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

Subj: ENTERPRISE INFORMATION TECHNOLOGY SERVICE MANAGEMENT REQUEST
FULFILLMENT MANAGEMENT PROCESS GUIDE

Ref: (a) MCO 5271.1B

Encl: (1) IRM-2300-08D

1. <u>PURPOSE</u>. The purpose of the Enterprise Information Technology Service
Management (E-ITSM) Request Fulfillment Process Guide is to update the
previously defined foundation for process implementation and execution across
the Marine Corps Enterprise Network (MCEN). Process implementation and
execution at lower levels (e.g., Regional, Local, and Programs of Record)
must align with and adhere to directives and schema documented within this
guide. This guide enables USMC Information Technology (IT) activities through
promoting standardization of work instructions and operating procedures
across a continuum of document specificity.

2. <u>CANCELLATION</u>. IRM-2300-08C

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

4. <u>APPLICABILITY</u>. This publication is applicable to the Marine Corps Total
Force.

5. <u>SCOPE</u>.

    a. <u>Compliance</u>. Compliance with the provisions of this publication is
required unless a specific waiver is authorized.

    b. <u>Waivers</u>. Waivers to the provisions of this publication will be
authorized by Director, Command, Control, Communications and Computers (C4).

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

C. O. URBINA
By direction

Enterprise IT Service Management
Request Fulfillment
Process Guide

Release Date:
11 October 2018

Document Approval / Major Revision Change History Record

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

Release Date (MM/DD/YY)	Release No.	Approvals		Change Description
		Author	**Process Owner/Approver**	
09/14/2011	0.1			Draft Release
		Printed Name	Printed Name	
10/13/2011	1.0			Initial Release
		Printed Name	Printed Name	
08/04/2014	1.1			Updated Release
		Printed Name	Printed Name	
03/22/2017	2.0			Updated Release
		Printed Name	Printed Name	
08/03/2018	2.1			Updated Release
		Printed Name	Printed Name	

Table of Contents

List of Tables

List of Figures

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 Marine Corps Enterprise Network (MCEN). Process
5   implementation and execution at lower levels (e.g., Regional, Local, and Programs of Record)
6   must align and adhere to directives and schema documented within this guide. The use of this
7   guide enables the United States Marine Corps (USMC) Information Technology (IT) activities
8   through promoting standardization of work instructions and operating procedures across a
9   continuum of document specificity as represented in Figure 1-1.

10
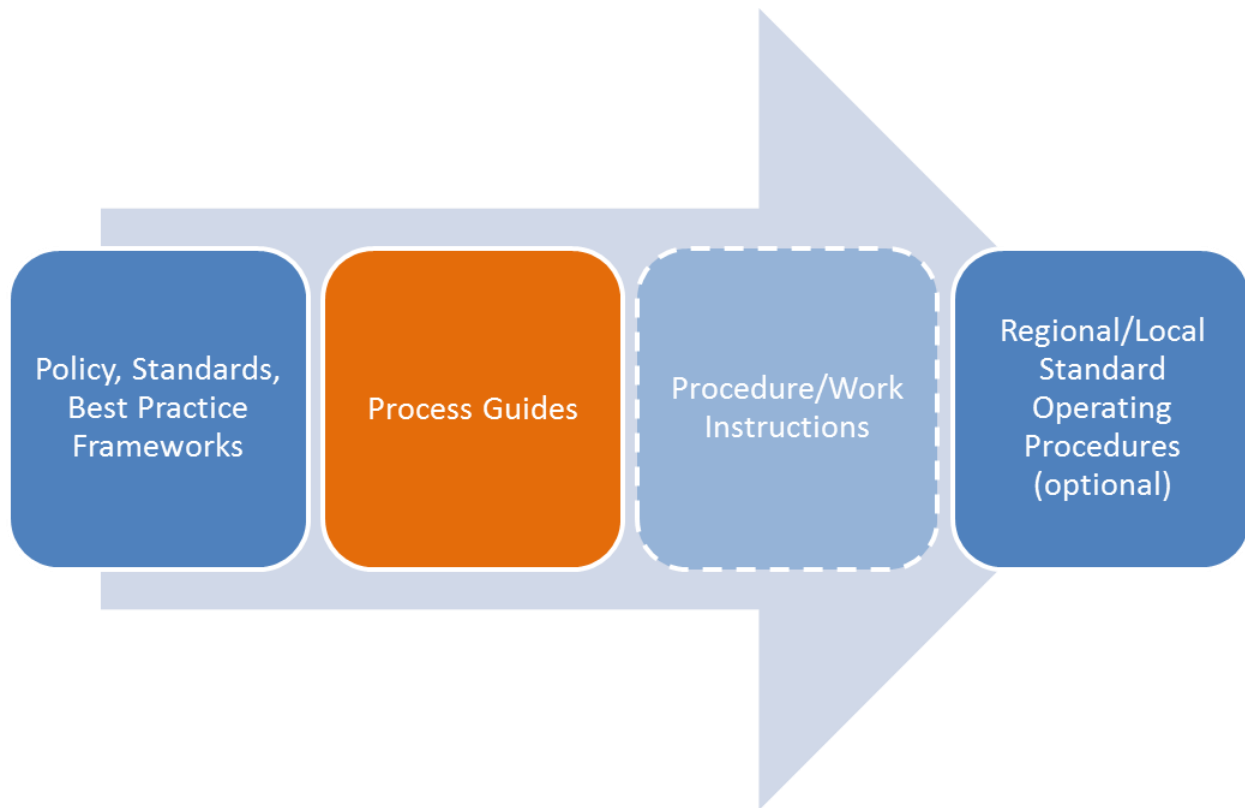
11   *Figure 1: Process Document Continuum*

12

13 **1.2   Scope**

14 The scope of this document covers all services provided in support of the MCEN for both the
15 Secret Internet Protocol Router Network (SIPRNET), and the Non-Secure Internet Protocol Router
16 Network (NIPRNET). Information remains relevant for the global operations and defense of the
17 MCEN as managed by the Marine Corps Cyberspace Operations Group (MCCOG) including all
18 Regional Network Operations and Security Centers (RNOSC) and Marine Air Ground Task Force
19 Information Technology Support Center (MITSC) assets and supported Marine Expeditionary

20 Forces (MEF), Supporting Establishments (SE) organizations, and Marine Corps Installation
21 (MCI) commands.

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

26

27 *Table 1: Document Design Layers*

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

28

1.3   Document and Process Change Procedures

30 This document will be reviewed semi-annually for accuracy by the Process Owner with designated
31 team members. Questions pertaining to the conduct of the process should be directed to the Process
32 Owner. Suggested Changes to the process should be directed to USMC Command, Control,
33 Communications, and Computers (C4) Concepts and Plans (CP) in accordance with Marine Corps
34 Order (MCO) 5271.1C Information Resource Management (IRM) Standards and Guidelines
35 Program.

2.0   PROCESS OVERVIEW

2.1   Purpose, Goals, and Objectives

38 Request Fulfillment (RqF) is the process for managing Service Requests from users. Service
39 Requests are tracked and managed by the Regional Service Desks, hereafter referred to as Service
40 Desk. The Service Desk will monitor, escalate, dispatch and ensure fulfillment of Service
41 Requests.

42 The purpose of RqF is to process Service Requests from users.

43 The goal of RqF is to support USMC IT control objectives and requirements by providing a
44 mechanism for the fulfillment of Service Requests. Service Requests are identified as standard
45 changes, access to a service, questions, complaints, and comments submitted to the Service Desk.
46 Standard changes are high volume, low risk, low cost changes that have a predefined set of
47 instructions for processing. The Change Advisory Board (CAB) is responsible for designating
48 specific types of changes as standard changes which may be processed without additional CAB
49 approvals. Standard changes may require additional approvals before they can be fulfilled.

50 Primary objectives of the RqF process include:

51 • To provide a conduit for USMC users to request and receive services from the Service
52   Catalog for which a predefined approval and fulfillment procedure exists;

53 • To provide information to MCEN users and customers about the availability of Standard
54   Services and the procedures for obtaining them;

55 • To source and deliver the Standard Services components from the Service Catalog (e.g.,
56   licenses and software applications);

57 • To assist MCEN users with Enterprise IT Service Management (E-ITSM) general
58   information, complaints or comments.

59 • Provide professional handling of Service Requests and maintain MCEN user satisfaction
60   with quality of information technology services.

2.2   Relationships with other Processes

62 All IT Service Management processes are interrelated. The E-ITSM processes in Figure 2 were
63 selected due to the strength of the relationships and dependencies between them and the degree to
64 which they underpin USMC near-term objectives. While any one of the E-ITSM processes can
65 operate in the presence of an immature process, the efficiency and effectiveness of each is greatly
66 enhanced by the maturity and integration of all E-ITSM processes.
67

68 **2.2.1   Relationships with other Processes**

69

70
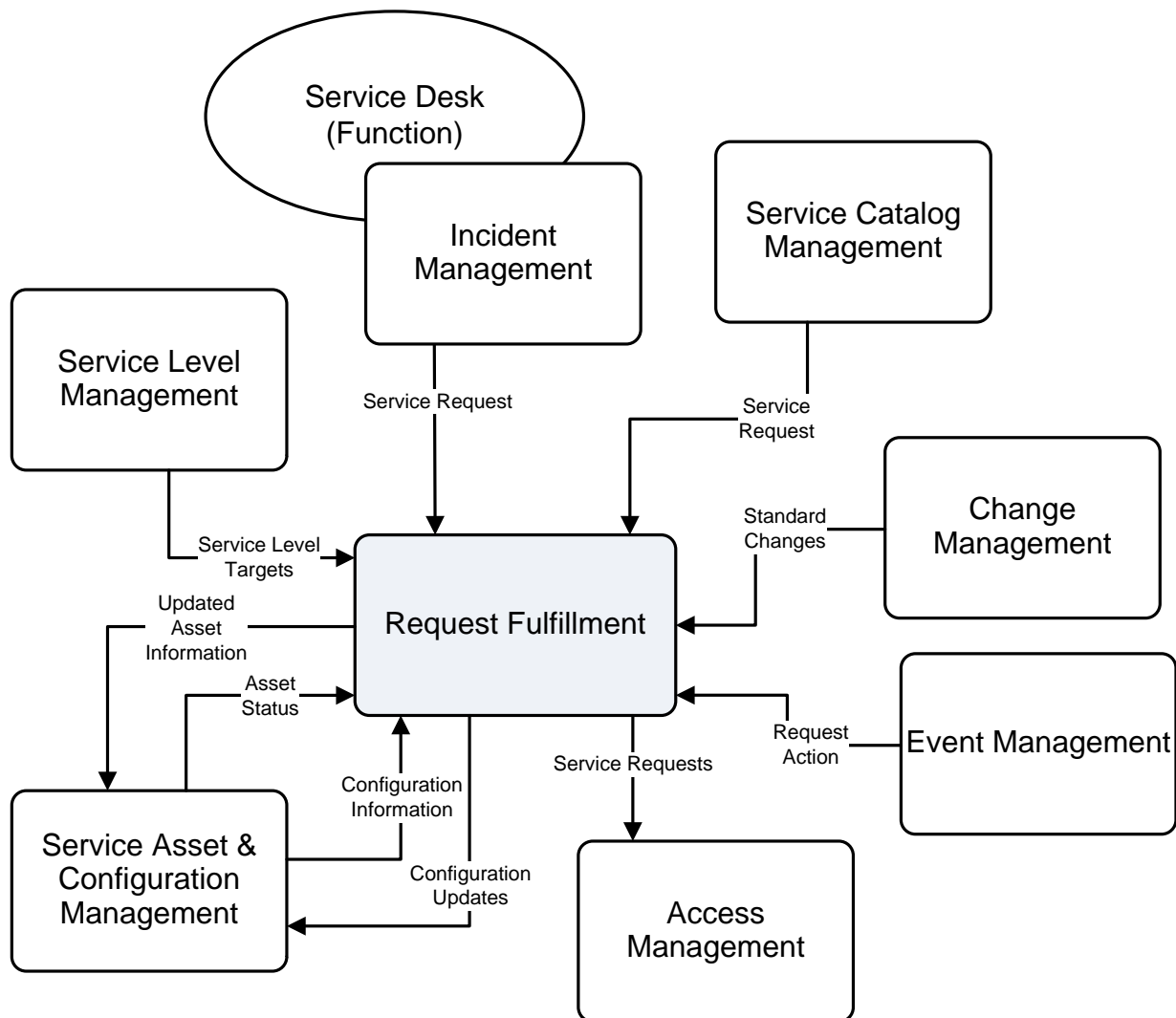
71   *Figure 2: RqF Relationship with other E-ITSM Processes*

