Event Management

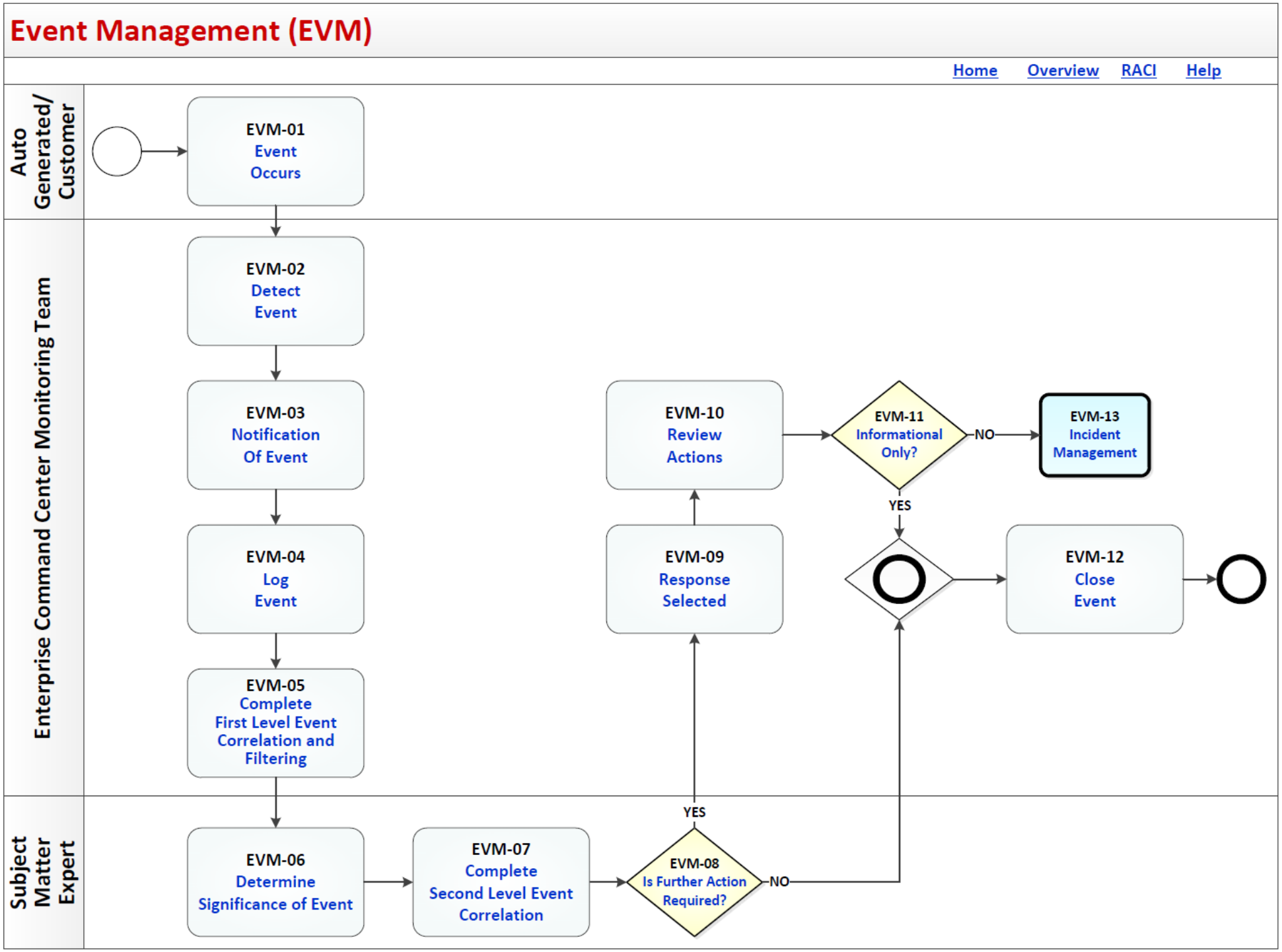
Process Asset Library

Office of Information and Technology

Table of Contents

Event Management Process Map 1
Process: Event Management 3
Event Management Description and Goals 4
Description 4
Goals 4
Event Management RACI Information 5
Event Management Associated Artifacts Information 8
Event Management Tools and Web Sites Information 8
Event Management Standards Information 8
Event Management Process 9
Process Activity Name: EVM-01 Event Occurs 9
Process Activity Name: EVM-02 Detect Event 10
Process Activity Name: EVM-03 Notification of Event 11
Process Activity Name: EVM-04 Log Event 12
Process Activity Name: EVM-05 Complete First Level Event Correlation and Filtering 13
Process Activity Name: EVM-06 Determine Significance of Event 14
Process Activity Name: EVM-07 Complete Second Level Event Correlation. 15
Process Activity Name: EVM-08 Is Further Action Required? 16
Process Activity Name: EVM-09 Response Selected 17
Process Activity Name: EVM-10 Review Actions 18
Process Activity Name: EVM-11 Information Only? 19
Process Activity Name: EVM-12 Close Event 20
Process Activity Name: EVM-13 Incident Management 21

Event Management Process Map



The links in this process map are inactive. Please scroll to view activity data.

