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

IN REPLY REFER TO:
IRM 2300-03C
C4
14 Nov 17

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

Subj: ENTERPRISE INFORMATION TECHNOLOGY SERVICE MANAGEMENT EVENT MANAGEMENT PROCESS GUIDE

Ref: (a) MCO 5271.1B

Encl: (1) IRM-2300-03C

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

2. CANCELLATION. IRM-2300-03B

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

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

5. SCOPE.

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

b. Waivers. Waivers to the provisions of this publication will be authorized by the Commanding Officer, Marine Corps Cyberspace Operations Group.

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

P. G. ANTEKEIER
By direction

Enterprise IT Service Management
Event Management
Process Guide

Release Date:
14 November 2017

Document Approval / Major Revision Change History Record

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

Release Date (MM/DD/YY)	Release No.	Approvals		Change Description
		Author	Process Owner/Approver	
09/21/09	0.1	Printed Name	Printed Name	Draft Release
11/24/09	1.0	Printed Name	Printed Name	Initial Release
12/03/09	1.1	Printed Name	Printed Name	Updated as per RFAs post CR
06/18/10	2.0	Printed Name	Printed Name	Updated as per CRMs from follow-on Task Order 13, CDRL L0012
08/24/10	3.0	Printed Name	Printed Name	Updated as per CRMs from follow-on Task Order 13, CDRL L0012
12/17/10	4.0	Printed Name	Printed Name	Updated as per CRMs from follow-on Task Order 13, CDRL L0012
02/17/11	5.0	Printed Name	Printed Name	Updated as per CRMs from follow-on Task Order 13, CDRL L0012
06/06/11	6.0	Printed Name	Printed Name	Updated as per CRMs from follow-on E-ITSM Task Order, CDRL L3001
03/07/13	7.0	Printed Name	Printed Name	Updated Text and edited diagrams to reflect the incorporation of VIEWS. Edited diagrams where errors were detected.
04/22/13	8.0	Printed Name	Printed Name	Updated all Process Flow Diagrams. Wrote / Modified all sub-process Tables.
11/18/13	9.0	Printed Name	Printed Name	Updated content based on final review. Prepared for technical editing.
02/05/14	10.0	Printed Name	Printed Name	Revised content to remove material for strategic EM plan.
02/20/14	11.0	Printed Name	Printed Name	Minor revisions based on comments in CRM
08/04/14	12.0	Printed Name	Printed Name	Minor revisions based on comments in CRM
10/22/15	13.0	Printed Name	Printed Name	Major revisions based on input from new Enterprise Event Management Process Owner
06/07/16	14.0	Printed Name	Printed Name	Major revisions based on input from new Enterprise Event Management Process Owner
08/01/17	15.0	Printed Name	Printed Name	Adjudicated and updated based on comments in CRM

Table of Contents

List of Tables

List of Figures

Enterprise Event Management Process Guide

1.0 INTRODUCTION

1.1 Purpose

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

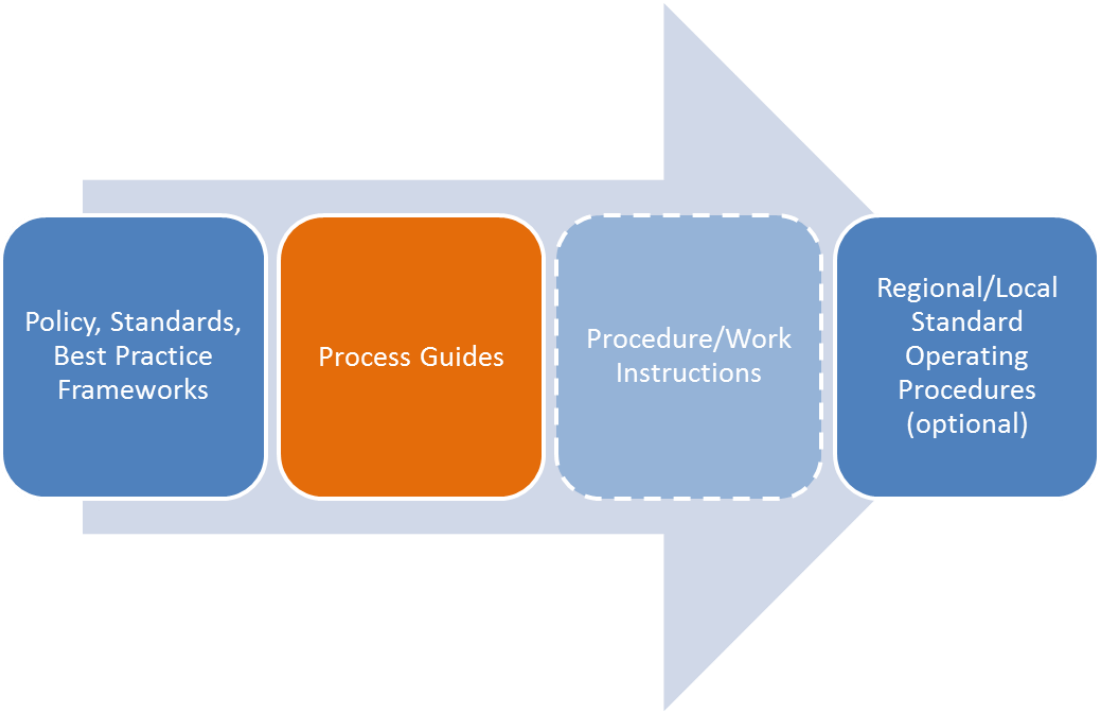


Figure 1-1 Process Document Continuum

1.2 Scope

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

Table 1-1 depicts the various layers of document design. Each layer has discrete entities, each with their own specific authority when it comes to promulgating documentation. This enterprise

process operates at Level B, sub-processes such as procedures and work instructions are not included within the scope of this document.

Table 1-1 Document Design Layers

	ENTITIES	DOCUMENTS GENERATED
LEVEL A	Federal Government Department of Defense (DOD) Department of the Navy (DoN) Marine Corps Headquarters	Statutes/Laws DoD Issuances DoN Policies Marine Corps Orders/IRMS
LEVEL B	MARFORCYBER HQMC C4 Marine Corps System Command (MCSC)	MCOs IRMs (Process Guides) Directives MARADMINS
LEVEL C	Marine Corps Cyberspace Operations Group (MCCOG) MITSC	Regional Procedures Work Instructions
LEVEL D	Marine Corps Bases Marine Corps Posts Marine Corps Stations	Locally Generated SOP's

1.3 Process and Document Control

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

2.0 PROCESS OVERVIEW

2.1 Purpose and Objectives

The general purpose of Event Management (EM) is to manage Events throughout their lifecycle, including detecting events, analyzing their significance, and taking appropriate action.

An Event represents any change of state that has significance for the management and the operation of a Configuration Item (CI) or service. This is accomplished through monitoring and control of networked systems that communicate operational information to the EM system. Events are detected through alerts, sometimes referred to as notifications in other contexts, from either a monitoring tool or the CI itself and require some level of engagement on the part of IT Operations personnel.

The EM Process identifies and establishes the appropriate response to infrastructure, service, business process, and security events that could lead to incidents. EM enables early detection of incidents, possibly before a service outage occurs. The process utilizes monitoring, filtering, correlation, alert and notification tools to correct out-of-sync conditions and communicate status to the service owner and/or administrative group for remediation. This ensures that restoration of service is as rapid as possible, minimizing user impact. The ability to detect and respond quickly to Events enhances user satisfaction with the overall IT environment.

The objectives of the EM process are to:

- Detect meaningful changes to the status of a CI, a service, or the IT infrastructure.
- Detect and alert appropriate technical resources/EMS of any service level degradations prior to becoming an incident.
- Route event notifications to the appropriate department or group, based on event classification.
- Initiate the execution of service operation processes and operations management activities.
- Provide the means to compare actual operating performance and behavior against design standards and Service Level Agreements (SLAs).
- Provide a basis for service assurance, reporting and improvement.

The focus of USMC Enterprise EM is to present Network Operations (NetOps) personnel with situational awareness (SA) of MCEN services in real-time. Notifications generated by EM enable personnel to interpret events, possible incidents, and problems; understand their operational impact; and decisively and rapidly take action to restore services and protect information on the MCEN.

The USMC Enterprise EM process monitors, detects, and manages events throughout their lifecycle. During the EM lifecycle, events are detected, filtered, analyzed, correlated, and

categorized to support the assignment of control actions for the given event condition. The EM process provides the entry point for Service Operations activities within Cyber Operations. In addition, it provides the basis for monitoring Service Delivery and is leveraged to measure Service Improvement using several reporting mechanisms.

The dependency on mission-critical applications necessitates 24x7 availability of Enterprise Services and Systems. Operators within the NetOps Command and Control (C2) community need to know immediately when Enterprise Services, Systems or capabilities:

- Are not operating efficiently
- Have exceeded allowable thresholds
- Have breached an SLA
- Have been compromised
- Have failed
- Have been added, removed or changed

The objectives of the USMC EM process are to:

- Ensure the EM process and capabilities are integrated with USMC Cyber Operations. This provides critical support to USMC Cyber Operations C2 and other IT Service Management (ITSM) processes.
- Detect significant changes in monitored CIs or IT services.
- Determine the appropriate action for significant events and communicate information to the appropriate functional area.
- Provide information related to operating performance, in order for it to be compared to design specifications and SLAs.
- Provide real-time situational awareness of the USMC NIPRNET and SIPRNET to include facilities and other CIs not connected to the MCEN (i.e. Environmental Controls).
- Provide information relevant for continual service improvement.

2.2 Relationships with other Processes

All ITSM processes are interrelated. The processes in Figure 2-1 were selected due to the strength of the relationships and dependencies between them and the degree to which they underpin USMC near-term objectives. While any one of the processes can operate in the presence of an immature process, the efficiency and effectiveness of each is enhanced by the maturity and integration of all processes. Figure 2-1 depicts key relationships which exist between EM and other mature ITSM processes within the USMC.

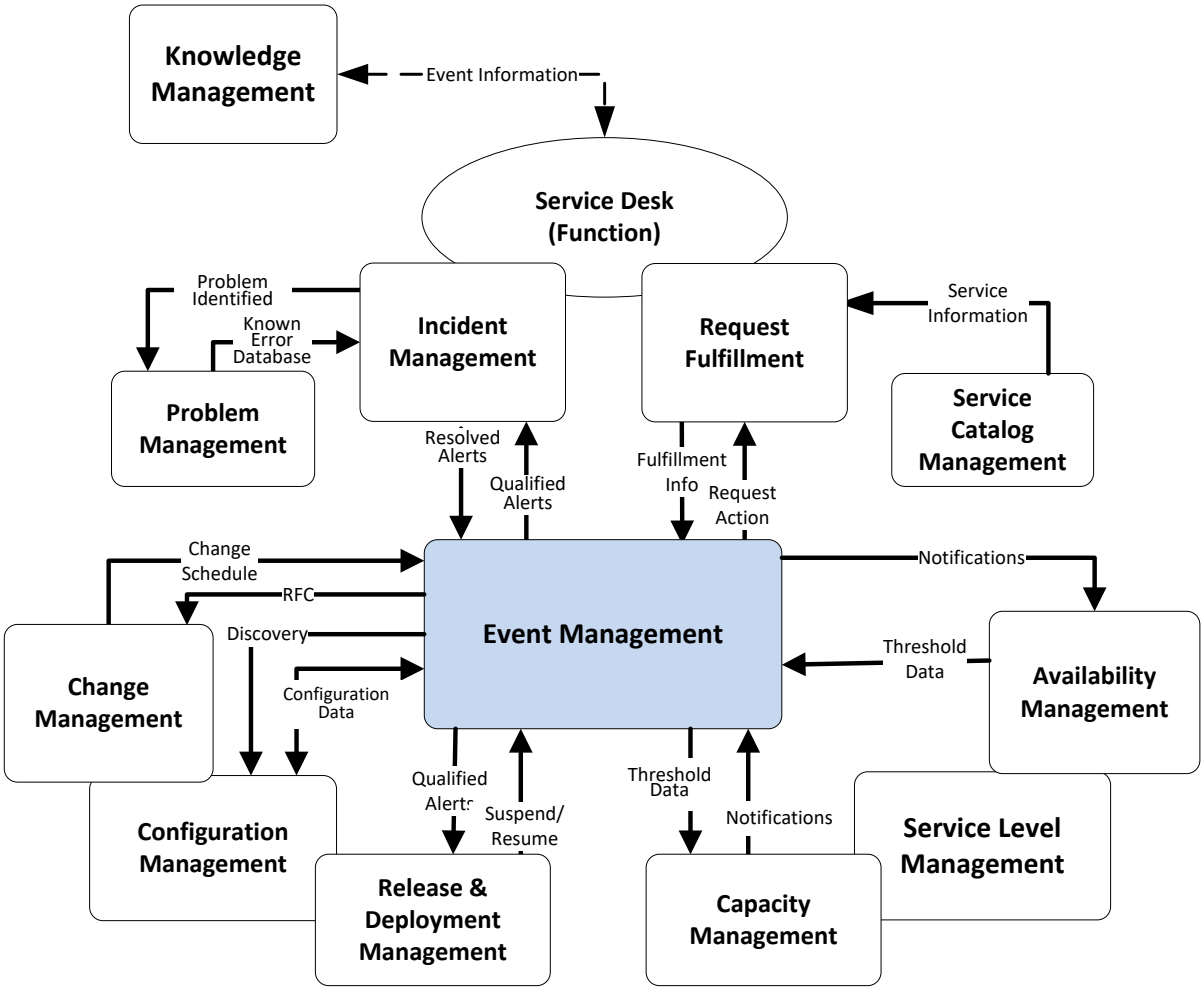


Figure 2-1 EM Relationship with other processes

Event Management enhances every other process with regard to early detection, proactive responses and automation of ordinary and monotonous operations as it matures. The following list describes the EM relationship (input or output) to other process areas, as depicted in Figure 2-1 above:

Knowledge Management (KM)

- Knowledge Management (KM) does not directly interface with Event Management. However, Problem Management, Incident Management, Request Fulfillment, and Service Catalog Management as well as the Service Desk all receive information from KM. The KM System is updated as EM feeds information to and from these intermediary Processes via its various data collection activities, trending analysis and correlation efforts.

Problem Management (PbM)

- While direct communication does not occur, EM Alerts received by Incident Management (IM) are communicated to Problem Management (PbM), as documented, for root cause analysis or known error identification.

Incident Management (IM) and the Service Desk

- Incident Management (IM) receives notification from EM for known exceptions and new conditions that impact Service Delivery. Qualified and categorized event conditions are transmitted into the IM process by various methods. Known exceptions can be configured to automatically generate an Incident Record, while unknown conditions require human intervention to generate an Incident Record.

- The Service Desk processes incident records and service requests through IM and RqF, respectively.

Request Fulfillment (RqF)

- Request Fulfillment (RqF) is engaged as needed to implement service requests to close events. Once the RqF process has been completed, fulfillment activities will be communicated through EM.

Service Catalog Management (SCM)

- Service Catalog Management (SCM) does not directly interface with EM. However, SCM provides service related information to EM via RqF and ChM processes.

Change Management (ChM)

- Change Management (ChM) may be triggered by the detection of events that require modification to the environment via a Request for Change (RFC). The ChM process communicates to EM the schedule in which the requested change can be implemented.

- Request for Change (RFC): EM will identify qualified event conditions that will require a RFC prior to execution of corrective action.

- Change Schedule: EM utilizes the Change Schedule to prepare to temporarily suspend monitoring and EM activities associated with changes that will impact any service attributes being monitored (e.g., availability, performance, capacity, etc.).

Release and Deployment Management (RDM)

- Release and Deployment Management (RDM) is in constant communication with EM to provide and update scheduled releases to the IT environment in an effort to prevent false alarms/alerts. EM provides notification to the Deployment Manager regarding success, error or failure of the deployment in production.

- Suspend/Resume: RDM notifies EM to suspend monitoring of services or service components that will be interrupted or otherwise impacted for the duration of the

deployment activity; this eliminates false identification of Incidents. RDM also notifies EM to resume monitoring once deployment activities have completed.

Capacity Management (CpM)

- Capacity Management (CpM) provides EM with predefined event conditions leveraged from operational metrics that are utilized for configuring monitoring thresholds. An event notification occurs when pre-defined thresholds have been exceeded.

Availability Management (AvM)

- Availability Management (AvM) provides EM with predefined event conditions leveraged from operational metrics that are utilized for configuring monitoring thresholds. An event notification occurs when pre-defined thresholds have been exceeded.

Service Asset and Configuration Management (SACM)

- Service Asset and Configuration Management (SACM) provides EM with predefined event conditions based on the configuration baseline of a CI within the Configuration Management Database (CMDB). The CI configuration baseline is utilized for configuring monitoring thresholds. EM then monitors the operational configuration of the CI; if the operational configuration changes, an event notification or alert is generated.

- Configuration Data: Configuration data, present in the CMDB, provides target and scope information necessary to engineer service monitoring and establish correlation rules for event notification/alerts.

- Discovery: The CMDB leverages discovery information from EM for audits and reconciliation activities.

Service Level Management (SLM)

- Capacity Management and Availability Management interface with Service Level Management (SLM) to establish predefined thresholds in the form of SLAs. EM can monitor for SLA breaches based on established criteria provided by CpM and AvM.