72

73 **Service Catalog Management/Self Service:**

74   — Service Request: Service Requests will come into RqF via various request mechanisms.
75   Depending upon the point of entry, either the Service Desk or the self-service portal
76   routes the service request to the appropriate technical resource or request fulfillment
77   team to fulfill the request.

78 **Change Management:**

79   — Approved Standard Changes: Change Management (ChM) routes Requests For
80   Change (RFC) to Request Fulfillment when it is determined within ChM that an RFC

81   can be processed as a standard change. ChM also provides RqF with specifics related
82   to the defined CAB approved standard changes.

Service Asset & Configuration Management:

84   — Updated Asset Information: The asset information and status is sent to Service Asset
85   Configuration Management (SACM) to update the asset database. SACM uses RqF
86   updates to determine the lifecycle status of assets.

87   — Asset Status: Asset Status is obtained from the Configuration Management Database
88   (CMDB) when a Service Request involves changes that require information such as
89   available inventory of hardware or software licenses.

90   — Configuration Information: RqF uses Configuration Item (CI) relationship information
91   to determine potential impact of standard changes.

92   — Configuration Updates: RqF provides information to Configuration Management
93   (CfM) when Service Requests are deployed that have impact on CI information,
94   including status changes.

Incident Management:

96   — Service Requests: Service Requests are not handled by the Incident Management (IM)
97   process and when identified are routed to the RqF process for completion.

Service Level Management:

99   — Service Level Targets: Commitments documented within Service Level Agreements
100   (SLAs) based on Service Level Requirements.

Identity and Access Management:

102   — Service Requests: Service Requests for access to systems and applications are
103   identified by RqF and routed to Identity and Access Management (IdAM) for
104   completion.

Event Management:

106   — Events that require Request Action will be routed from Event Management to (EM)
107   RqF for completion.

2.3   High-Level Process Model

109   The RqF process consists of seven distinct sub-processes and is highly integrated with other E-
110   ITSM processes. The following workflow depicts these processes and sub-processes that

111   collectively enable and underpin RqF. See Section 4.0 for complete descriptions of the sub-process
112   activities.

```
┌───────────────┐  ┌───────────────┐  ┌───────────────┐  ┌───────────────┐
│   Incident    │  │     Event     │  │    Change     │  │Service Catalog│
│  Management   │  │  Management   │  │  Management   │  │  Management   │
└───────────────┘  └───────────────┘  └───────────────┘  └───────────────┘
                           │
                  ┌─────────────────┐
                  │      1.0        │
                  │ Indentification │
                  └─────────────────┘
                           │
                  ┌─────────────────┐
                  │      2.0        │
                  │    Logging      │
                  └─────────────────┘
                           │
                  ┌─────────────────┐
                  │      3.0        │
                  │ Categorization  │
                  └─────────────────┘
                           │
                  ┌─────────────────┐
                  │      4.0        │
                  │ Prioritization  │
                  └─────────────────┘
                           │
                  ┌─────────────────┐
                  │      5.0        │
                  │  Authorization  │
                  └─────────────────┘
                           │
                  ┌─────────────────┐
                  │      6.0        │
                  │   Fulfillment   │
                  └─────────────────┘
                           │
                  ┌─────────────────┐
                  │      7.0        │
                  │    Closure      │
                  └─────────────────┘
                           │
                  (       End       )
```

113

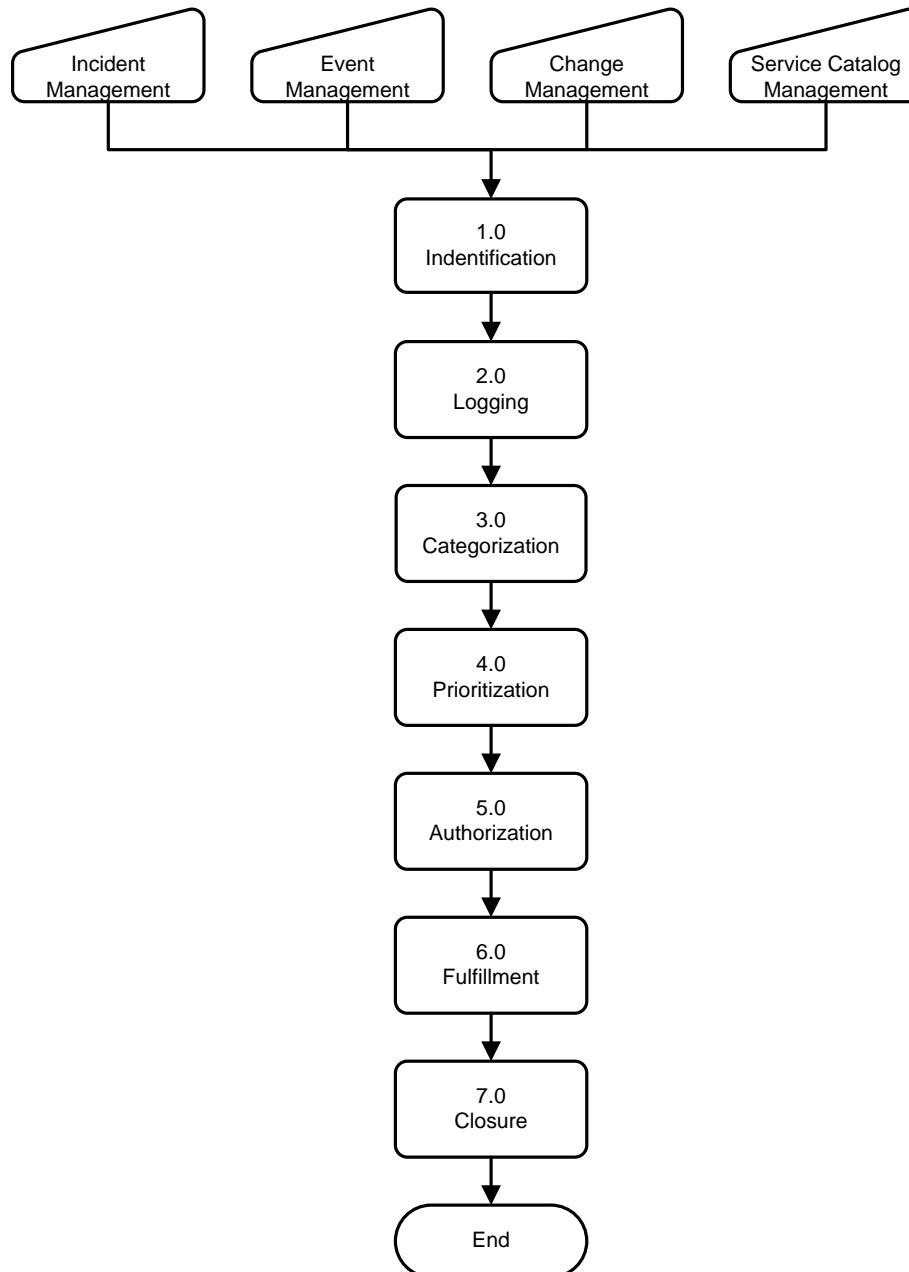114   ***Figure 3: High-Level RqF Workflow***

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

117

118   *Table 2: RqF Process Activity Descriptions*

Number	Process Activity	Description
1.0	Identification	This activity is to identify Service Requests submitted by users through a web-enabled portal, via appropriate interface with the ticketing system or other pre-approved methods. Service Requests submitted through the portal do not flow through Incident Management and therefore need to be identified, logged, categorized and prioritized. Additionally, the portal facilitates many self-help capabilities to fulfill Service Requests.
2.0	Logging	Service Requests are logged with a date/time stamp into a RqF tracking tool. A Service Request record is created with relevant information such as the user profile and a description of the request.
3.0	Categorization	Categorization identifies the type and nature of the request. Categorization is critical to ensure proper authorizations and routing to the appropriate Fulfillment Resources.
4.0	Prioritization	Service Requests are prioritized in relation to other new and existing requests to determine the sequence in which they will be fulfilled. Priority is determined based on Level of Effort or benefit to the organization and Urgency to the Requestor.
5.0	Authorization	Categorization, prioritization and user profiles are used to determine the correct level of Authorization. Requests may have functional and/or financial impacts which are factors considered during authorization.
6.0	Fulfillment	Service Requests are routed to the appropriate fulfillment team, which follows the documented procedures for fulfilling the request. Certain requests, such as questions or inquiries, may be completed by the Authorized Requestor, acting as first-line support, while other Service Requests are forwarded to specialist groups and/or suppliers for fulfillment. Procedures and Work Instructions for fulfillment of standard changes are accessed from a repository, having been previously developed, tested, and documented in ChM and Release and Deployment Management (RDM). A goal of the RqF process is to automate fulfillment activities as much as possible.
7.0	Closure	The Authorized Requestor checks that the Service Request is fulfilled and that the user is satisfied and agrees the Service Request can be closed. The Service Request is then closed.