Process: Event Management

Overview: The process map for Event Management cycles through the following process and review activities:

EVM-01 Event Occurs
EVM-02 Detect Event
EVM-03 Notification of Event
EVM-04 Log Event
EVM-05 Complete First Level Event Correlation and Filtering
EVM-06 Determine Significance of Event
EVM-07 Complete Second Level Event Correlation
EVM-08 Is Further Action Required?
EVM-09 Response Selected
EVM-10 Review Actions
EVM-11 Information Only?
EVM-12 Close Event
EVM-13 Incident Management

Event Management Description and Goals

Description

Event Management is the process that monitors, identifies and prioritizes infrastructure, service, business and security events and filters events to be responded to according to event status, especially focusing on conditions that could lead to potential faults or Service Level exceptions. Event Management is therefore the basis for Operational Management Monitoring, Control, and Notification and is ITIL conformant. The process is made up of interrelated activities, including activities that measure the effectiveness of the process, as well as provide for continued process improvement.

Goals

The goals of Event Management are to:

- Provide the ability to detect events, make sense of them and determine the appropriate control action is provided.

- Automate many routine Operations Management activities like executing scripts on remote devices, submitting jobs for processing, or even dynamically balancing the demand for a service across multiple devices to enhance performance.

- Provide a way of comparing actual performance and behavior against design standards and Service Level Agreements (SLAs).

- Provide a basis for Service Assurance and Reporting; and Service Improvement.

- Provide a standard and filtered view of all events including those from other event management systems and from enterprise applications.

- Associate one or more events with a single cause in determining root cause analysis.

- Automatically inform the appropriate stakeholders of events that require action to drive timely response.

- Attach descriptive information to events to facilitate incident resolution and root cause analysis.

- Provide up-to-date roles and responsibilities charts to support event management.

- Ensure there is vendor involvement during event investigation and resolution, as required.

- Provide post analysis of event handling procedures that were conducted and applied.

- Ensure interaction with other Service Management processes.

Event Management RACI Information

The following describes the RACI information for this process:

EVM-01 Event Occurs

Responsible Role: Customer
Accountable Role: Enterprise Command Center Monitoring Team
Consulted Role: None Listed
Informed Role: None Listed

EVM-02 Detect Event

Responsible Role: Enterprise Command Center Monitoring Team
Accountable Role: None Listed
Consulted Role: Event Management Staff; Customer
Informed Role: Event Management Process Owner; Stakeholders

EVM-03 Notification of Event

Responsible Role: Enterprise Command Center Monitoring Team
Accountable Role: None Listed
Consulted Role: Event Management Staff
Informed Role: Event Management Process Owner; Stakeholders

EVM-04 Log Event

Responsible Role: Enterprise Command Center Monitoring Team
Accountable Role: None Listed
Consulted Role: Event Management Staff; Stakeholders
Informed Role: Event Management Process Owner; Stakeholders

EVM-05 Complete First Level Event Correlation and Filtering

Responsible Role: Enterprise Command Center Monitoring Team

Accountable Role: None Listed
Consulted Role: Customer
Informed Role: None Listed

EVM-06 Determine Significance of Event

Responsible Role: Subject Matter Expert(s)
Accountable Role: Enterprise Command Center Monitoring Team
Consulted Role: Event Management Staff
Informed Role: Event Management Process Owner; Stakeholders

EVM-07 Complete Second Level Event Correlation

Responsible Role: Subject Matter Expert(s)
Accountable Role: Enterprise Command Center Monitoring Team
Consulted Role: None Listed
Informed Role: None Listed

EVM-08 Is Further Action Required?

Responsible Role: Subject Matter Expert(s)
Accountable Role: Enterprise Command Center Monitoring Team
Consulted Role: None Listed
Informed Role: None Listed

EVM-09 Response Selected

Responsible Role: Enterprise Command Center Monitoring Team
Accountable Role: Subject Matter Expert(s)
Consulted Role: None Listed
Informed Role: Customer

EVM-10 Review Actions

Responsible Role: Enterprise Command Center Monitoring Team
Accountable Role: Subject Matter Expert(s)
Consulted Role: Event Manager; Stakeholders
Informed Role: Event Management Process Owner; Customer

EVM-11 Information Only?