2.3 High-Level Process Model

As illustrated in Figure 2-2, the EM process contains multiple sub-processes, decision points, and integrations with the IM, PbM, ChM, and RqF processes. The following workflow depicts these processes and sub-processes that collectively enable and underpin EM. See Section 4.0 for complete descriptions of the sub-process activities.

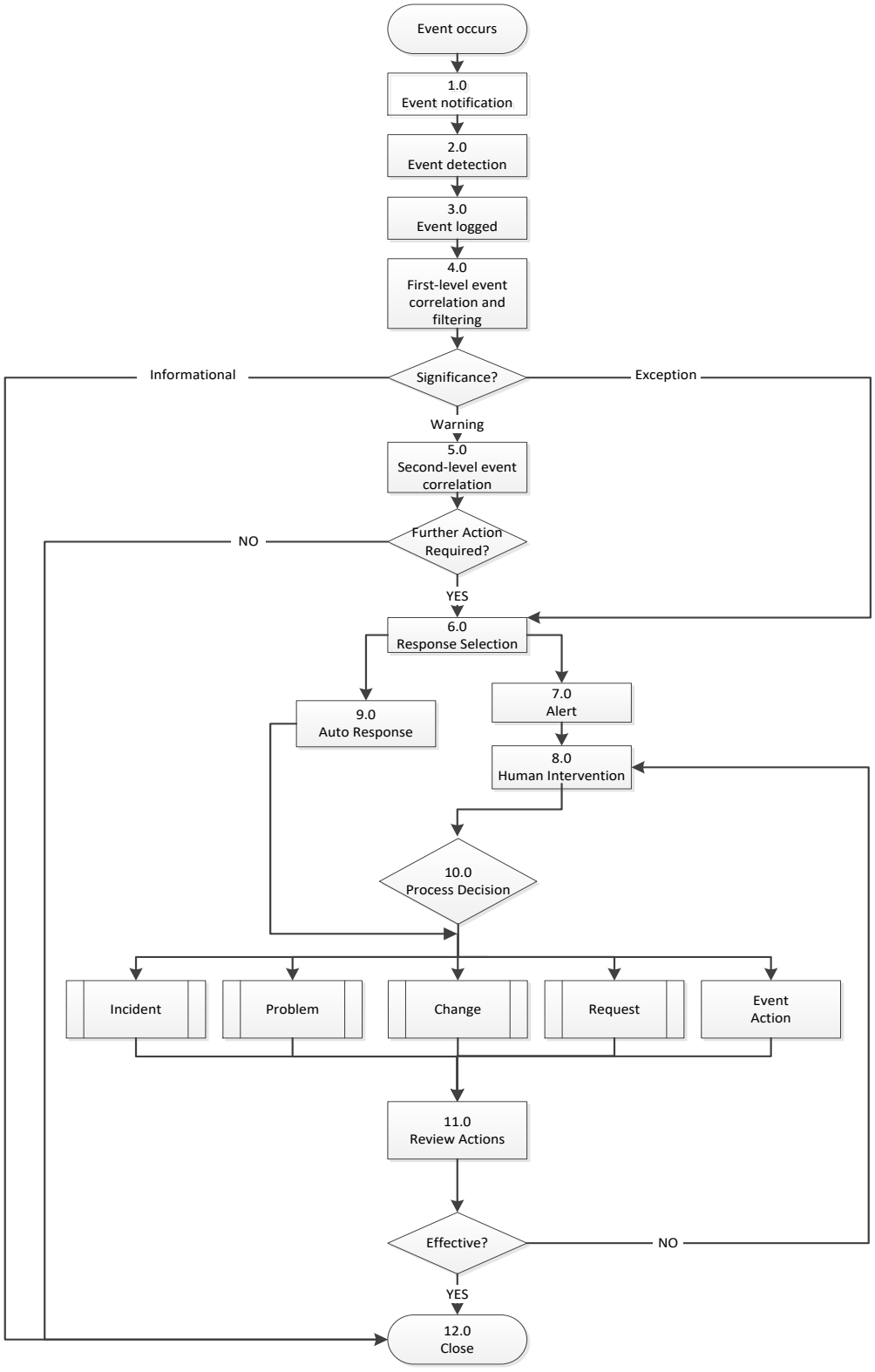


Figure 2-2 High-Level Event Management Workflow

Table 2-1 contains descriptions of each sub-process.

Table 2-1 EM Sub-Process Descriptions

Number	Sub-Process	Description
4.1	Event Notification	The Enterprise Event Management System (EMS) provides notification that an event has occurred. The device or service must generate messages whether through the native device, hardware, operating system, application or an agent/agentless monitoring software.
4.2	Event Detection	Operational monitoring data is scanned to identify events that should be logged and examined. Not all events require further examination.
4.3	Event Logged	An event resulting from an entry into a device or application is recorded into an EM log.
4.4	First-Level Event Correlation and Filtering	The stream of logged events is examined and filtered to identify only those defined events for which a response is warranted. Duplicate events are eliminated. The first level of evaluation or correlation occurs. Significance This is a decision box where the Event is classified as Informational, Warning or Exception and processed accordingly. • **Informational** – For logging purposes only (no action required) • **Warning** – Whenever a threshold is being approached or breached • **Exception** – Event is impacting the mission and needs to be evaluated as a potential Incident, Problem, Change or Request
4.5	Second-Level Event Correlation	This activity correlates multiple events, and throttles processing of repeated events. Warning events are assessed to determine if they should be escalated. Exception events are assessed for the appropriate response. The USMC current monitoring tools are employed as Element Managers. Through leveraging of event integration with the Enterprise EMS event processing, correlation occurs at the local and regional levels with critical alert forwarding to Regional RNOSCs and MITSCs with Manager of Managers (MoM) at MCCOG.
4.6	Response Selection	Based on Event Correlation results, specific activities are initiated. These activities include internal EM processes such as visual alert generation and/or an external activity such as manually opening a Service Desk record.
4.7	Alert	Alert ensures that the responsible support person/team with the skills appropriate to deal with the event is notified. The alert contains the information necessary for that person to determine the appropriate action. USMC handles notifications in the following manner: • Event alerts are visible via event consoles in the USMC operations centers at MCCOG, RNOSC, MITSC, Base, and Tenant Commands. • Event alerts are sent via e-mail to the person/team responsible for supporting the managed element. • Event alerts are not sent as SMS text messages.
4.8	Human Intervention	Event requires a person or team to carry out the corrective action to restore the affected CIs.
4.9	Auto Response	A predefined activity can initiate an auto response. This is a pre-defined set of procedures. Examples of auto responses include: • Rebooting a device • Restarting a service • Changing a parameter on a device • Incident created in Service Desk software Immature tools with little or no integration provides only the visual icon and message changes as auto response for USMC.
4.10	Process Decision (IM, PbM, ChM or RqF, Event Action)	Event is routed as an input to other process(es) (IM, PbM, ChM, RqF or Event Action is taken).

Number	Sub-Process	Description
4.11	Review Actions	It is not possible to formally review every individual event. However, it is important to check that any significant events or exceptions have been handled appropriately, or to track trends or counts of event types, etc. USMC follows the practice of checking significant events or exceptions. Was the Event handled correctly, including the handoffs to other ITSM processes and did the expected outcome occur correctly? If yes, then the process continues on to Close (Step 12.0). If no, then it circles back to Human Intervention (Step 8.0) for evaluation prior to routing to other processes like IM and ChM as an update to existing or creation of new incidents or RFCs.
4.12	Close	Review shows effective handling of the event and it is closed. Events are also closed automatically when a CI returns to a "Normal" state, thereby closing the original alert. If the Event is handed off to another ITSM process, that process creates an appropriate link back to EM and the USMC considers it formally closed.

2.3.1 Process Description

EM is the process through which event records are managed. An event represents any change of state that has significance for the management and the operation of a Configuration Item (CI) or service. Events usually become known through alerts or notifications from either a monitoring tool or the CI itself and require some level of engagement on the part of IT Operations personnel. If the event results in an unplanned interruption of an IT Service or impacts a CI, it would be reported and recorded as an incident.

The majority of work in EM is done by the monitoring tools. However, integration of disparate tools is required along with inputting rules for filtering and correlation to determine significance and escalation of an event. The rules are based on USMC requirements at local, regional and enterprise levels.

As the EM solution matures and false-positives are eliminated, automated responses will be developed and implemented. This reduces the manual intervention burden. Currently automated responses are limited to changing visual icons and messages to a prominent color to draw attention to them.

2.4 Key Concepts

The mission of EM is to effectively and efficiently process events generated by network and system management tools in order to clear these events as quickly as possible. The majority of events are informational status and are logged only. Significant events such as warnings and exceptions require further processing. Event type is determined by rules established in the filtering and correlation steps.

A fault is an event that has a negative impact on the service level of a CI or service. One objective of EM is to recognize, isolate, correct and log faults that occur on the network. An event can represent a fault in the infrastructure, or it can simply represent the fact that the status of a CI or process has changed. Furthermore, a repetitive series of events can represent a fault. Techniques within EM are used to determine whether a fault has actually occurred.

The process of determining which events are identical is referred to as duplicate detection. The process of reporting events after a certain number of occurrences is known as throttling. Furthermore, it uses trend analysis to predict errors so that the network is always available. This can be established by monitoring different indicators for abnormal behavior.

When a fault or event occurs, a network component will often send a notification to the network operator using a proprietary or open protocol such as Simple Network Management Protocol (SNMP). The notification initiates automatic or manual activities. Alternatively, network components will write a message to its console. The console server will catch and log the fault or event for further processing. For example, EM initiates the gathering of more data to identify the nature and severity of the alert or to bring backup equipment on-line.

The following describes key concepts of EM:

2.4.1 Monitoring vs. EM

These two areas are closely related, but there are key differences between monitoring and EM.

EM is focused on generating and detecting meaningful notifications about the status of the infrastructure and services. EM works with occurrences that are specifically generated to be monitored. Monitoring tracks these occurrences, but it will actively seek out conditions that do not generate events

Monitoring is required to detect and track events but it is broader than EM. For example, monitoring tools will check the status of a device to ensure that it is operating within acceptable limits, even if the device is not generating events.

The Views displayed at the various locations and levels of operation will constantly display the current state of the Network; this is monitoring. However, when this monitoring system detects a fault, the View will change to display (to the operator(s)) the Event in progress. The Event Management System (EMS) is configured to provide the appropriate response which ensures the Event is properly handled.

2.4.2 Event Filtering

Event filtering is a process of filtering Events which are merely informational and can be ignored, and communicating any Warning or Exception Events.

Event filtering is needed to restrict the data entering the EM system. The amount of data produced by managed objects in a complex IT environment can reach high amounts of discrete events being sent to a single management instance.

Redundant information produced by various monitoring agents inside a single managed object occurs. For example, the syslog subsystem on a UNIX server provides critical information, while the SNMP agent running on that server provides trap information about the same event.

Network and bandwidth considerations require Event-related traffic to occupy a reasonable amount of bandwidth. This applies both to the traffic produced from status polling of devices and the traffic generated by devices sending asynchronous unsolicited events over the network.

After the set of event sources is specified, the EM Manager/Analyst needs to address all events of each event source and analyze them for their value to the EM process. The analysis goes beyond determining which events to filter and includes whether to log the events to the device log file or the EM system that passes the event to Event Significance sub-process.

Note: For auditing purposes, retention of event logs is directed by a Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG).

2.4.3 Event Significance

Assigning the appropriate event significance is critical for effective event processing. The toolset currently in use by EM has three event types to provide more granularity for the EM Analyst. The event types are informational, warning, or exception.

Examples of the three types of events:

Events that are informational:

- Notification that a scheduled workload has completed
- A user has logged in to use an application
- An e-mail has reached its intended recipient

Events that signify a warning:

- A user attempts to log on to an application with an incorrect password
- A server's hard drive free space is below optimum percentage
- A PC scan reveals the installation of unauthorized software
- Completion of a backup is 10% longer than normal

Events that signify an exception:

- A server's memory utilization reaches within 5% of its highest acceptable performance level
- A user makes multiple attempts to log on to an application when access is restricted
- A network device stops working

Best practice places events into six categories, shown in Table 2-2. An event can be in any of these categories and still be an unusual event requiring further investigation. Each message relies on the sending and receiving of a message that is referred to as an Event Notification. There is not a definitive rule regarding disposition of events. The rules governing thousands of messages becoming intelligent data is handled by Event Filtering and Event Correlation based on the governing rules set into the monitoring tools.

Table 2-2 Event Significance

EVENT SIGNIFICANCE		
TYPE	**CATEGORY**	**DESCRIPTION/LIST**
INFORMATIONAL	**NORMAL**	• Does not require any action • Used to check on the status of a device or service • Confirms the successful completion of an activity • Typically stored in the system or service log files and saved • Can be used to generate statistics • Not an exception
WARNING	**WARNING**	• Event is generated when a service or device approaches a threshold • Notification that appropriate action needs to be taken to prevent an exception • Situation needs to be checked • Not typically raised for a service or device failure
	UNKNOWN	
EXCEPTION	**MINOR**	• Total service or device failure, impaired functionality or degraded performance of service or device • Appropriate action must be taken to resolve the failure • Business is being impacted due to a breach in the Operational Level Agreement (OLA) and/or Service-Level Agreement (SLA)
	MAJOR	
	CRITICAL	

2.4.4 Event Escalation

An event, signifying a fault, is useless in managing IT resources if no action is taken to resolve it. A way to ensure that an event is handled properly is for an event processor to escalate its severity if it has not been acknowledged or closed within an acceptable timeframe. Timers can be set in some event processors to automatically increase the severity of an event if it remains in an unacknowledged state.

The higher severity event is generally highlighted in some fashion to draw greater attention to it on the operator console on which it is displayed. The operators viewing the events may inform management that the event has not been handled, or this notification may be automated. In addition to serving as a means of ensuring that events are not missed, escalation is useful in situations where the IT department must meet service-level objectives.

EM handles escalation differently than IM. Event escalation gives the most immediate notification to IT Operations through greater visibility and is not limited to IM software.

Severity in EM is similar to priority in IM. However, IM defines the sequence that an incident is worked based on its priority, whereas EM uses the alert system which predefines the escalation based on the severity of an event. How quickly an event escalates depends upon its severity as defined in the Event Correlation rules.

USMC Operations defines impact as the number of users affected and correlates to logical organizational structure or a physical location. Criticality is somewhat more objective and can depend on a number of factors. When determining criticality, the following factors and criteria are considered:

- Critical nature of the service, system or application

- VIP status of the impacted user
- Point in time
    - Is a critical deployment or tactical operation underway that is being impacted by the event?
    - Is a time sensitive business process or operation underway, for example payroll processing
- Impact to service
    - Total loss of all services; pre-defined failure of any critical or safety systems
    - Loss of single service
    - Degraded service
    - Intermittent service

2.4.5 Visualization

Tools are utilized to provide a detailed status of the network at all times. The Network Common Operational Picture (NetCOP) is a subset of the enterprise ITSM toolset, and is used to display integrated and customized views of the status, performance, events, threats and vulnerabilities for certain aspects of the MCEN. The views range from high-level global views down to more granular views of each region, base, LAN, command, and end device.

The primary purpose of NetCOP is to present NetOps personnel with Situational Awareness (SA) of MCEN services in near real-time in order to interpret events, incidents, and problems; understand their operational impact; and decisively and rapidly take action to restore services and protect information on the MCEN.

To assemble NetOps SA information, NetCOP correlates data from multiple sources as part of the overall ITSM toolset. EM tools monitor and poll service components and configuration items such as network elements, storage devices, applications, and critical network services. NetCOP correlation engines also map multiple event notifications into smaller, collective events to aid human comprehension. Visualization tools provide different types of views (overlays) of services, devices, and software at varying levels of granularity.

2.5 Reporting

2.5.1 Event Notifications

Event notifications are key components of communicating event type, criticality, and required activities and responses. Event notifications are sent to the individuals or groups responsible for execution of response activities. Event notifications may also be displayed on Event Consoles to inform all stakeholders of current event warnings and exceptions. Incident records and change requests which result from event notifications inform stakeholders of impending actions that may affect IT resources and services.

2.5.2 Process Interfaces

As depicted in Section 2.2 above, EM has relationships and dependencies with other process areas. The strength of these relationships depends on communication of events and activities which affect other process areas. IM is directly affected when the EM process provides event information leading to the creation of incident records. EM reports out information that is used by other process areas as described below:

- Service Level Management (SLM) – ensure potential impact on SLAs is detected early and that any failures are rectified as soon as possible
- Information Security Management (ISM) - allow potentially significant business events to be detected and acted upon
- Capacity and Availability Management (CpM/AvM) - defines what events are significant, what appropriate thresholds should be and how to respond to them
- Change Management (ChM) – identify conditions that may require a response or action
- Access Management (AM) – detect unauthorized access attempts and security breaches
- Knowledge Management (KM) – source of information such as patterns of performance and business activity that may be used as input to future design and strategy decisions

2.5.3 Commander's Critical Information Requirements

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

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

2.5.4 Friendly Forces Information Requirements (FFIR)

Friendly Forces Information Requirements (FFIR) is information the commander needs about friendly forces in order to develop plans and make effective decisions. Depending upon the circumstances, information on unit location, composition, readiness, personnel status and logistics status could become a friendly information requirement.

