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

IN REPLY REFER TO:
2300/03B
CP

From: Commandant of the Marine Corps

Subj: ENTERPRISE INFORMATION TECHNOLOGY SERVICE MANAGEMENT EVENT MANAGEMENT PROCESS GUIDE

Ref: (a) MCO 5271.1B

Encl: (1) IRM-2300-03B Enterprise Information Technology Service Management Event Management Process Guide

1. PURPOSE. The purpose of the Enterprise Information Technology Service Management (ITSM) Event Management 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 Information Technology (IT) activities through promoting standardization of work instructions and operating procedures across a continuum of document specificity.

2. CANCELLATION. 2300-03A.

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 Director, Command, Control, Communications and Computers.

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

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

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

DISTRIBUTION: PCN 18623001100

Enterprise IT Service Management
Event Management
Process Guide

Release Date:
04 August 2014

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

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.

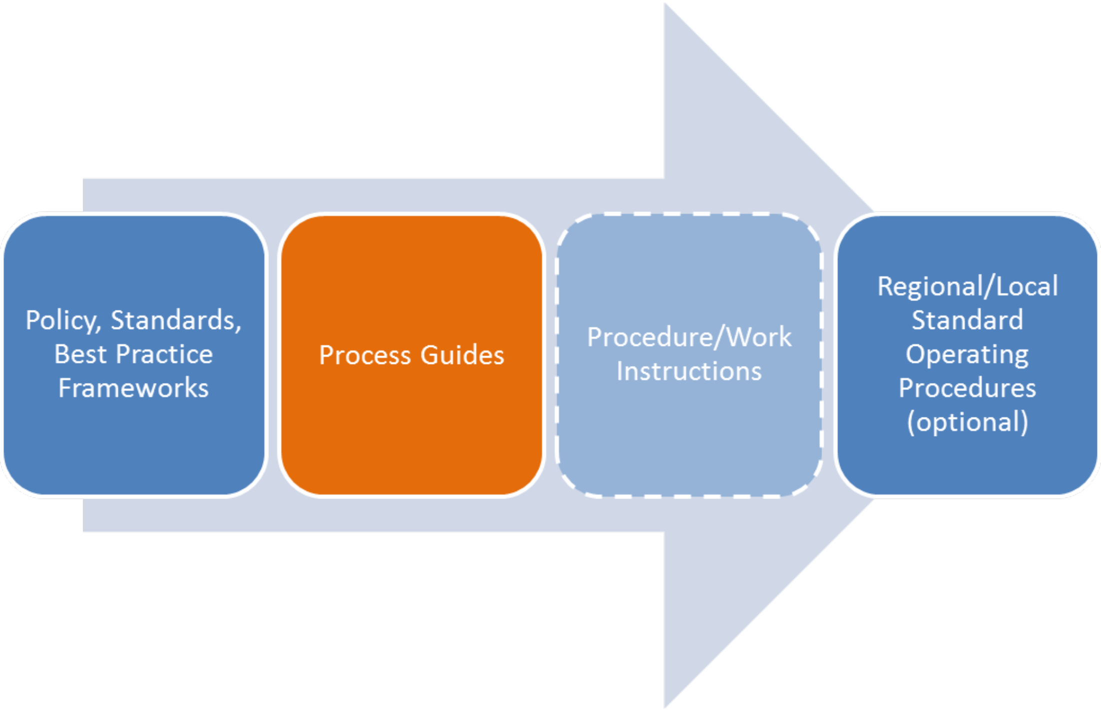

Policy, Standards, Best Practice Frameworks
Process Guides
Procedure/Work Instructions
Regional/Local Standard Operating Procedures (optional)

Figure 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 Network Operations and Security Center (MCNOSC) including all Regional Network Operations and Security Centers (RNOSC) and Marine Air Ground Task Force Information Technology Support Center (MITSC) assets and supported Marine Expeditionary Forces (MEF), Supporting Establishments (SE) organizations, and Marine Corps Installation (MCI) commands.

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

Table 1 Document Design Layers

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

1.3 Process and Document Control

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

2.0 Event Management 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 which 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 usually detected 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.

The EM Process identifies and establishes the appropriate response to infrastructure, service, business process, and security events that could lead to incidents. Event Management 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-synch 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. User satisfaction with the overall IT environment is enhanced by the ability to detect Events and respond quickly to them.

Event Management includes:

- ownership of the process.
- assigning roles and responsibilities for operational support.
- identifying and measuring critical success factors and establishing thresholds/standards.
- receiving guidance on what is going to be monitored (component, system, or service).
- identifying the means to address events as defined by the Service Owner or Service Level Agreement (SLA).
- documenting event-handling procedures.

The focus of USMC Enterprise Event Management is to present Network Operations (NetOps) personnel with situational awareness (SA) of MCEN services in near real-time in order 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 many 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 and Systems:

- are not operating efficiently.
- have exceeded allowable limits.
- have breached an SLA.
- have been compromised.
- have failed.

The objectives of the USMC EM process are to:

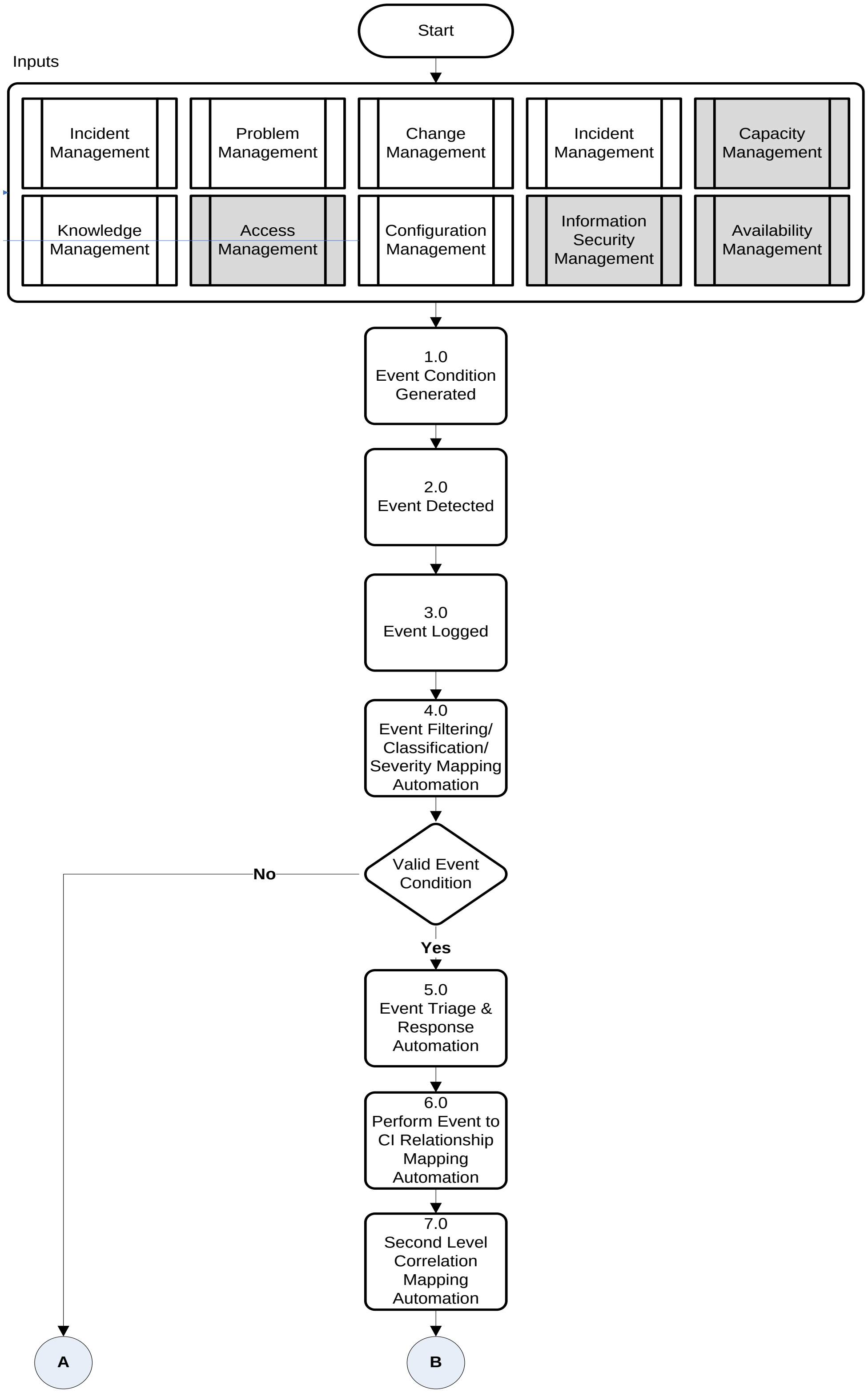
- provide real-time situational awareness of the USMC NIPRNet and SIPRNet.
- fully integrate the EM process and capabilities within USMC Cyber Operations. This provides critical support to USMC Cyber Operations C2 and other ITSM processes.
- detect all significant changes in CIs or IT services.
- determine the appropriate action for significant events and communicate information to the appropriate functional area.
- provide information related to operating performance so that it can be compared to design specifications and SLAs.
- provide information relevant for continual service improvement.

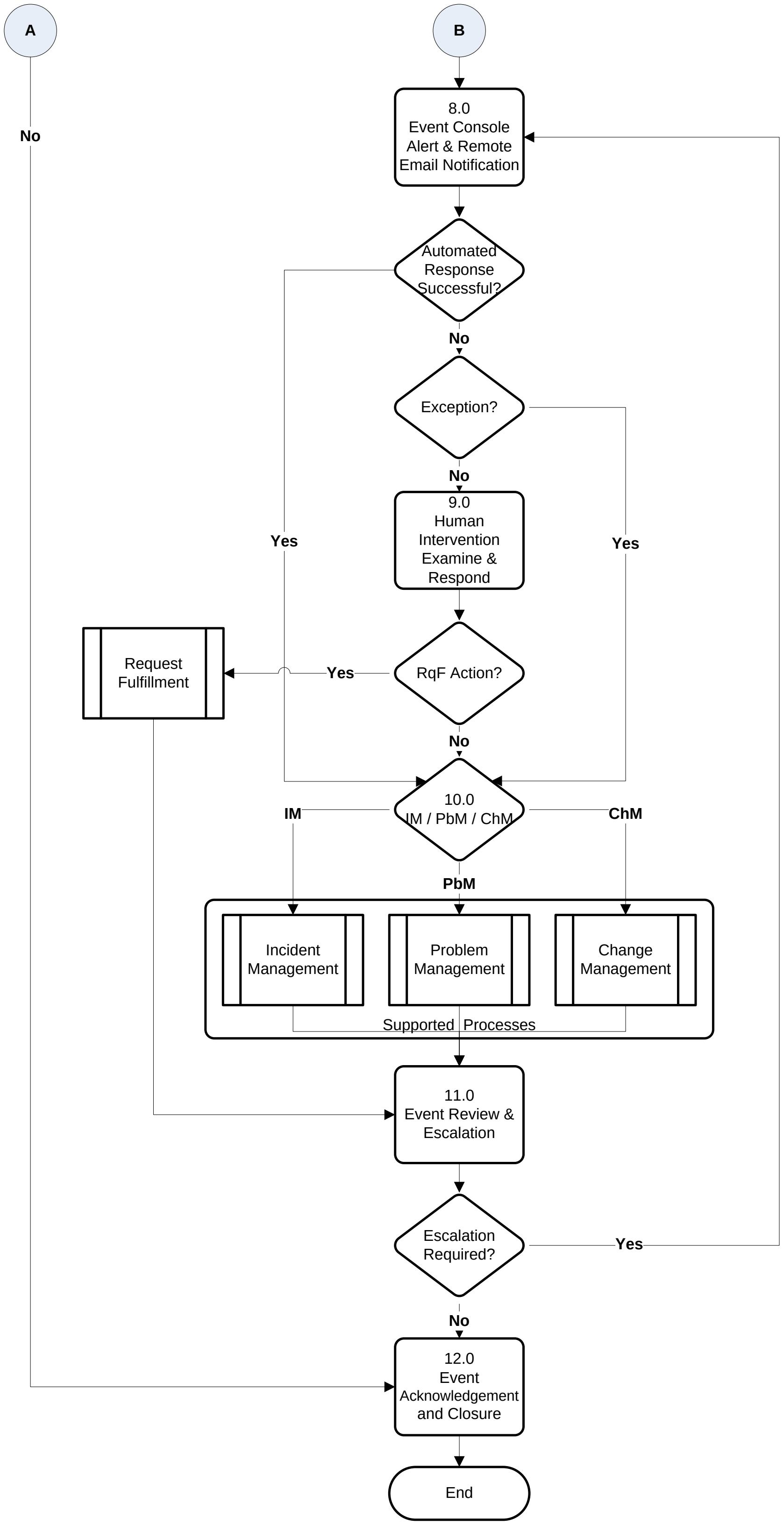
EM is more than fault management. EM aligns with Fault, Configuration, Administration, Performance and Security (FCAPS), and follows the Open Systems Interconnection (OSI) Systems Management Overview (SMO) standard to present both an integrated and role-based situational awareness view for the Cyber Operations Community. The Event Management System (EMS) monitors network devices, servers, network traffic, enterprise services, and applications, and manages all events detected. This monitoring capability covers all OSI layers. For example:

1. Physical hardware and protocol network connectivity
2. Data Link transmission protocols and hardware access permissions
3. Network switching and routing
4. Transport of data between operating systems
5. Session management of connections between applications
6. Presentation of data independent of differences and incompatibility
7. Application and end user processes identified and monitored for quality of service and appropriate access

2.2 High-Level Process Model

The high-level EM process model shows decision points and inputs to other processes, which is the starting and overarching level for scoping processes down to the sub-process level. The EM high-level process consists of 12 sub-processes and six decision blocks. The workflow shown on the following two pages depicts these processes and sub-processes that collectively enable and underpin EM.