119

120   **2.3.1   Process Description**

121   A key purpose of RqF is to provide USMC MCEN users an efficient means of handling changes
122   that are low risk, high volume, and have a pre-defined procedure for implementation, which
123   reduces the volume of activity routed through the ChM Process. RqF also provides efficient means
124   of obtaining answers to questions, making general inquiries, and filing complaints.

125   The scope of the RqF process includes a standard set of processes, procedures, responsibilities,
126   and metrics utilized by all MCEN-related services applications, systems and network support
127   teams.

128   **2.4   Key Concepts**

129   The following key concepts are utilized extensively in this RqF Process Guide:

130   **2.4.1   Approval**

131   Many types of requests require financial, hierarchical, or other organizational approval. In those
132   cases, Authorized Approvers are consulted prior to the delivery of fulfillment actions. Approval

133 requirements for specific Service Requests are pre-defined, documented, and stored with the
134 specific request type procedures.

2.4.2   Commander's Critical Information Requirements

136 All commands are required to produce command specific Commander's Critical Information
137 Requirements (CCIR) guidance with detailed ITSM requirements and are required to adhere to the
138 current CCIR guidance of their superior commands. Common CCIR categories are Enterprise
139 Service Management, Network Defense, Content Management, and MCEN, however, others may
140 be applicable based upon the commander's requirements.

141 CCIRs are the commander's "need to know immediately" information and response requirements.
142 From Marine Corps Techniques Publication (MCTP) 3-30B Information Management, "CCIRs
143 are tools for the commander to reduce information gaps generated by raw data to a manageable
144 set, and ensure that key information requirements are not inadvertently filtered out. Define the
145 information required by the commander to better understand the battlespace and to identify risks
146 as well as to make sound, timely decisions in order to retain the initiative."

2.4.3   Fulfillment Resources

148 Fulfillment Resources specialize in the fulfillment of specific categories of Services Requests.
149 These resource teams receive requests from the Authorized Requestor and maintain
150 communication with the Authorized Requestor on the status of the request throughout the
151 fulfillment stage of the process.

2.4.4   Service Request

153 The term 'Service Request' is used as a description for many varying types of demands that are
154 placed upon the IT department by the users. Many of these are actually small changes – low risk,
155 frequently occurring, low cost, etc. (e.g., a request to change a password, a request to install an
156 additional software application onto a particular workstation, a request to relocate some items of
157 desktop equipment) or a question requesting information. However, their scale and frequent, low-
158 risk nature means that they are better handled by a separate, less complex process, rather than
159 being allowed to congest and obstruct the normal IdAM and ChM Processes.

2.4.5   Service Request Status

161 Service Requests are tracked through the RqF lifecycle. A status designation is used to indicate
162 which stage a Service Request is in as it progresses through the lifecycle. This is important for
163 reporting and for Continual Process Improvement (CPI). Top-level status designations are shown
164 in Table 3.
165

166   ***Table 3: Request Status Designations***

Status	Designation
Assigned	Service Request has been identified, logged, categorized, prioritized, and assigned
Pending	Waiting on input or approval from third party
Approved	Service Request has been authorized (where required)
In-Progress	A fulfillment group is currently working on fulfilling the request
Denied	The request was not authorized for fulfillment
Completed	Service Request has been fulfilled and is awaiting acknowledgment
Cancelled	User contacts the Authorized Requestor and cancels the service request
Closed	Service Request record closed

167   **2.4.6   Standard Change**

168   Standard changes are smaller, lower-risk, frequently occurring, lower-cost changes (e.g., request
169   to change a password, a request to relocate some items of desktop equipment) that are initiated via
170   the Service Desk. A CAB must approve the designation of a change as a standard change, thus
171   allowing it to subsequently be managed by RqF. To be approved, a repeatable procedure for
172   fulfillment must be thoroughly tested and documented.

173   **2.5   Quality Control**

174   **2.5.1   Metrics, Measurements and Continual Process Improvement**

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

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

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

189   **2.5.2   Critical Success Factors with Key Performance Indicators**

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

195   CSFs are defined as process- or service-specific goals that must be achieved if a process or IT
196   service is to succeed. KPIs are the metrics used to measure service performance or progress toward
197   stated goals.

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

201   Table 4 describes the metrics that shall be monitored, measured and analyzed:

202   *Table 4: Critical Success Factors with Key Performance Indicators*

CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Benefits
1	Ability to fulfill Service Requests efficiently and effectively.	1	Number of Service Requests in a defined period by status, location and category.	Increased user satisfaction, timely enablement of business process activity, accurate fulfillment of requests to eliminate rework.
		2	Size and percent (of total number) of the current backlog of outstanding Service Requests reported by status, location and category.	
		3	Average time and/or mean time for approval, fulfillment and closure handling for each type of Service Request. For example, Average Time Fulfillment.	
		4	Number and percent of Service Requests completed within agreed target times.	

CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Benefits
		5	Number and percent of requests fulfilled by status, location, and category.	
		6	User Satisfaction scores obtained via surveys for a defined period.	
2	Agreement on the services that can be requested, who can request them, and the associated costs involved.	1	Number of Service Requests that are designated as "standard changes" through CAB approval.	Increased efficiency of IT utilizes fewer resources to deliver services at agreed levels.
		2	Number and percent of requests fulfilled by status, location, and category.	Provides an indicator of the number of users seeking types of services requests.
		3	Number and percent of requests rejected due to denial during additional authorization (see sub-process 5.2) by status, location and category.	Provides an indicator of the number of users seeking types of Service Requests with insufficient privileges.
		4	Cost KPI is to be determined, pending additional financial information.	Indicator of costs related to individual request types.
3	Standard procedures in-place for each type of requested service.	1	Number and percent of Service Requests with associated, documented procedures.	Fulfillment resources do not have to develop method of fulfillment, increased quality of fulfillment results.
4	Integration of front-end self-help tools with the back-end processes.	1	Number and percent of requests completed through self-help capability.	Increase productivity of IT and consistent quality of fulfillment through automation.

203

204   Other qualitative factors to consider:

205   • Agreements of what services are available and who is authorized to request them.
206   • Publication of the services to users as part of the Service Catalog. The Service Catalog
207   should be kept accurate and updated to reflect available service offerings and support
208   RqF approvals and workflows.
209   • Definition of a standard fulfillment procedure for each of the services being requested.
210   This includes all procurement policies and the ability to generate purchase orders and
211   work orders.
212   • A single point of contact which can be used to request the service. Service Requests can
213   be initiated via phone call, email, in person, and direct entry to the request system (via
214   tool or web for operations personnel).
215   • Self-service tools needed to provide a front-end interface to the users. It is essential that
216   these tools integrate with the back-end fulfillment tools.
217   • Customer/User satisfaction surveys will be conducted automatically after the service
218   request is fulfilled. Care should be taken to limit the number of questions to reduce
219   impact on time spent by users completing the surveys. Survey questions must be carefully
220   designed in a way to collect the desired data. Survey design is a specialized discipline
221   that requires a good understanding of statistics and survey techniques.

222

223 ## 3.0   ROLES AND RESPONSIBILITIES

224 Each process has roles and responsibilities associated with design, development, execution and
225 management of the process. A role within a process is defined as a set of responsibilities. Process
226 managers' report process deviations and recommended corrective action to the respective process
227 owner. Authoritative process guide control is under the purview of the process owner. The process
228 owner for RqF is from the USMC C4 organization.

229 Management (i.e., responsibility) of the process may be shared; generally, a single manager exists
230 at the enterprise and at each MITSC. For certain processes, especially those within Service Design
231 and Service Transition, managers also exist within Marine Corps Systems Command and Programs
232 of Record. Some Service Operation processes will require managers at the RNOSC. RNOSC is
233 responsible for Situational Awareness (SA) to the Marine Corps forces G6 in addition to
234 responsibilities outlined in the SIPRNet Concept of Employment (COE). There can also be
235 instances where a single person is responsible for multiple roles. Factors such as Area of
236 Responsibility (AOR), size of user base and size of the process support team dictate exactly which
237 roles require a dedicated person(s) and the total number of persons performing each role. This
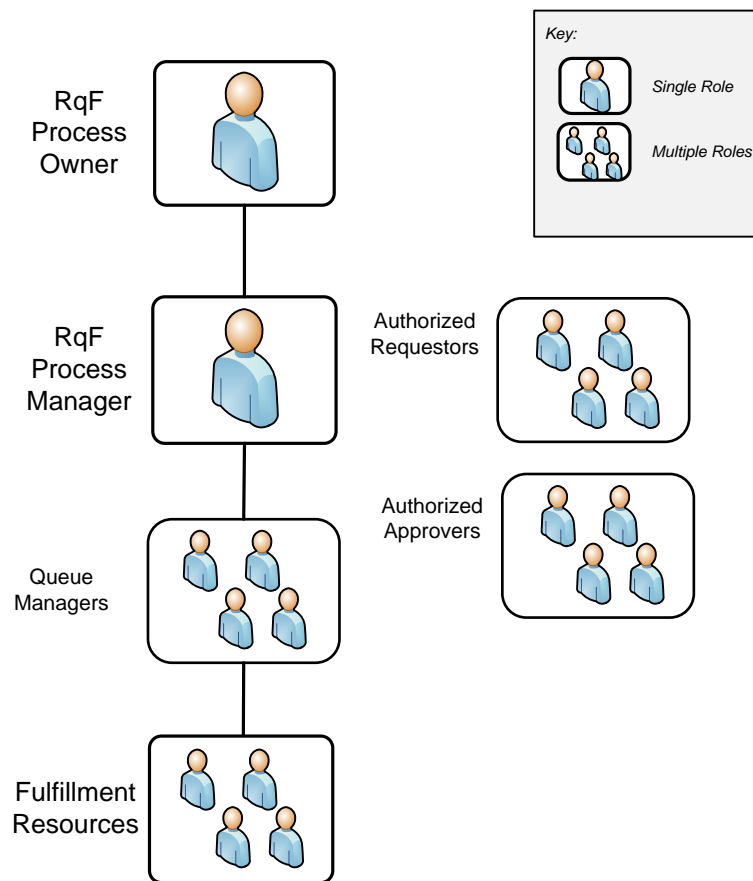238 process guide defines all *mandatory* roles.

