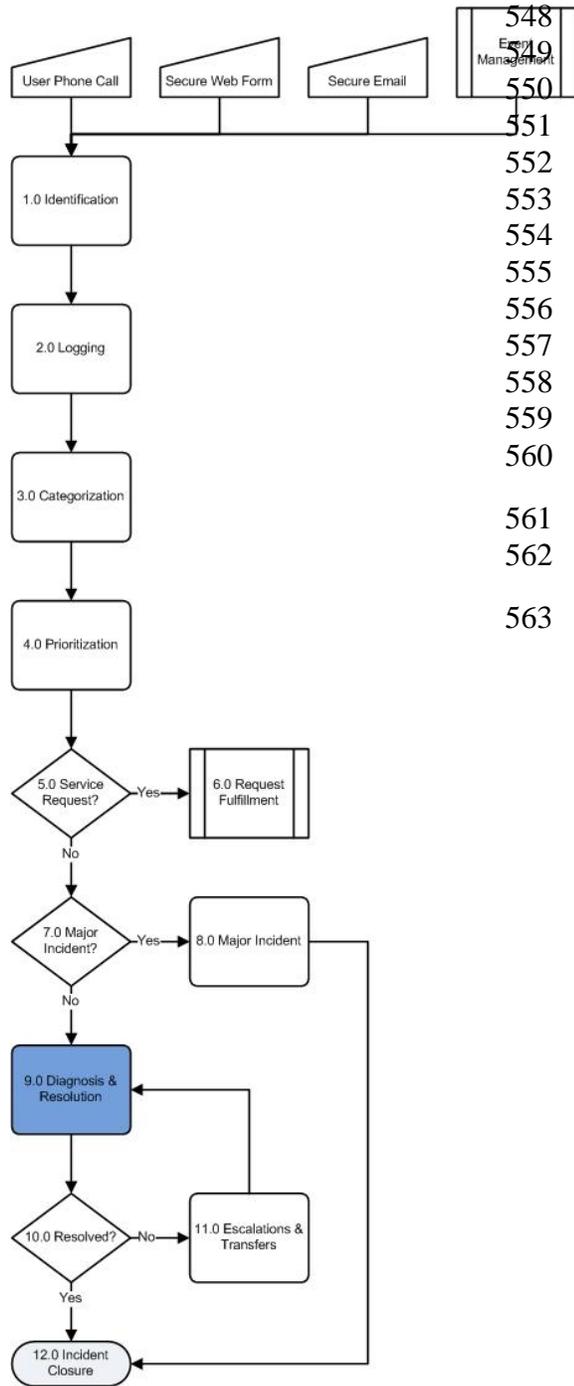
8.0 Major Incident		
Number	Process Activity	Description
8.5	Submit Emergency RFC?	If necessary, submit an Emergency RFC and prepare documentation for ECAB meeting.
8.6	Apply Solution	Execute the remediation plan.
8.7	Verify Incident Resolution is Complete	Execute necessary procedures to confirm the problem has been resolved.