Start
Inputs
Incident Management
Problem Management
Change Management
Incident Management
Capacity Management
Knowledge Management
Access Management
Configuration Management
Information Security Management
Availability Management
1.0 Event Condition Generated
2.0 Event Detected
3.0 Event Logged
4.0 Event Filtering/ Classification/ Severity Mapping Automation
Valid Event Condition
No
Yes
5.0 Event Triage & Response Automation
6.0 Perform Event to CI Relationship Mapping Automation
7.0 Second Level Correlation Mapping Automation
A
B



High-Level Event Management Workflow

Table 2 contains descriptions of each sub-process. Each sub-process number is hyperlinked to its detailed description in Section 3.0, Sub-processes. The decision diamonds are numbered but not considered sub-processes themselves and do not have hyperlinks.

Table 2 EM Process Activity Descriptions

Section	Process Activity	Description
3.1	Event Condition Generated	Event Condition Generated involves ensuring Events are captured by the EMS. Each Configuration Item (CI) to be monitored will be configured to either actively or passively communicate its status to the EMS. The status is displayed in the various Views.
3.2	Event Detected	When an Event condition occurs, it is detected by an agent or an agentless monitoring capability surveilling the system or the system transmits directly to the EM tool.
3.3	Event Logged	All Event conditions are logged within the local EMS and only actionable Event Conditions are forwarded to the Manager of Managers (MoM) or Enterprise EMS. Event Logs are available as needed for trending data, security research, problem research, and reporting.
3.4	Event Filtering / Classification / Severity Mapping Automation	Event Filtering is the activity of the EM process that supports two possible outcomes: either to 1) communicate and pass the Event to the next activity for the determination of significance, or to 2) ignore, suppress, and close the Event. The Aggregator evaluates the Event and determines if this new Event relates to one previously identified. Event conditions are evaluated for validity and classified as: Critical; Major; Minor; Warning; OK; or Informational. 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.
3.5	Event Triage and Response Automation	Triage is the process of sorting, categorizing, correlating, prioritizing, and assigning incoming Events, incidents, vulnerability reports, and other general information requests. The triage function provides an immediate snapshot of the current status of all activity reported — what reports are open or closed, what actions are pending, and how many of each type of report has been received.
3.6	Perform Event to CI Relationship Mapping Automation	The Event to CI relationship mapping supports identifying the device information, physical location, and owner of the asset.
3.7	Second Level Correlation Mapping Automation	The correlation engine compares the Event with business rules and initiates changes or provides alerts to the Event that needs attention. The Event Correlation engine eliminates false positive messages through impact and root cause analysis. Rules, models and policy-based correlation technologies derive and isolate the true cause and impact as well as provide data for meaningful reports. Multiple monitoring and managing tools will each have a correlation engine.
3.8	Event Console Alert & Remote Email Notification	Alerts ensure the personnel with the appropriate skills are notified so they can resolve the Event conditions. Alerts contain all the information necessary for those personnel to determine the appropriate action. If correlated Events determine a master Event should be escalated, it is escalated through an alert.
3.9	Human Intervention Examine and Respond	Alert notifications are presented to the EMS console where Human Intervention begins to assess the Event condition. Human intervention prevents false-positives from initiating incorrect automated responses.
3.10	IM / PbM / ChM (Other Processes)	When an Event cannot be resolved, it is escalated to one or more of the other processes, sometimes to multiple processes.
3.11	Event Review and Escalation	Event Review and Escalation checks that any significant Events or exceptions have been handled appropriately, or tracks trends or counts of Event types. Review Actions are used as input into continual improvement and the evaluation and audit of the EM process.

Section	Process Activity	Description
3.12	Event Acknowledgement and Closure	Events are not “opened” or “closed” in the dictionary definition sense. Rather, Events “occur.” Even though the EM Console(s) should re-set to show the Event has cleared, administrators cannot assume that has happened and are required to validate that the Event is cleared.

2.3 Key Concepts

2.3.1 Event Monitoring Tools and Configuration

Standard EM activities include conducting an initial review of the event/alert, performing initial analysis to validate and make sense of it, and routing the event/alert for corrective action. An Event is a change of state that has significance for the management of an IT Service or other CI. An Alert is a notification that a threshold has been reached, something has changed, or a failure has occurred.

The event flow begins at the point of generation (event source). It then moves into the event processor where the automation, correlation, filtering, consolidation, and initiation of recovery actions occur. To properly manage the number of events/alerts taking place, the system must be capable of performing logical checks of those events and making some determination as to how to handle each one. Event Management provides a capability to determine how events should be classified and prioritized based on circumstances. The EM system includes various views, and based on those views, the operational entities within the organization can monitor and investigate events as they take place. These views consist of:

- Enterprise View (MCNOSC)
- Regional View (RNOSC)
- MITSC View
- Base, Post, Station View

Last, the appropriate control actions are performed based on the event details. This includes assignment of an Incident Ticket and routing to the relevant support queue for action.

The overall concept of USMC EM is depicted in Figure 2.

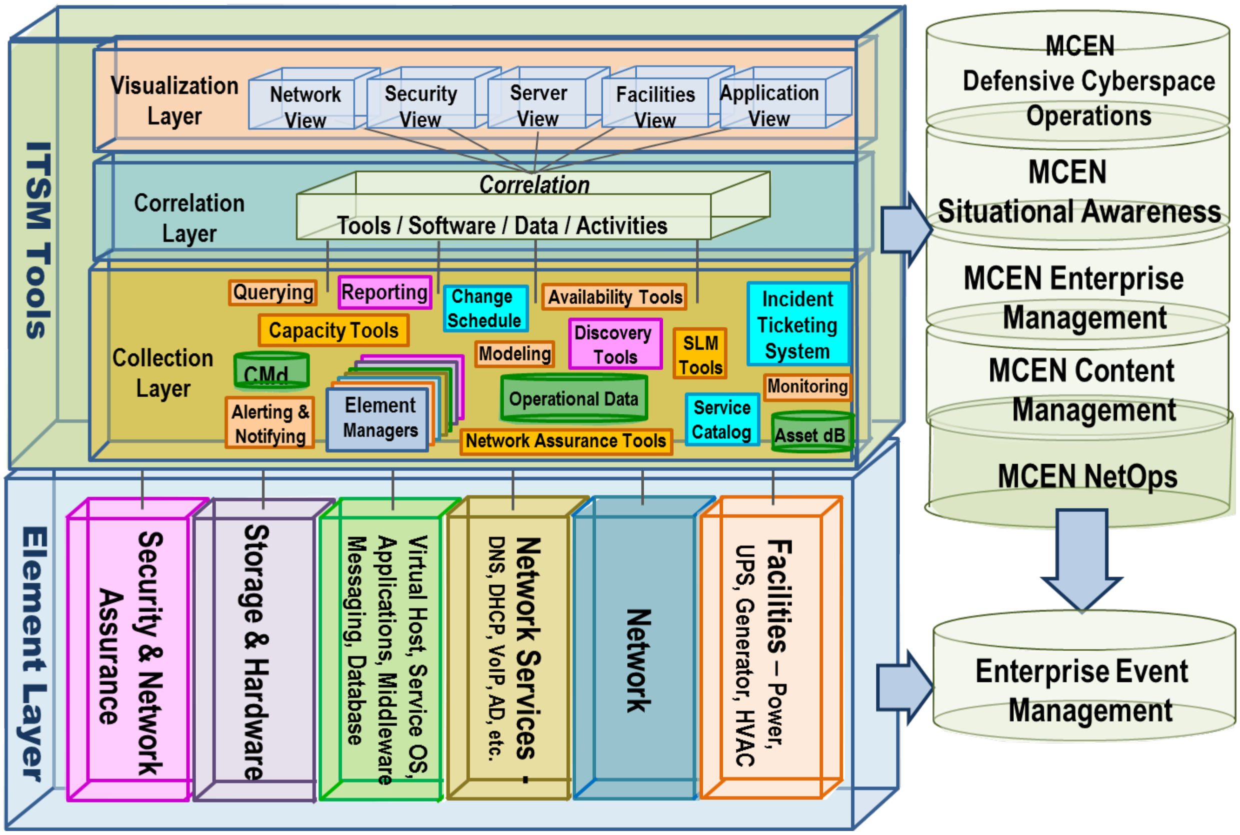


Figure 2 USMC Event Management

The bottom (Element Layer) of Figure 3 depicts data that is monitored and managed by several systems, tools, and processes. Once collected and assembled, information is fed up to systems that aggregate and correlate the various feeds to parse relevant details. The information is then presented in customizable formats for various users and operators.

The majority of work in EM is done by the monitoring tools. Several tools provide a detailed status of the network at all times. When properly configured, tools address potential faults or trends and identify the resources to be monitored. Triggers must be identified that the tool will respond to, such as when high utilization on a service or a capacity threshold on a storage array is reached. The Service Owner must identify the service components and the end-to-end service capability that is to be monitored and measured. Established SLAs provide input into setting those threshold targets and triggers.

Integration of disparate tools is required, along with 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. The USMC process currently requires that all critical or significant event alerts be handled using manual intervention, rather than automated responses. Automated responses are limited to changing visual icons and messages to a prominent color to draw attention to them. As the EM solution matures, false-positives will be eliminated and automation will be increased.

To assemble NetOps SA information, Event Management correlates data from multiple sources as part of the overall ITSM toolset. Event Management tools monitor and poll service components and configuration items such as network elements, storage devices, applications, and critical network services. Network Common Operatonal Picture 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.

Triggers for alerts are configured and stored in Hewlett Packard (HP) Tool Business Service Management (BSM) components, to proactively inform defined recipients when predefined performance limits are breached. These alerts can be displayed on Event Management Operator Consoles for action. Examples of HP Operations Manager i (OMi) Alert Types include:

- Application alerts. There are two types of application alerts: CI Status alerts for high level information, and End User Management (EUM) alerts for low level information. Both types of alerts can be configured to generate Events.
  - CI Status alerts are triggered by a change in status of the relevant KPI, calculated in Service Health.
  - EUM alerts can be triggered based on Business Process Monitor and Real User Monitor data, including synthetic transactions and real user transactions.
- Service Level Agreement (SLA) alerts are configured in Service Level Management Administration. The SLA alerts are triggered by the relevant change in SLA status.
- SiteScope alerts are triggered by an event or change of status in some element or system in the infrastructure. An alert definition contains settings that tell SiteScope what monitors can trigger the alert, what condition to watch for, and what information to send to recipients.

Alerts are viewed using the Operations Management (OMi) Event Browser. Event Browser is a central event console enabling management of the lifecycle of events. EM operators use the Event Browser to:

- See an overview of all the active events that occur in the monitored environment, including event severity and type, event time and location, event source, and the affected CI.
- View events automatically correlated and filtered, to determine priority for actions.
- Display, monitor, and manage the events using graphs and tables, including display of alternative perspectives of the events.
- Launch HP Operations Orchestration run books to take action on the event.

2.3.2 Event Definition and Severity Levels

Because Event Management centers on the processing of events, it is important to clearly define what is meant by an event. An event can be defined as any change of state that has significance for the management of a CI or IT service. Events can be triggered when monitored system resources exceed their configured thresholds. Events may also be used as reminders to take action manually or as notification that an action has occurred.

The severity assigned to an event is an indication of the how critical a problem is, which relates to how quickly service must be restored to the failing system or resource. The classification of an event determines how it is handled in the EM process. An event can be classified as either informational, a warning, or an exception, and also be an unusual event requiring further investigation. There are several different types of events, for example:

Events that are Informational:

- 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 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

EM is not system monitoring which evaluates all things that happen to a system. EM takes monitoring to a mature level and identifies meaningful changes of state that may represent faults.

A fault is an event that has a negative significance. An event may represent a fault in the infrastructure, but it may also simply represent the fact that the status of something has changed. Sometimes, a repetitive series of events represents a fault.

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 SNMP (Simple Network Management Protocol), or at least write a message to its console for a console server to log. This notification triggers automatic or manual activities. 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.

2.3.3 Event Correlation

When multiple events are generated as a result of the same condition or provide information about the same system resource, the relationship between the events should be identified. The process of defining this relationship is event correlation.

There are several different types of correlation:

- Root Cause Correlation – A condition may trigger other conditions, and each condition may be reported by events. One example would be an event that reports a "File System Full" condition. The full file system may cause a process or service to stop working, producing a secondary event.
- Cross-Platform Correlation – Cross-platform correlation refers to correlated events of different types of system resources, such as operating systems, databases, middleware, applications, and hardware.
- Cross-Host Correlation – Conditions on one system that affect the proper functioning of another system result in cross-host correlation. For example, a web application may rely on a series of web, applications, and database servers to run a transaction.
- Topology-based Correlation – When networking resources such as routers fail, they may cause a large number of other systems to become inaccessible and events may be reported that refer to several unreachable system resources.
- Timing Considerations – It is not always the case that the primary event is received first. Network delays may prevent the primary event from arriving until after the secondary is received.

2.3.1 Event Deduplication and Throttling

The process of determining which events are identical is referred to as deduplication or duplicate detection. The purpose of deduplication is to save cycles and system resources on event processors, and minimize bandwidth used to send unnecessary events. Events that are deemed necessary must be forwarded to at least one event processor to ensure that they are handled by either manual or automated means. However, sometimes the event source generates the desired message more than once when a condition occurs. Usually, only one event is required for action.

The time frame in which a condition is responded to may vary, depending upon the nature of the condition being reported. Often, these reports are addressed immediately when the first indication of a condition occurs. This is especially true in situations where a device or process is down. Subsequent events can then be discarded. Other times, a condition does not need to be investigated until it occurs several times. For example, a high CPU usage condition may not be a problem if a single process, such as a backup, uses many cycles for a minute or two. However, if the condition happens several times within a certain time interval, it is most likely significant. The process of reporting events after a certain number of occurrences is known as throttling.