2.6 Quality Control

2.6.1 Metrics, Measurements and Continual Process Improvement

Continual process improvement depends on accurate and timely process measurements and relies upon obtaining, analyzing, and using information that is practical and meaningful to the process

at hand. Measurements of process efficiency and effectiveness enable the USMC to track performance and improve overall end user satisfaction. Process metrics are used as measures of how well Service Level Targets are being met.

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

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

2.6.2 Critical Success Factors with Key Performance Indicators

A CSF is a metric that represents key operational performance requirements and indicates whether a process or operation is performing successfully from a customer or business perspective.

A KPI is used to measure the achievement of each CSF. Many metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the process, IT service, or activity. A KPI should lead to action and be a driver for improvement.

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

Table 2-3 lists the metrics that will be monitored, measured, and analyzed:

Table 2-3 Critical Success Factors with Key Performance Indicators

CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Benefits
1	Actionable Events are detected and recorded	1	Percent of incidents that originate from EM Calculation: Number of actionable alerts that have an incident ID assigned divided by total incidents over a period of time	Events are being detected and assigned proper severity. Ensure proper tool utilization and value.
		2	Percent of Actionable Events (Critical or Major) that become incidents Calculation: Number of Event-generated Incidents divided by the total number of Incidents over a period of time	
2	Minimize event impact on Service	3	Message age Calculation: Time from event occurrence to correlated normal event occurrence	Maximizes rapid restoration of service and minimizes customer impact
3	The EM process is not burdened by duplicate and informational events	4	Reduction in number of duplicated events Calculation: Volume of duplicate events trended over time (reduction, by category over time) Trend report showing number of informational events at each level	Promotes effectiveness of EMS and reduces monitoring traffic across the network

3.0 Roles and Responsibilities

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

Management (i.e., responsibility) of the EM process is shared; an EM Enterprise Process Manager exists at the MCCOG, whereas at each MITSC an EM Regional Process Manager exists. For certain processes, especially those within Service Design and Service Transition, managers also exist within MCSC and Programs of Record. RNOSC is responsible for Situational Awareness (SA) to the MARFOR G6 in addition to responsibilities outlined in the SIPRNET Concept of Employment (COE). This process guide defines all EM mandatory roles.

3.1 Roles

The following drawing (Figure 3-1) depicts EM process roles for the USMC, followed by a description of these roles.

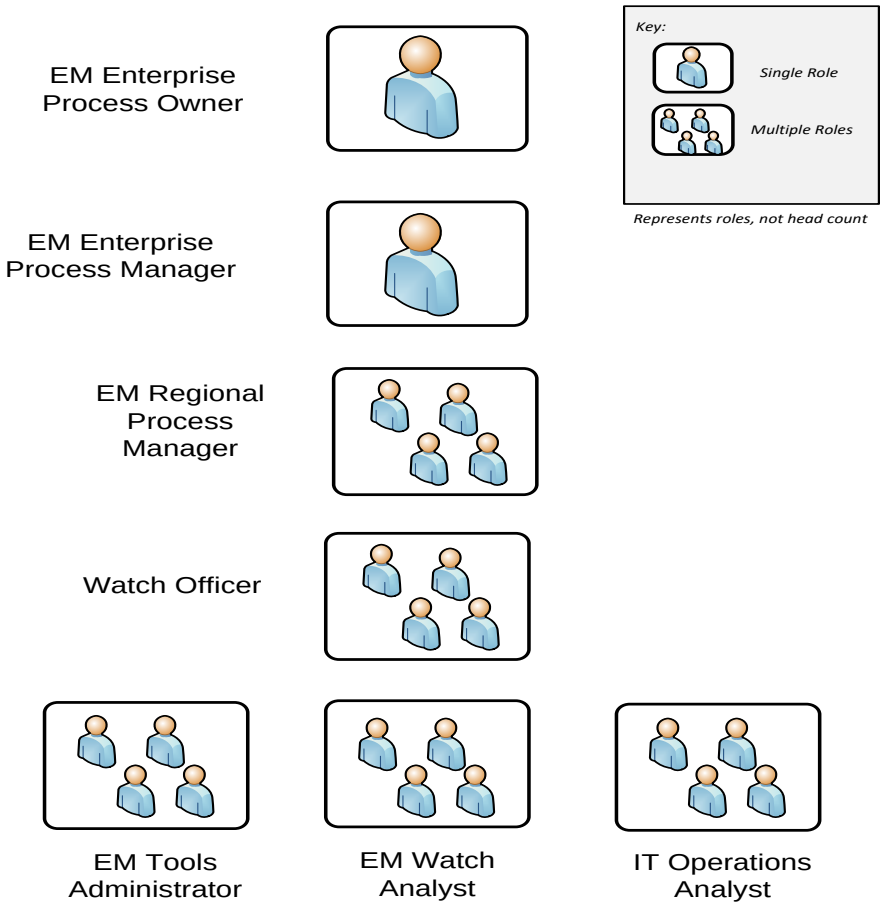


Figure 3-1 EM Roles

Table 3-1 describes the roles depicted in Figure 3-1 with their responsibilities.

Table 3-1 EM Roles and Responsibilities Defined

Description	Overall Responsibility
Role #1 EM Enterprise Process Owner	
The EM 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. The Process Owner will oversee the process, ensuring that the process is followed by the organization. When the process is not being followed or is not working well, the Process Owner is responsible for identifying and ensuring required actions are taken to correct the situation. This includes enabling the roles within EM to do their job and to identify areas of improvement. In addition, the Process Owner is responsible for the approval of all proposed changes to the EM process, and development of process improvement plans. The Process Owner may delegate specific responsibilities to another individual, but will always remain ultimately accountable for the results of the EM process.	• Defines process policies, standards and conceptual models when EM framework is implemented • Specifies process purpose, scope, goals and capabilities when EM framework is implemented • Publishes and communicates the EM process as appropriate • Decision maker on any proposed enhancements to the process or the EM Tools • Interacts with all of the EM Managers and the enterprise EM team • Publishes and communicates the EM metrics and results • Develops continual improvement process opportunities

Role #2 EM Enterprise Process Manager	
The Enterprise EM Process Manager is a pivotal role that performs day-to-day overall management of the process. The Enterprise Process Manager's responsibilities include ensuring all process activities are being performed and are staffed adequately, working with the customer to define requirements, and receiving feedback regarding process performance satisfaction. It is important to have a good working relationship with the IT Operations Technical and Applications staff due to monitoring and analytical assessment activities in support of each event/alert.	• Supports assessment of new EM technology • Drives the efficiency and effectiveness of the EM process • Ensures compliance with EM standards and policies • Collaborates with other processes and Regional EM Process Managers • Periodically reviews significant events and exceptions • Analyzes event records to detect positive trends • Develops proposals for correcting EM process limitations • Regularly produces accurate management reports that contain information valuable to the mission • Makes recommendations for improvement
Role #3 Regional EM Process Manager	
Regional EM Process Managers perform day-to-day overall management of the process at regional locations. The Regional EM Process Managers ensure that all process activities are being performed and that they are staffed adequately. They work with the customer to define requirements and receive feedback regarding process performance satisfaction. It is important to have a good working relationship with the IT Operations Technical and Applications staff due to monitoring and analytical assessment activities in support of each event/alert. It is recommended to have one Regional Event Process Manager at the MCCOG and all MITSCs. MITSC EM Process Managers will coordinate EM Cyber Ops through the MCCOG EM Managers to promote a unified approach to EM Cyber Ops.	• Ensures timely handling of events to maintain targeted service-levels • Drives the efficiency and effectiveness of the EM process • Ensures compliance with EM standards and policies • Collaborates with other processes and other EM Managers • Provides input to management regarding staff skill levels as they relate to EM • Provides input into important decisions regarding EM supporting technology requirements • Speaks with and for customers, giving input to the process • Periodically reviews significant events and exceptions • Analyzes event records to detect positive trends • Regularly produces accurate management reports that contain information valuable to the mission • Makes recommendations for improvement
Role #4 Watch Officer	
The Watch Officer will monitor the EM console and ensure that a Watch Analyst or IT Operation Analyst is readily available to assist with the processing of alerts/events accordingly. It is recommended that an EM Watch Officer be assigned at the MCCOG, each RNOSC, and all MITSCs.	• Ensures the Event Management System (EMS) is manned during all periods of operation • Provides management and oversight to the EM Analysts on duty • Oversees the monitoring of Event Consoles • Provides mentoring to the EM Watch Analyst to ensure training and standards are met • Evaluates reports to determine health of the systems in the AOR • Ensures EM is following USMC policies • Provides guidance and direction on possible corrective actions • Ensures resources follow quality assurance checks • Monitors Event Consoles at the MCCOG, RNOSCs,

	MITSCs (respectively) • Monitors progress of events/alerts • Ensures that IM, ChM, PbM records are opened based on actionable event conditions as required to support Cyber Operations
Role #5 EM Tools Administrator	
The EM Tools will be administered by the NETCOP group within the MCCOG. Ownership of the tools will be from the IT Service Management (ITSM) Team within MCSC. Authorization for changes to these tools will be coordinated through Change Management, but the ultimate approval must come from the owner of the tools. Execution of changes and maintenance of the tools will be conducted by the Tools Administrator.	• Provides administrative support for the management of the process • Administers process management tools • Performs day-to-day process administration • Facilitates resource commitment and allocation • Creates, analyzes and distributes process reports • Ensures completeness and integrity of information collected to conduct daily operations • Establishes measurements and targets to improve process effectiveness and efficiency
Role #6 EM Watch Analyst	
Watch Analysts will monitor the EM console and address events/alerts within their respective AOR.	• Provides quality assurance checks on the workflows • Monitors Event Consoles • Addresses actionable events within their AOR • Assigns Events to entity responsible for resolution (this may be automated) • Opens IM, ChM, PbM records based on actionable event conditions as required to support Cyber Operations • Initiates RFCs based on an actionable event conditions or regarding the EM process
Role #7 IT Operations Analyst	
Based on the AOR (i.e. network section), the Technical Resources which support specific Configuration Items (CIs) requiring monitoring will be engaged to review and conduct initial analysis and review of alerts/events and provide proper recommendations for courses of action.	• Works with EM Watch Analysts to resolve assigned IM records based on actionable event conditions • Works with the EM Tools Administrator in configuring the EM system for effective EM, which includes setting thresholds and correlation rules • Makes EM Tool configuration recommendations and submits RFCs to support the configuration changes through the ChM process • Brings unique knowledge to the EM team as the technical specialist (SME) • Views technical and role-based console messages

3.2 **Responsibilities**

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

The Responsible, Accountable, Supporting, Consulted, Informed (RASCI) model is a method for assigning the type or degree of responsibility for roles (or individuals) which have specific tasks. Table 3-2 displays the RASCI model for EM.

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

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

Supporting – Assists in the execution of process or activity.

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

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

Table 3-2 Table 3-2 Responsibilities for Enterprise EMdescribes responsibilities for high-level process activities by organization.

Table 3-2 Responsibilities for Enterprise EM

EM Process Activities	Process Owner	Enterprise and Regional Process Managers	Watch Officer	EM Tools Administrator	EM Watch Analyst	IT Operations Analyst
Event Notification	A	C	S	R	I	S
Event Detection	A	C	C	R	I	S
Event Logged	A	C	C	R	I	S
First-Level Event Correlation and Filtering	A	C	C	R	I	S
Second-Level Event Correlation	A	C	C	R	I	S
Response Selection	A	C	C	R	I	S
Alert	A	C	C	R	I	S
Human Intervention	A	C	R	S	S	S
Auto Response	A	C	C	R	I	S
Incident/ Problem/Change/Request/Event Action	A	C	R	S	S	C
Review Actions	A	R	S	I	S	S
Close	A	C	I	R	I	S

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

Note: Any role which 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 role is designated as Informed only if that role is not designated as having any of the other four responsibilities.

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

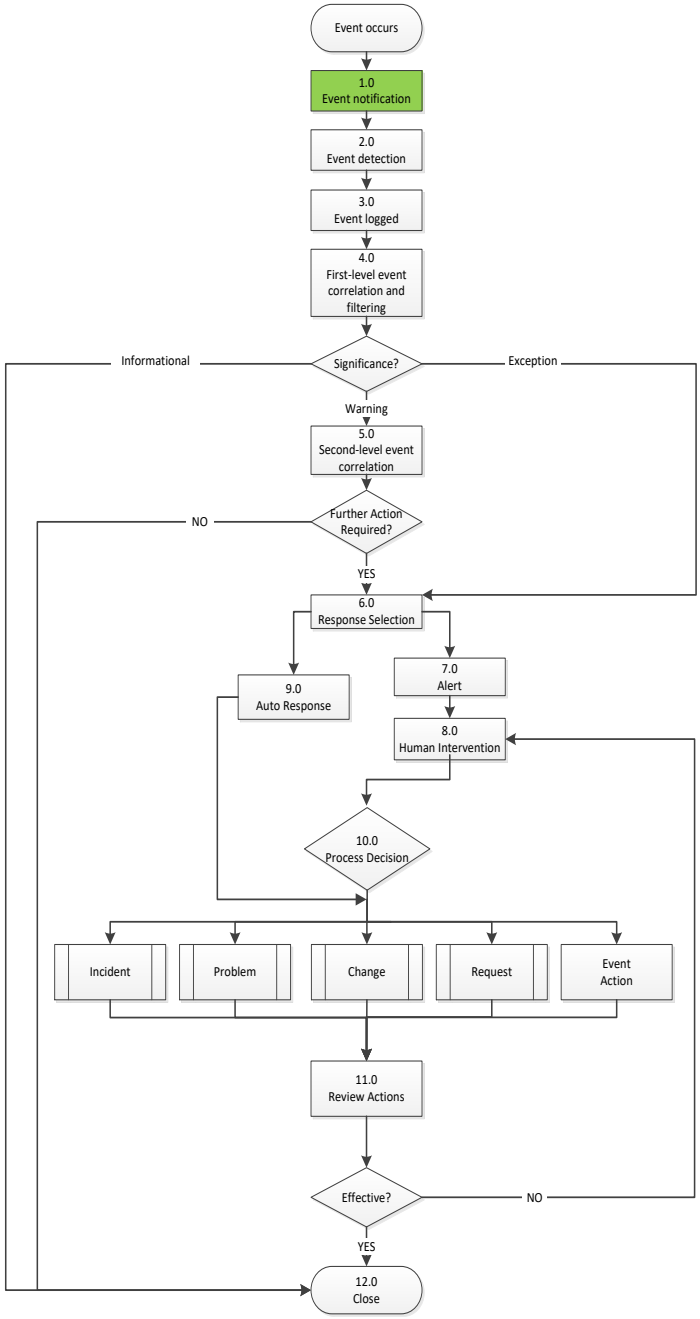
4.0 SUB-PROCESSES

The Enterprise EM process consists of multiple sub-processes; not every activity within each sub-process is utilized for every type of event. For example, informational events do not require Event Correlation or Response Selection. Warning events which are unique to a particular server do not utilize every phase or type of remediation associated with Auto Response and Alert. Therefore, to understand EM in its entirety, it is necessary to look at the sub-processes.

The sub-process diagrams in this section are developed using the following concepts and standards:

- The lifecycle diagrams will have the sub-process highlighted to show its location in the lifecycle process flow.
- Each sub-process diagram will begin with its predecessor sub-process, illustrate the activities within the sub-process and terminate with the successor sub-process.
- Predecessor and successor sub-processes will be represented by a start/end object (oval shape).
- Sub-processes will be represented by a process object (rectangle shape).
- External processes will be represented by a process object (rectangle shape with vertical lines on each end).
- Decisions will be represented by a decision object (diamond shape).

4.1 Event Notification



The Event Notification sub-process defines how event information and the IT components that generated them are captured.

The Event Monitoring System (EMS) refers to the tools that provide notification that an event has occurred.

This first step in the EM process involves various IT Operations Analysts working with the EM Tools Administrator to ensure events are captured by the EMS. The status of each CI monitored through EM will be actively or passively communicated to the EMS. The CI's status is then displayed through the EMS monitoring displays.

Monitored CIs communicate information about themselves in one of two ways:

- The EMS tools interrogate or poll the CI on a regular interval collecting specified data.
- Monitored CIs are configured to generate an alert when specified criteria are met.

Event notifications can be proprietary, in which case only the manufacturer's management tools can be used to detect events. Most CIs, however, generate Event Notifications using an open standard such as SNMP (Simple Network Management Protocol).

Figure 4-1 illustrates the Event Notification sub-process.