545

546



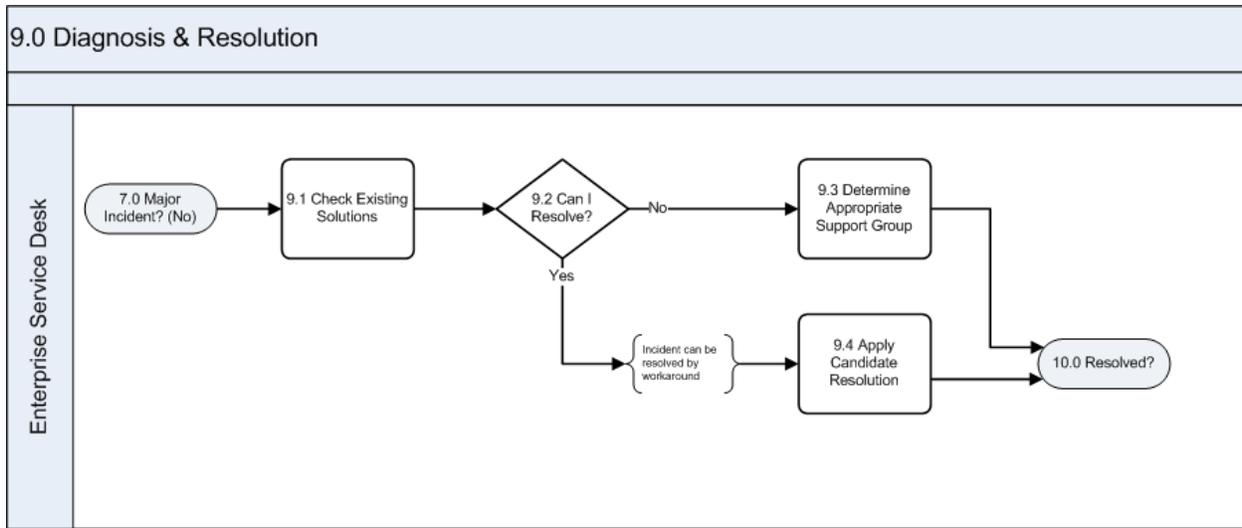
547 **4.7 Diagnosis and Resolution**



548 When an incident is received at the ESD, and after
549 the incident has been identified, logged,
550 categorized, and prioritized, the 1st Tier Analyst
551 ascertains as much information as possible about
552 the incident. Utilizing remote control capabilities,
553 the user manual, operations manuals and any other
554 available capabilities, the 1st Tier Analyst should
555 attempt to resolve the incident on the first call. If
556 the incident cannot be resolved, the 1st Tier
557 Analyst should follow the escalation/transfer SOPs
558 and/or consult the Incident Manager to determine
559 the appropriate escalation or transfer course of
560 action.

561 The following workflow (Figure 8) depicts the
562 Initial Diagnosis and Resolution sub-process.
563





564

565

Figure 8. IM Diagnosis & Resolution Sub-Process

566

Table 11 describes the Diagnosis & Resolution sub-process steps as depicted in Figure 8.

567

Table 11. IM Diagnosis & Resolution Sub-Process Descriptions

9.0 Diagnosis & Resolution		
Number	Process Activity	Description
9.1	Check Existing Solutions	Perform the following actions to ensure there are no existing solutions: <ul style="list-style-type: none"> • Verify if the incident matches any Known Errors or existing work-arounds • Search Incident and Problem Records • Consult Operational and User Documentation • Check Recent Changes or Releases
9.2	Can I resolve?	
9.3	Determine Appropriate Support Group	Consult escalation SOPs and/or the Watch Officer to determine where to functionally escalate the incident.
9.4	Apply Candidate Resolution	Apply steps to restore service

568

569



570 **4.8 Resolved?**



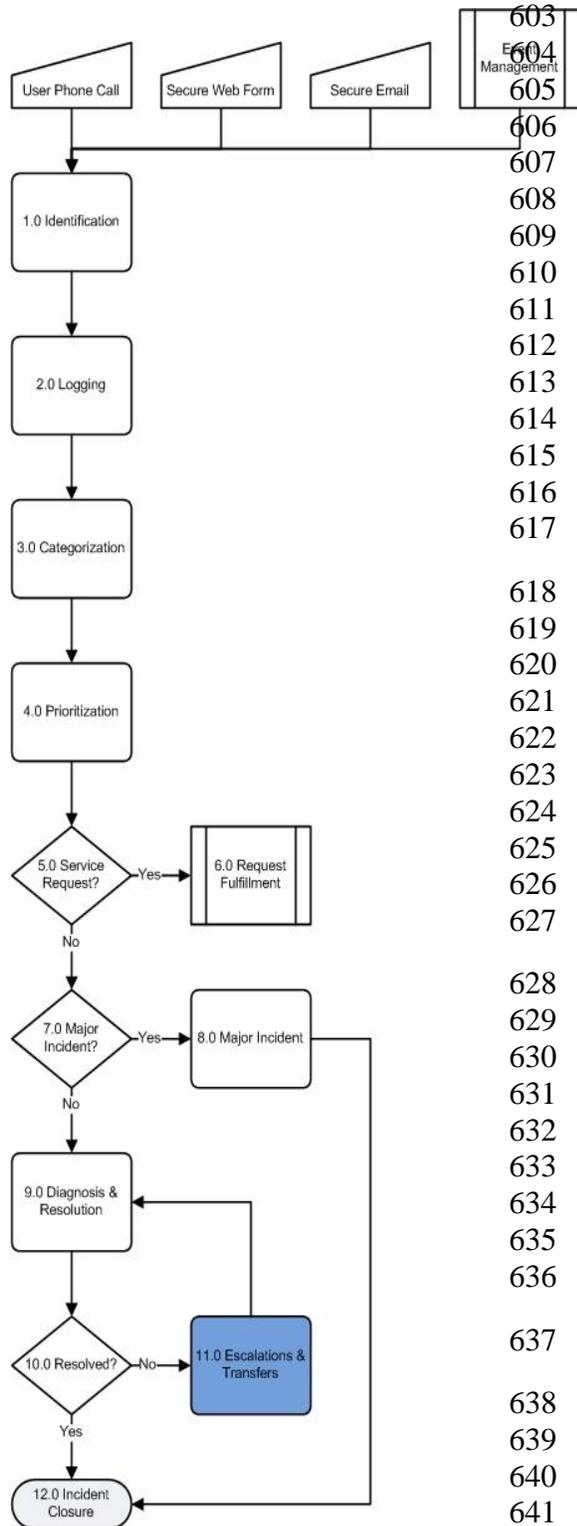
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600