2.3.2 Event Synchronization

Changes made to events at one event processor can be propagated to others through which the event has passed. This is known as event synchronization.

Conditions can arise when one event processor reports that an event is in a certain state and another processor reports that it is in a different state. For example, assume that the condition reported by an event is resolved, and the event is closed at the central event processor but not at the local event processor. The condition recurs, and a new event is generated. The local event processor shows an outstanding event already reporting the condition and discards the event. The new condition is never reported or resolved. To ensure that this situation does not happen, status changes made to events at one event processor can be propagated to others through which the event has passed. This process is known as event synchronization.

There are two main areas where event synchronization is important:

- Forwarding and receiving Events through a hierarchy of event processors
- Integrating with an Incident Management system/tool

Any event processor or Incident Management system/tool can change an event. Depending on the event processor that performs the update, the event changes must be propagated throughout the system. Typically, the Incident Management system/tool notifies support personnel about problems. Therefore, changes made to trouble tickets must be propagated to the event processors. If any event processor modifies an event, synchronization with the Incident Management system/tool and any other event processors must occur.

2.3.3 Event Filtering

Filtering is defined as the process of blocking information based on a defined set of rules and standards. Filtering removes as much redundant and unnecessary data as possible.

The most difficult part of event filtering is to determine the correct data required to effectively configure Alert Notifications for an EMS. Many devices generate informational messages that are not indicative of problems. Sending these messages as events through the event processing hierarchy is not recommended because of the amount of processing power and bandwidth it takes to handle them. These messages also clutter operator consoles, possibly masking true problems.

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.

There are several ways to perform event filtering. Events can be prevented from ever entering the event processing hierarchy. This is referred to as filtering at the source. Event processors can discard or drop the unnecessary events. Likewise, consoles can be configured to hide them from view.

2.3.4 Alert Notification

Alert notification is the process of informing support personnel that an event has occurred. It is typically used to supplement the event processor’s primary console, not to replace it. Alert notification is useful in situations when the assigned person does not have access to the primary console, such as after hours, or when software licensing or system resource constraints prevent its use. It can also be helpful in escalating events that are not handled in a timely manner. Paging, e-mail, and pop-up windows are the most common means of notification.

Notification procedures are handled in different ways depending on the needs of the USMC. Three common notification methods are shown in Figure 3 and explained below.

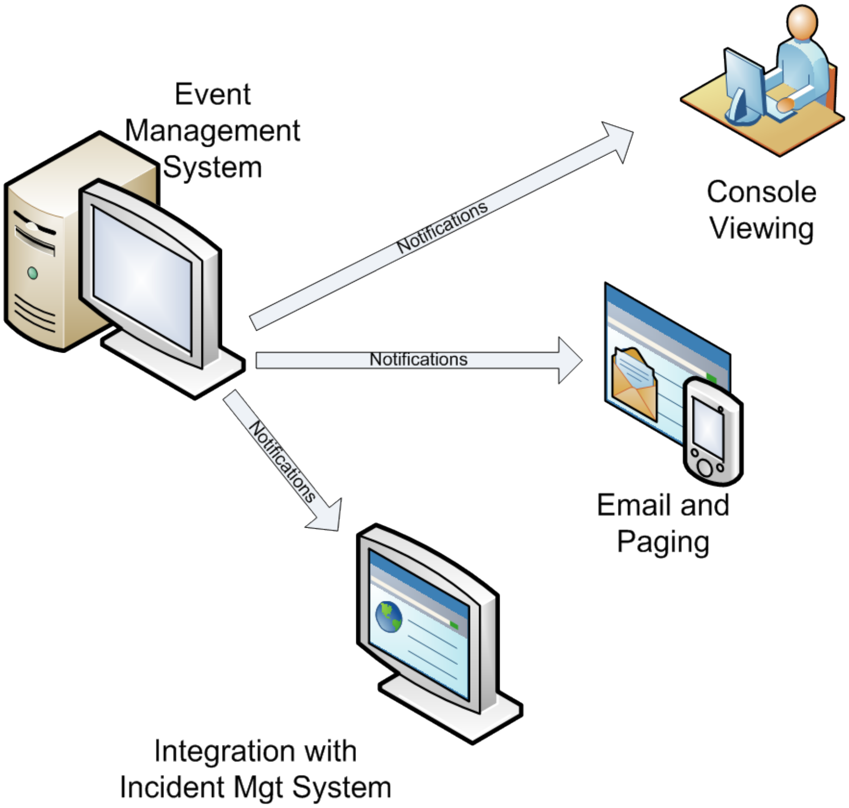


Figure 3 Event Management Notification Methods

- Console viewing by operators: Operators watch the console, looking for events that require action. When they see an event, they respond by taking action themselves or informing another person. Having operators view the console and then notify support teams provides the advantage of having someone verify events when they happen and notify the right person. The disadvantages include human error, for example missing an event on the console. The disadvantages also involve the costs of keeping and training a person to watch the console.
- Direct paging or e-mailing from the Event Management system/tool: Directly paging from the event processor, through scripts or executables that are triggered by criteria, eliminates the need for an operator to continuously watch the console. However, it is difficult to maintain the proper lists of which groups to notify for which problems. This information, already kept in the Incident Management system/tool, would need to be duplicated in the event processor. It is also difficult to track notifications or ensure they are received.
- Integration with an Incident Management system/tool for automatic notifications: The main advantage of integrating with an Incident Management system/tool is that there is a

tie-in with tools and processes that already exist within the organization at the help desk. It is much easier to track on-call lists and the right support groups for notifications. Timetables for notifications are also easier to create and maintain within Incident Management system/tools. It is also easier to assign each trouble ticket to the proper group based on information within each event. For example, if the Incident Management system/tool and Asset Management system are integrated, tickets can be automatically assigned to the proper support group based on the ownership of the asset ID or CI.

2.3.5 Event Escalation

Escalation is the process of increasing the severity of events to correct perceived discrepancies in their importance and to ensure appropriate and timely attention is received. An event, signifying a fault, is useless in managing IT resources if no action is taken to resolve it. An event processor can escalate the severity of an Event if it has not been acknowledged or closed within an acceptable time frame. Timers can be set to automatically increase the severity of an Event if it remains in an unacknowledged state. The higher severity event is highlighted to draw greater attention to it on the operator console.

Escalation in EM is handled differently from IM. An event escalation gives the most immediate alerting to IT Operations through more visibility. Severity in EM is similar to priority in IM. However, IM defines the sequence an incident is worked based on its priority whereas EM predefines the severity escalation of an event.

The USMC defines impact as the number of users affected. Criticality is more objective and can depend on a number of factors. When determining criticality, the following factors 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 a single service
    - Degraded service
    - Intermittent service

2.4 Relationships with other ITSM Processes

All IT Service Management processes are interrelated. EM is highly integrated with the IM, Problem Management (PbM) and Change Management (ChM) processes. Additionally, EM interfaces directly with Request Fulfillment (RqF) for specific service requests. EM provides notification to the Deployment Manager during Release and Deployment Management (RDM) regarding success, error, or failure of the deployment in production. EM notifies Service Catalog Management (SCM) regarding status of services listed as active in the Service Catalog.

The ITSM processes shown in the diagram below were selected due to the strength of the relationships and dependencies among them. While any one of the ITSM Processes can operate in the presence of an immature process, the efficiency and effectiveness of each is greatly enhanced by the maturity and integration of other ITSM Processes. Figure 4 depicts key direct or indirect relationships that exist between EM and some of the other ITSM processes.

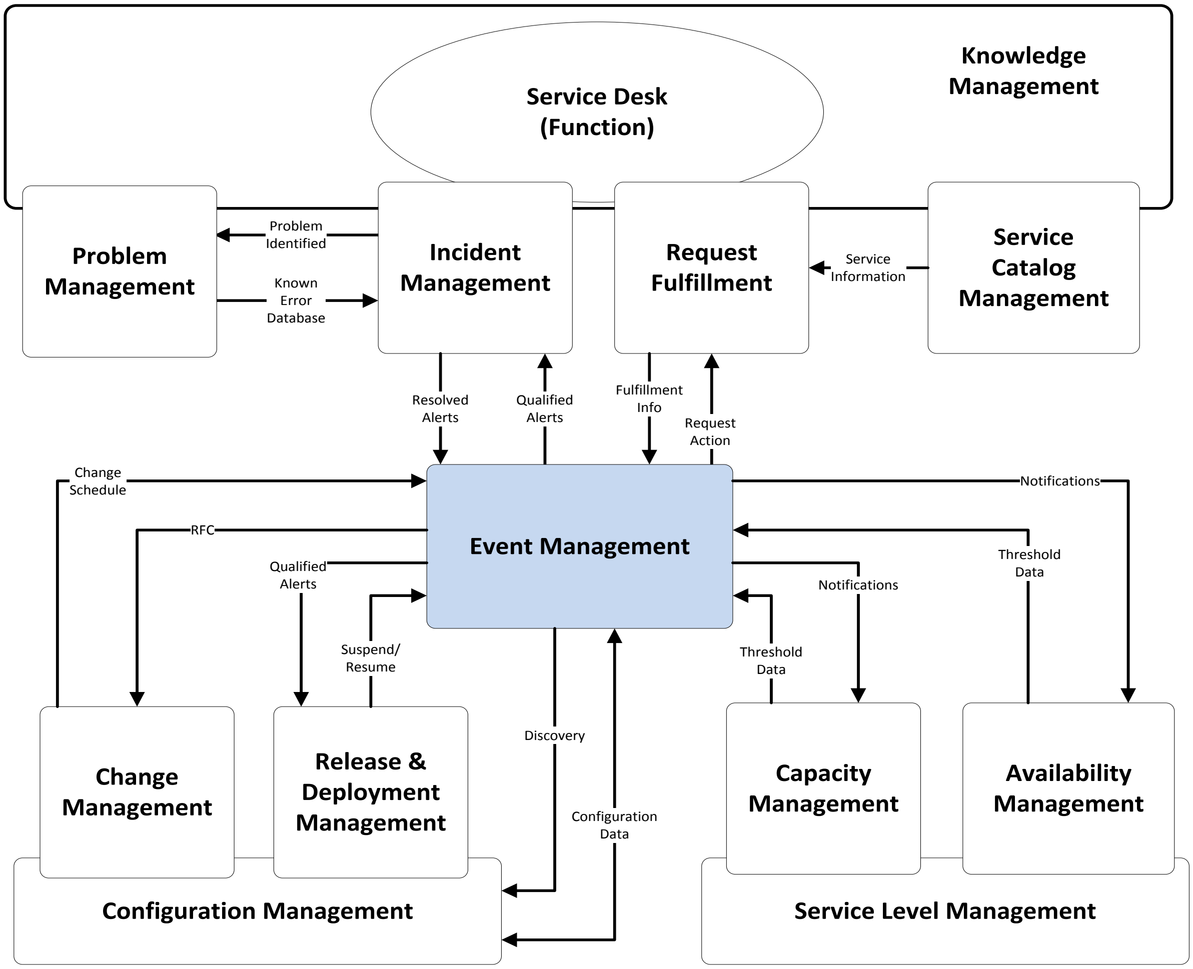


Figure 4 EM Relationships with other ITSM Processes

The following list describes the EM relationship (input or output) to other ITIL process areas, as depicted in the figure above:

Knowledge Management (KM)

- Knowledge Management does not directly interface with Event Management. However, Problem Management, Incident Management, Request Fulfillment, Service Catalog Management, and the Service Desk all receive information from EM. The KM System is updated as EM feeds information to these intermediary Processes.

Problem Management (PbM)

- Problem Management receives notification and trending data from EM for known Problem conditions, OLA/SLA, and Security breaches. New event conditions are normally forwarded to PbM by way of IM.

Incident Management (IM)

- Incident Management 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. Objectively known exceptions are automated to generate an Incident Record; while new conditions require human intervention to generate an Incident Record.

Request Fulfillment (RqF)

- Request Fulfilment receives notification from EM for Standard Service Requests found in the Service Catalog and new Service Requests that have yet to be categorized as Standard Service Offerings.

Service Catalog Management (SCM)

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

Change Management (ChM)

- Change Management receives notification from Event Management for Change/ Maintenance/Release Scheduling and Requests for Change based on predefined triggers.
- Change/Maintenance/Release Schedules: EM utilizes the Change/Maintenance/Release Schedules to prepare for the potential need to suspend and resume monitoring activities associated with changes that will impact any service attributes being monitored (e.g., availability, performance, capacity, etc.).
- Request for Change: EM will identify qualified event conditions that are not covered by known exceptions that will require a Request for Change (RFC) prior to the execution of corrective action.

Release and Deployment Management (RDM)

- Release and Deployment Management receives notification from EM for Change/Maintenance/Release Scheduling based on predefined triggers.
- Release and Deployment Management is in constant communication with EM to provide and update scheduled releases to the IT environment in an effort to prevent false alarms/alerts.
- Suspend/Resume: Release and Deployment Management 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 ensures that false Incidents are not triggered. RDM also notifies EM to resume monitoring once deployment activities have completed.

- Qualified Alert Conditions: EM notifies RDM about unusual events occurring during and after a release.

Capacity Management (CM)

- Capacity Management provides EM with predefined event conditions leveraged from operational metrics that are utilized for configuring monitoring thresholds. These thresholds are then leveraged for the development of event notification triggers. An event notification or alert occurs when established thresholds are breached.
- Capacity Management receives event notification or alerts from EM based on predefined event conditions that trigger an event notification.