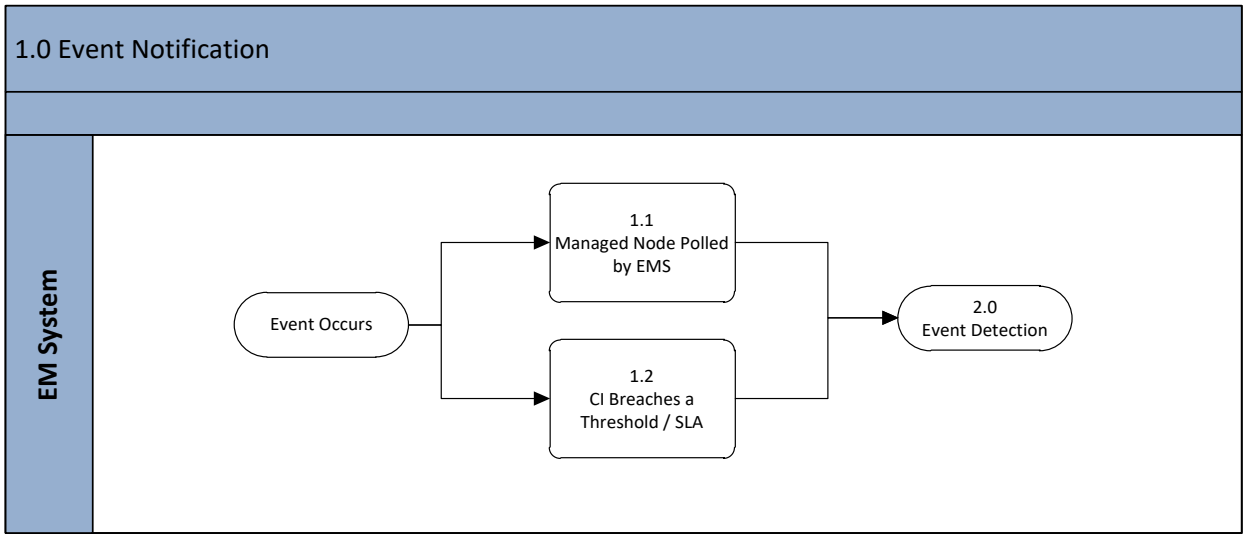


Figure 4-1 Event Notification Sub-Process

The Event Notification sub-process provides for the scheduled polling of monitored CIs. Additionally, monitored CIs are configured to generate an alert outside of the normal polling cycle when specified conditions are met.

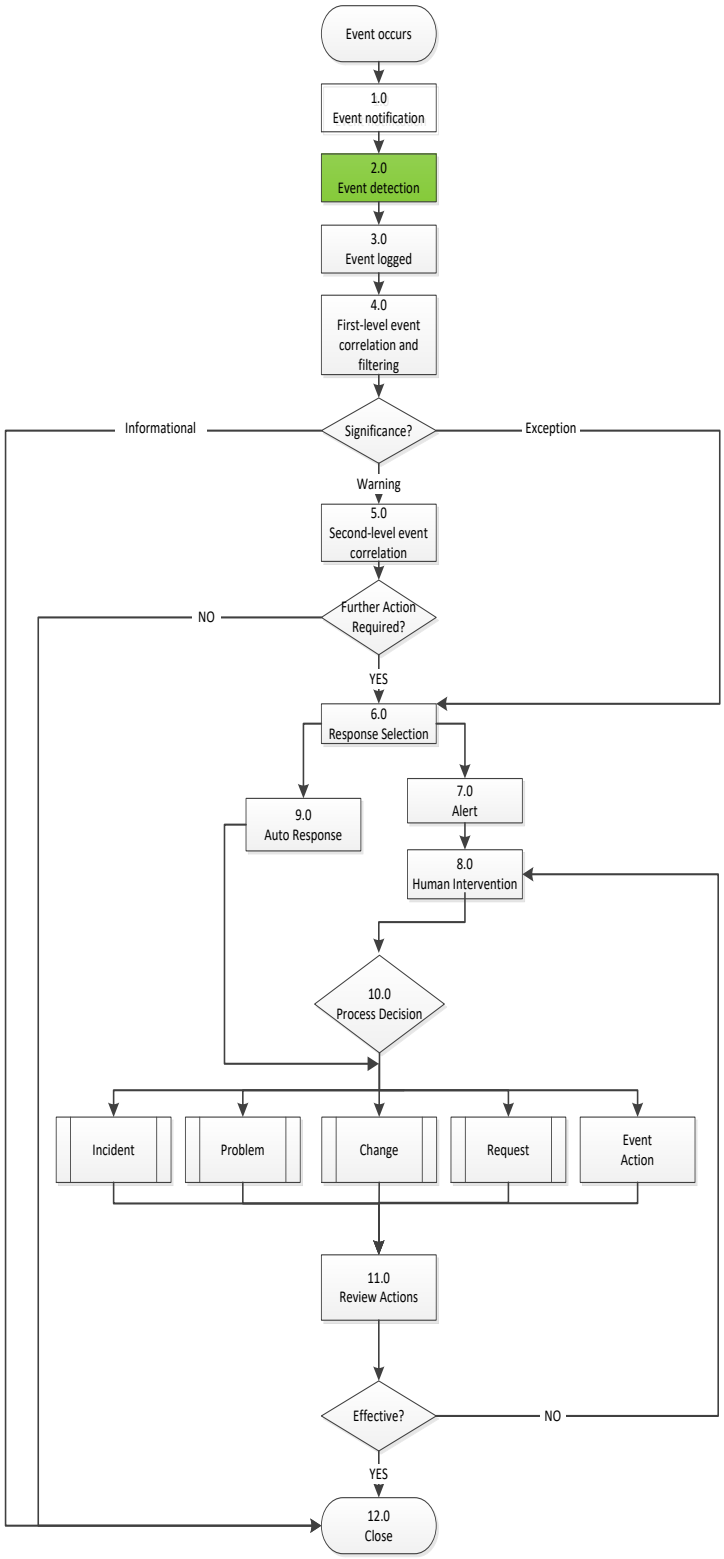
While events occur continuously, not all meet specified detection criteria. Therefore, it is essential the IT Operation team identifies what type of events are required to be detected.

Table 4-1 describes each activity as illustrated in Figure 4-1.

Table 4-1 Event Notification Sub-Process Descriptions

1.0 Event Notification		
Number	**Process Activity**	**Description**
1.1	Managed Node polled by EMS	A device is interrogated by the EMS, which collects specified data. This is referred to as polling.
1.2	CI Breaches a threshold / SLA	The CI generates an alert when certain conditions are met. This ability must be designed and built into the CI monitoring.

4.2 Event Detection



Event Detection takes place when an event is generated which meets specified criteria. EMS scans operational monitoring data to identify a significant event for logging and examination.

When an Event Notification has been generated, it will be detected by an agent running on the same system, or transmitted directly to a management tool specifically designed to read and interpret the meaning of the event.

Not all events should be analyzed by the tools. The IT Operations Analysts work with the EM Tools Administrator to ensure EMS is capturing what must be analyzed.

Figure 4-2 illustrates the Event Detection sub-process.

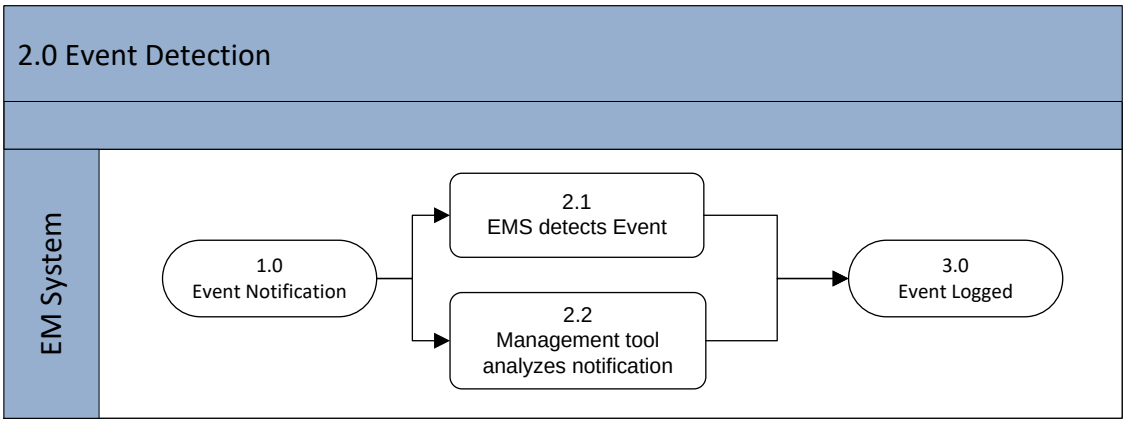


Figure 4-2 Event Detection Sub-Process

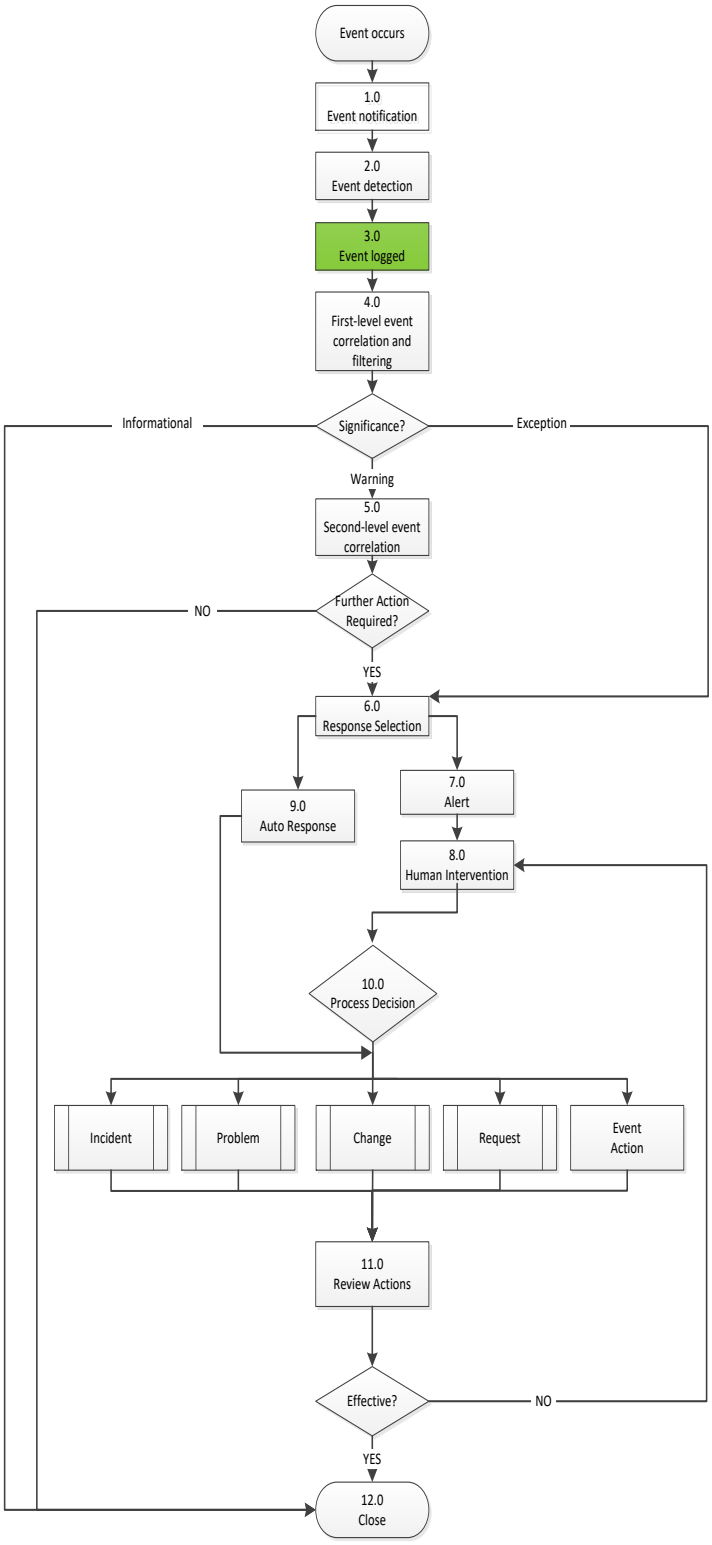
Once an Event notification has been generated, it will be detected by an agent running on the same system, or transmitted directly to a management tool specifically designed to interpret the meaning of the event.

Table 4-2 describes each activity as illustrated in Figure 4-2.

Table 4-2 Event Detection Sub-Process Descriptions

2.0 Event Detection		
Number	**Process Activity**	**Description**
2.1	EMS detects Event	The EMS system detects an anomaly in the environment.
2.2	Management tool analyzes notification	The EMS tool analyzes each event using a prescribed configuration specified for the monitored CI.

4.3 Event Logged



Events are logged as Informational, Warning, or Exception. The event can be logged as an Event Record in the EMS or simply kept in the CIs log file. It is available if needed for trending data, security research, problem research or reports.

To prevent logs from becoming too big, procedures for checking, archiving and retrieving log entries are established and followed. Requirements for each system or team define standards about how long events are kept in the logs before being archived and deleted.

The Event Logged sub-process is illustrated in Figure 4-3.

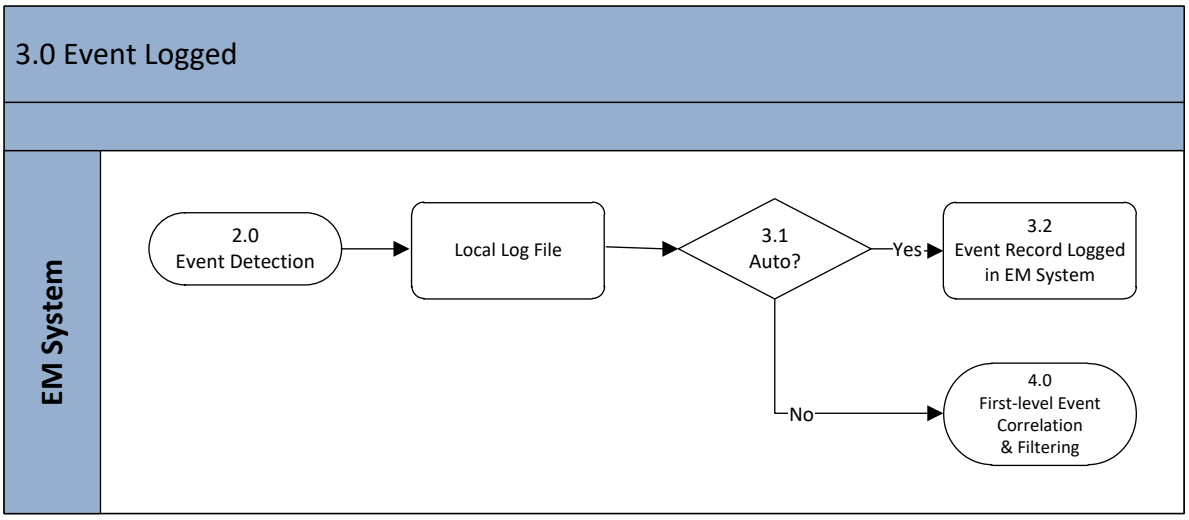


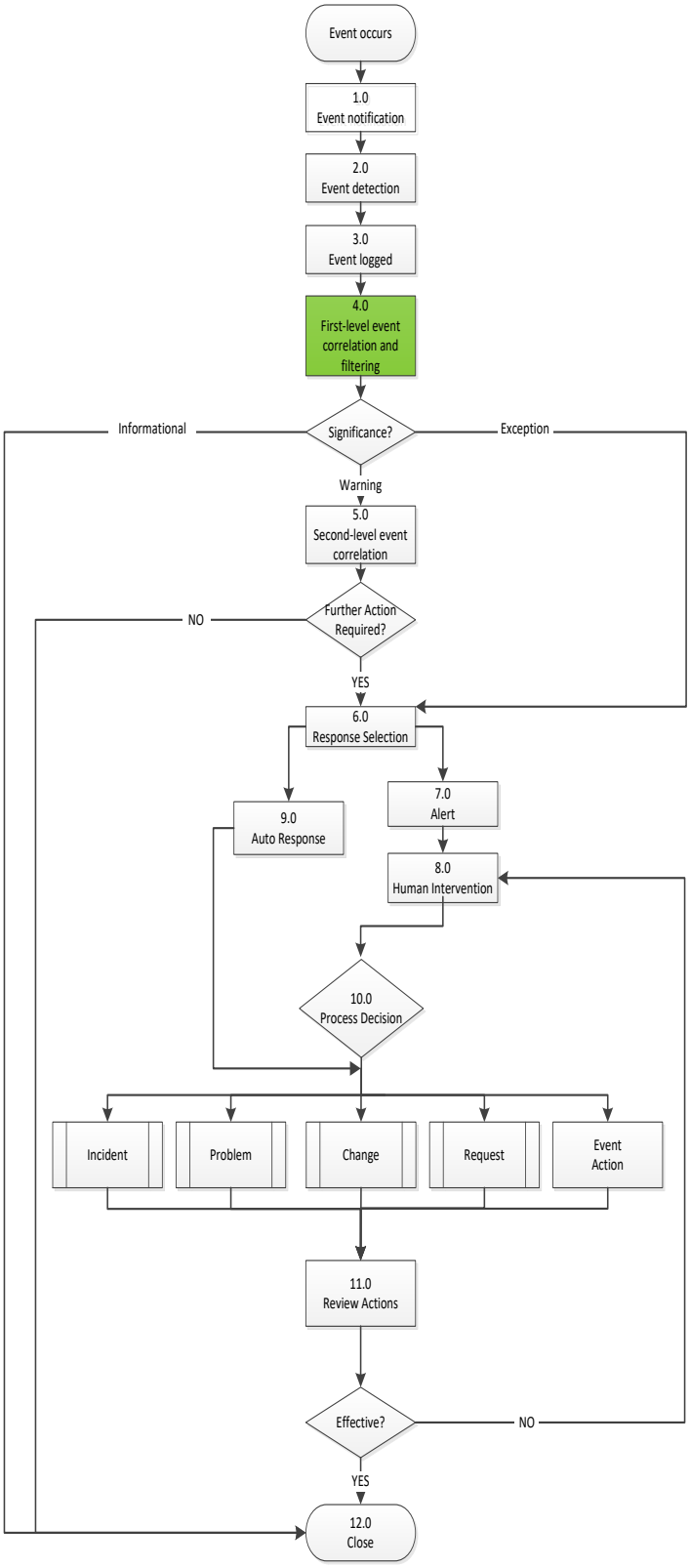
Figure 4-3 Event Logged Sub-Process

Table ***4-3*** describes each activity as illustrated in Figure 4-3.