571 After the Initial Diagnosis and
572 Resolution step is completed the 1st Tier
573 Analyst will decide if the Incident is
574 resolved; meaning service has been
575 restored to the customer. If the Incident
576 is resolved then update the status of the
577 incident record and proceed to the
578 Incident Closure step. If service has not
579 been restored, than route the incident to
580 a 2nd Tier Analyst who has more
581 experience and training on the specific
582 type of Incident.



601

602 **4.9 Escalations and Transfers**



603 Escalation can take place at any moment during
604 the IM process when it is likely that a resolution
605 will breach agreed upon service levels, the
606 resolution will prove unsatisfactory to the
607 customer or there is contention about an incident
608 assignment. Functional Escalation is the process
609 of routing an incident to a technical team with a
610 higher level (or tier) of knowledge or expertise.
611 There are many tiered support structures within
612 the MCNOSC, MITSCs and the base echelons.
613 Given this, functional escalations will
614 predominately occur within an organizational
615 echelon with functional teams that have a
616 predefined times before an incident must be
617 resolved, escalated or transferred.

618 Hierarchical Escalation requires communications
619 to a superior commanding operating officer or
620 echelon to affect the resolution of the incident. It
621 is primarily utilized in circumstances that warrant
622 the intervention and/or notification of senior staff
623 and/or superior commands. Depending on the
624 point of origin, this communication will be in the
625 form of a CCIR, phone call, SIPRNet email,
626 NIPRNet email or any other official form of
627 communication.

628 Transfers are very similar to escalations. Transfers
629 involve routing an incident to the appropriate
630 AOR. The ESD can transfer tickets down to the
631 MCNOSC or a MITSC, but tickets intended for a
632 base must pass through the appropriate MITSC to
633 ensure accurate routing to the base level. If an
634 incident has been incorrectly transferred down to
635 an echelon level, it must be routed back through
636 the ESD to avoid repeated incorrect routing.

637 Two types of transfers take place in IM:

638 **Internal Transfers** – Internal Transfers are
639 utilized to route resolution responsibility to
640 another organizational echelon within the USMC.
641 Transferring an incident from the MCNOSC to a