Availability Management (AvM)

- Availability Management provides EM with predefined event conditions leveraged from operational metrics that are utilized for configuring monitoring thresholds. These thresholds are then leveraged for the development of an event notification trigger. An event notification or alert occurs when established thresholds are breached.
- Availability Management receives event notifications or alerts from EM based on predefined event conditions.

Configuration Management (CfM)

- Configuration Management 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 which are leveraged for the development of event notification triggers. Event Management 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.

Service Level Management (SLM)

- Configuration Management provides operational metrics that are leveraged in the development of thresholds to support monitoring and measuring SLAs. EM monitors these predefined thresholds for SLA performance and breaches.

2.5 Quality Control

2.5.1 Metrics, Measurements and Continual Process Improvement

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

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

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

2.5.2 Critical Success Factors with Key Performance Indicators

CSFs are defined as something that must happen if a process (or IT service) is to succeed. CSFs are process or service-specific goals that must occur. KPIs are the metrics used to measure process or service performance toward stated goals.

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

Table 3 EM 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

CSF #	Critical Success Factors	KPI #	Key Performance Indicators	Benefits
3	The event management 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

2.6 Governance

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

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

Enterprises have always strived for effective administration, direction and control. However, there is an increased focus on IT governance because of federal regulations related to privacy, antiterrorism, security, and other factors.

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

2.7 Roles and Responsibilities

Roles and responsibilities specifically to address Event Management Process activities include several key roles. These roles are critical for the success of the process to achieve effectiveness and efficiency.

EM 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 MCNOSC organization.

Management (i.e., responsibility) of a process may be shared; generally, a single manager exists at the MCNOSC and at each MITSC. There will be instances where roles are combined or a person is responsible for multiple roles. Factors such as Area of Responsibility (AOR), size of user base, and size of the process support team dictate exactly which roles require a dedicated person(s) and the total number of persons performing each role. This process guide defines all mandatory roles.

2.7.1 Roles

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

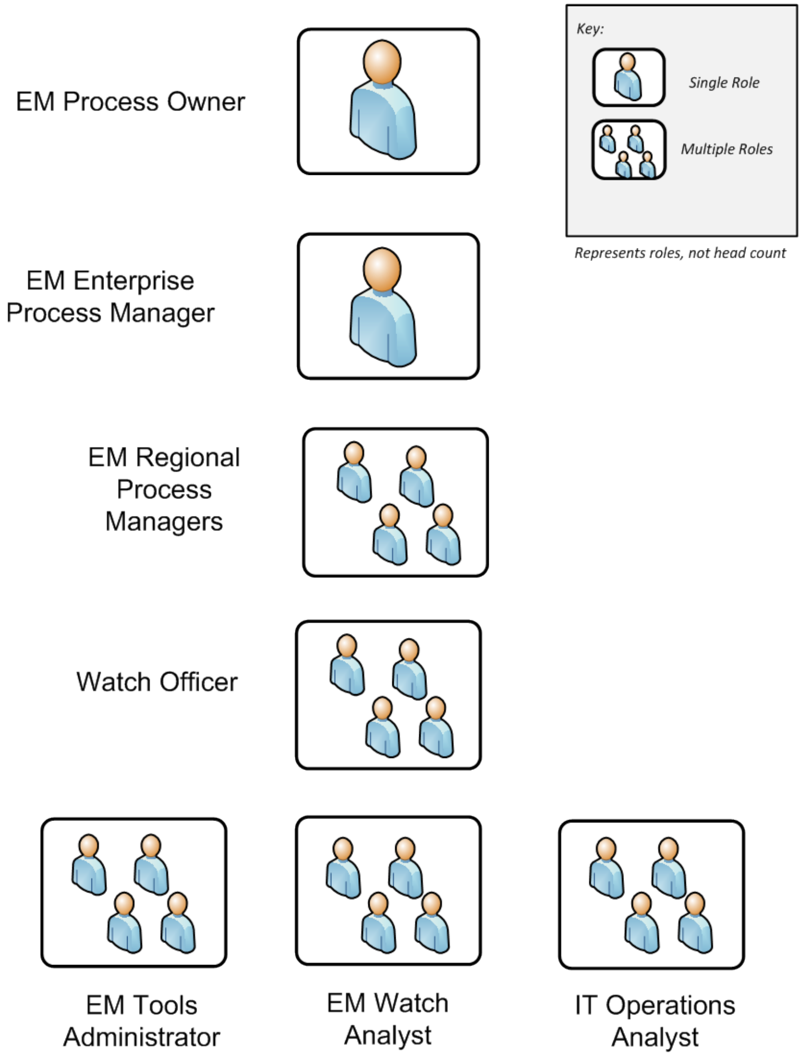


Figure 5 Event Management Roles

Table 4 describes EM roles and their responsibilities.

Table 4 EM Defined Roles and Responsibilitiesies

Description	Overall Responsibility
Role #1 EM Process Owner	
The Event Management 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 Event Management 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 Event Management 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 Enterprise Event Management Process Manager	
The Enterprise Process Manager is a pivotal role that performs day-to-day overall management of the process. The Process Manager ensures that all process activities are being performed and that they are staffed adequately and works with the customer to define requirements and receives 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 other EM 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 Event Management Process Managers	
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 per watch shift at the MCNOSC, each RNOSC,	• 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

and all MITSCs. RNOSC/MITSC EM Process Managers will coordinate EM Cyber Ops through the MCNOSC EM Managers to promote a unified approach to EM Cyber Ops.	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 Event Management Tools Administrator	
The Event Management Tools will be administered by the NETCOP group within the MCNOSC. 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 #5 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 MCNOSC, each RNOSC, and all MITSCs.	• Ensures the Event Management System is manned during all periods of operation • Provides management and oversight to the EM Analysts on duty • Oversees the monitoring of Event Consoles at the MCNOSC, RNOSCs, and MITSCs • Provides mentoring to the EM 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 MCNOSC, 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 #6 Event Management Watch Analysts	
Watch Analysts will monitor the EM console and address events/alerts within their respective AOR. It is recommended that an EM Watch Analyst be assigned at the MCNOSC, each RNOSC, and all MITSCs.	• Provides quality assurance checks on the workflows • Monitors Event Consoles at the MCNOSC, RNOSCs, MITSCs • Addresses actionable events within their AOR • 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 Area of Responsibility (AOR), the Technical Resources supported 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 tickets 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 • Views technical and role-based console messages

2.7.2 Responsibilities

Because processes may span departmental boundaries, procedures and work instructions 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, Participant (RASCI-P) model is a method for assigning the type or degree of responsibility that roles (or individuals) have for specific tasks.

- Responsible – Completes the process or activity; responsible for action/implementation. The degree of responsibility is determined by the individual with the ‘A’.
- Accountable – Approves or disapproves the process or activity. Individual who is ultimately answerable for the task or a decision regarding the task.
- 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.
- Participant –Assists “R” in the execution of the process and/or activity.

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

Table 5 Responsibilities for Enterprise EM

EM Process Activities	MCNOSC	HQMC (C4)	MCSC	MCCDC	RNOSC	MITSC	Base	Application Owner	Tenant/Supported Command
Event Notification Generated	AR	I	I	I	I	RS	RS	RS	I
Event Detected	AR				I	RS	RS	RS	I
Event Filtered	AR				I	RS	RS	RS	
Event Correlation	AR				I	RS	RS	RS	
Trigger	AR				I	RS	RS	RS	
Event Logged	AR				I	RS	RS	RS	I
Auto Response	AR				I	RS	RS	RS	
Alert	AR	I	I	I	I	RS	RS	RS	I
Human Intervention	AR				I	RS	RS	RS	I
Incident/ Problem/Change?	AR	I			I	RS	RS	RS	I
Review Actions	AR				S	RS	RS	RS	
Close Event	AR				S	RS	RS	RS	I

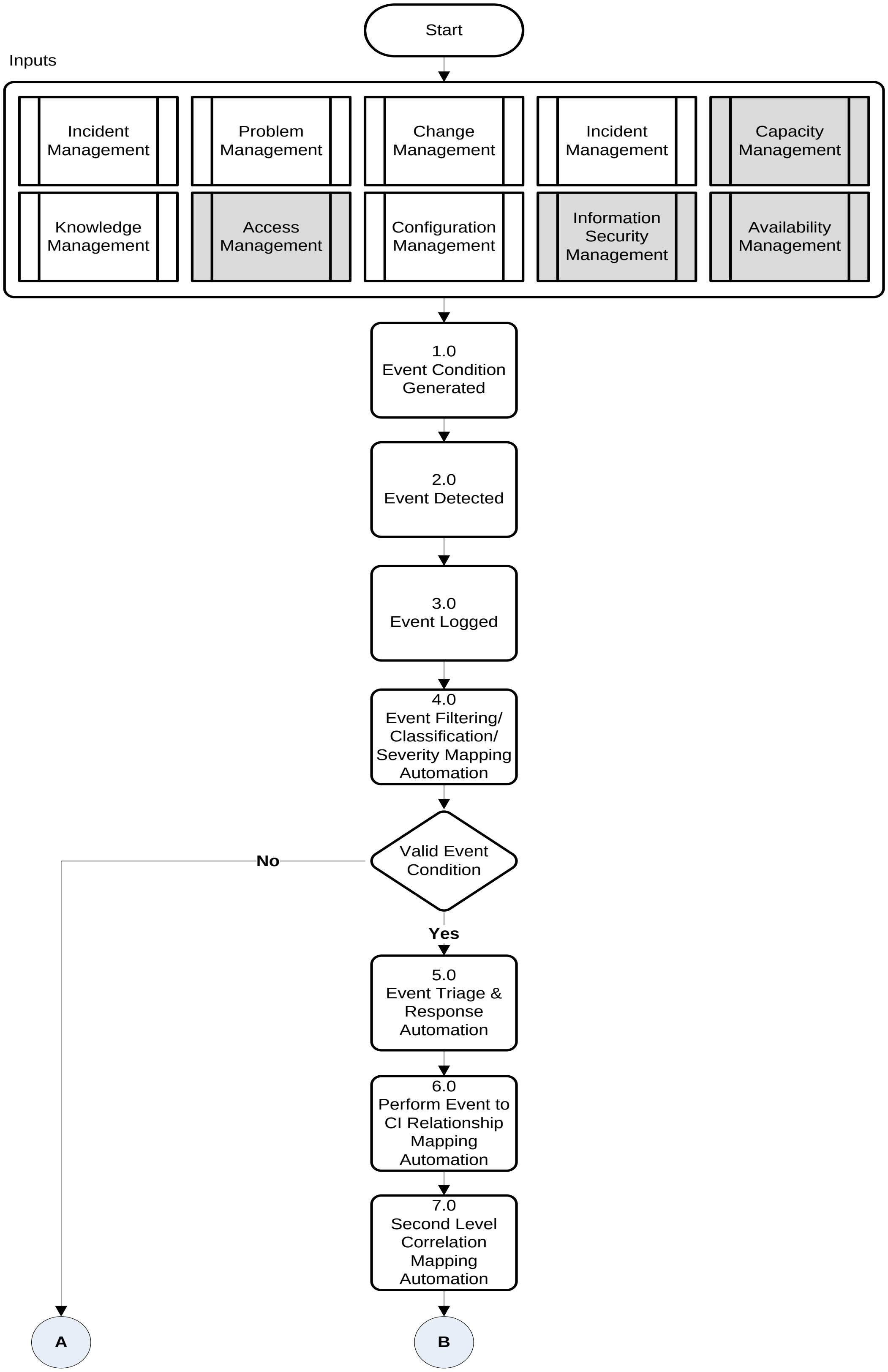
Legend:
Responsible (R) – Completes the process or activity
Accountable (A) – Authority to approve or disapprove the process or activity
Supporting (S) – Assists in execution of process or activity
Consulted (C) – Experts who provide input
Informed (I) – Notified of activities

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

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

3.0 Sub-Processes

The USMC EM process consists of twelve (12) sub-processes. While each Event will follow each sub-process on some level, not every activity within each sub-process is utilized for every USMC organization or type of Event. For example, Informational Events do not require Event Correlation or Trigger. Warning Events that are unique to a particular server do not utilize every phase or type of remediation associated with Auto Response and Alert. Therefore, to understand the USMC EM in its entirety, it is necessary to refer to the sub-process. Figure 6 depicts the overall flow of the EM System as well as the inputs and outputs to and from external processes. Shaded processes are shown because they are inter-related to EM, but do not specifically appear within the sub-processes.