Table 4-3 Event Logged Sub-Process Descriptions

3.0 Event Logged		
Number	**Process Activity**	**Description**
3.1	Auto Logging	Certain Event Logging can be configured to be automatically recorded in the CI's local logging system. IT Operations Analysts managing the affected CI are required to routinely check these log files. Events which are informational significance are only logged (with no further action required) until an incident occurs, upon which technical staff utilizes these logs to investigate the root cause of the Incident.
3.2	Event Record Logged into EM System	The EMS tool logs specified events into its own event log database.

4.4 First-Level Event Correlation & Filtering



First-Level Event Correlation and Filtering occurs after events are locally logged in order to separate events by significance. Significant events are acted on based upon established specifications and further evaluated through advanced or second-level correlation. Informational events are immediately closed. All events are maintained for possible future reference, regardless of significance.

Without filtering it is possible that 'information only' alerts can obscure more significant alerts that require immediate attention. In addition, it is possible for serious failures to cause 'alert storms' due to very high volumes of repeat alerts, which again must be filtered so that the most meaningful messages are not obscured.

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, that event is forwarded for action.

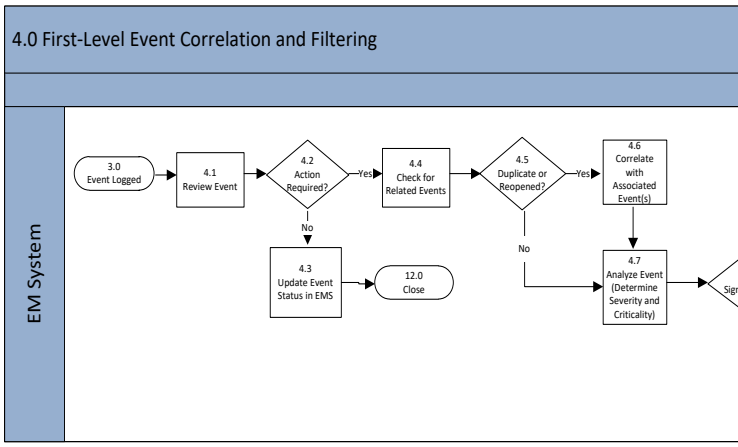


Figure 4-4 illustrates the Event First-level Correlation and Filtering sub-process.

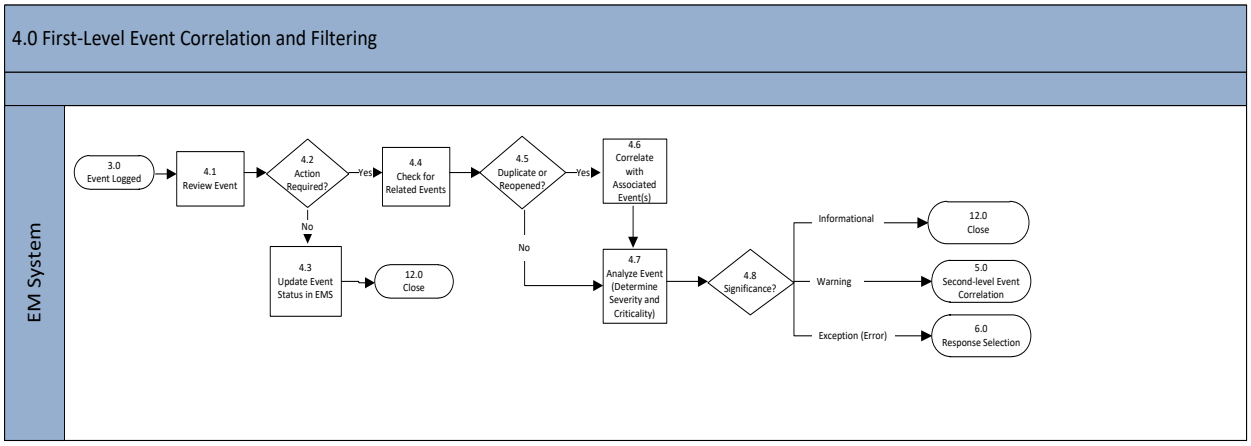


Figure 4-4 First- Level Event Correlation and Filtering Sub-Process

The EM System automates the Correlation and Filtering of events as shown in

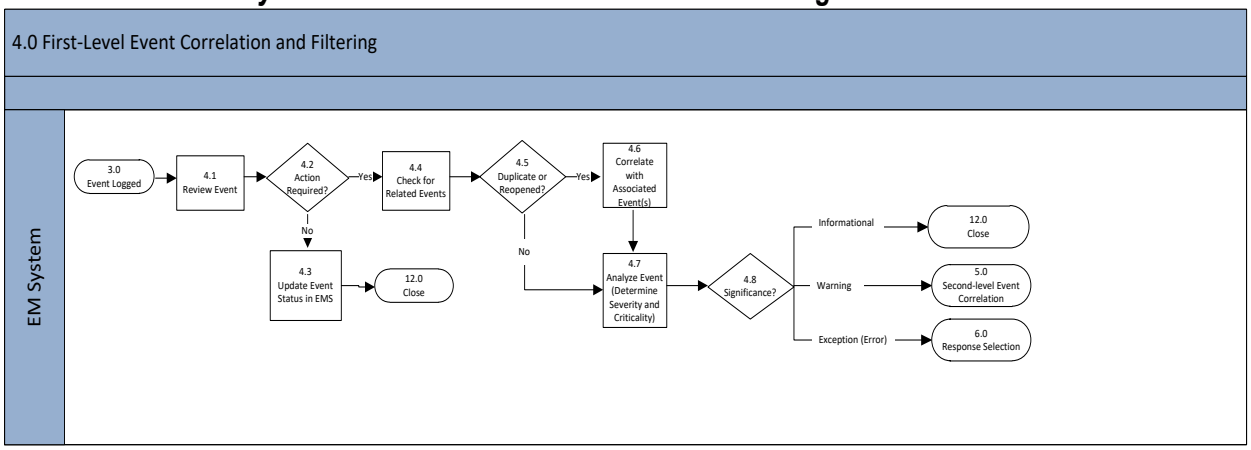


Figure 4-4 through the installed and configured tools. The EM Tools Administrator ensures that the EMS supports the specified functions necessary for correlation and filtering. The Process Manager, Watch Officers, EM Watch Analysts and IT Operations Analyst contribute to configurations, adjustments and requests for changes to the tools. However, event filtering is done by a configured EMS.

Table 4-4 describes each activity as illustrated in

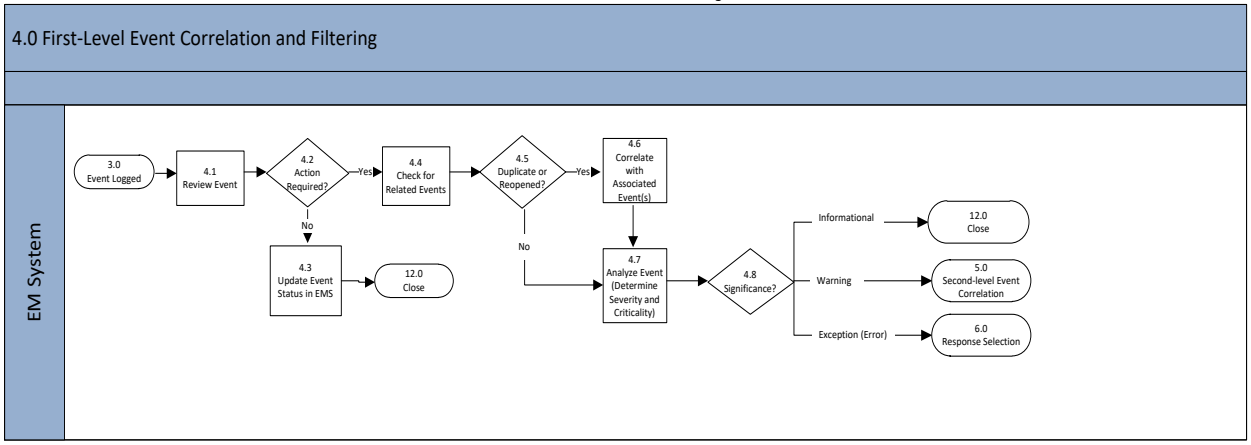


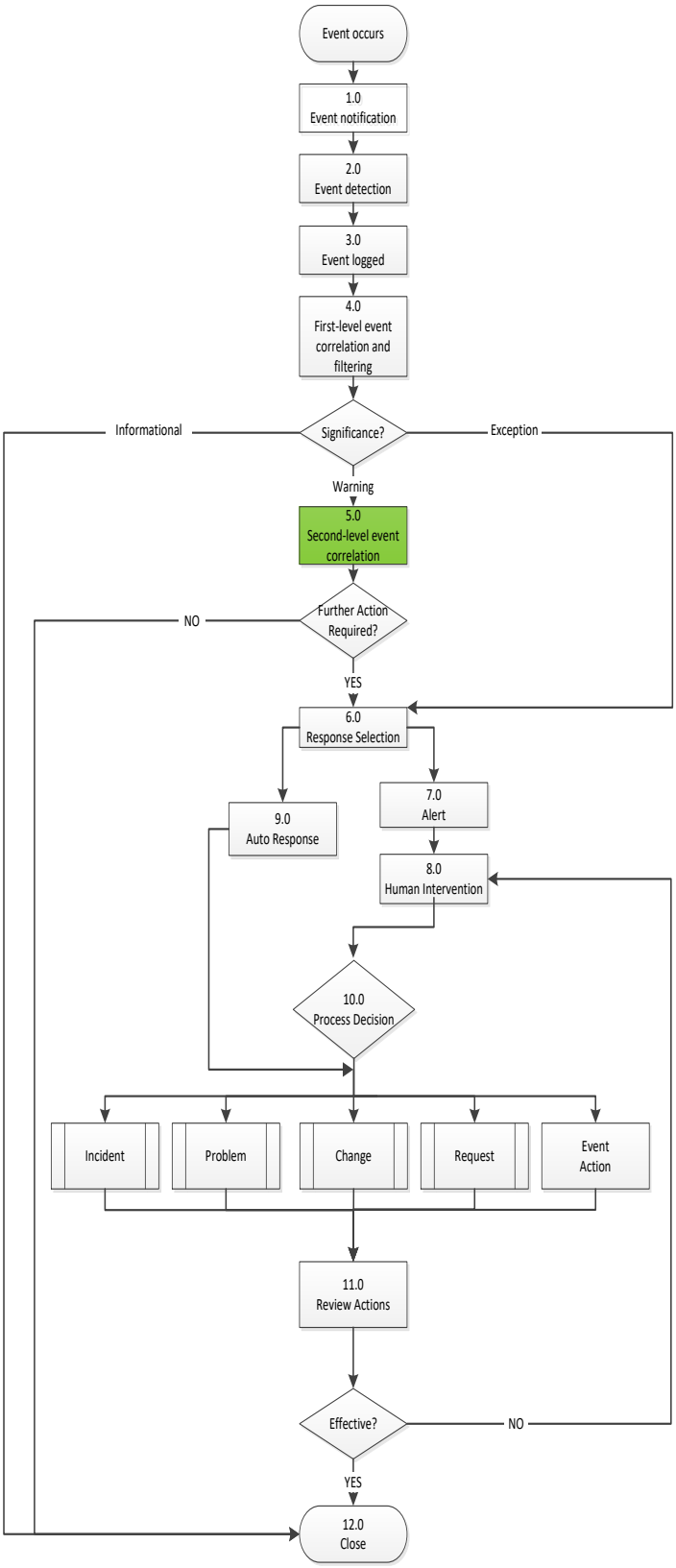
Figure 4-4.

Table 4-4 First-Level Event Correlation and Filtering Sub-Process Descriptions

4.0 First-Level Event Correlation and Filtering		
Number	**Process Activity**	**Description**
4.1	Review Event	The EMS is configured to automatically respond toTable 4-4 IT operational events that arise from system and service monitoring. The event is reviewed by the EMS by using specified criteria to determine if it is informational or an exception.
4.2	Action Required?	If Yes, the event has met the established analysis criteria and is passed along to Check for Related Events (4.4). If No, Event is moved to Update Event Status in EMS (4.3).
4.3	Update Event Status in EMS	The event information is retained within the EMS log for future reference, or simply logged to the CIs log file. Then passed to Close (Step 12.0)
4.4	Check for related events	The Event is checked to see if it is part of a larger event (Multiple CI's) or perhaps caused by another CI's event.
4.5	Duplicate or Repeated	Check event to determine if a previous instance has already been logged. If Yes, event is moved to Correlate with associated Event(s) (4.6). If No, Event is moved to Analyze Event (4.7).
4.6	Correlate with associated Event(s).	Matches the new event with those already acted upon or related.
4.7	Analyze Event (Determine Criticality and Severity)	The Event Analyst responds to IT operational events that arise from systems and services monitoring The Event is analyzed in order to determine its significance. The Criticality and Severity of the event is determined and logged. Significance of the event is based on the specified criteria configured in the EMS. • Informational events are logged with no further action. • Warning events are passed to Second-level Event Correlation. • Exceptions, also known as critical events, are passed on to Response Selection.
4.8	Significance?	The level of significance determines the routing of the event.

4.0 First-Level Event Correlation and Filtering		
Number	**Process Activity**	**Description**
		If Informational, routed to Close (Step 12.0). If Warning, routed to Second-level Event Correlation (Step 5.0). If Exception, routed to Response Selection (Step 6.0).

4.5 Second-Level Event Correlation



Second-Level Event Correlation is the sub-process activity that determines, through automation, that an appropriate response to an event is needed based on a set of criteria and rules in a prescribed order. The EMS correlation engine compares the event with configured organizational rules to alert EM and IT Operations Analysts to the Event that needs attention.

Event Correlation also eliminates false-positive messages through impact and root cause analysis. Rules, models and policy-based correlation are configured to derive and isolate the true cause and impact as well as provide data for meaningful reports. Examples of what correlation engines will take into account include:

- Number of similar events
- Number of CIs generating similar events
- Whether the event represents an exception
- Utilization threshold information, both maximum and minimum standards
- Categorization and severity of an event

Input to Second-Level Event Correlation comes when First-Level Event Filtering shows a significance of Warning.

Figure 4-5 illustrates the Second-Level Event Correlation sub-process.

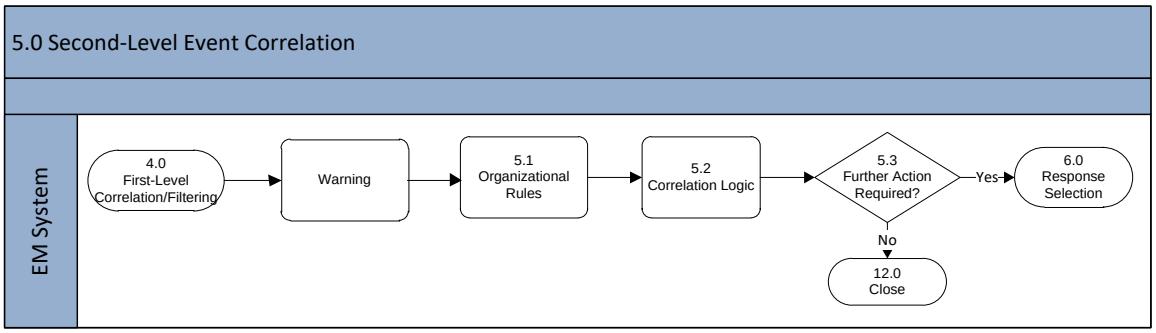


Figure 4-5 Second-Level Event Correlation Sub-Process

Table 4-5 describes each activity as illustrated in Figure 4-5.

Table 4-5 Second-Level Event Correlation Sub-Process Descriptions

5.0 Second-Level Event Correlation		
Number	**Process Activity**	**Description**
5.1	Organizational Rules	Concurrent events are examined to determine correlation and relevance. Determination is made based upon established criteria or business rules of the organization.
5.2	Correlation Logic	Correlation logic is applied to determine if events are duplicated or repeated. Duplicated events are filtered out during the correlation of repeated events. The remaining, related events share the same fault. These events are correlated so that they can be collectively addressed. If an event is related to the same infrastructure fault as an existing event, this event is then correlated with the existing event and the existing event becomes the Master event. The master event serves as the primary record of the fault to be resolved.
5.3	Further Action Required	Correlation is performed again after looking at other related events to see if the status of the master event changes (e.g. a warning event reaches a critical threshold). If Yes, the event proceeds Response Selection (Step 6.0). If no further action is required the event passes to Close (Step 12.0).

4.6 Response Selection

A response selection is required after an Event passes second level correlation if further action is still required. This is the means of initiating task(s), either automated or through human intervention. Responses are selected depending on the technology affected by the event. One or more activities are initiated by the response selection activity. Generally they occur simultaneously.

Events which occur frequently in the environment are assigned appropriate responses and will be automated where applicable.

Once it has been determined that further action is required, there is either an auto response or a required human intervention. If human intervention is required, an alert must be sent to trigger 8.0 in the Event Management process flow.