Responsible Role: Enterprise Command Center Monitoring Team
Accountable Role: None Listed
Consulted Role: None Listed
Informed Role: None Listed

EVM-12 Close Event

Responsible Role: Enterprise Command Center Monitoring Team
Accountable Role: Subject Matter Expert(s)
Consulted Role: None Listed
Informed Role: Event Management Staff; Event Management Process Owner; Stakeholders

EVM-13 Incident Management

Responsible Role: Enterprise Command Center Monitoring Team
Accountable Role: None Listed
Consulted Role: None Listed
Informed Role: None Listed

Event Management Associated Artifacts Information

There are no artifacts associated with this process.

Event Management Tools and Web Sites Information

The Tools and Web Sites associated with this process (including hyperlinks) include:

Enterprise Operations (EO) Monitoring Team website

Service Operations Insight (SOI) Web

Event Management Standards Information

Standards associated with this process (including hyperlinks) include:

Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1

OI&T Event Management Process Document

Event Management Process

Process Activity Name: EVM-01 Event Occurs

Previous Activities

Process Begins

Next Activities

EVM-02 Detect Event

Description

The Customer, or an Auto Generated device, notifies the Enterprise Command Center Monitoring Team that an event is about to occur, or has occurred. There are multiple ways for customers to notify the Enterprise Command Center Monitoring Team. (Auto generated at the VA Command Center, Emails, phone calls, VA Pulse, and other sources).

Input

Email

Phone Call

VA Command Center Notification

VA Pulse

Output

Event Identified

Associated Artifacts

None Listed

Responsible Role

Customer

Accountable Role

Enterprise Command Center Monitoring Team

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Enterprise Operations (EO) Monitoring Team website

Service Operations Insight (SOI) Web

Standards

None Listed

More Info

The Service Operations Insight (SOI) Web is accessed in the Operation Tools Links of the EO Monitoring Team Web Page. Access to the Service Operations Insight (SOI) event management tool requires the user to obtain access to the site. The user can gain access to the SOI Web by contacting Enterprise Operations SharePoint Site Collection Administrator.

Process Activity Name: EVM-02 Detect Event

Previous Activities

EVM-01 Event Occurs

Next Activities

EVM-03 Notification of Event

Description

The Enterprise Command Center Monitoring Team monitors data from various system resources in the VA infrastructure, service, business and security to detect events. This includes various system resources in the VA infrastructure, service, business and security. The Configuration Item or Service being monitored goes into an abnormal state which causes an Event to be generated by a monitoring tool.

Input

Event Identified

Output

Detected Event

Associated Artifacts

None Listed

Responsible Role

Enterprise Command Center Monitoring Team

Accountable Role

None Listed

Consulted Role

Event Management Staff; Customer

Informed Role

Event Management Process Owner; Stakeholders

Tools and Websites

Enterprise Operations (EO) Monitoring Team website

Service Operations Insight (SOI) Web

Standards

None Listed

More Info

The Enterprise Command Center Monitoring Team configures the Service Operations Insight (SOI) Web event management tool for the design and thresholds of the data element fields. The Service Operations Insight (SOI) Web is accessed in the Operation Tools Links of the EO Monitoring Team Web Page. Access to the Service Operations Insight (SOI) event management tool requires the user to obtain access to the site. The user can gain access to the SOI Web by contacting Enterprise Operations SharePoint Site Collection Administrator.

Process Activity Name: EVM-03 Notification of Event

Previous Activities

EVM-02 Detect Event

Next Activities

EVM-04 Log Event

Description

The Enterprise Command Center Monitoring Team configures the Service Operations Insight, the event management tool to filter events and determines whether to communicate the event to a management tool.

A general principle of event notification is that the more meaningful the data it contains and the more targeted the audience, the easier it is to make decisions about the event. Meaningful notification data and clearly defined roles and responsibilities need to be articulated and documented.

Input

Detected Event

Output

Event Notification

Filtered Event

Associated Artifacts

None Listed

Responsible Role

Enterprise Command Center Monitoring Team

Accountable Role

None Listed

Consulted Role

Event Management Staff

Informed Role

Event Management Process Owner; Stakeholders

Tools and Websites

Enterprise Operations (EO) Monitoring Team website

Service Operations Insight (SOI) Web

Standards

None Listed

More Info

See Event Management Process Document for additional information regarding significance of the event.