239

240 **3.1   Roles**

241

242   *Figure 4: RqF Roles*

243

244 ***Table 5: RqF Defined Roles and Responsibilities***

Description	Overall Responsibility
Role #1 RqF Process Owner	
The RqF Process Owner owns the process and the supporting documentation for the process. The primary functions of the RqF Process Owner are oversight and continuous process improvement. To these ends, the RqF 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 RqF Process Owner is responsible for identifying and ensuring required actions are taken to correct the situation. In addition, the RqF Process Owner is responsible for the approval of all proposed changes to the process, and development of process improvement plans.	• Reviews and understand all references pertaining to process ownership • Documents and publicizes the process • Establishes and communicates the process roles and responsibilities • Ensures updates to the Process Guide are performed according to the Change Management Process • Defines the Key Performance Indicators (KPIs) to evaluate the effectiveness and efficiency of the process • Reviews KPIs and acts required following the analysis • Assist with and being ultimately responsible for the process design • Ensures RqF processes and tools integrate with other E-ITSM processes and that requirements for the tools are defined • Ensure the effectiveness and efficiency of the Request Fulfillment Process and working practices through continuous improvement • Reviews any proposed enhancements to the process • Provides input to the ongoing Service Improvement Plan • Address any issues with the execution of the process • Ensures all relevant staff have the required training and are aware of their role in the process • Ensures that the process, roles, responsibilities and documentation are regularly reviewed and audited • Interfaces with appropriate organizations to ensure that the process receives the necessary staff resources • Ensure all stakeholders are sufficiently involved in the Request Fulfillment Process • Ensures tight linkage between the Request Fulfillment Process and other related processes • Ensure organizational adherence to the process • Identifies opportunities to improve the process
Role #2 RqF Process Manager	
The RqF Manager ensures effective coordination of activities to fulfill user requests. The RqF Manager manages, reports, and coordinates all activities necessary to identify, log, route for approval (where required), fulfill and close requests. RqF Managers will communicate and coordinate with their counterparts on requests or the process when required/beneficial.	• Maintains awareness of USMC and Department of Defense (DoD) directives • Interfaces with various enterprise, regional and local representatives to monitor effectiveness of RqF process • Develops, documents and follows up on action plans • Provides data on escalation history managing requests for information regarding escalations • 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 • Tactical role that performs end-to-end implementation of the Request Fulfillment process • Reviews effectiveness and efficiency of the RqF Process execution at their level of the enterprise • Ensures that the process is executed at his or her level

Description	Overall Responsibility
	• Verify utilization of a request tracking system at the appropriate level • Maintains contact with other groups and organizations performing related work, and coordinates new ideas and developments • Reviews requests not fulfilled through the standard RqF Process • Identifies opportunities to improve the process
Role #3 Authorized Requestor	
The Authorized Requestor, formerly known as the Information Service Coordinator (ISC), interfaces with the Customer as the initial point of contact for Request Fulfillment. The Authorized Requestor owns the request records he or she generates. As the record owner, the Authorized Requestor tracks all record activities/statuses, remaining the single point of contact for the customer throughout the lifecycle of the record.	• Receives the request • Authenticates the Requestor information (check information in the Global Address List, confirm location, etc.) • Creates a Service Request record (ticket) in the Service Request Module (SRM) if the record does not already exist • Categorizes the record • Applies procedures applicable to the Requestor and categorization • Qualifies request record • Knowledgeable of the service level requirements and executes the procedures accordingly • Provides technical communication to customer when needed for informational requests • Uses available resources to fulfill request types identified for completion • Communicates the status and completion to the user/external help desk and other staff/interested parties • Once a request is fulfilled, ensures the customer agrees that the request has been met. Either closes the record or returns the record to the Queue Manager for further work • Informs procedure owners if issues are detected in procedures • Provide feedback via survey • Identifies opportunities to improve the process
Role #4 Authorized Approver	
Authorized Approvers grant or deny permission for Service Requests. They are identified with each Service Request type. Identification and routing instructions for Authorized Approvers is included within the procedures for each type of request.	• Authorized Approver role is to a request type • Authorized Approver for a request type is identified in the request handling procedures and routing instructions • Authorized Approvers provide and/or deny Request Authorization for their request type(s) • Provide response information within the request system as defined within the Authorization response routing instructions • Identifies opportunities to improve the process
Role #5 Queue Manager	
The Queue Manager ensures effective coordination of activities to fulfill requests with a primary focus on escalations, prioritizations, routing and queue management.	• Awareness of USMC and DoD directives • Ensures Service Requests are accurately transferred and/or escalated to the appropriate Resolution Team/AoR • Requests, reviews, and reports metric performance • Assists the support engineers through the Service Request process within their domain • Identifies opportunities to improve the process
Role #6 Fulfillment Resources	
Fulfillment Resources specialize in the fulfillment of specific categories of Services Requests. These resource teams receive the requests from the Authorized Requestor and maintain communication with Authorized	• Provides all facets of support concerning the fulfillment of specialized categories of Service Requests. • Maintains and updates work instruction level documentation specific to the fulfillment of their specific category of service request • Fulfills Service Requests • Updates where necessary, IT asset management information

Description	Overall Responsibility
Requestor on the status of the request throughout the fulfillment stage of the process.	• Understands the service level and executes accordingly • Provides technical communication to customer/caller regarding quick fixes • Uses available resources to fulfill requests (people, tools and processes), escalating as needed • Provides knowledge and training as required to other support teams • Identifies opportunities to improve the process

245

3.2   Responsibilities

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

251 The Responsible, Accountable, Consulted, Informed, Participant (RACI-P) model is a method for
252 assigning the type or degree of responsibility that roles (or individuals) have for specific tasks.

253 **R**esponsible – Completes the process or activity; responsible for action/implementation. The
254 degree of responsibility is determined by the individual with the "A".

255 **A**ccountable – Approves or disapproves the process or activity. Individual who is ultimately
256 answerable for the task or a decision regarding the task.

257 **C**onsulted – Gives needed input about the process or activity. Prior to final decision or action,
258 these subject matter experts or stakeholders are consulted.

259 **I**nformed – Needs to be informed after a decision or action is taken. May be required to take action
260 as a result of the outcome. This is a one-way communication.

261 **P**articipant –Assists 'R' in the execution of the process and/or activity.

262

263   Table 6 establishes responsibilities for high-level process activities by organization.

264   *Table 6: Responsibilities for Enterprise RqF Organizations*

RqF Process Activities	Requestor	Service Desk	MARFORCYBER\MCCOG	RNOSC	MCSC	MITSC	Base	USMC C4
Identification	(R)P	(R)	P	P		P	P	A
Logging	(R)C	(R)	P	C		C	C	A
Categorization	I	R	P	C		C	C	A
Prioritization	C	R	P	C		C	C	A
Authorization*	I	P	(R)P	(R)C	(R)C	(R)C	(R)C	A(R)C P
Fulfillment*	I	(R)	(R)P	(R)P	(R)P	(R)P	(R)P	A
Closure	C	R	P					A

*** Authorization and Fulfillment Responsibilities varies by Request and, therefore, the Responsible roles may fall within any one of the listed organizations for fulfillment depending upon the type of request.*

Legend:
Responsible (R) – Completes the process or activity. The (R) indicates that Responsibility will vary depending upon the request type and could fall within any of the designated columns.
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.

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

265
266

267 Table 7 establishes process role responsibilities for high-level process activities as they relate to
268 process roles. Process roles transcend organizational boundaries; therefore, a role-based RACI-P
269 chart ensures proper assignment of responsibilities to individuals.

270   *Table 7: Responsibilities for Enterprise RqF Roles*

RqF Process Activities	RqF Process Owner	RqF Process Manager	Queue Manager	Authorized Requestor	Fulfillment Resources	Authorized Approver
Identification	A	P		R		
Logging	A	P	I	R		
Categorization	A	P	I	R		
Prioritization	A	P	P	R		C
Authorization	A	P	C	P		R
Fulfillment	A	P	P	P	R	I
Closure	A	P	I	R		

Legend:
Responsible (R) – Completes the process or activity. Only one Role will be responsible for an activity. The (R) indicates that Responsibility will vary depending upon the request type and could fall within any of the designated columns.
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.

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

271

272

4.0   SUB-PROCESSES

274 The USMC RqF process consists of seven sub-processes. While every Service Request will
275 follow each sub-process on some level, not every activity within each sub-process is utilized for
276 every USMC organization or type of Service Request.

4.1   Identification

278 Identification is the activity of determining how the Service Request is to be routed within the
279 RqF process. The RqF process is triggered through request inputs from the Service Catalog.
280 The Service Request ticket is opened to capture the Requestor's pertinent information (i.e.,
281 name, location and contact
282 information) and a description of
283 the Service Request.   The Service
284 Request is identified as pertaining
285 to the Classified (SIPRNET) or
286 Unclassified (NIPRNET) ticketing
287 systems.

288
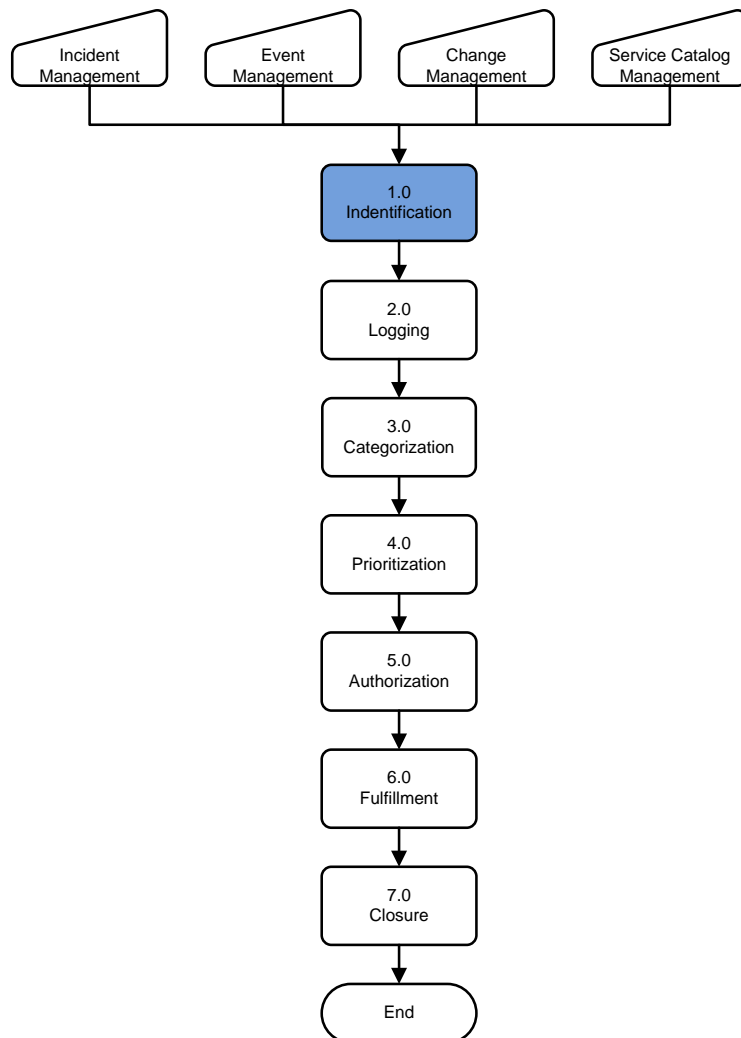
289   The following workflow (Figure 5) depicts the Identification sub-process.
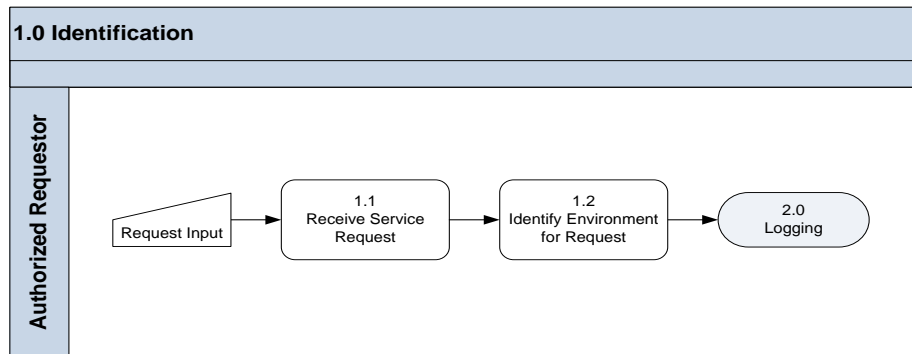
290