Examples of responses include the following:

Example 1: Multiple devices send repetitive warning messages which exceed a pre-defined threshold (organizational rule). It has been determined that further action is required. Response Selection simultaneously initiates the following:

- Alert to initiate notification for immediate Human Intervention
- Event is logged and registered in the appropriate database (i.e. ITSM tool) for follow-up as required

Example 2: An exception event comes from a critical e-mail server agent showing the software service has stopped running. The Auto Response process will

simultaneously do the following:

- Auto response to instruct the tool to restart the service
- Alert to initiate notification for immediate Human Intervention and notifies the technical person responsible for e-mail
- Event is logged and registered in the appropriate database (i.e. ITSM tool) for follow-up as required

Figure 4-6 illustrates the Response Selection sub-process.

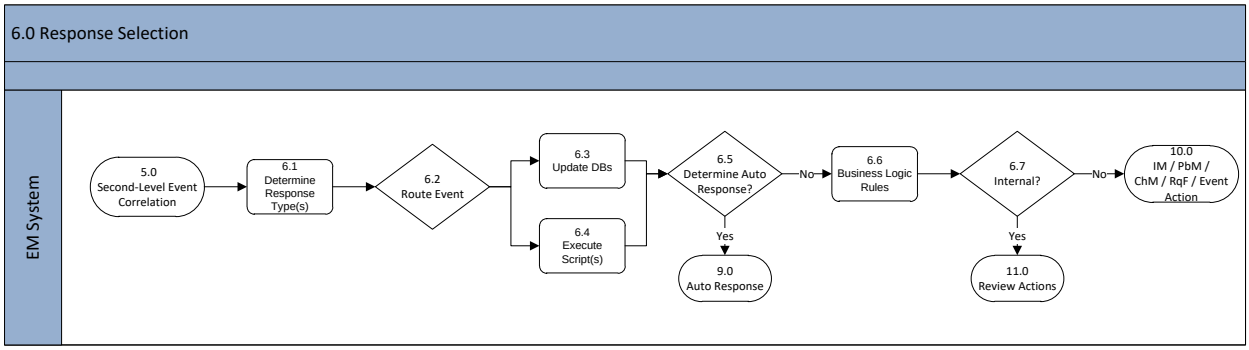


Figure 4-6 Response Selection Sub-Process

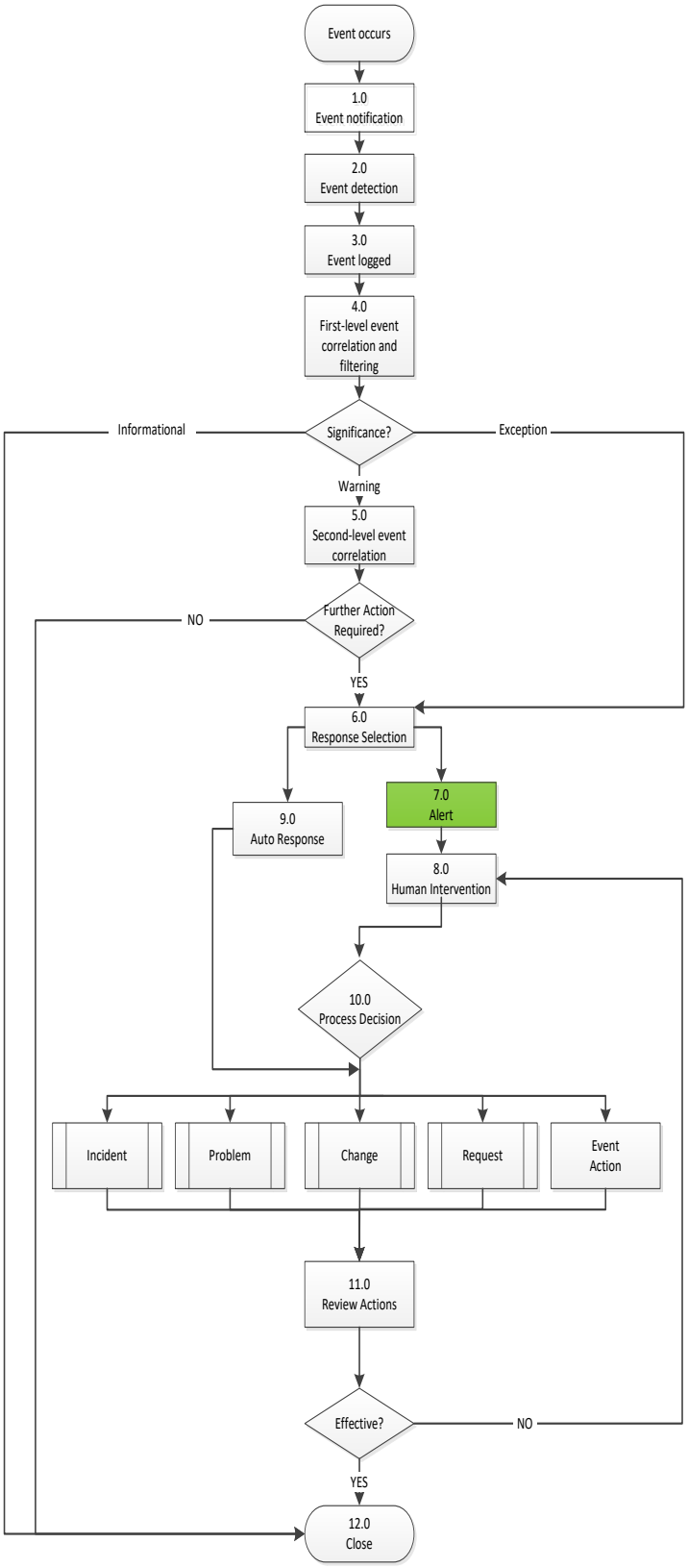
The Response Selection sub-process contains important activities necessary for successful EM. Table 4-6 describes each activity as illustrated in Figure 4-6.

Table 4-6 Response Selection Sub-Process Descriptions

6.0 Response Selection		
Number	**Process Activity**	**Description**
6.1	Determine Response Type	The EM system will determine how to respond to the event based on the output from the correlation steps.
6.2	Route Event	At this point EM is still handling the event internally. Multiple automated tasks are happening concurrently, logs are being updated, and appropriate pre-defined scripts are initiated.
6.3	Update Database(s)	EM Log Files are updated
6.4	Execute Scripts	Internal pre-defined scripts are initiated.
6.5	Determine Auto Response	Determine if internal automated responses are warranted. If Yes, the event is escalated to Auto Response (Step 9.0). If No, an Alert (Step 7.0) is initiated and Human Intervention (Step 8.0) is required.

6.0 Response Selection		
Number	**Process Activity**	**Description**
6.6	Business Logic Rules	Determines if the Event will be routed one of two ways: - Internally – handled by the analyst within the EMS or appropriate tool. For example, an Event Analyst makes a decision on the execution of the appropriate script. - External (Step 10.0) - The IT Operations Analyst may open a record in the ITSM tool to follow the appropriate process. For example, Event Analysts can initiate an RFC to the ChM process or initiate an Incident record to resolve the incident and close the event.
6.7	Internal? (Route Event)	Is the event subject to additional handling? If No, the event moves External (Step 10.0) IM/PbM/ChM/RqF/Event Action. If Yes, it is internal and handled by EM, passing along to the next step in the sub-process, Review Actions (Step 11.0)

4.7 **Alert**



When an event does not have an associated auto response, an Alert is sent to initiate notification for immediate Human Intervention. This alert ensures that the person or team with the appropriate skills is notified. The alert must contain all the information necessary for that person or team to determine the appropriate action – including reference to any required documentation.

Examples of alerts which require Human Intervention are warnings that a threshold has been reached, something has changed, or a failure has occurred.

An alert that goes to human intervention in the workflow requires an acknowledgement. An alert requires a person, or team, to perform a specific action, possibly on a specific device and/or at a specific time. For example, clearing the cache memory or changing access permissions to a named machine or CI.

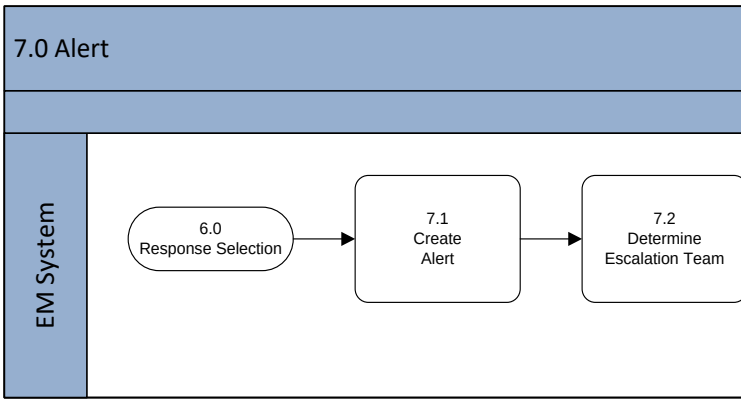


Figure 4-7 illustrates the Alert sub-process.

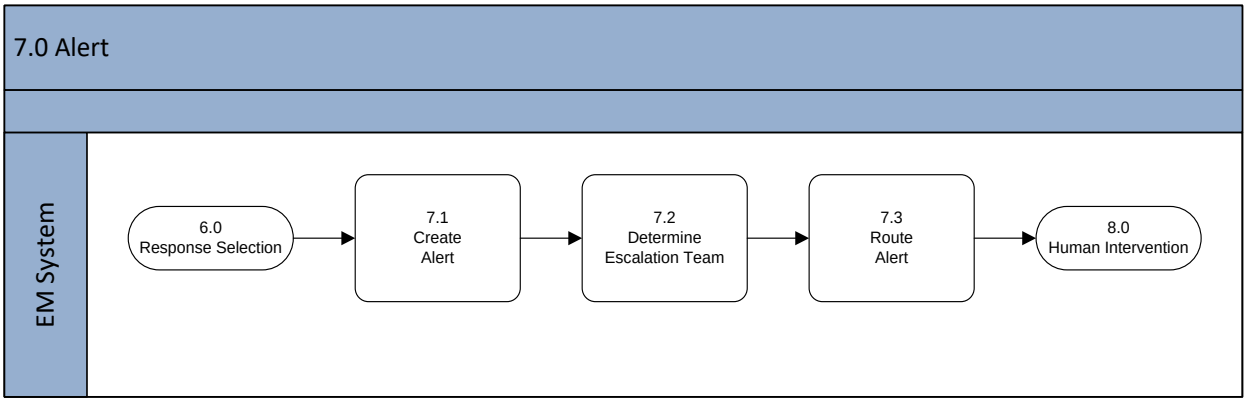


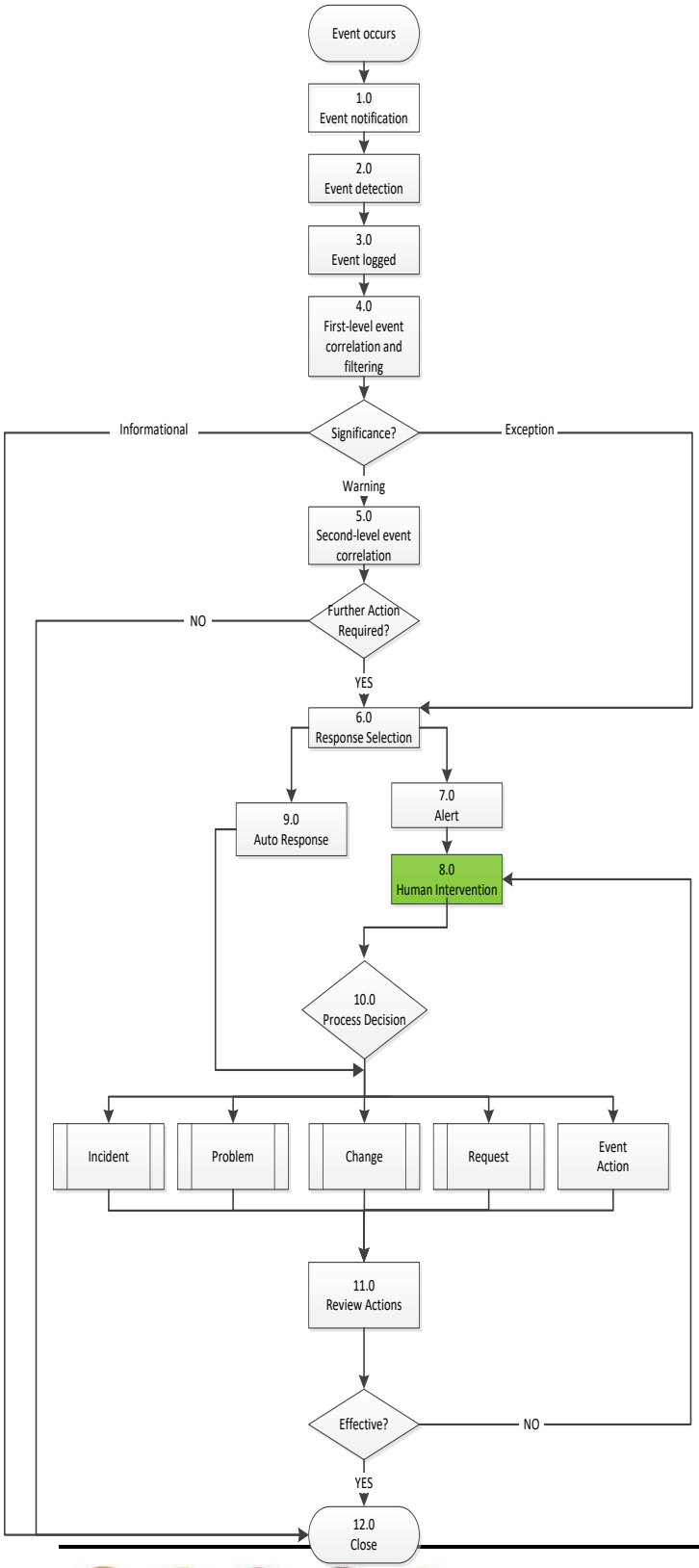
Figure 4-7 Alert Sub-Process

Table 4-7 describes each activity as illustrated in Figure 4-7.

Table 4-7 Alert Sub-Process Descriptions

7.0 Alert		
Number	**Process Activity**	**Description**
7.1	Create Alert	The EM system creates the alert.
7.2	Determine Escalation Team	Based on pre-determined factors such as CI type, the person or group to whom the event is to be escalated is determined.
7.3	Route Alert	The specific team is sent the alert through pre-defined methods. (E-mail, phone, etc.) The alert will contain all the information necessary for that person or team to determine the appropriate action.

4.8 Human Intervention



The Human Intervention sub-process is followed when step 6.0 Response Selection is determined to not have an Auto Response associated with a specific event. Human intervention is critical for the following reasons:

- To mitigate risk
- To ensure optimal event filtering
- To improve Event Correlation
- To check automated action
- To bring in technical expertise swiftly

Only when an event exceeds pre-determined thresholds is human intervention summoned to the process to resolve the issue. The EM process requires human intervention to prevent false-positives from initiating incorrect automated responses. When EM tools have proven accurate and effective, the response selection for events move from Alerts and Human Intervention to Auto Response.

Internal Human Intervention is handled through the EM tools and the EM process. External Human Intervention sends the event to another process(es) (Incident, Problem, Change, Request) or additional Event Action is taken.

A detail of the Human Intervention activity is illustrated in

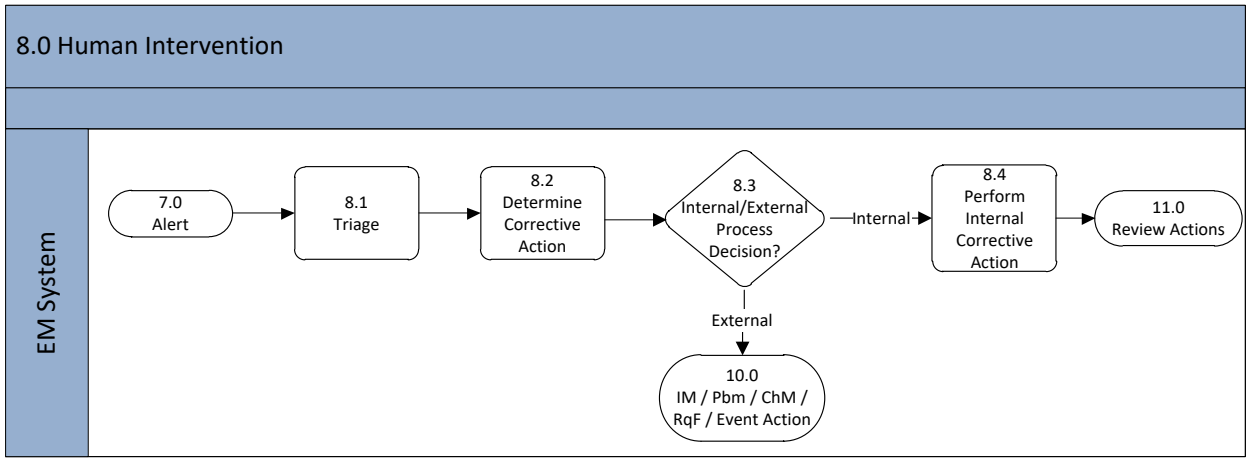


Figure 4-8.