642 MITSC is considered an “Internal Transfer” and primarily takes place based on organizational

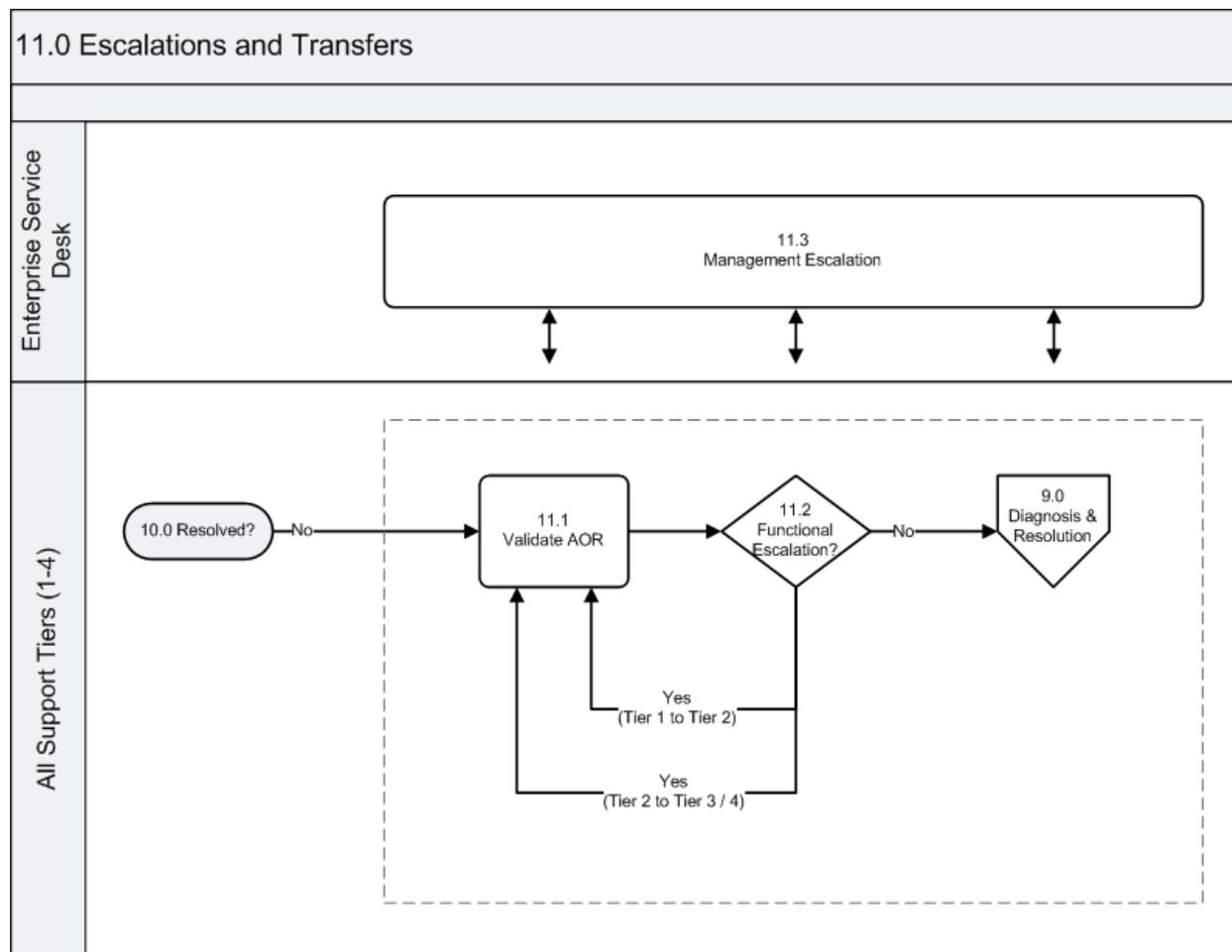


643 Area of Responsibility, level of expertise, capabilities or core competencies. Internal Transfers
 644 are bi-directional and Incident Managers should analyze root causes for any regular or excessive
 645 transfers.

646 **External Transfers** – External Transfers are utilized to route resolution responsibility to a Tier 4
 647 vendor, contractor or other organization such as USCYBERCOM, HQMC I&L, HQMC PP&O, and
 648 DISA that are outside the influence or governance of the USMC E-ITSM processes.

649 It is the responsibility of all Incident Managers, Incident Dispatchers, Queue Managers and
 650 Watch Officers at all levels of the organization to insure proper transfers and routing at their
 651 respective levels. In instances where there is escalation or transfer contention that cannot be
 652 resolved, the matter is escalated to the Incident Manager or Watch Officer for resolution.