291   ***Figure 5: Identification Sub-Process***

292   Table 8 describes the Identification sub-process steps as depicted in Figure 5.

293   ***Table 8: Identification Sub-Process Descriptions***

1.0 Identification		
Number	**Process Activity**	**Description**
1.1	Receive Service Request	Service Requests can be initiated via phone call, e-mail, in person, and direct entry to the request system (via tool or web for operations personnel). The Identification sub-process is triggered when a Service Request is submitted, and the Authorized Requestor begins identification.
1.2	Identify Environment for Request	Determine if the Service Request applies to the NIPRNET or SIPRNET for requests that do not originate through a portal or a catalog. Requests submitted through a portal or catalog will already have a SIPRNET or NIPRNET designation.

294

295

296   **4.2   Logging**

297   Once a Service Request has been identified it is logged in the request management system.
298   Information about the Requestor must also be added to the request record so that prioritization,
299   authorization and fulfillment can be completed in the most efficient manner. The accuracy and
300   completeness of Logging is also
301   critical to reporting, tracking, and
302   service management.

303

| Incident Management | Event Management | Change Management | Service Catalog Management |

```
              ┌─────────────┐
              │     1.0     │
              │Indentification│
              └─────────────┘
                     │
              ┌─────────────┐
              │     2.0     │
              │   Logging   │
              └─────────────┘
                     │
              ┌─────────────┐
              │     3.0     │
              │Categorization│
              └─────────────┘
                     │
              ┌─────────────┐
              │     4.0     │
              │Prioritization│
              └─────────────┘
                     │
              ┌─────────────┐
              │     5.0     │
              │Authorization│
              └─────────────┘
                     │
              ┌─────────────┐
              │     6.0     │
              │ Fulfillment │
              └─────────────┘
                     │
              ┌─────────────┐
              │     7.0     │
              │   Closure   │
              └─────────────┘
                     │
              (    End    )
```
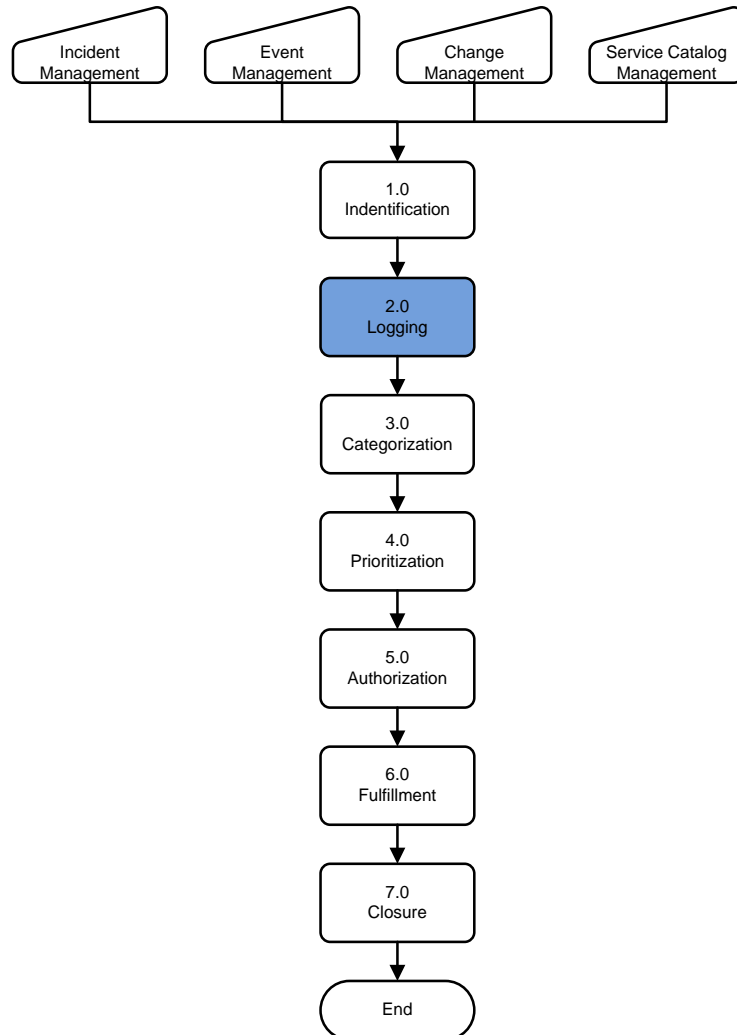
304   The following workflow (Figure 6) depicts the Logging sub-process.
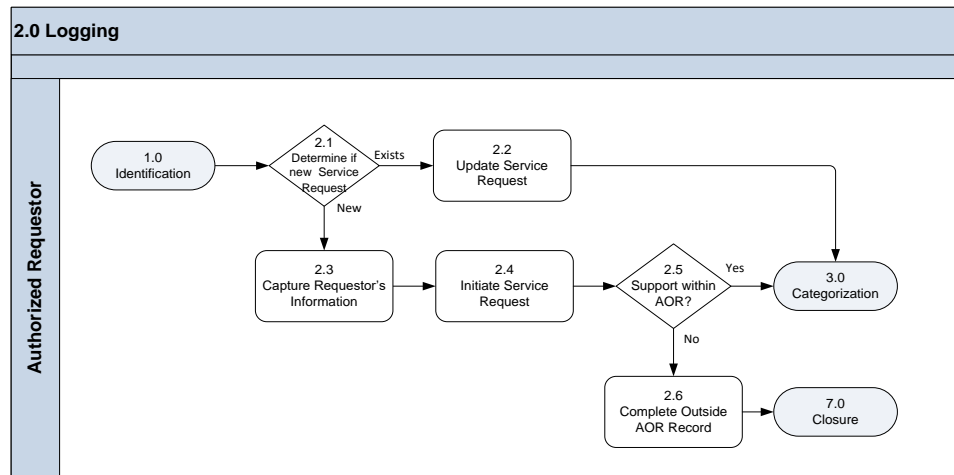
305

306   ***Figure 6: Logging Sub-Process***

307   Table 9 describes the Logging sub-process steps as depicted in Figure 6.

308   ***Table 9: Logging Sub-Process Descriptions***

| 2.0 Logging		
Number	**Process Activity**	**Description**
2.1	Determine if New or Existing Request	The Authorized Requestor determines if this a new or existing Service Request 1. New: If this is a new request, then continue to capture Requestor's information. 2. Exists: If this is an existing request, then proceed to update Service Request.
2.2	Update Service Request	The Authorized Requestor reviews and updates the existing Service Request.
2.3	Capture Requestor's Information	The Authorized Requestor captures the Requestor's name, location and contact information, updating the people record as required, and a description of the Service Request. In addition, there is a method to verify which user is receiving the service.
2.4	Initiate Service Request	Any information that has been collected by the Authorized Requestor is formally initiated in a record and a specific request record number is assigned.
2.5	Support within AOR?	The Authorized Requestor determines if the inquiry is within the MCEN AOR and updates the Customer on the next step. 1. Yes: If within AOR, then proceed to Request Categorization. 2. No: If not within AOR, then proceed to Complete Outside AOR Record.
2.6	Complete Outside AOR Record	The Authorized Requestor updates the Requestor on the next step in the process, completes the Service Request using the Outside AOR template, and routes to Request Closure.

309

310 **4.3   Categorization**

311   Service Request Categorization is conducted to facilitate correct and timely authorization,
312   fulfillment, and accuracy in reporting. Categorization identifies the IT Service to which the
313   request is associated. The IT Service has predefined routing instructions, authorization contacts,

314   and fulfillment procedures that are
315   associated with the related request
316   category. These services are
317   related to specific product and
318   operational categories, or request
319   for information, comments and
320   complaints. Additionally,
321   categorization is corrected when
322   necessary throughout the lifecycle
323   of the service request to ensure
324   proper routing and accuracy in
325   reporting.

326   The Marine Corps product
327   categorization structure contains
328   three tiers designed to quickly and
329   accurately identify technologies,
330   manufacturers, products, versions,
331   and configuration items.

332   Operational categories define the
333   work for particular types of
334   Service Requests and their related
335   tasks.

336   The Marine Corps operational
337   categorization is a three-tier
338   structure used to enable quality
339   reporting in the record system, to
340   qualify groups and support staff
341   assignments, and to manage the routing for authorization.