Start
Inputs
Incident Management
Problem Management
Change Management
Incident Management
Capacity Management
Knowledge Management
Access Management
Configuration Management
Information Security Management
Availability Management
1.0 Event Condition Generated
2.0 Event Detected
3.0 Event Logged
4.0 Event Filtering/ Classification/ Severity Mapping Automation
Valid Event Condition
No
Yes
5.0 Event Triage & Response Automation
6.0 Perform Event to CI Relationship Mapping Automation
7.0 Second Level Correlation Mapping Automation
A
B

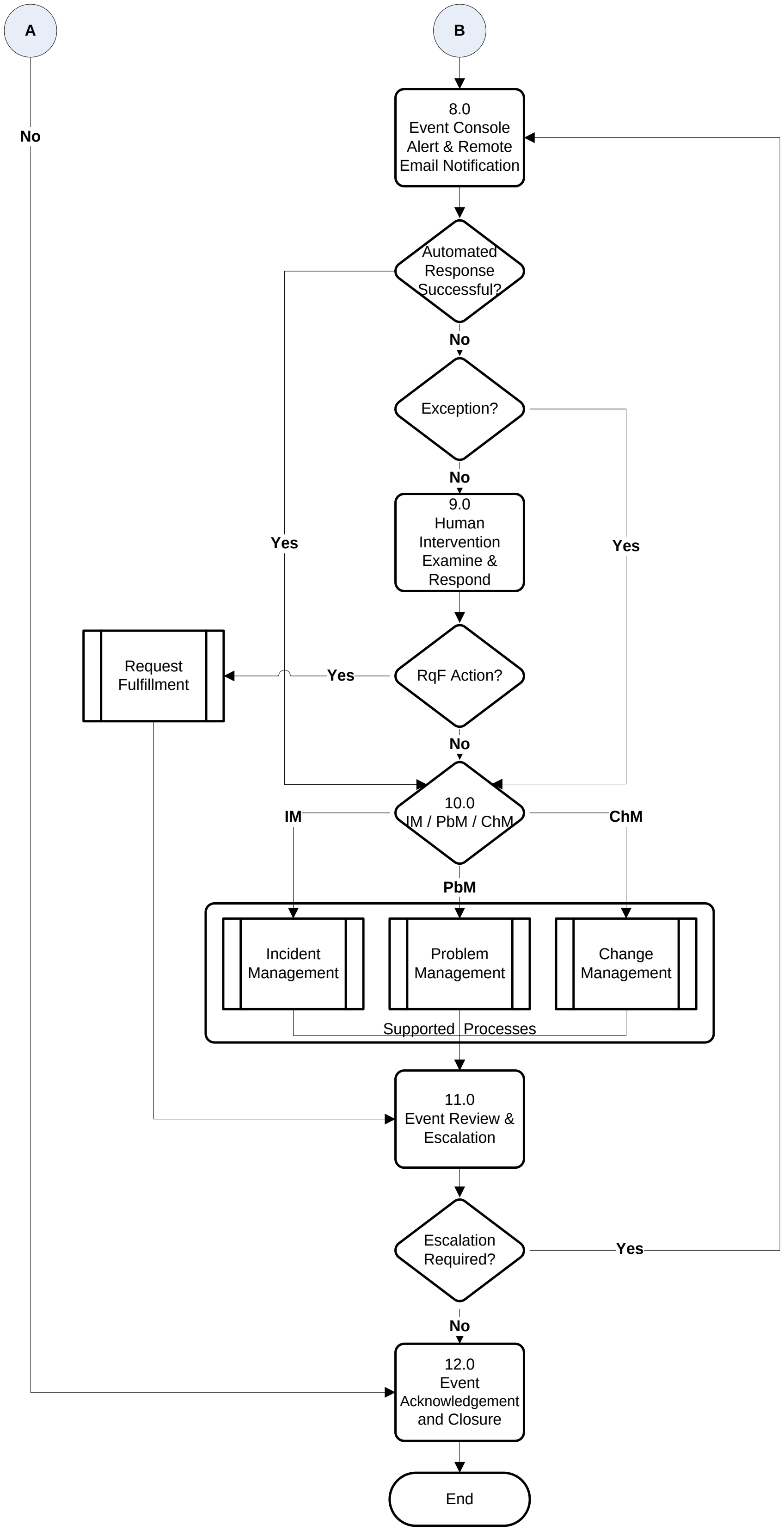


Figure 6 Event Management System Flow

3.1 Event Condition Generated

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

This first step in the EM workflow involves IT Operations Analysts working with the EM Tools Administrator to ensure Events are captured by the EMS. Each CI to be monitored will be configured to either actively or passively communicate its status to the EMS. It is this status that is displayed in the various Views.

Most CIs communicate information about themselves in at least one of two ways:

- The EMS tools poll the CI on a regular interval collecting certain data.
- CIs are configured to generate a notification when certain criteria are met.

Event generation and notifications can be proprietary, in which case only the manufacturer's management tools can be used to detect Events. Most CIs, however, generate Event conditions using an open standard such as SNMP.

Figure 7 depicts the Event Condition Generated sub-process.

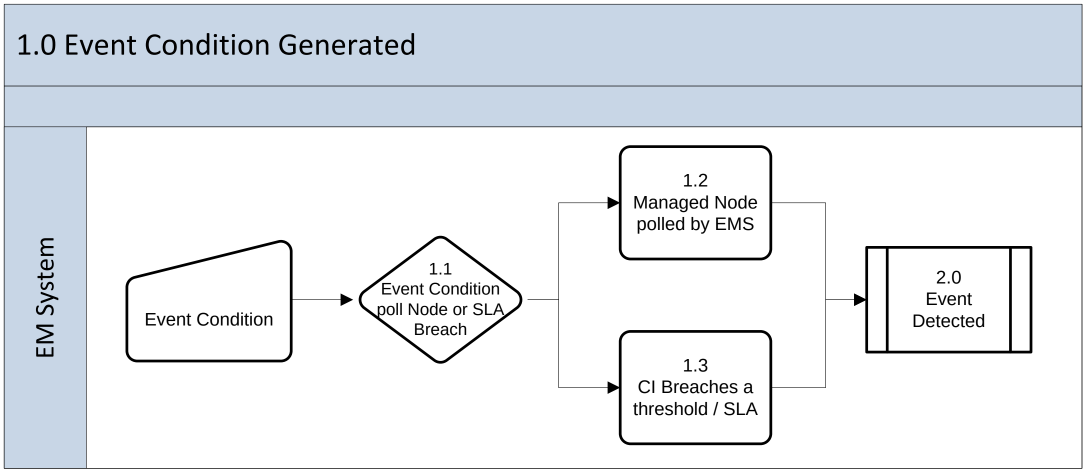

1.0 Event Condition Generated
EM System
Event Condition
1.1
Event Condition poll Node or SLA Breach
1.2
Managed Node polled by EMS
1.3
CI Breaches a threshold / SLA
2.0
Event Detected

Figure 7 Event Condition Generated

The Event Condition Generated sub-process is continuously polling CIs. While Events happen continuously, not all Event conditions are registered or reported to the EMS. Therefore, it is essential that all personnel involved in the design, development, support and operation of the IT infrastructure understand what type of Event condition signatures need to be monitored by the EMS.

Table 6 describes the Event Condition Generated sub-process steps.

Table 6 Event Condition Generated Sub-Process

1.0 Event Condition Generated		
Number	**Process Activity**	**Description**
1.1	Is Event Condition on EMS node or an SLA breach?	Determination is made on Event condition. If the Event is on an EMS polled node then proceed to 1.2. If the Event is an SLA breach then proceed to 1.3.
1.2	Managed Node polled by EMS	A device is monitored by the EMS, which collects a diverse scope of data metrics. This is often referred to as polling.
1.3	CI Breaches a threshold / SLA	Passive or Active polling of a CI reveals that a predetermined SLA threshold has been breached. This SLA breach generates an Event condition and triggers an alert notification.
2.0	Event Detected	Control is passed to 2.0; Event Detected.

3.2 Event Detected

When an Event condition is generated, it is detected by an agent or an agentless monitoring capability surveilling the system or the system transmits directly to the EM tool specifically designed to read and interpret the meaning of the Event condition.

Not all Event conditions are examined and escalated to the EMS. The IT Operations Analysts work with the Enterprise EM Tools Administrators to ensure the EMS is configured to monitor for actionable Event condition signatures to support cyber-operations.

Figure 8 depicts the EMS Event Detected sub-process.

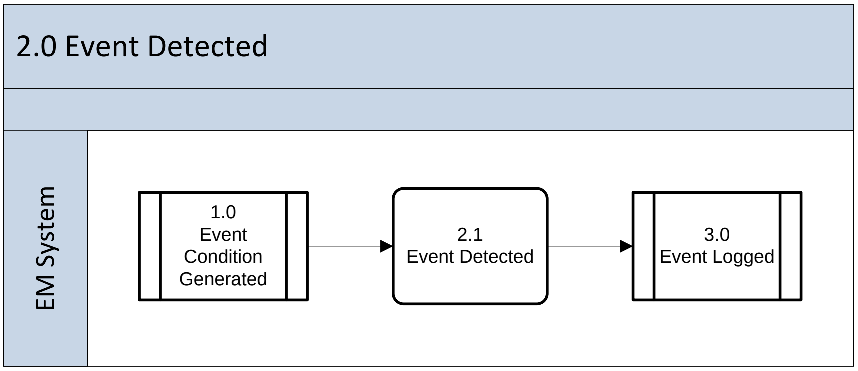


Figure 8 Event Detected

Table 7 describes the Event Detected sub-process steps.

Table 7 Event Detected Sub-Process

2.0 Event Detected		
Number	**Process Activity**	**Description**
2.1	Event Detected	The Local EMS detects an Event condition generated by a CI.
3.0	Event Logged	Control is passed to 3.0; Event Logged.

3.3 Event Logged

All Event conditions are logged within the local EMS and only actionable Event Conditions are forwarded to the Manager of Managers (MoM) or Enterprise EMS.

Event Logs are available as needed for trending data, security research, problem research, and reporting.

The Event Logged sub-process is defined in Figure 9 below.

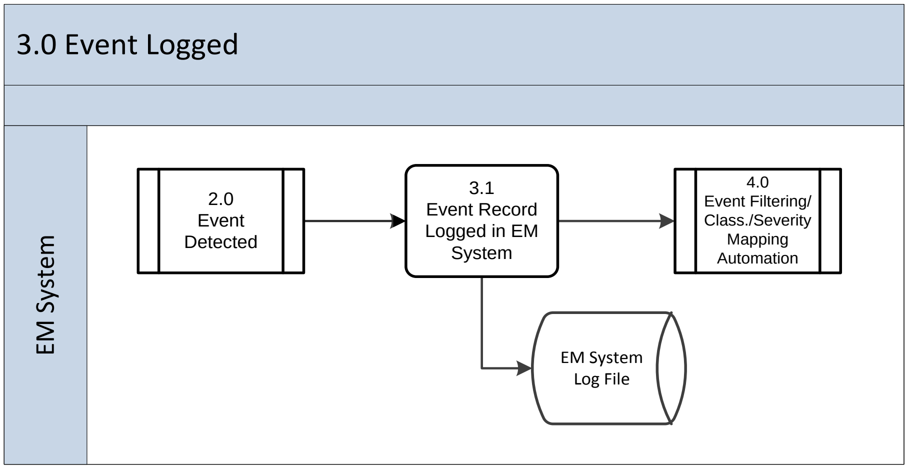

3.0 Event Logged
EM System
2.0 Event Detected
3.1 Event Record Logged in EM System
4.0 Event Filtering/ Class./Severity Mapping Automation
EM System Log File

Figure 9 Event Logged

Table 8 describes the Event Logged sub-process steps.

Table 8 Event Logged Sub-Process

3.0 Event Logged		
Number	**Process Activity**	**Description**
3.1	Event Record Logged into EM System	The EMS tool will log all captured Events within the logging database. The contents of the log file will vary depending on the Event Condition.
4.0	Event Filtering / Classification / Severity Mapping Automation	Control is passed to 4.0; Event Filtering / Classification / Severity Mapping Automation.

3.4 Event Filtering / Classification / Severity Mapping Automation

A significant challenge within EM is establishing the correct level of Event filtering. Establishing an effective Event filtering strategy is a critical success factor to the Enterprise Event Management Process. A poorly configured EMS will inundate Operations Analysts with an unmanageable amount of information. This flood of information will conceal critical actionable Event conditions causing an "alert storm." Figure 10 depicts the Event Filtering / Classification / Severity Mapping Automation sub-process.

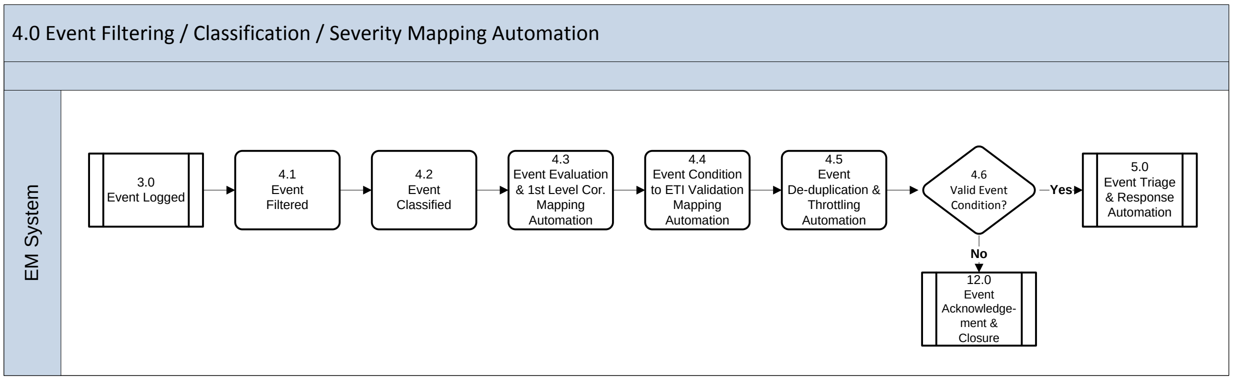

4.0 Event Filtering / Classification / Severity Mapping Automation
EM System
3.0 Event Logged
4.1 Event Filtered
4.2 Event Classified
4.3 Event Evaluation & 1st Level Cor. Mapping Automation
4.4 Event Condition to ETI Validation Mapping Automation
4.5 Event De-duplication & Throttling Automation
4.6 Valid Event Condition?
Yes
5.0 Event Triage & Response Automation
No
12.0 Event Acknowledge-ment & Closure

Figure 10 Event Filtering / Classification / Severity Mapping Automation

Table 9 describes the Event Filtering / Classification / Severity Mapping Automation sub-process steps.