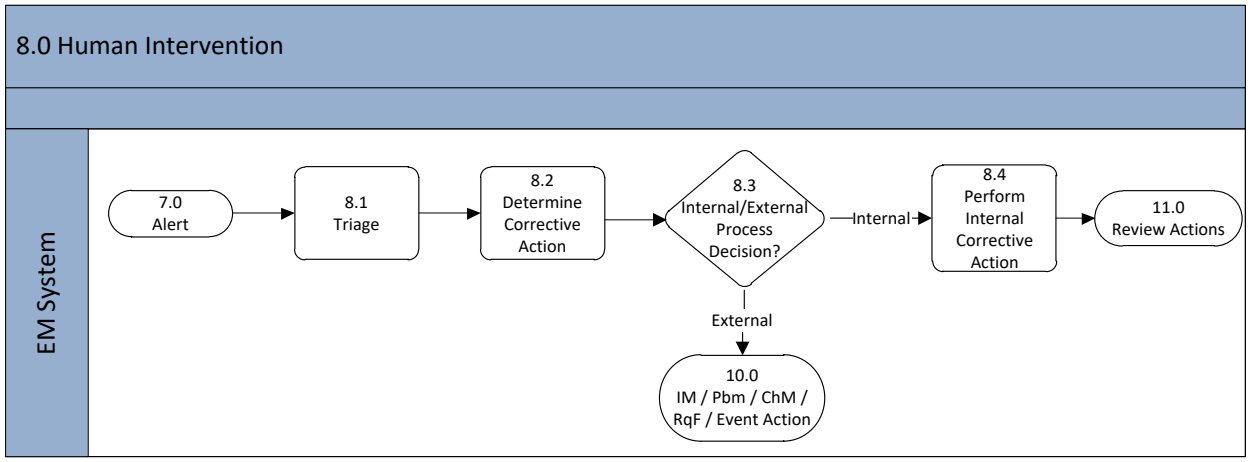


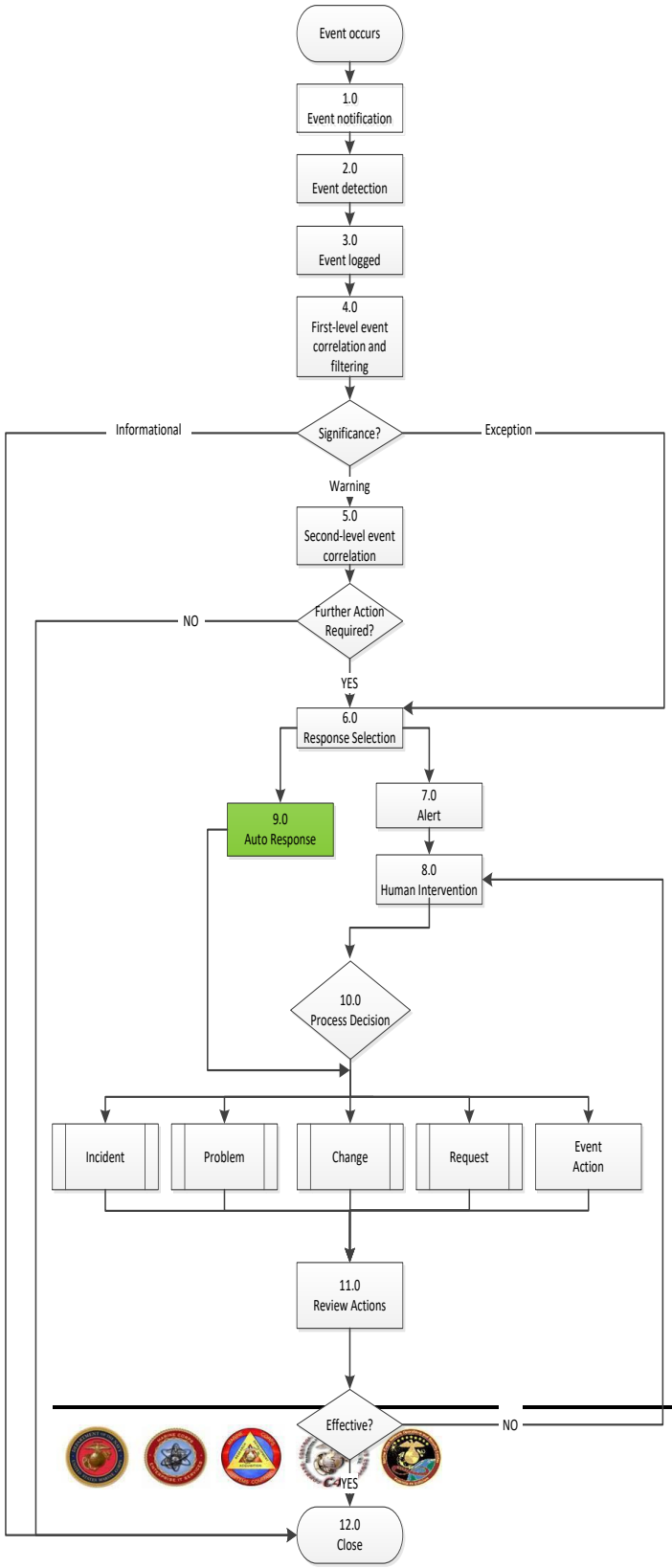
Figure 4-8 Human Intervention Sub-Process

Table 4-8 describes each activity as illustrated in Figure 4-8.

Table 4-8 Human Intervention Sub-Process Descriptions

9.0 Human Intervention		
Number	**Process Activity**	**Description**
8.1	Triage	The Event Analyst, Level 1 support, begins analysis of the Event.
8.2	Determine Corrective Action	After triage has been completed a determination needs to be made how to process the Event.
8.3	Internal/External Process Decision?	If External, another process(es) is engaged (Step 10.0). If Internal, proceed to 8.4
8.4	Perform Internal Corrective Action	The Event Analyst finds a preexisting corrective action to perform. This may be an established response to an event or may be creating a new corrective action for the event.

9.0 Human Intervention		
Number	**Process Activity**	**Description**
		This event will be handled by the analyst within the EMS or appropriate tool. For example, an Event Analyst makes a decision on the execution of the appropriate script. Proceed to Review Actions (Step 11.0).



4.9 Auto Response

Auto Response is a pre-defined process that can be fully or partially automated, or have known manual steps that need to be performed to clear an event. There are different auto responses for different technologies and scenarios. Auto Response examples follow:

- Sending a visual notification to appropriate person or group
- Rebooting a device
- Restarting a service
- Submitting a job into batch
- Changing a parameter on a device
- Locking a device or application to prevent unauthorized access

As the EM process matures, repeated manual processes should be automated. An Auto Response is limited to immediate visual notifications at this time.

Auto Response then proceeds to Review Actions in preparation to closing the event.

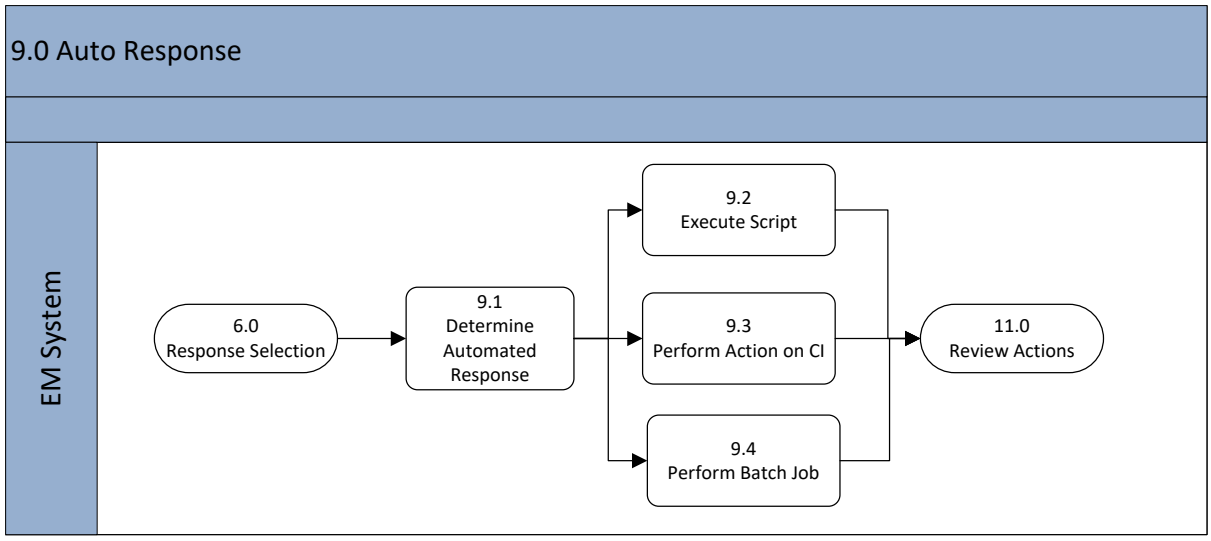


Figure 4-9 illustrates the Auto Response sub-process.

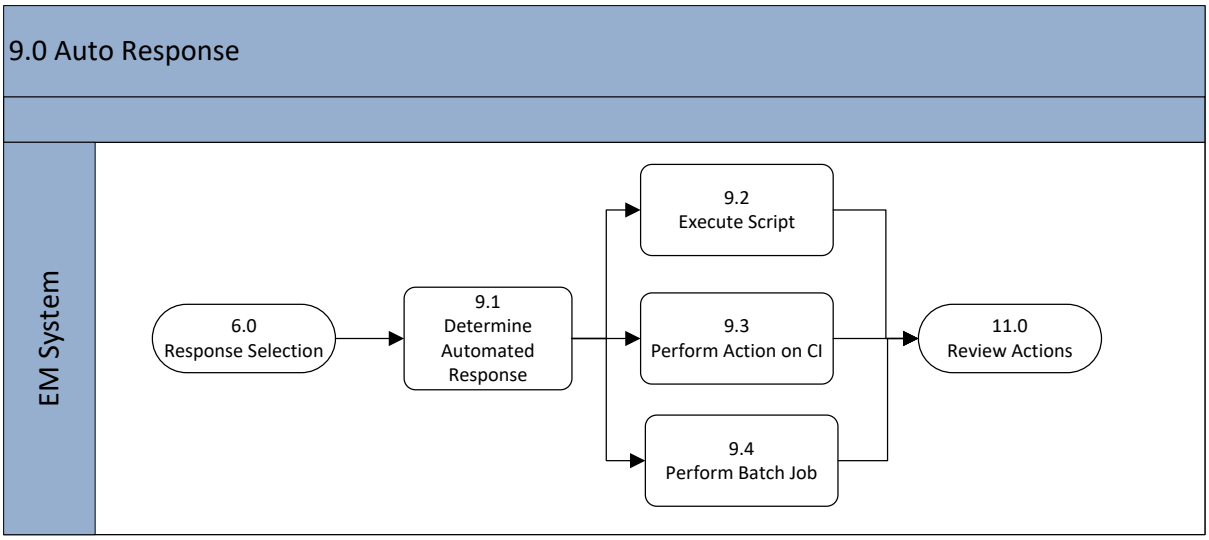


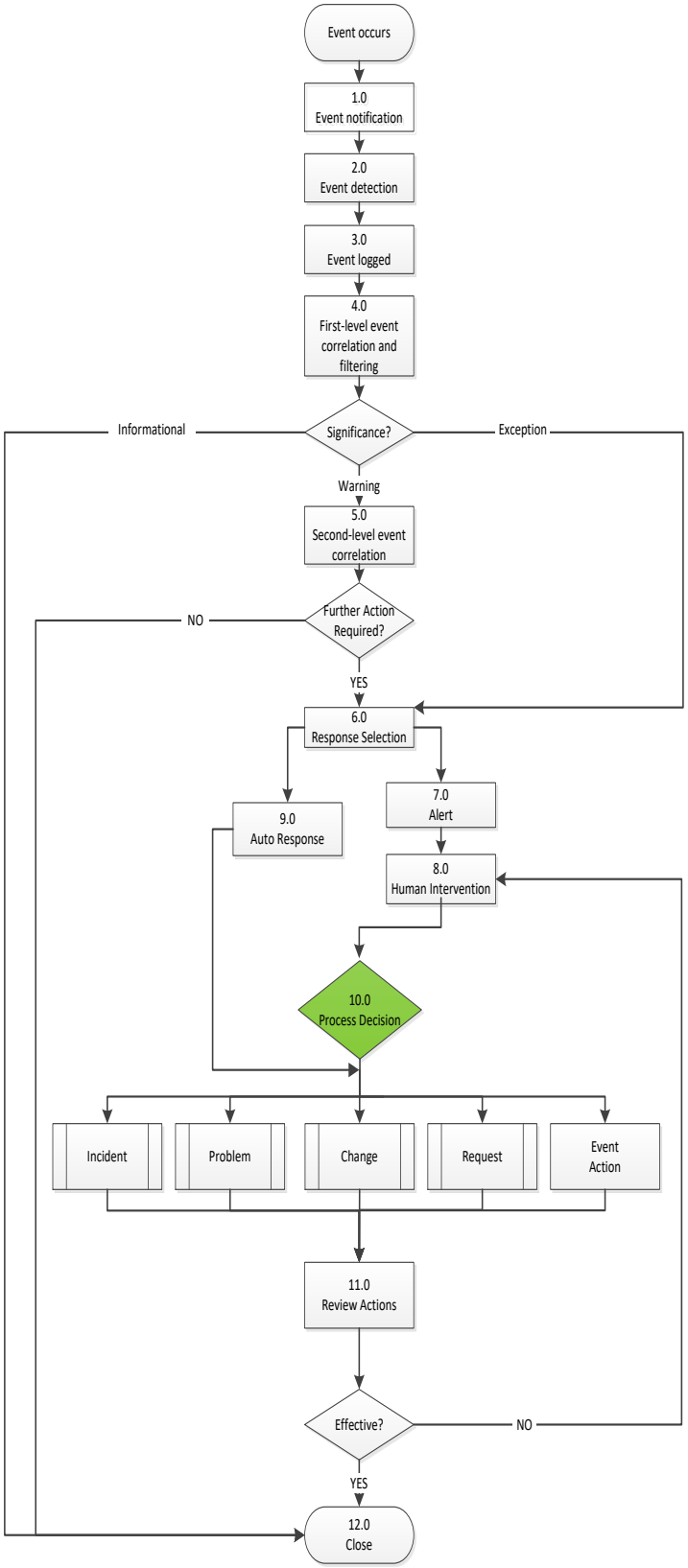
Figure 4-9 Auto Response Sub-Process

The Auto Response sub-process executes pre-defined activities without involving outside processes. Table 4-9 describes each activity as illustrated in Figure 4-9.

Table 4-9 Auto Response Sub-Process Descriptions

9.0 Auto Response		
Number	**Process Activity**	**Description**
9.1	Determine Automated Response	The EM system will determine which automated processes to execute based on information passed from the Second-Level Correlation (Step 5.0) above.
9.2	Execute Script(s)	Internal pre-defined scripts are initiated.
9.3	Perform Action on CI	Direct Action on the CI is initiated; examples include re-booting a server, restarting a service or changing a parameter on the device.
9.4	Perform a Batch Job	An approved batch job is scheduled to run during a maintenance period or during an approved change.

4.10 Process Decision (IM / PbM / ChM / RqF / Event Action)



EM interacts and integrates with other process areas. Events are frequently transferred or escalated to other process areas; sometimes to multiple process areas.

Examples of opening RFCs and Incidents:

RFC: An alert has been received in reference to a performance threshold which has been reached. The Process Decision activity determines that the appropriate response to this event is for a parameter on a server to be modified. An RFC is opened as a result of a hand-off to the Change Management (ChM) process.

Incident Record: As with an RFC, an incident record would be generated when the Process Decision activity determines that a specific type or combination of events represent an incident. The Event Analyst ensures that when an incident record is created, the appropriate information (i.e. complete diagnostics script, links, detailed event attributes) is included within the IM record.

Figure 4-10 illustrates the Process Decision (IM / PbM / ChM / RqF, Event Action) sub-process.