653 The following workflow (Figure 9) depicts the IM Escalations and Transfers sub-process.



654
 655 **Figure 9. IM Escalations and Transfers Sub-Process**

656 Table 12 describes the IM Escalations and Transfers sub-process steps as depicted in Figure 9.



657

Table 12. IM Escalations and Transfers Sub-Process Descriptions

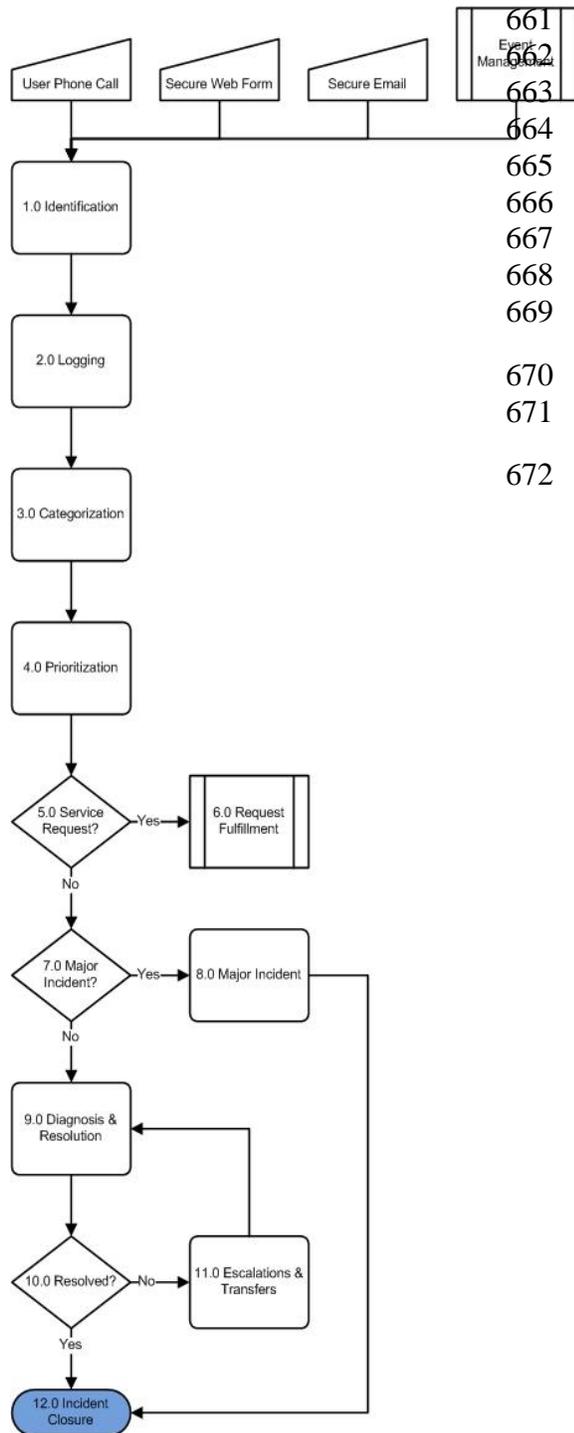
11.0 Escalations & Transfers		
Number	Process Activity	Description
11.1	Validate AOR	Determine if the incident is within the scope of MCNOSC capabilities or services. If not, determine if the incident should be escalated to a functional support group or transferred to another AOR.
11.2	Functional Escalation?	Determine if incident needs to be escalated.
11.3	Escalation Management	The Incident Manager must determine the best course of action to resolve the incident. This may involve establishing an Escalation Team, engaging other Tier 4 support options or passing the incident to other processes.