342
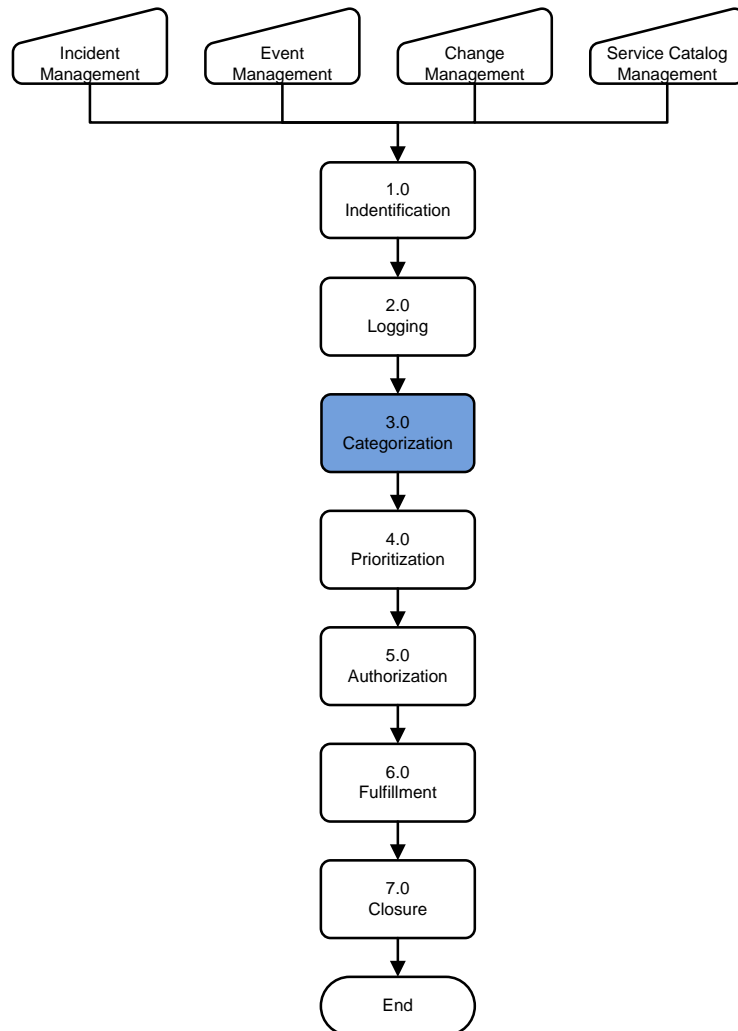
343   Table 10 provides an example of possible categorization options.

344   *Table 10: Categorization and Sub-Process Descriptions*

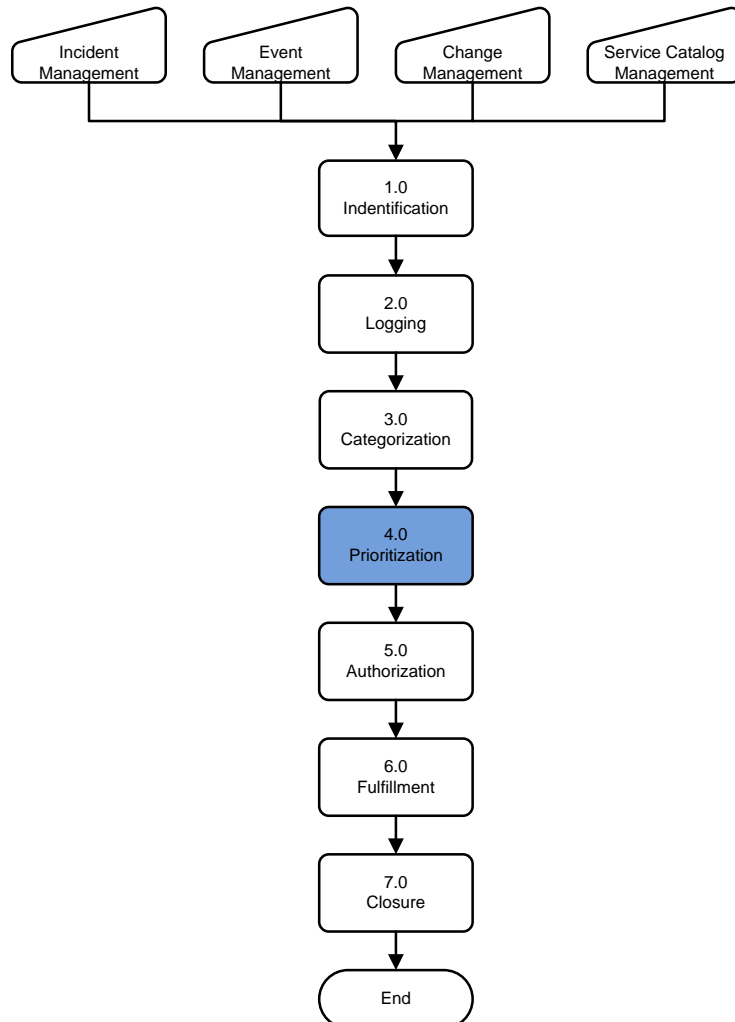| Operational Categorization		
Tier 1	**Tier 2**	**Tier 3**
Service Request	Move	Same Building
		Different Building
	Add/Install	Approved Hardware
		Unapproved/Non-Standard Hardware
	Change Existing	
	Replace/Swap	Improve Utility or Performance
		Lemon – Previous Issues
	Decommission	
	Training/How-To	
	Request New Category	

345

346 **4.4   Prioritization**

347   Service Request prioritization is based upon several components of which one is service level
348   objectives. These objectives must be defined within the specific SLA for each request type. Service
349   Level Objectives, once defined, will establish time boundaries that may impact prioritization. The

350   Prioritization sub-process is used to
351   determine the sequence of
352   fulfillment. Considerations when
353   determining prioritization include:

354   • VIP status of the Requestor
355   • Time Sensitive – Is a critical
356   deployment or tactical
357   operation underway?
358   • As greater levels of detail are
359   available for types of
360   requests, then more specific
361   Priority definitions can be
362   provided for each type of
363   Service Request.

364   The resulting Prioritization for the
365   Service Request may be adjusted
366   based on management review.

367

```
┌──────────┐ ┌──────────┐ ┌──────────┐ ┌──────────────┐
│ Incident │ │  Event   │ │  Change  │ │Service Catalog│
│Management│ │Management│ │Management│ │ Management   │
└────┬─────┘ └────┬─────┘ └────┬─────┘ └──────┬───────┘
     └───────────┴────────────┴───────────────┘
                         │
                  ┌──────────────┐
                  │     1.0      │
                  │Indentification│
                  └──────┬───────┘
                         │
                  ┌──────────────┐
                  │     2.0      │
                  │   Logging    │
                  └──────┬───────┘
                         │
                  ┌──────────────┐
                  │     3.0      │
                  │Categorization│
                  └──────┬───────┘
                         │
                  ┌──────────────┐
                  │     4.0      │
                  │Prioritization│
                  └──────┬───────┘
                         │
                  ┌──────────────┐
                  │     5.0      │
                  │Authorization │
                  └──────┬───────┘
                         │
                  ┌──────────────┐
                  │     6.0      │
                  │ Fulfillment  │
                  └──────┬───────┘
                         │
                  ┌──────────────┐
                  │     7.0      │
                  │   Closure    │
                  └──────┬───────┘
                         │
                    ╭─────────╮
                    │   End   │
                    ╰─────────╯
```

368   The following workflow (Figure 7) depicts the Prioritization sub-process.
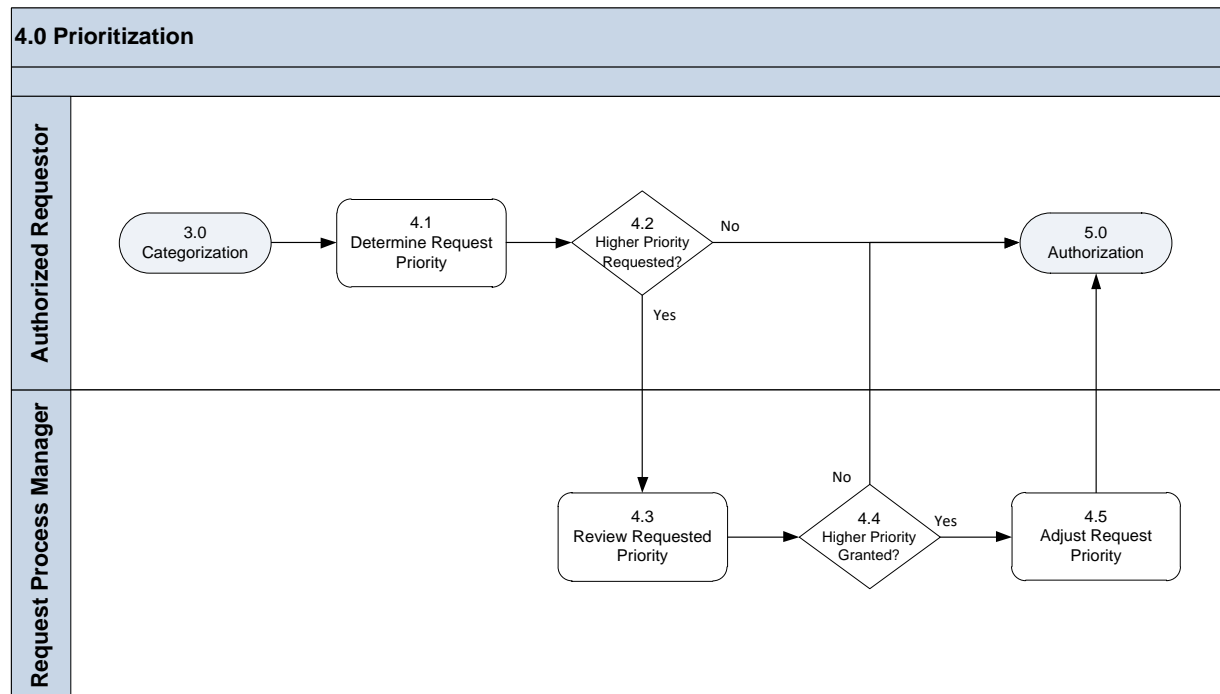
369

370   *Figure 7: Prioritization Sub-Process*

371   Table 11 describes the Prioritization sub-process steps as depicted in Figure 7.

372   *Table 11: Prioritization Sub-Process Descriptions*

4.0 Prioritization		
Number	**Process Activity**	**Description**
4.1	Determine Request Priority	The Authorized Requestor utilizes the requestor's input to determine Priority and the request type. The Authorized Requestor assigns a Priority based upon the level designated for the Service Request type as defined within the procedures for that type. An initial Prioritization is derived based upon the Requestor's input, request type, and VIP status of the Requestor.
4.2	Higher Priority Requested?	If the user requests a review for potential higher priority, then the Service Request is sent to an RqF Process Manager for review. 1. Yes: The user requests a higher level of Priority. Proceed to review request priority. 2. No: The user does not request a higher level of Priority. Proceed to Authorization with the established Priority.
4.3	Review Requested Priority	The MITSC Queue Manager reviews the requested higher level of Priority based upon the request type and requestor's input.