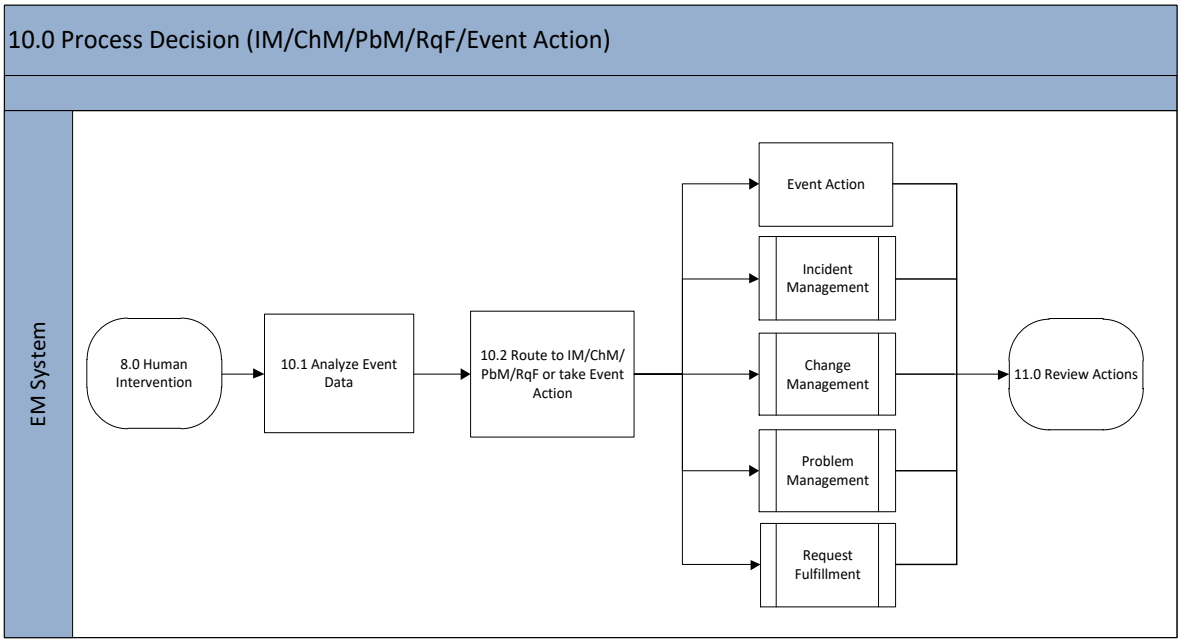


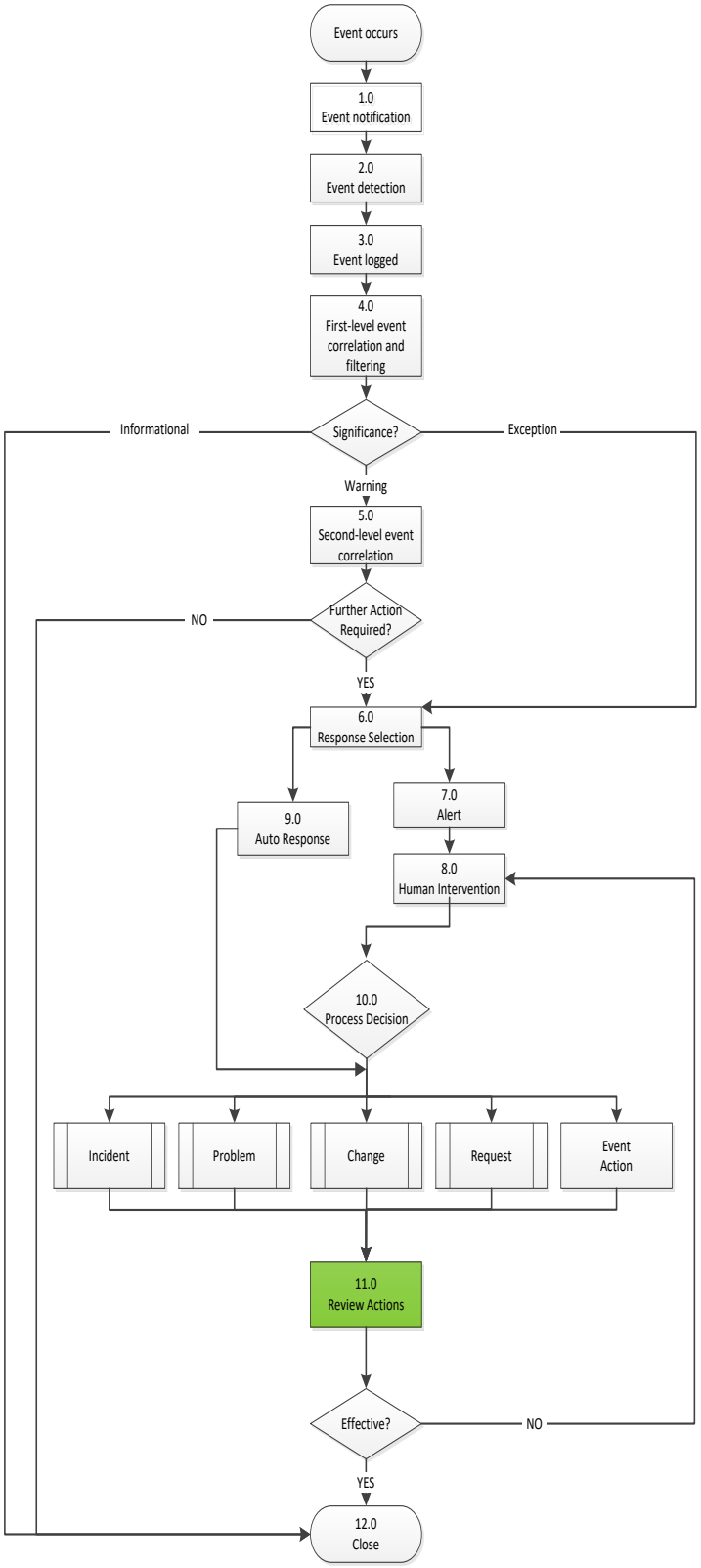
Figure 4-10 Process Decision Sub-Process

The proper routing of the event is critical to success. The logic of how an event is routed to the appropriate group is pre-defined in the Design Process. Table 4-10 describes each activity as illustrated in Figure 4-10.

Table 4-10 Process Decision (IM / PbM / ChM / RqF / Event Action) Sub-Process Descriptions

10.0 Process Decision (IM / PbM / ChM / RqF, Event Action)		
Number	**Process Activity**	**Description**
10.1	Analyze Event Data	A decision is made about the appropriate process(es) to route the event.
10.2	Route IM / PbM / ChM / RqF or take Event Action	The Incident, Problem, Change, Request is routed appropriately or Event Action is taken.

4.11 Review Actions



The Review Actions sub-process ensures that significant events have been responded to appropriately, and event trends are analyzed and documented.

The Review Action sub-process does not duplicate reviews which have been performed in the IM, ChM, PbM, or RqF process areas. Rather, the intention is to ensure the coordination between EM and other process areas performs as designed, and the appropriate action was accomplished. This optimizes working relationships among process areas.

Information gleaned from the Review Actions sub-process is used as input into continual improvement, evaluation, and audit of the EM process.

Review Actions sub-process is initiated after the event has cleared all preceding processes.

Figure 4-11 illustrates the Review Actions sub-process.

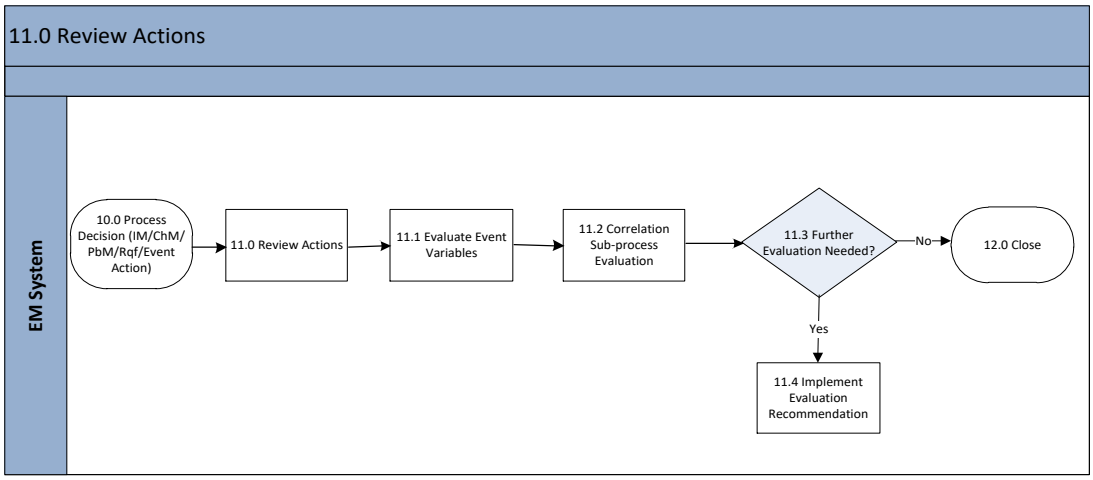


Figure 4-11 Review Actions Sub-Process

There are two main steps in Review Actions:

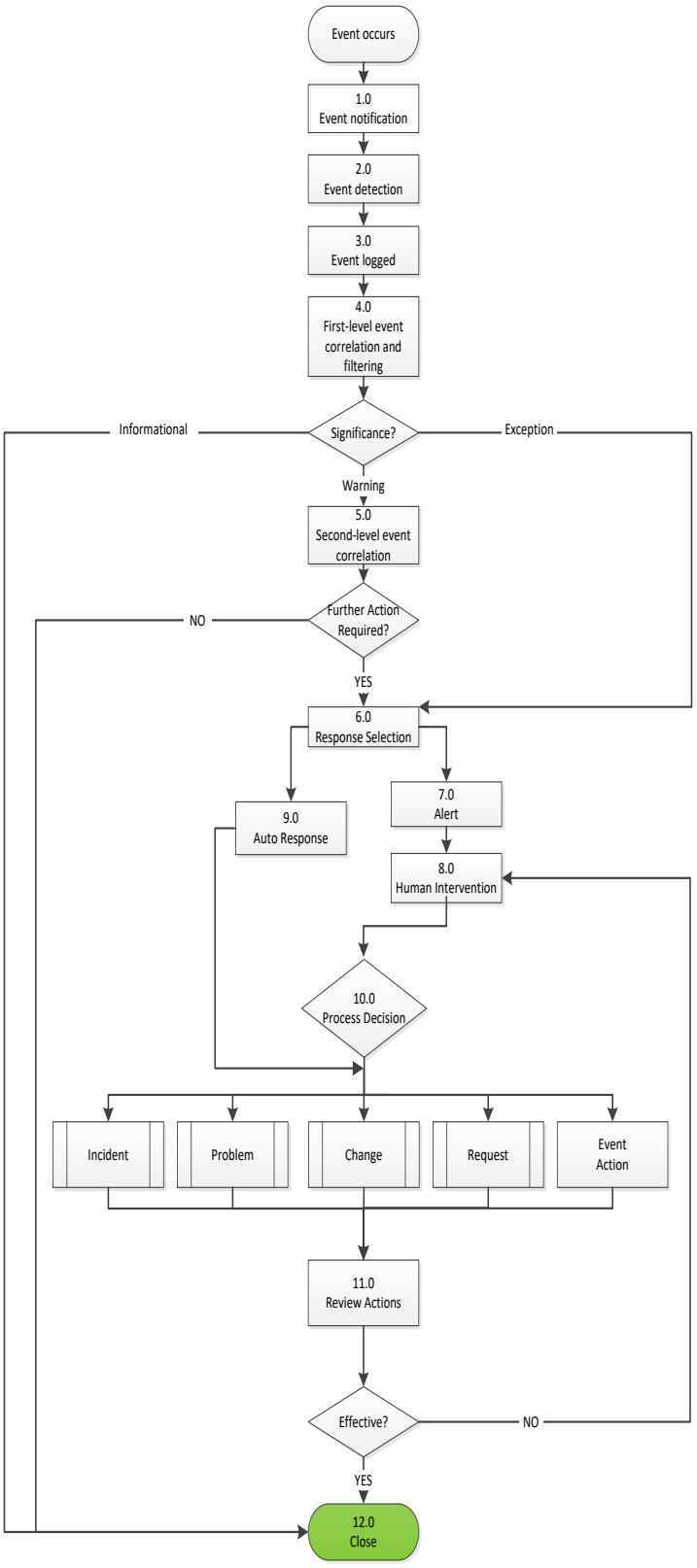
1. Ensure the handover of Events to Incident, Problem, Change or Request resulted in the expected outcome.
2. Ensure the event logs are analyzed in order to identify trends or patterns which suggest corrective action must be taken.

Table 4-11 describes each activity as illustrated in Figure 4-11.

Table 4-11 Review Actions Sub-Process Descriptions

11.0 Review Actions		
Number	**Process Activity**	**Description**
11.1	Evaluate Event Variables	Review of completed events. The intent is NOT to repeat reviews already performed in other processes. Rather the intent is to ensure that handoffs between processes were performed as designed.
11.2	Correlation Sub-process Evaluation	The correlation sub-processes are reviewed. The filtering and activities are evaluated.
11.3	Further Evaluation Needed?	A more formal review of the event and its associated processes could be warranted.
11.4	Implement Evaluation Recommendation(s)	If determination is made to implement new recommendations, external process(es) are engaged as required.

4.12 **Close**



Events are not closed per the dictionary definition of closed. Events remain open until another action occurs that clears the previous event.

Informational events are logged and do not require further action, therefore they are immediately closed. Warnings which do not require further action are closed as well. If action is required for warning or exception, they proceed to their appropriate response selection process (Auto Response or Human Intervention). Auto Response and Human Intervention have two separate closing processes.

Auto Response events are closed by the generation of a second event. For example, a device generates an event and is rebooted through auto response – as soon as that device is successfully back online, it generates an event that effectively closes the loop and clears the first event.

Events that have Human Intervention are closed after completing the Review Actions process.

It is optimal that devices in the infrastructure produce ‘open’ and ‘close’ events in the same format and specify the change of status. This allows the correlation step in the process to easily match ‘open’ and ‘close’ notifications.

In the case of events that generated an incident, or change, information about the event should be included in the appropriate record of the incident or change process.

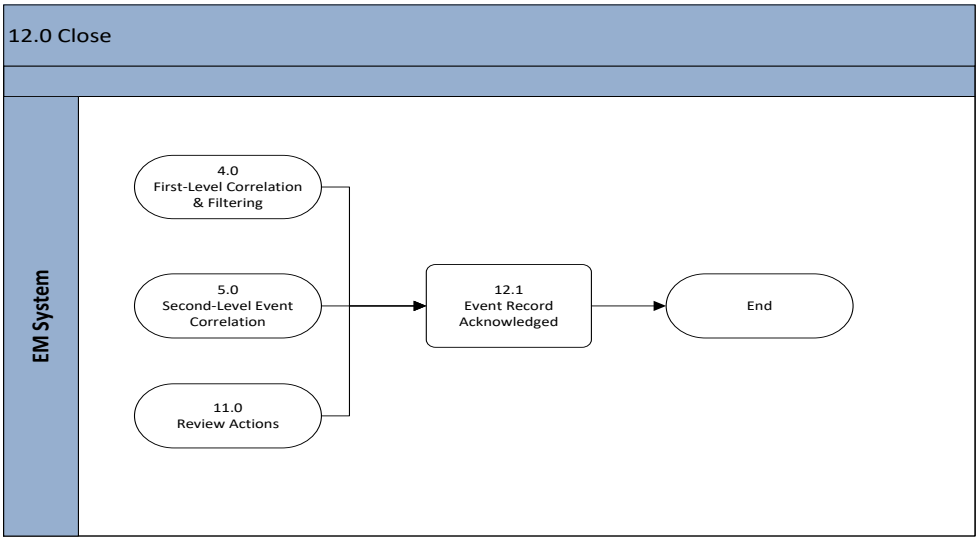


Figure 4-12 illustrates the Close sub-process.

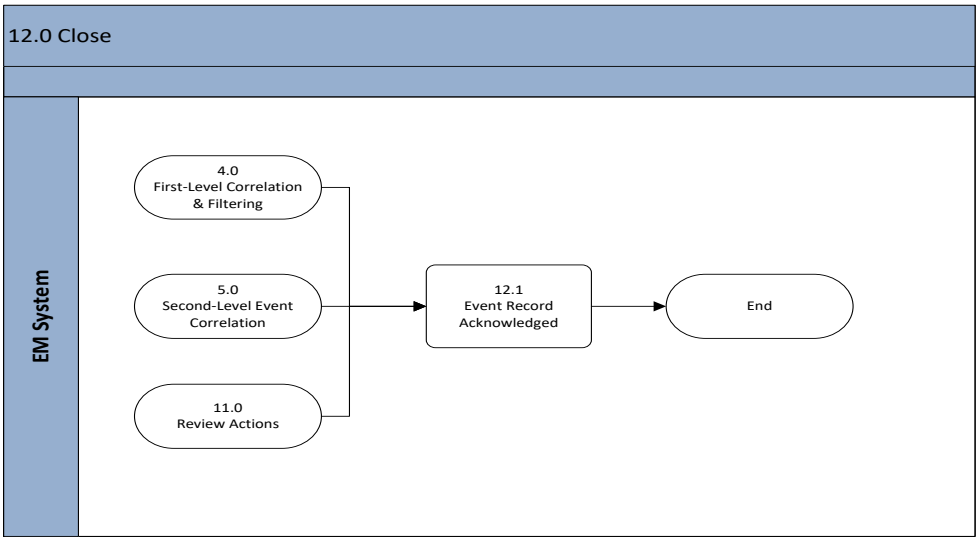


Figure 4-12 Close Sub-Process

Table 4-12 describes each activity as illustrated in Figure 4-12.

Table 4-12 Close Sub-Process Descriptions

12.0 Close		
Number	**Process Activity**	**Description**
12.1	Event Record Acknowledged	It is optimal that events “auto-close”. For example, a previously off-line device was auto-rebooted. As it comes back on-line, it generates a second event signaling that it is now on-line. The EM Tool correlates this new event with the previous negative event and is able to close the first event.

APPENDIX A - ACRONYMS

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

APPENDIX B - GLOSSARY

Term	Definition
Alert	An Alert is a communication that provides information.
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 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.
Close Event	Events are not closed per the dictionary definition of closed. Events remain open until another action occurs that clears the previous event.
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.
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.
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 that 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.
Event Management System	The Event Management System (EMS) is comprised of tools that 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.
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.

Term	Definition
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 status is known.
Notification	See Alert.
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.
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.
Test	A Test is an activity that verifies that a CI, IT service, or process meets its specification or agreed requirements.
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.
Work Instruction	The Work Instruction is a document containing detailed instructions that specify exactly what steps are followed to carry out an activity. A work instruction contains much more detail than a procedure and is only created if very detailed instructions are needed.

APPENDIX C - REFERENCES

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

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