Table 9 Event Filtering / Classification / Severity Mapping Automation Sub-Process

4.0 Event Filtering / Classification / Severity Mapping Automation		
Number	**Process Activity**	**Description**
4.1	Event Filtered	Event Filtering is the activity of the EM process that supports two possible outcomes: either to 1) communicate and pass the Event to the next activity for the determination of significance, or to 2) ignore, suppress, and close the Event.
4.2	Event Classified	Events are classified into one of five key categories. See the HP Operations Manager Classifications Chart below.
4.3	Event Evaluation and First Level Correlation Mapping Automation	The local EM system(s), referred to as an "Aggregator," evaluates the Event and determines if this new Event relates to one previously identified.
4.4	Event Condition to Event Type Indicators (ETI) Validation Mapping Automation	Event conditions are compared against the ETIs for validity. Examples of valid ETIs include: Known issue, Infrastructure Problem, Minor, Major, Reoccurrence, Critical and Noise.
4.5	Event Deduplication & Throttling Automation	The Aggregator determines if the new Event is a duplicate of an existing Event condition already identified.
4.6	Valid Event Condition	Determination if the Event Condition meets the criteria outlined within the ETI's.
5.0	Event Triage and Response Automation	If the condition is met, control is passed to 5.0, Event Triage and Response Automation.
12.0	Event Acknowledgement and Closure	If the condition is not met, control is passed to 12.0, Event Acknowledgement and Closure.

The HP Operations Manager Classifications for Events are displayed in Table 10.

Table 10 HP Operations Manager Classifications

Icon	Description	Status Name	Numerical Code	Definition
✖	Red circle with "X"	Critical	0	The measurement calculated for the Key Performance Indicator (KPI) that fell within the value range for the Critical threshold.
⚠	Orange Triangle with exclamation mark	Major	5	The measurement calculated for the KPI that fell within the value range for the Major threshold.
⚠	Yellow Triangle with exclamation mark	Minor	10	The measurement calculated for the KPI that fell within the value range for the Minor threshold.
⚠	Aqua triangle with exclamation mark	Warning	15	The measurement calculated for the KPI that fell within the value range for the Warning threshold.
✅	Green circle with check mark	OK	20	The measurement calculated for the KPI that fell within the value range for the OK threshold.
ℹ	Dark blue circle with lowercase i	Informational	-1	The KPI has a value and no status. The reason is that the KPI's thresholds have not yet been specified. For details on setting the thresholds, see How to Define Thresholds for KPIs and Health Indicators (HI) in the BSM Application Administration Guide.

3.5 Event Triage and Response Automation

Triage is the process of sorting, categorizing, correlating, prioritizing, and assigning incoming events, incidents, vulnerability reports, and other general information requests.

Triage is an essential element of any Event Management capability and is on the critical path for understanding what is being reported throughout the organization. It serves as the vehicle by which all information flows into a single point of contact, allowing for an enterprise view of ongoing activity and a comprehensive correlation of all reported data. Triage allows for an initial assessment of an incoming Event and queues it for further handling. It also provides a venue for beginning the initial documentation and data entry of a report or request, if this has not already been done in the Detect process.

The triage function provides an immediate snapshot of the current status of all activity reported — what reports are open or closed, what actions are pending, and how many of each type of report has been received. This process can help to identify potential security problems and prioritize the workload. Information gathered during triage can also be used to generate vulnerability and incident trends and statistics for upper management. Triage can be of particular importance when an emergency request occurs, as triage can elevate the priority of an Event, escalate the handling of the Event, and notify relevant parties and stakeholders, especially in the case of a critical or major Event.

Figure 11 depicts the Event Triage and Response Automation Process.

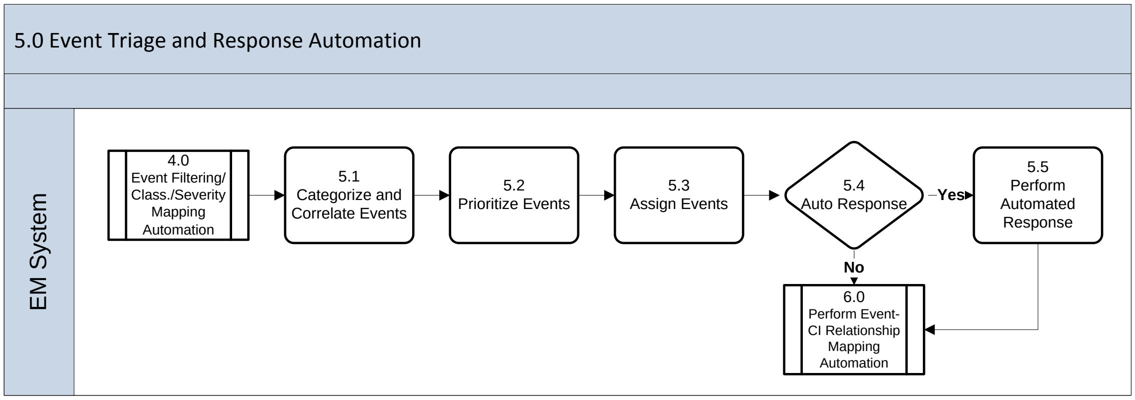

5.0 Event Triage and Response Automation
EM System
4.0 Event Filtering/ Class./Severity Mapping Automation
5.1 Categorize and Correlate Events
5.2 Prioritize Events
5.3 Assign Events
5.4 Auto Response
Yes
5.5 Perform Automated Response
No
6.0 Perform Event-CI Relationship Mapping Automation

Figure 11 Event Triage and Response Automation

Table 11 describes the Event Triage and Response Automation sub-process steps.

Table 11 Event Triage and Response Automation Sub-Process

5.0 Event Triage and Response Automation		
Number	**Process Activity**	**Description**
5.1	Categorize and Correlate Events	Using predefined criteria, incoming Events are classified. If an Event is determined to be part of an ongoing incident, its priority and assignment may be automatically set to be the same as that incident. In this case, the correlation actually impacts and affects the categorization, priority, and assignment of the Event.
5.2	Prioritize Events	The system analyzes the Event to determine the level of priority. This prioritization can be determined by a number of pre-defined factors such as number of users affected, down time of the service, or multitude of factors.
5.3	Assign Events	Because Event Management provides the ability to detect incidents early, an organization can configure technology to support an Event Management process to trigger an incident or automated response. Assignment business rules are specialized business rules that search for conditions and then run an assignment script. This is used to auto-assign tasks to appropriate parties or run an automated script that attempts to resolve the Event.
5.4	Auto Response	If the system has determined that an auto-response is available for the Event, control passes to 5.5. If an auto-response is not available then control passes to 6.0; Perform Event to CI Relationship Mapping Automation.
5.5	Perform Automated Response	The EMS will initiate a predetermined automated response for the applicable Event condition; examples of which can include scripts, batch files or the re-start of a stopped service.
6.0	Perform Event to CI Relationship Mapping Automation	Control is passed to 6.0; Perform Event to CI Relationship Mapping Automation after either 5.4 or 5.5.

3.6 Perform Event to CI Relationship Mapping Automation

The Event to CI relationship mapping supports identifying the device information, physical location, and owner of the asset.

Prior to this step, only the Internet Protocol (IP) information and asset name were available to the Event. By mapping this information to the corresponding record within the global CMDB, all available information regarding the asset causing the alert becomes available.

This information is critical in the creation of support tickets and requests created downstream and passed to supporting processes outside of Event Management.

Figure 12 depicts the Perform Event to CI Relationship Mapping Automation.

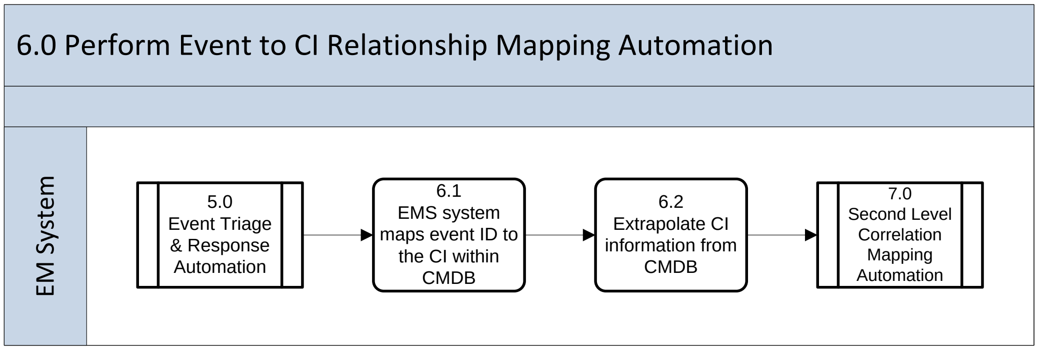

6.0 Perform Event to CI Relationship Mapping Automation
EM System
5.0 Event Triage & Response Automation
6.1 EMS system maps event ID to the CI within CMDB
6.2 Extrapolate CI information from CMDB
7.0 Second Level Correlation Mapping Automation

Figure 12 Perform Event to CI Relationship Mapping Automation

Table 12 describes the Perform Event to CI Relationship Mapping Automation sub-process steps.

Table 12 Perform Event to CI Relationship Mapping Automation Sub-Process

6.0 Perform Event to CI Relationship Mapping Automation		
Number	**Process Activity**	**Description**
6.1	EMS system maps Event ID to the CI within CMDB	Using the IP address and asset name from the Event record, the EMS maps the Event ID to the CI ID of the asset within the CMDB.
6.2	Extrapolate CI information from CMDB	The data contained within the CMDB pertaining to the CI, such as location, asset owner, nomenclature, etc.; are made available to the Event record for potential inclusion in Incident, Problem, or Change records that may be created downstream in supporting process.
7.0	Second Level Correlation Mapping Automation	Control is passed to 7.0; Second Level Correlation Mapping Automation.

3.7 Second Level Correlation Mapping Automation

The correlation engine, which is a component of monitoring software tools, is programmed to compare the Event with business rules and to initiate changes or alert Event and IT Operations Analysts to the Event that needs attention.

It is the Event Correlation engine that eliminates false positive messages through impact and root cause analysis. Rules, models and policy-based correlation technologies derive and isolate the true cause and impact as well as provide data for meaningful reports. Multiple monitoring and managing tools will each have a correlation engine.

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

The EMS performs Event Correlation within the tools except for initial setup and minor maintenance changes when correlation rules are established through software wizards. Input to Event Correlation comes when Event Filtered shows a significance of Warning and/or Exception. The Second Level Correlation Mapping Automation sub-process contains the most important activities necessary for successful Event Management.

Figure 13 depicts the Second Level Correlation Mapping Automation sub-process.

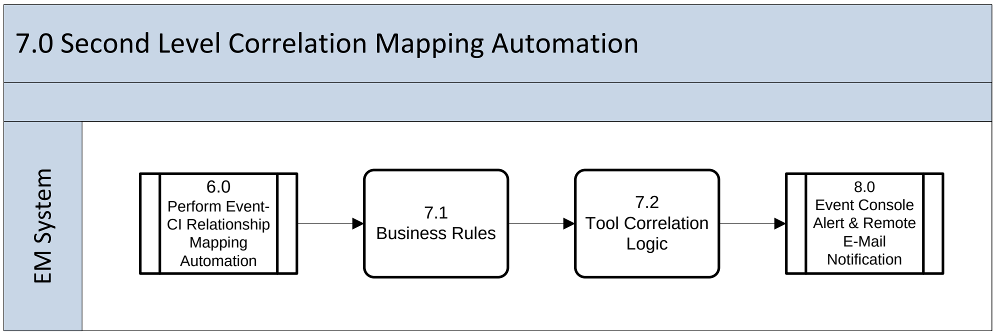

7.0 Second Level Correlation Mapping Automation
EM System
6.0 Perform Event-CI Relationship Mapping Automation
7.1 Business Rules
7.2 Tool Correlation Logic
8.0 Event Console Alert & Remote E-Mail Notification

Figure 13 Second Level Correlation Mapping Automation

A description of each activity is included in Table 13 below.

Table 13 Second Level Correlation Mapping Automation

7.0 Second Level Correlation Mapping Automation		
Number	**Process Activity**	**Description**
7.1	Business Rules	Business Rules outline predetermined logic to support SLA and Event Handling conditions.
7.2	Tool Correlation Logic	This is a search for Events related to the root Event causing the service impacts. These are not duplicate Events; duplicates have already been filtered out. These are Events that share the same infrastructure service impact. These Events are correlated and related to the root Event so that when one is addressed, they are all addressed. If this Event is related to the same infrastructure service impact as another Event, this Event is correlated with the master Event. The root Event serves as the primary record of the service impact to be resolved and this Event is recorded with the root Event.
8.0	Event Console Alert and Remote Email Notification	Control is passed to 8.0; Event Console Alert and Remote Email Notification.

3.8 Event Console Alert and Remote Email Notification

The purpose of alerts is to ensure the personnel with the appropriate skills are notified so they can resolve the Event conditions. Alerts contain all the information necessary for those personnel to determine the appropriate action. It is important to note that this is not the same as the functional escalation of an incident, where the emphasis is on restoring service within an agreed time and may require a variety of activities. In addition, if correlated Events determine a master Event should be escalated, it is escalated through an alert. Alerts that require Human Intervention in the workflow also require manual acknowledgement. These alerts require personnel to perform specific actions to resolve the Event Condition on a particular CI. Figure 14 depicts the Event Console Alert and Remote Email Notification.