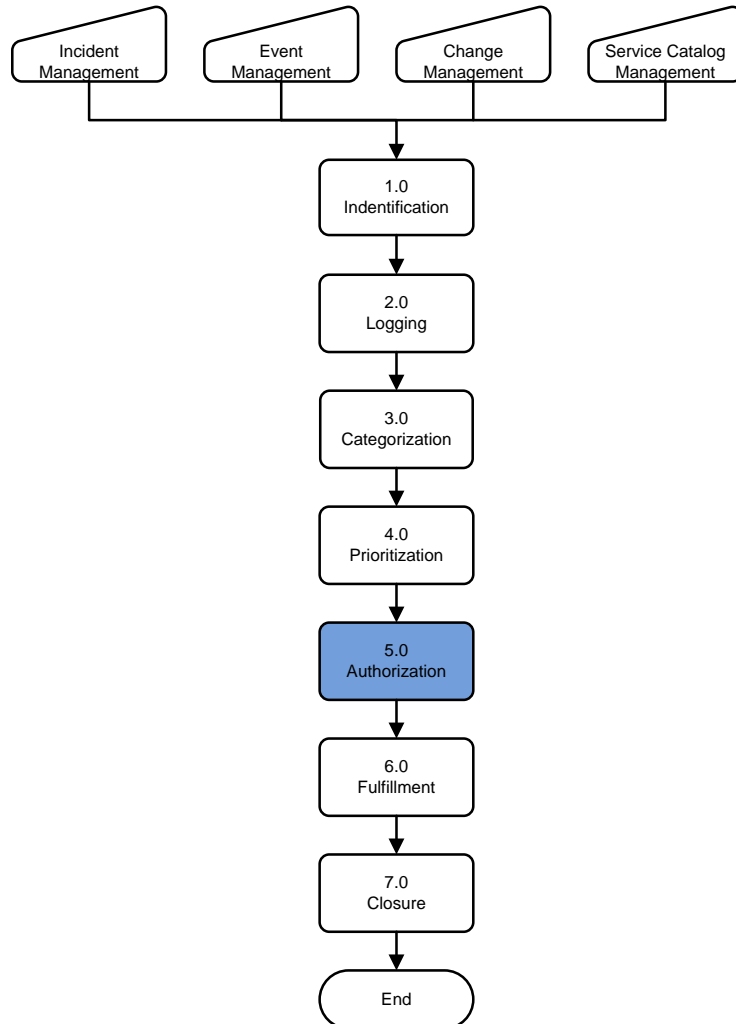| 4.0 Prioritization		
Number	**Process Activity**	**Description**
4.4	Higher Priority Granted?	The MITSC Queue Manager determines if elevated Priority is required. 1. Yes: The request proceeds to adjust request priority. 2. No: The request retains its assigned level of Priority. The request proceeds to Authorization.
4.5	Adjust Request Priority	The request is assigned a higher Priority. The request proceeds to Authorization.

373

374 *Table 12: Priority Descriptions*

Priority Descriptions	
Level	**Description**
Critical	o Immediate fulfillment of a Service Request is required -or- o The customer billet or mission is such that immediate fulfillment is required (VIP)
High	o User is unable to perform job functions without requested action
Medium	o User can perform parts of job functions without requested action
Low	o User can continue to perform job functions without requested action

375

376 The priority may also be adjusted by the approval authority. It is the responsibility of RqF Process
377 Managers at all levels of the organization to review incoming Service Requests, to ensure priorities
378 are accurately set, and to make adjustments when appropriate.

379 **4.5   Authorization**

380 Authorization is the sub-process that enables appropriate decision making for a specific service
381 request. Many types of Service Requests require financial, hierarchical, or other organizational
382 approval before the request can be fulfilled. The category of the Service Request and the identity

383 of the requestor are used to
384 determine if authorization is
385 required prior to fulfillment. In
386 those instances, authorization roles
387 are consulted before the request
388 enters the Fulfillment sub-process.
389 Approval requirements for specific
390 Service Requests are pre-defined,
391 documented, and stored with the
392 specific procedures for that request
393 type.

394

| Incident Management | Event Management | Change Management | Service Catalog Management |

1.0 Indentification

2.0 Logging

3.0 Categorization

4.0 Prioritization

5.0 Authorization

6.0 Fulfillment

7.0 Closure

End

395   The following workflow (Figure 8) depicts the Authorization sub-process.

396

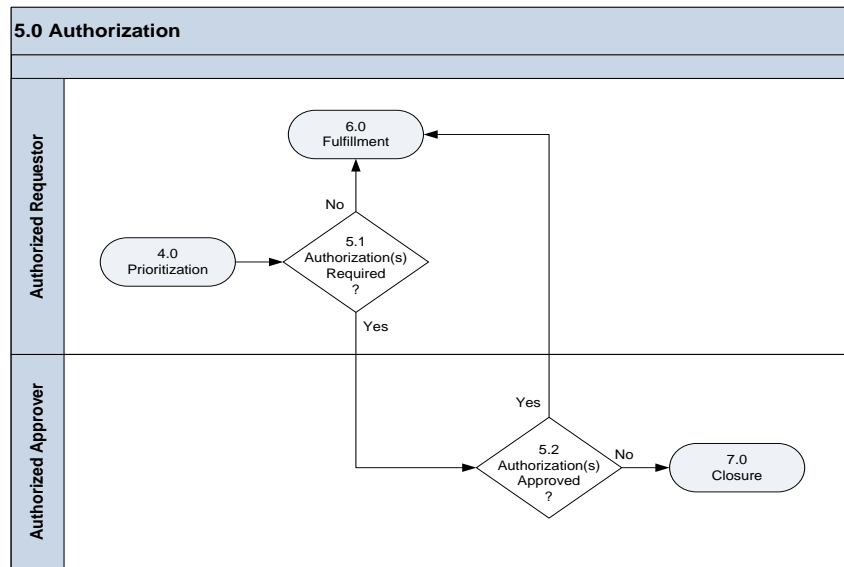397   *Figure 8: Authorization Sub-Process*

398   Table 13 describes the Authorization sub-process steps as depicted in Figure 8.

399   *Table 13: Authorization Sub-Process Descriptions*

5.0 Authorization		
Number	**Process Activity**	**Description**
5.1	Authorization(s) Required?	The type and categorization of the request as well as the identity of the user, is used to determine if authorization is required prior to fulfillment. 1. Yes: If authorization is required, then proceed with routing for approval. Requests requiring authorization are routed to the predefined approving authorities for decision. 2. No: If authorization is not required, then proceed to Request Fulfillment.
5.2	Authorization(s) Approved?	One or more predefined authorities are consulted for decision on authorization to proceed with fulfilling the request. These authorities are defined within the instructions for each request type requiring authorization. 1. Yes: If authorization is granted, then proceed to Request Fulfillment. 2. No: If authorization is not granted, then the Authorized Requestor informs the requestor of the denial of the request by the approving authority. The request is routed to Request Closure.

400

401 **4.6   Fulfillment**

402 The RqF activity delivers the authorized service, component and/or information to the requestor.
403 The actual fulfillment activity depends on the categorization of the Service Request. Certain
404 requests, such as questions or inquiries, may be completed by the Authorized Requestor, acting as
405 first-line   support,   while   other
406 Service Requests are forwarded to
407 specialist groups and/or suppliers
408 for fulfillment.   Procedures and
409 work instructions for the fulfillment
410 of standard changes are accessed
411 from   a   controlled   repository,
412 having been previously developed,
413 tested, and documented in ChM and
414 RDM.

415
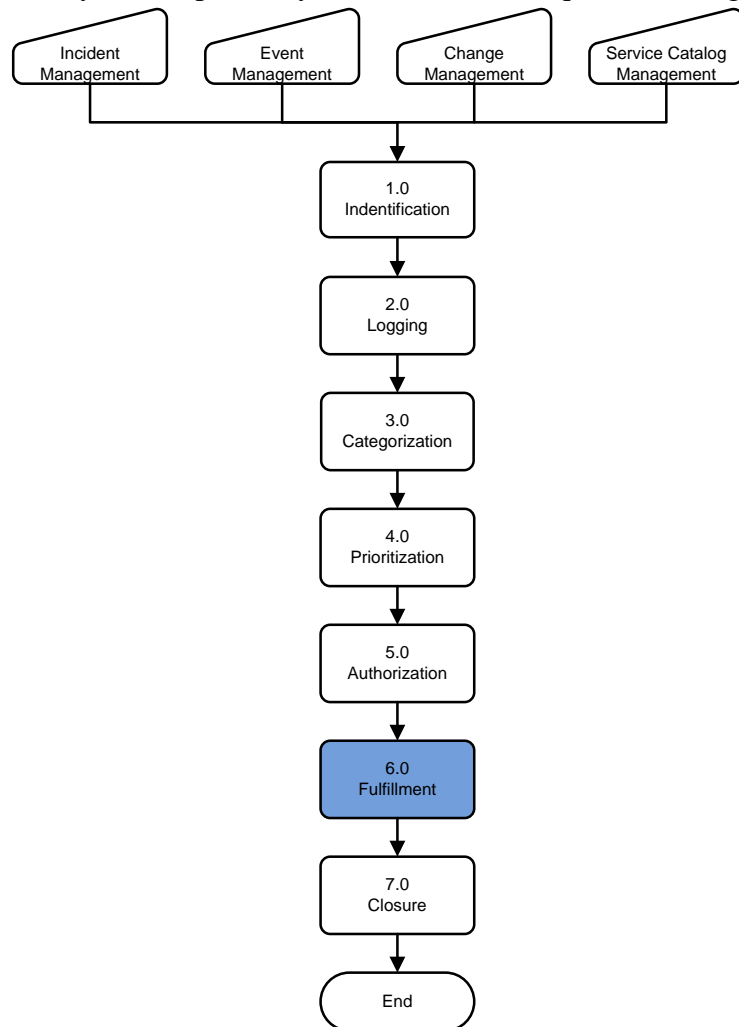
416   The following workflow (Figure 9) depicts the Fulfillment sub-process.

417
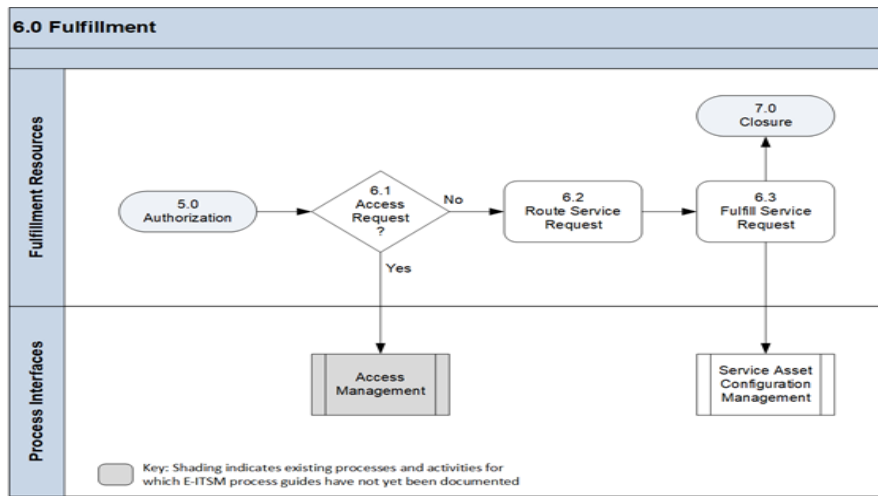
418   *Figure 9: Fulfillment Sub-Process*

419   Table 14 describes the Fulfillment sub-process steps as depicted in Figure 9.

420   *Table 14: Fulfillment Sub-Process Descriptions*

| 6.0 Fulfillment		
Number	**Process Activity**	**Description**
6.1	Access Request?	Some request types require that Access Management perform Fulfillment activities. The type and categorization of the request are used to determine if the request will be routed to Access Management. 1. Yes: If the inclusion of Access Management is required, then route to the Access Management process. 2. No: If the inclusion of Access Management is not required, then proceed with routing for fulfillment.
6.2	Route Service Request	Service Requests are passed to the predefined fulfillment team for completion.
6.3	Fulfill Service Request	The Request Fulfillment resources complete the request as defined within the procedures related to the request type. If the fulfillment of the request involves adding, modifying, or decommissioning a Configuration Item (through a standard change), then information is provided to Asset Management and Configuration Management. Additionally, the Fulfillment resources: 1. Execute necessary procedures to confirm the Service Request has been completed. 2. Ensure the applied solution, escalation, transfer and activity information is recorded. 3. Provide Service Request status to the Service Catalog interface for user retrieval. 4. Route the Request for Closure.