658

659



660 **4.10 Incident Closure**

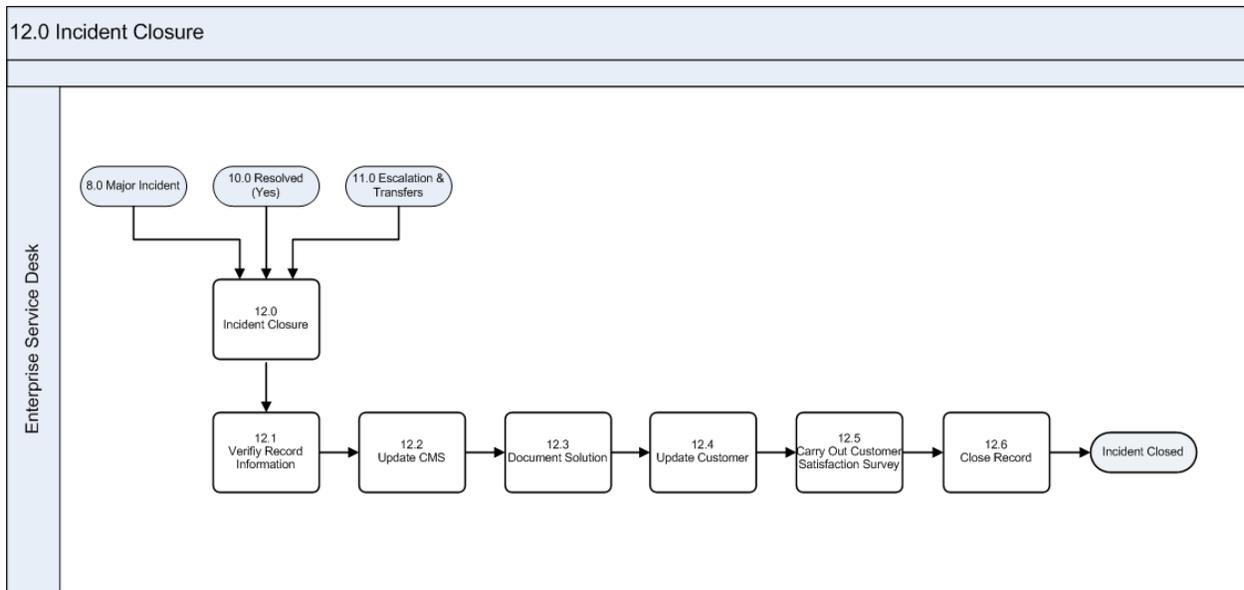


661 The ESD is responsible for record closure. It is the
662 final sub-process of the IM lifecycle. An incident
663 record can be manually closed once the user
664 confirms that the incident has been resolved, or
665 automatically after seven (7) business days
666 transpire without any response from the user to
667 multiple, automated emails. Once an incident
668 record has been closed, an automated customer
669 satisfaction survey will be sent to the user.

670 The following workflow depicts the Incident
671 Closure sub-process.

672





673

674

Figure 10. IM Incident Closure Sub-Process

675 Table 13 describes the Incident Closure sub-process steps depicted in Figure 10.

676

Table 13. IM Incident Closure Sub-Process Descriptions

12.0 Incident Closure		
Number	Process Activity	Description
12.1	Verify Record Information	The 1 st Tier Analyst ensures the applied solution, escalation, transfer and activity information is complete on the record.
12.2	Update CMS	The 1 st Tier Analyst updates the CMS in the case of standard, pre-approved (minor) changes. Major modifications to the CMS require the involvement of Configuration Management.
12.3	Document Solution	If the solution to the incident is new and/or undocumented, the incident can be submitted as a solution to future incidents of like symptoms.
12.4	Update User	Because the user is notified whenever there is a record status change, the user is notified at the close of the record.
12.5	Carry Out User Satisfaction Survey	This is an automatic function of the tool.
12.6	Close Record	Set incident record status to "Closed".

677

678



679

Appendix A – ACRONYMS

680

The official list of E-ITSM acronyms can be found through the link referenced below:

681

https://ips.usmc.mil/sites/pg10docr/pm_ccr/E-ITSM/Shared%20Documents/Forms/AllItems.aspx

682



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.
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.
Deployment	Deployment is the activity responsible for movement of new or changed hardware, software, documentation, process, etc. to the live environment. Deployment is part of the Release and Deployment Management Process.
Deployment Readiness Test	A Deployment Readiness Test is conducted to ensure that the deployment processes, procedures, and systems can deploy, install, commission, and decommission the release package and resultant new or changed service in the production/deployment environment.
Deployment Verification Test	A Deployment Verification Test is conducted to ensure the service capability has been correctly deployed for each target deployment group or environment.



Term	Definition
Early Life Support	Early Life Support (ELS) involves Technical Management or IT Operations providing support for a new or changed IT service for a period of time after it is released. During ELS, the IT service provider may review the KPIs, service levels, and monitoring thresholds and provide additional resources for incident management and problem management (when implemented).
EM System	The EM System (EMS) is 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	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 <i>normal</i> 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.
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.
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.