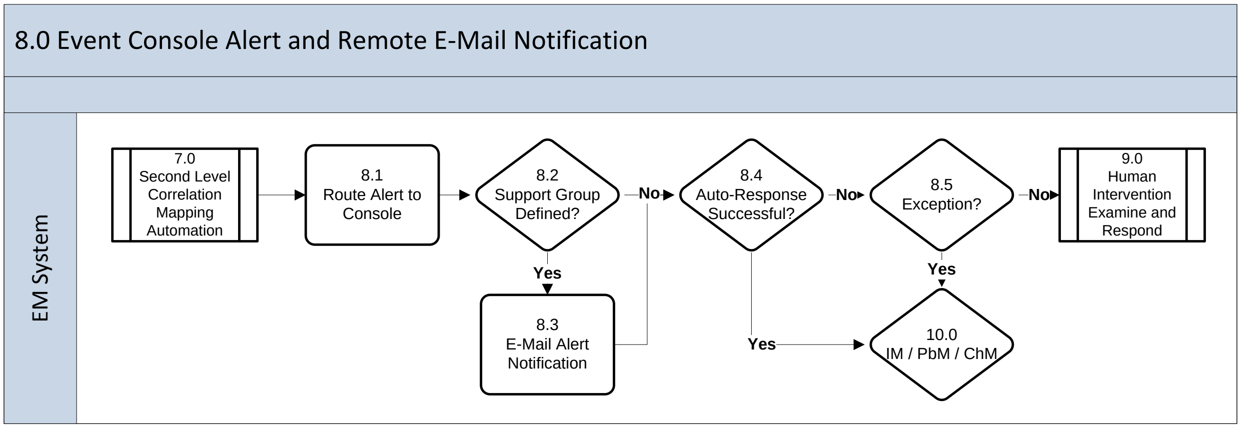

8.0 Event Console Alert and Remote E-Mail Notification
EM System
7.0 Second Level Correlation Mapping Automation
8.1 Route Alert to Console
8.2 Support Group Defined?
No
8.4 Auto-Response Successful?
No
8.5 Exception?
No
9.0 Human Intervention Examine and Respond
Yes
8.3 E-Mail Alert Notification
Yes
Yes
10.0 IM / PbM / ChM

Figure 14 Event Console Alert and Remote Email Notification

Table 14 describes the Event Console Alert and Remote Email Notification steps.

Table 14 Event Console Alert and Remote Email Notification Sub-Process

8.0 Event Console Alert & Remote Email Notification		
Number	**Process Activity**	**Description**
8.1	Route Alert to Console	The EMS displays the Alert on the Monitoring screen.
8.2	Support Group Defined	The data collected in the CMDB is used to identify the appropriate support group in Remedy.
8.3	E-mail Alert Notification	The appropriate support group responsible for the CI is sent an email alert notification based on business rules.
8.4	Automated Response Successful	The system validates the automated response(s) in 8.4. If the automated response is successful, control passes to 10.0. If an exception is detected the control passes to 9.0.
8.5	Exception	The system validates whether the Event meets the predetermined criteria for a known exception (Re-occurring Incidents, Problems or Changes) and passes control to 10.
9.0	Human Intervention Examine and Respond	Control is passed to 9.0, Human Intervention Examine and Respond.
10.0	IM / PbM / ChM (Other Processes)	Control is passed to 10.0, IM / PbM/ ChM (Other Processes).

3.9 Human Intervention Examine and Respond

Alert notifications are presented to the EMS console where Human Intervention begins to assess the Event condition. Human intervention is critical during initial implementation 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, the USMC requires human intervention to prevent false-positives from initiating incorrect automated responses. When EM tools have proven accurate and effective, more Events move from 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 Other Processes (Incident, Problem, or Change). The details of the Human Intervention Examine and Respond activity are shown in Figure 15 below.

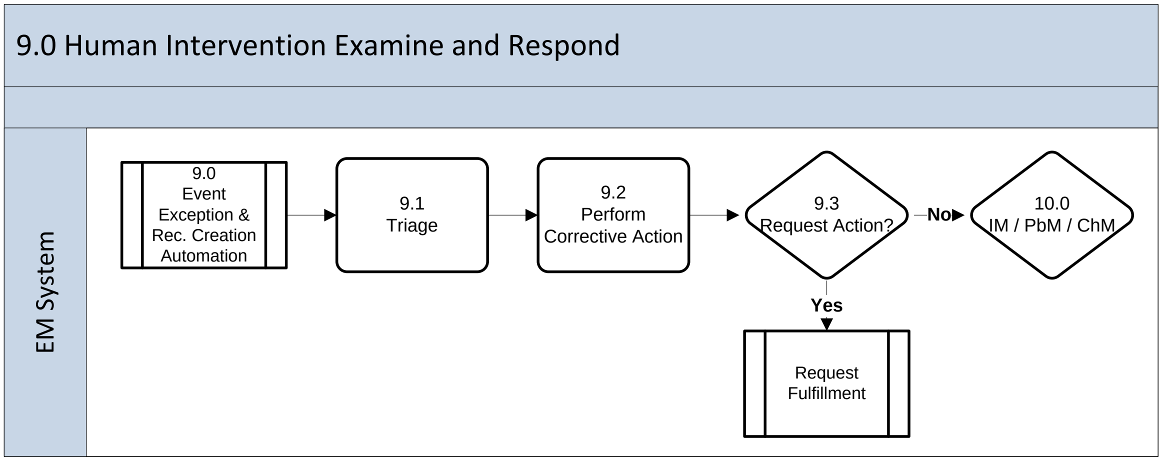

9.0 Human Intervention Examine and Respond
EM System
9.0 Event Exception & Rec. Creation Automation
9.1 Triage
9.2 Perform Corrective Action
9.3 Request Action?
No
10.0 IM / PbM / ChM
Yes
Request Fulfillment

Figure 15 Human Intervention Examine and Respond Sub-Process

The Human Intervention Examine and Respond sub-process is explained in Table 15 below.

Table 15 Human Intervention Examine and Respond Sub-Process Descriptions

9.0 Human Intervention Examine and Respond		
Number	**Process Activity**	**Description**
9.1	Triage	The Operations Analyst, Level 1 support, performs analysis of the Event to ascertain whether it meets the requirements for Service Request, Incident, Problem, or Change Record.
9.2	Perform Corrective Action	The Operations Analyst will either create a Service Request, Incident, Problem, or Change record.
9.3	Request Action	Determine if criteria are met to pass control to Request Fulfillment. If not, control passes to 10.0 – Other Processes.
10.0	Other Processes	Control is passed to 10.0 (IM / PbM / ChM [Other Processes]) if Request Fulfillment is not engaged.

3.10 IM / PbM / ChM (Other Processes)

Event Management is a prime example of interaction and integration with the other IT Service Management processes. When an Event cannot be resolved, it is escalated to one or more of the other processes, sometimes to multiple processes. For example, a non-critical server failure is logged as an incident and an emergency RFC is logged to relocate the workload to an alternate server until it is resolved.

The description of opening RFCs and incidents is below.

Correlation identifies that a change is needed: The Event Correlation activity determines that the appropriate response to an Event is for something to be changed. For example, a performance threshold has been reached and a parameter on a major server needs to be tuned. An RFC is opened through Human Intervention. An unauthorized configuration change is detected as occurring on a router and must be reset or approved.

Open an Incident Record: As with an RFC, an incident can be generated when the Correlation Engine determines that a specific type or combination of Events represents an incident. The Operations Analyst ensures that when an incident record is opened, as much information as possible is included – with links to the Events concerned and, if possible, a completed diagnostic script.

Figure 16 describes the IM / PbM / ChM sub-process.

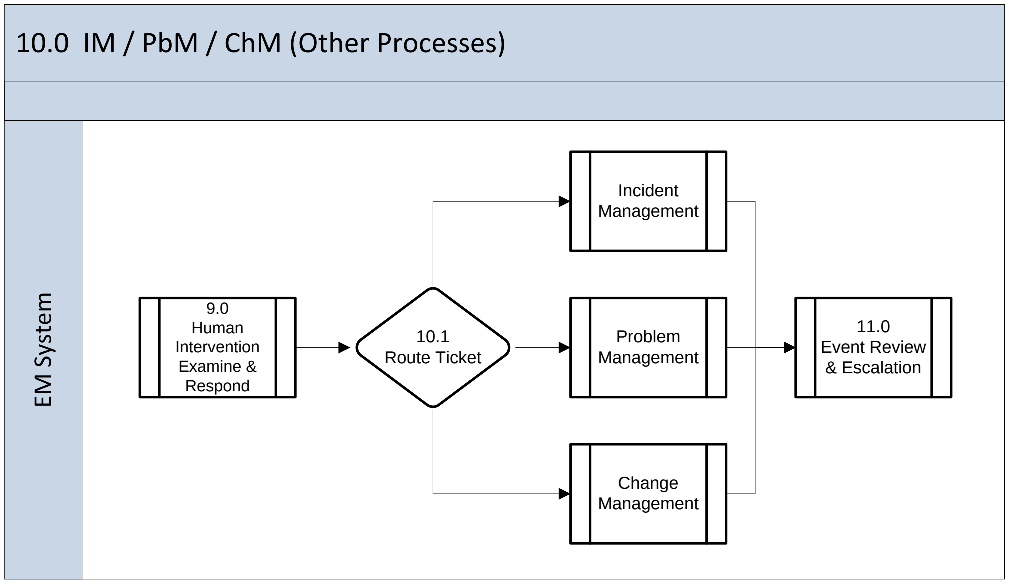

10.0 IM / PbM / ChM (Other Processes)
EM System
9.0 Human Intervention Examine & Respond
10.1 Route Ticket
Incident Management
Problem Management
Change Management
11.0 Event Review & Escalation

Figure 16 IM / PbM / ChM 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.

The IM / PbM / ChM sub-process is explained in Table 16 below.

Table 16 IM / PbM / ChM Sub-process Descriptions

10.0 IM / PbM / ChM (Other Processes)		
Number	**Process Activity**	**Description**
10.1	Route IM / PbM / ChM	The Condition and supporting information is routed to Incident, Problem or Change appropriately. The condition under which an Event is escalated varies and is unique to the KPIs and thresholds designed into the system.
11.0	Event Review and Escalation	Control is passed to 11.0; Event Review and Escalation.

3.11 Event Review and Escalation

Although it is not possible to formally review every individual Event, it is important to check that any significant Events or exceptions have been handled appropriately, or to track trends or counts of Event types. This can be done automatically, for example polling a server that had been rebooted using an automated script to see that it is functioning correctly.

Where Events have initiated an incident, and/or change, the Review Action does not duplicate any reviews that are done as part of those processes. Rather, the intent is to ensure that the handover between EM and other processes takes place as designed and that the expected action did indeed take place. This ensures that incidents or changes originating within Operations Management do not get lost between the teams or departments.

Review Actions are used as input into continual improvement and the evaluation and audit of the EM process.

The Review Actions sub-process is initiated after the Event has cleared all previous processes.

Figure 17 depicts the Event Review and Escalation sub-process.

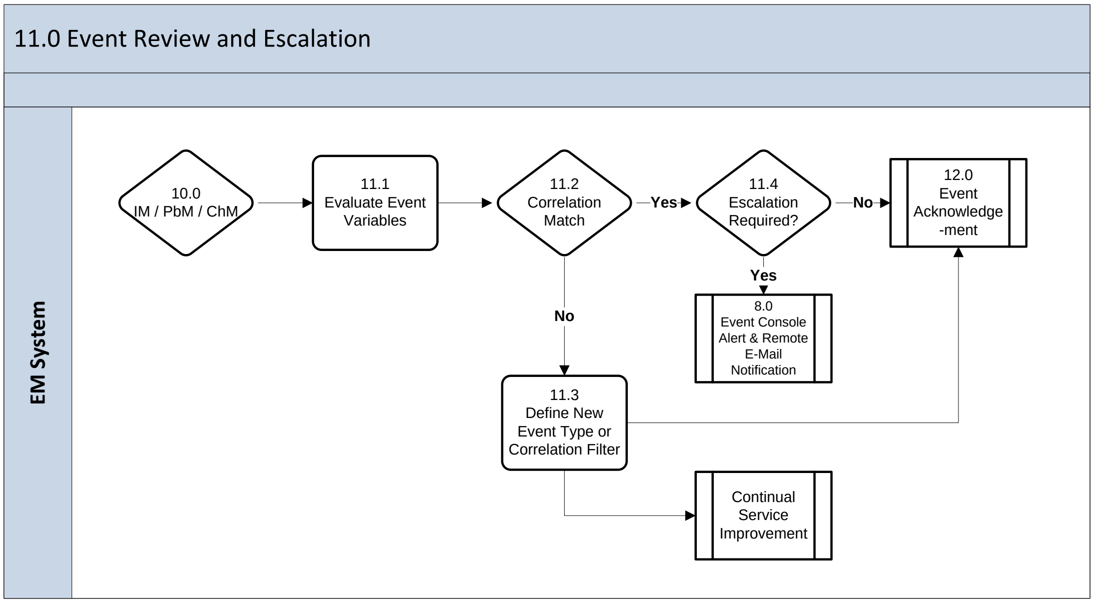

11.0 Event Review and Escalation
EM System
10.0
IM / PbM / ChM
11.1
Evaluate Event Variables
11.2
Correlation Match
Yes
11.4
Escalation Required?
No
12.0
Event Acknowledge -ment
Yes
8.0
Event Console Alert & Remote E-Mail Notification
No
11.3
Define New Event Type or Correlation Filter
Continual Service Improvement

Figure 17 Event Review and Escalation

Informational Events are logged and used as input to other processes, such as Backup, Capacity, and Storage Management.

There are two main steps in Review Actions:

1. Check whether handover of Events to Incident/Problem/Change Management resulted in the expected action.
2. Make sure that Event logs are analyzed in order to identify trends or patterns that suggest corrective action must be taken.

Table 17 below describes the Event Review and Escalation sub-process steps.

Table 17 Event Review and Escalation Sub-Process Descriptions

11.0 Event Review and Escalation		
Number	**Process Activity**	**Description**
11.1	Evaluate Event Variables	Review Event condition to ensure proper Event handling. • Verify Event Condition • Verify Event Correlation • Verify Event Status • Verify Event Ownership • Verify Event Routing • Verify Event to Service Request, Incident, Problem, Change Record relationship
11.2	Correlation Match	Reviewed Event to ensure proper correlation match with the appropriate Event Type Indicator (ETI) or Correlation Filter.