421 **4.7   Closure**

422   The Authorized Requestor verifies that the Service Request is fulfilled and can be closed. A
423   Service Request can be manually closed after three attempted contacts, with the user, or once the
424   user confirms that the Request has
425   been fulfilled. A Service Request
426   will be automatically closed after
427   seven business days transpire
428   without any response from the user.
429   The Service Request is then closed.

430
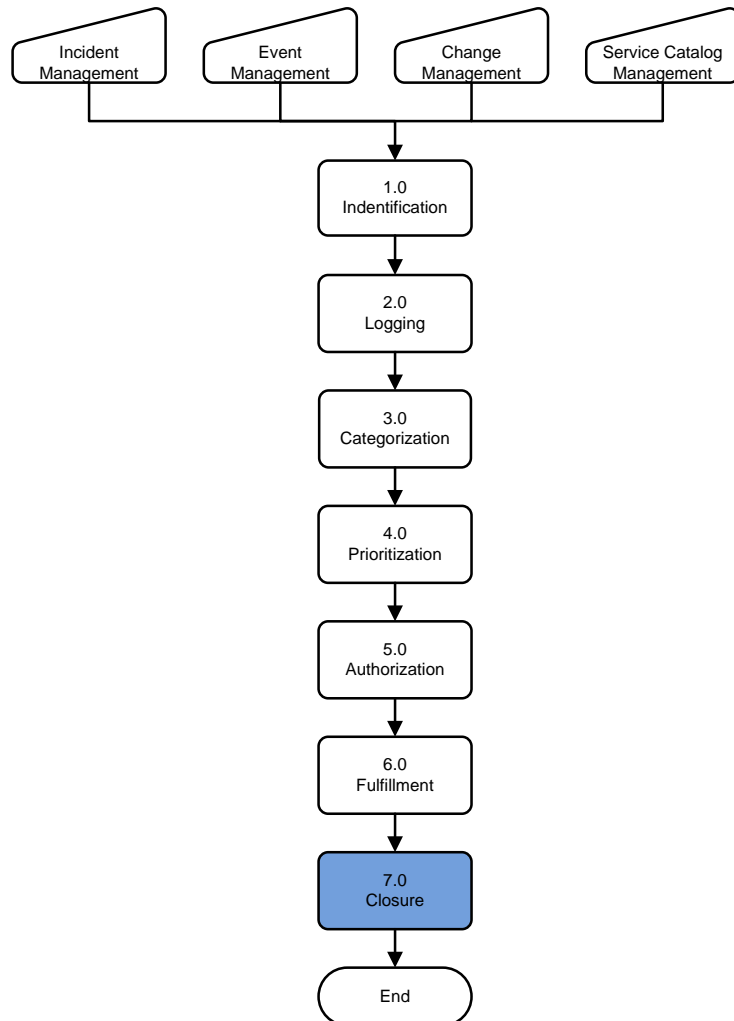
431   The following workflow (Figure 10) depicts the Closure sub-process.
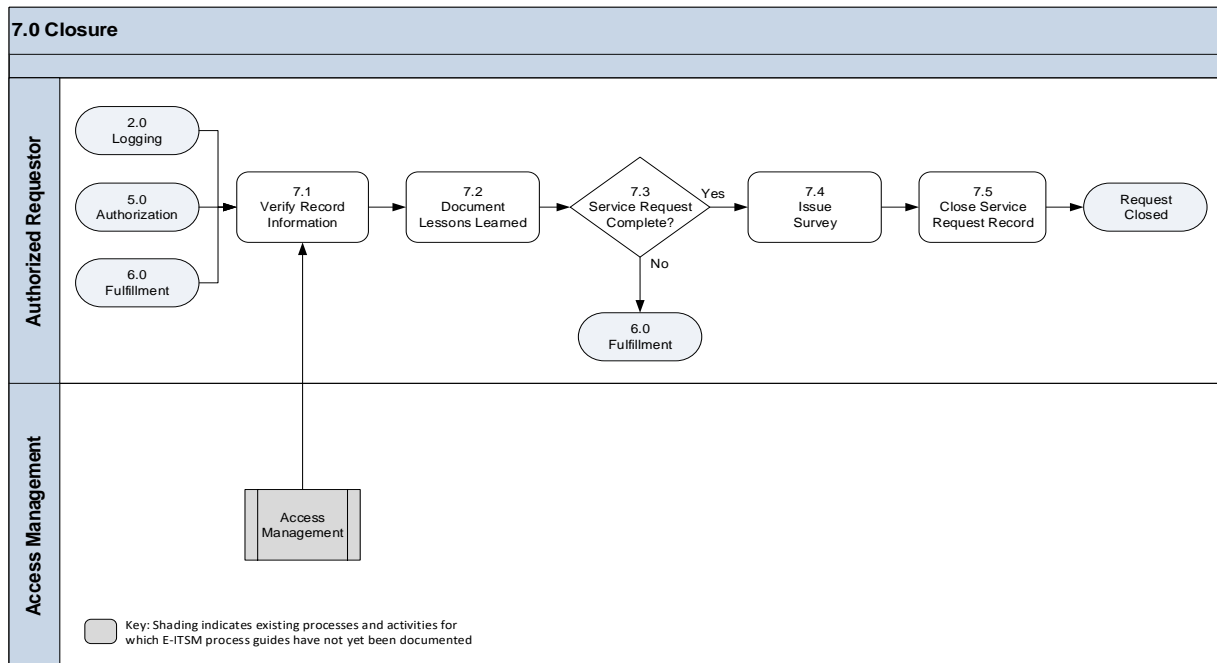
432

433   ***Figure 10: Closure Sub-process***

434   Table 15 describes the Closure sub-process steps as depicted in Figure 10.

435   ***Table 15: Closure Sub-Process Descriptions***

7.0 Closure		
Number	**Process Activity**	**Description**
7.1	Verify Record Information	The Authorized Requestor ensures the routing, authorization, and fulfillment procedure information is accurately referenced in the record. Outside AOR records flow in to the Closure sub-process from Logging. Requests denied by approval authorities flow to the Closure sub-process from Authorization. Fulfilled requests flow to the Closure sub-process from Fulfillment. Access requests flow to the Closure sub-process from Access Management.
7.2	Document Lessons Learned	The Authorized Requestor ensures the fulfillment description, escalation, transfer and activity information is complete on the record. Improvement opportunities identified during the fulfillment of the Service Request are also documented and forwarded to the appropriate Service Owner. Does not apply to an Outside AOR record.

7.0 Closure		
Number	**Process Activity**	**Description**
7.3	Service Request Complete?	The Authorized Requestor verifies with the requestor that the Service Request has been completed. Each attempt to reach the requestor is documented in the request record. 1. Yes: If the requestor verifies that the Service Request has been completed, then continue to issue survey. 2. No: If requestor indicates that the Service Request has not been completed, then return to routing for fulfillment. If the requestor has not responded within the timeframe specified for that type of request/service, then proceed to Issue Survey. Does not apply to an Outside AOR record.
7.4	Issue Survey	Issue customer satisfaction survey. Survey is automatically sent through the ITSM Tool. Does not apply to an Outside AOR record.
7.5	Close Service Request Record	Close the Service Request request record.

436

437 **Appendix A – ACRONYMS**

AOR	Area of Responsibility	MCEN	Marine Corps Enterprise Network
C4	Command, Control, Communications and Computers	MCI	Marine Corps Installation
CAB	Change Advisory Board	MCO	Marine Corps Order
CCIR	Commander's Critical Information Requirements	MCTP	Marine Corps Techniques Publication
CfM	Configuration Management	MEF	Marine Expeditionary Forces
ChM	Change Management	MITSC	Marine Information Technology Support Center
CI	Configuration Item	NIPRNET	Non-Secure Internet Protocol Router Network
CMDB	Configuration Management Database	QA	Quality Assurance
CMS	Configuration Management System	RACI-P	Responsible, Accountable, Consulted, Informed, Participant
COE	Concept of Employment	RDM	Release and Deployment Management
CP	Concepts and Plans	RFC	Request for Change
CPI	Continual Process Improvement	RNOSC	Regional Network Operations and Security Centers
CSF	Critical Success Factor	RqF	Request Fulfillment
CSI	Continual Service Improvement	SA	Situational Awareness
DoD	Department of Defense	SACM	Service Asset Configuration Management
E-ITSM	Enterprise Information Technology Service Management	SDP	Service Design Package
ELS	Early Life Support	SE	Supporting Establishments
EM	Event Management	SIE	Systems Integration Environment
EMS	Event Management System	SIP	Service Improvement Plan
IdAM	Identity and Access Management	SIPRNET	Secret Internet Protocol Router Network
IM	Incident Management	SKMS	Service Knowledge Management Systems
IRM	Information Resource Management	SLA	Service Level Agreement
ISC	Information Service Coordinator	SOP	Standard Operating Procedure
IT	Information Technology	SPOC	Single Point of Contact
KPI	Key Performance Indicator	SRM	Service Request Module
MCCOG	Marine Corps Cyberspace Operations Group	USMC	United States Marine Corps

438

439

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 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).
Event Management 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 because of the same infrastructure fault. Events need correlation to prevent duplication of effort in resolving the original fault.
Exit and Entry Criteria (Pass/Fail)	These are criteria (defined well in advance and accepted by the stakeholders) defined at authorized points in the Release and Deployment Process to set expectations of acceptable/unacceptable results.
Fault	Fault is the deviation from *normal* operation of a CI or a series of CIs. A fault is a design flaw or malfunction that causes a failure of one or more CIs or IT services. Fault is also referred to as an error.
Governance	Governance is the process of ensuring policies and strategy are 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 Systems Integration Environment (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 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 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 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 several 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.

440
441