Term	Definition
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.
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.
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.

684

685



686

Appendix C – POLICIES

687 References to industry governing policies and laws can be found through the link referenced
688 below:

689 [https://ehqmc.usmc.mil/org/c4/projects/CP/eitsm/Shared%20Documents/E-](https://ehqmc.usmc.mil/org/c4/projects/CP/eitsm/Shared%20Documents/E-ITSM_TO_13_Government_Policies.doc)
690 [ITSM_TO_13_Government_Policies.doc](https://ehqmc.usmc.mil/org/c4/projects/CP/eitsm/Shared%20Documents/E-ITSM_TO_13_Government_Policies.doc)

691



692

Appendix D – IM SYSTEM RECORD ATTRIBUTES

693 To achieve a high level of ITIL process maturity, there must exist an architecture of process tools
 694 with a federated database architecture that share a common, or aligned, data dictionary and
 695 definitions all the related process. The following is a list of suggested fields for the Enterprise
 696 incident and Service Management tool.

697 An asterisk (*) indicates a record may have multiple instances of the same field.

<ul style="list-style-type: none"> • Record # (should be auto-generated) • Record Type (incident or Service Request) • *Record Status • Customer Information <ul style="list-style-type: none"> — First name — Last name — Name — Email address — Phone Number — Rank — Region — Base — Room — Building — POC/Proxy (for VIPs) • *incident Status <ul style="list-style-type: none"> — Status Type — Status Timestamp • *incident Priority <ul style="list-style-type: none"> — Priority Type — Priority Timestamp • incident Description • *incident Category • *Work Center Assigned • incident Manager • *Analyst Assigned • Environment (classified or unclassified, radio button, default="Classified") • Tech Journal (log of work done on record) • Reportable Record (radio button, default="Yes") • *Referred to (external Help Desk name) • *Reference # (refers to record number from external Help Desk) • *Reference POC 	<ul style="list-style-type: none"> • High Level Outage <ul style="list-style-type: none"> — Known Error — Server — Cable — Carrier • Most recent 5 records for this Customer <ul style="list-style-type: none"> — Record # — Status — System — Problem • Equipment ID <ul style="list-style-type: none"> — IP Address — Subnet — Default Gateway — Host/Machine Name — MAC Address — CATV Cable Box Number • Configuration Item Number • Solution Description • Solution Source (KEDB, Analyst Research, etc.)
--	---



698
699 Several of these data fields must have valid values assigned to them for the request or incident to
700 be actionable. These are:

- 701 • User first name
- 702 • User last name
- 703 • Phone number
- 704 • Marine Command Code (MCC)
- 705 • incident Type (Service request or incident)
- 706 • incident Status (per status list in Section 2.4)
- 707 • incident Priority (per priority levels in Section 2.3)
- 708 • incident Category (per categories listed in Section 2.2)
- 709 • Work Center Assigned
- 710 • Analyst Assigned (dynamic list to account for staff changes and role changes among staff)
- 711 Reporting level =Command Name (e.g., MARFOR/MEF/MSC)

712 In addition to the above-mentioned fields that will apply to calls regarding incidents and Service
713 Requests, an additional screen set is required to capture data relating to escalated incidents. The
714 required fields are as shown below. An asterisk (*) indicates that each record may have multiple
715 instances of the field.

- 716 • Escalation Team Lead
- 717 • *Escalation Team Member
- 718 • Customer Satisfaction Manager
- 719 • Customer Contact
- 720 • *Most Recent Status Check
- 721 • Next Status Check
- 722 • *Action
 - 723 — Owner
 - 724 — Status (open, closed)
 - 725 — Assigned (timestamp)
 - 726 — Completed (timestamp)
 - 727 — Type
 - 728 ■ Identify & Assign Team Members
 - 729 ■ Inform Stakeholders of Status
 - 730 ■ Review Status
- 731 • *Follow-up Action
 - 732 — Owner
 - 733 — Description
 - 734 — Status (open, closed)
 - 735 — Assigned (timestamp)
 - 736 — Completed (timestamp)
- 737