11.0 Event Review and Escalation		
Number	**Process Activity**	**Description**
11.3	Define New Event Type or Correlation Filter	If the Event condition does not match pre-defined ETIs or correlation filters, define a new ETI or correlation filter by submitting a Change Request.
11.4	Escalation Required?	A check is made to determine if the Event needs to be Escalated. If so, control is passed to 8.0.
12.0	Event Acknowledgement and Closure	Control is passed to 12.0; Event Acknowledgement and Closure.

3.12 Event Acknowledgement and Closure

Events are not “opened” or “closed” in the dictionary definition sense. Rather, Events “occur.”

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.

It is optimal that devices in the infrastructure produce “open” and “closed” Events in the same format and specify the change of status. This allows the correlation step in the process to easily match open and closed notifications.

Events that have Human Intervention are checked to see if they were handled appropriately.

In the case of Events that generated an Incident, Problem, or Change, these are formally closed with a link to the appropriate record from the other process.

Figure 18 depicts the Event Acknowledgement and Closure sub-process.

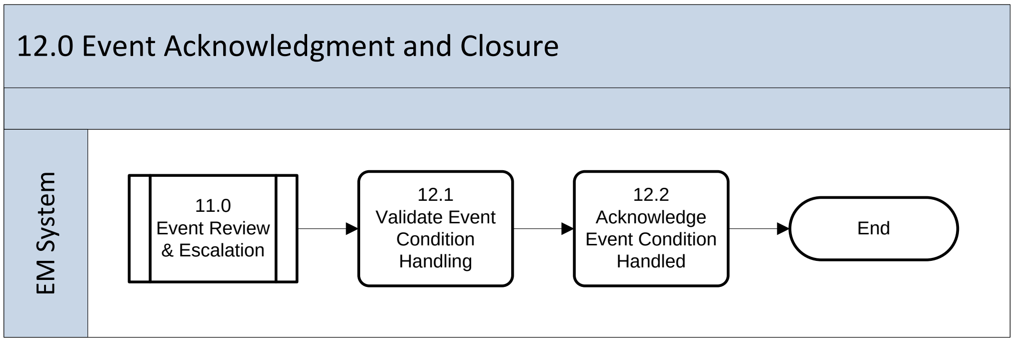


Figure 18 Event Acknowledgement and Closure

Table 18 describes the Event Acknowledgement and Closure sub-process steps.

Table 18 Event Acknowledgement and Closure Sub-Process Descriptions

12.0 Event Acknowledgement and Closure		
Number	**Process Activity**	**Description**
12.1	Validate Event Condition Handled	Even though the EM Console(s) should re-set to show the Event has cleared, administrators cannot assume that has happened and, at times, may be required to validate that the Event is truly cleared.
12.2	Acknowledge Event Condition Handled	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 working. The EM Tool correlates this new Event with the previous negative Event and is able to close the first Event. It is possible that an operator will have to manually clear Events until the tool matures.

APPENDIX A – Acronyms

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

https://mcscviper.usmc.mil/sites/mcnispi/st/_layouts/WordViewer.aspx?id=/sites/mcnispi/st/EITSUM%20Document%20Library/E-ITSM_TO_13_Acronyms_List.doc&Source=https%3A%2F%2Fmcscviper%2Eusmc%2Emil%2Fsites%2Fmcnispi%2Fst%2Fdefault%2Easpx%3FGroupString%3D%253B%2523General%253B%2523%26IsGroupRender%3DTRUE&DefaultItemOpen=1&DefaultItemOpen=1

APPENDIX B – Glossary

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

Term	Definition
Early Life Support	Early Life Support (ELS) involves Technical Management or IT Operations providing support for a new or changed IT service for a period of time after it is released. During ELS, the IT service provider may review the KPIs, service levels, and monitoring thresholds and provide additional resources for incident management and problem management (when implemented).
EM System	The EM System (EMS) is comprised of tools which monitor CIs and provide Event notifications. It is a combination of software and hardware which provides a means of delivering a message to a set of recipients. The EMS often requires real-time interaction, escalation, and scheduling.
Environment	Environment is a subset of the IT infrastructure used for a particular purpose (e.g., live environment, test environment or build environment). It is possible for multiple environments to share a CI (e.g., test and live environments may use different partitions on a single mainframe computer). In the term physical environment, environment can be defined as the accommodation, air conditioning, power system, etc. Environment can be used as a generic term defined as the external conditions that influence or affect something.
Error	An Error is a design flaw or malfunction that causes a failure of one or more CI or IT services. A mistake made by a person or a faulty process that affects a CI or IT service is also an error.
Escalation	Escalation is an activity that obtains additional resources when needed to meet service-level targets or customer expectations.
Event	An Event is a piece of data that provides information about one or more system resources. Most Events are benign. Some Events show a change of state which has significance for the management of a CI or IT service. The term ‘Event’ is also used to define an alert or notification created by any IT service, CI, or monitoring tool. Events typically require IT operations personnel to take actions and often lead to incidents being logged.
Event Correlation	Event correlation involves associating multiple related Events. Often, multiple Events are generated as a result of the same infrastructure fault. Events need correlation to prevent duplication of effort in resolving the original fault.
Exit and Entry Criteria (Pass/Fail)	These are criteria (defined well in advance and accepted by the stakeholders) defined at authorized points in the Release and Deployment Process to set expectations of acceptable/unacceptable results.
Fault	Fault is the deviation from *normal* operation of a CI or a series of CIs. A fault is a design flaw or malfunction that causes a failure of one or more CIs or IT services. Fault is also referred to as an error.
Governance	Governance is the process of ensuring policies and strategy are actually implemented and that required processes are correctly followed. Governance includes defining roles and responsibilities, measuring, and reporting and taking actions to resolve any issues identified.
Key Performance Indicator	A Key Performance Indicator (KPI) is a metric used to help manage a process, IT service, or activity. Many metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the process, IT service, or activity. KPIs are selected to ensure that efficiency, effectiveness, and cost effectiveness are all managed.
Known Error	A Known Error is a problem that has a documented root cause and a work-around. Known errors are created and managed throughout their lifecycle by Problem Management. Known errors may also be identified by SIE or suppliers.
Monitoring	Monitoring is the process of repeated observation of a CI, IT service, or process to detect Events and to ensure that the current status is known.
Notification	Notification is a communication that provides information.
Pilot	A Pilot is a limited deployment of an IT service, a release, or a process to the live environment. A pilot is used to reduce risk and to gain user feedback and acceptance.

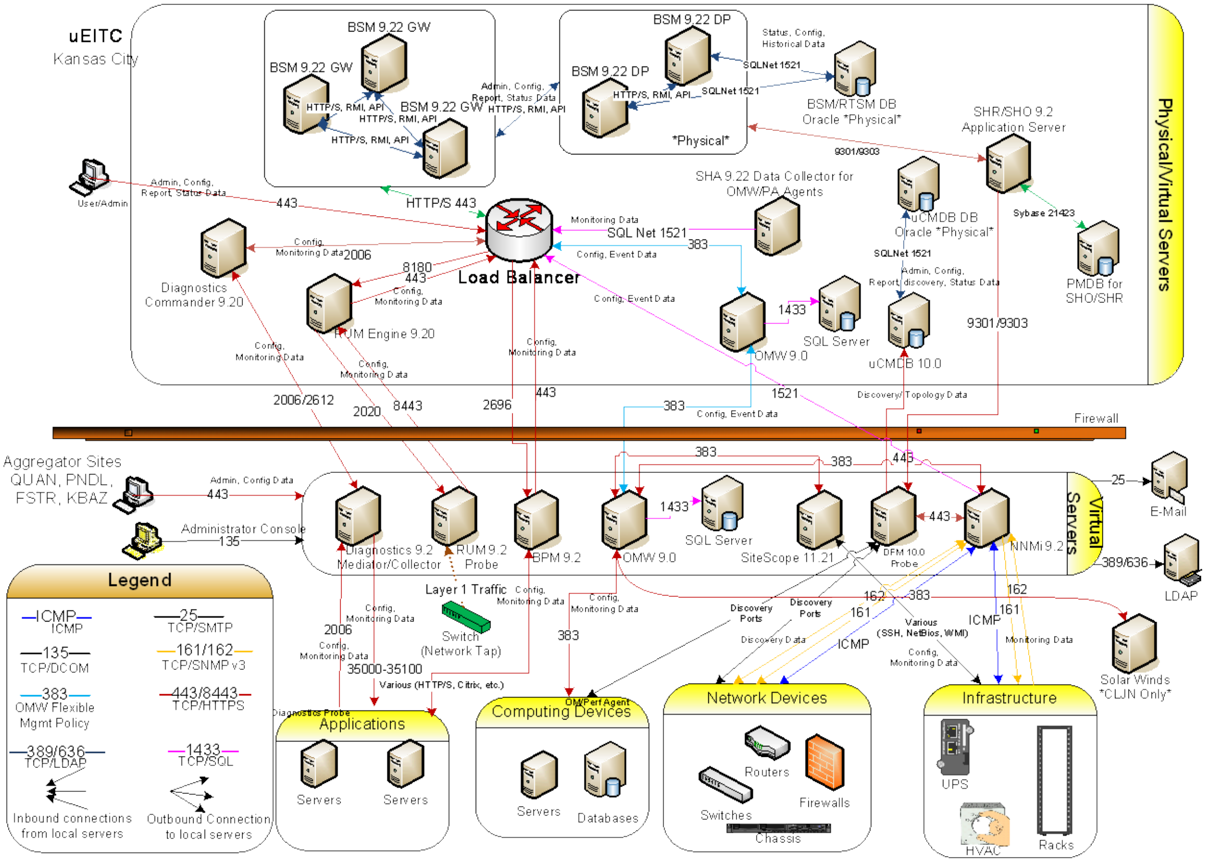
Term	Definition
Process	A Process is a structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. A process may include any of the roles, responsibilities, tools, and management controls required to reliably deliver the outputs. A process may define policies, standards, guidelines, activities, and work instructions, if needed.
Quality Assurance	Quality Assurance (QA) is the process responsible for ensuring the quality of a product and also ensuring it will provide its intended value.
Role	A Role refers to a set of connected behaviors or actions that are performed by a person, team, or group in a specific context.
Severity	Severity refers to the level or degree of intensity.
Service Design Package	A Service Design Package (SDP) is composed of document(s) defining all aspects of an IT service and its requirements through each stage of its lifecycle. An SDP is produced for each new IT service, major change, or IT service retirement.
Service Improvement Plan	A Service Improvement Plan (SIP) is a formal plan to implement improvements to a process or IT service.
Service Knowledge Management System	A Service Knowledge Management System (SKMS) is a set of tools and databases used to manage knowledge and information. The SKMS includes the Configuration Management System (CMS) as well as other tools and databases. The SKMS stores, manages, updates, and presents all information that an IT service provider needs to manage the full lifecycle of IT services.
Service Level Agreement	A Service-Level Agreement (SLA) is an agreement between an IT service provider and a customer. The SLA describes the IT service; a document service-level targets, and specifies the responsibilities of the IT service provider and the customer. A single SLA may cover multiple IT services or multiple customers.
Service Validation and Testing	Service Validation and Testing is the process responsible for validation and testing of a new or changed IT service. Service Validation and Testing ensures an IT service matches the design specification and will meet the needs of the business. Service Validation and Testing during release conducts testing in the pre-production Systems Integration Environment (SIE) and during deployment in the pilot production environment.
Single Point of Contact	A Single Point of Contact (SPOC) is an agreement used to assign a single, consistent way to communicate within an organization or unit. For example, the Service Desk will be the SPOC for a service provider.
Snapshot	A Snapshot is the baseline as captured by a discovery tool. A snapshot can also be called a benchmark.
Test	A Test is an activity that verifies that a CI, IT service, or process meets its specification or agreed requirements.
Test Environment	A Test Environment is a controlled environment used to test CIs, builds, IT services, and processes.
Throttling	Some Events do not need to be acted on until they have occurred a number of times within a given time period. This is called Throttling. Once a repeated Event has reached its limit for repetition, forward that Event to be acted upon.
User Acceptance Testing	User Acceptance Testing is a testing activity conducted by the user intended to verify a CI, IT service, or process meets a specification. It is also used to validate whether agreed requirements have been met.
Work-around	Work-around for problems are documented in known error records and are intended to reduce or eliminate the impact of an incident or problem for which a full resolution is not yet available. Work-around for incidents that do not have associated problem records are documented in the incident record.
Work Instruction	The Work Instruction is a document containing detailed instructions that specify exactly what steps are followed to carry out an activity. A work instruction contains much more detail than a procedure and is only created if very detailed instructions are needed.

APPENDIX C – Hewlett-Packard Operations Manager Tool Architecture

The USMC has chosen the Hewlett-Packard (HP) suite of applications to monitor, report, and perform routine patching and maintenance in the MCEN environment. The HP suite is an extensive collection of applications tailored to the USMC specifications. It is both adaptable, and scalable to the USMC computing environment.

For the purposes of monitoring the MCEN, it has been broken into sections. Each MITSC is considered a sub-set of the entirety of the MCEN. Operators may be located at these sites and tasked with monitoring their respective portions of the network. Additionally, to provide situational awareness across the network, a central, consolidated view of the network will also be maintained. At the consolidated site (currently the facility located in Kansas City) the HP tool-set is installed and configured to accept feeds from all downstream locations. This location and configuration is referred to as the “Manager of Managers” or MoM.

At select MITSC’s, a similar set of the HP tool-set is installed. These installations are configured to monitor only their respective site. They are referred to as “Aggregators.” In addition to collecting local data, they also communicate to the MoM in real time in order to provide SA of the environment. The figure below depicts these installations:



APPENDIX D – Works Cited

Hewlett-Packard Development Company, L.P. (2011). *HP Operations Manager i Software.* Retrieved June 17, 2013, from HP Official Site: http://www.hp.com/hpinfo/newsroom/press_kits/2011/optimization2011/HP_Operations_Manager_i_software_Data_Sheet.PDF