The Service Operations Insight (SOI) Web is accessed in the Operation Tools Links of the EO Monitoring Team Web Page. Access to the Service Operations Insight (SOI) event management tool requires the user to obtain access to the site. The user can gain access to the SOI Web by contacting Enterprise Operations SharePoint Site Collection Administrator.

Process Activity Name: EVM-04 Log Event

Previous Activities

EVM-03 Notification of Event

Next Activities

EVM-05 Complete First Level Event Correlation and Filtering

Description

The Enterprise Command Center Monitoring Team reviews and logs the event by category type from the Service Operations Insight tool.

Input

Filtered Event

Output

Event Notification

Log Event

Associated Artifacts

None Listed

Responsible Role

Enterprise Command Center Monitoring Team

Accountable Role

None Listed

Consulted Role

Event Management Staff; Stakeholders

Informed Role

Event Management Process Owner; Stakeholders

Tools and Websites

Enterprise Operations (EO) Monitoring Team website

Service Operations Insight (SOI) Web

Standards

None Listed

More Info

The Service Operations Insight (SOI) Web is accessed in the Operation Tools Links of the EO Monitoring Team Web Page. Access to the Service Operations Insight (SOI) event management tool requires the user to obtain access to the site. The user can gain access to the SOI Web by contacting Enterprise Operations SharePoint Site Collection Administrator.

Process Activity Name: EVM-05 Complete First Level Event Correlation and Filtering

Previous Activities

EVM-04 Log Event

Next Activities

EVM-06 Determine Significance of Event

Description

The Enterprise Command Center Monitoring Team completes a first level event correlation and filtering. This activity is designed to determine how the event is communicated. The Enterprise Command Center Monitoring Team applies filters to determine if the team ignores communicating the event as it is information only, warning, or an exception whereby the event will be handled as an incident or problem.

Input

Event Notification

Logged Event

Output

First Level Event Correlation and Filtering

Associated Artifacts

None Listed

Responsible Role

Enterprise Command Center Monitoring Team

Accountable Role

None Listed

Consulted Role

Customer

Informed Role

None Listed

Tools and Websites

Enterprise Operations (EO) Monitoring Team website

Service Operations Insight (SOI) Web

Standards

None Listed

More Info

The Service Operations Insight (SOI) Web is accessed in the Operation Tools Links of the EO Monitoring Team Web Page. Access to the Service Operations Insight (SOI) event management tool requires the user to obtain access to the site. The user can gain access to the SOI Web by contacting Enterprise Operations SharePoint Site Collection Administrator.

Process Activity Name: EVM-06 Determine Significance of Event

Previous Activities

EVM-05 Complete First Level Event Correlation and Filtering

Next Activities

EVM-07 Complete Second Level Event Correlation

Description

The Subject Matter Expert(s) (SMEs) determines the significance of the event and the ticket is updated. The SMEs categorization of the significance of an event is: Informational, Warning, or Exception.

Input

Event Notification

Filtered Event

Output

Updated Incident Ticket (Informational, Warning or Exception)

Associated Artifacts

None Listed

Responsible Role

Subject Matter Expert(s)

Accountable Role

Enterprise Command Center Monitoring Team

Consulted Role

Event Management Staff

Informed Role

Event Management Process Owner; Stakeholders

Tools and Websites

Enterprise Operations (EO) Monitoring Team website

Service Operations Insight (SOI) Web

Standards

None Listed

More Info

See Event Management Process Document for additional information regarding significance of the event. The Service Operations Insight (SOI) Web is accessed in the Operation Tools Links of the EO Monitoring Team Web Page. Access to the Service Operations Insight (SOI) event management tool requires the user to obtain access to the site. The user can gain access to the SOI Web by contacting Enterprise Operations SharePoint Site Collection Administrator.

Process Activity Name: EVM-07 Complete Second Level Event Correlation

Previous Activities

EVM-06 Determine Significance of Event

Next Activities

EVM-08 Is Further Action Required?

Description

The Subject Matter Expert(s) (SMEs) determines the appropriate action to take based on the second level event correlation. If it is a warning type event the SMEs must make a determination of the significance of the warning to determine the appropriate action. The system applies filters to access events by

- number of similar events

- number of Configuration Items generating similar events

- potential impact to medical centers, data centers, etc.

Input

Event Notification

Filtered Event

Output

Second Level Event Correlation

Associated Artifacts

None Listed

Responsible Role

Subject Matter Expert(s)

Accountable Role

Enterprise Command Center Monitoring Team

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Enterprise Operations (EO) Monitoring Team website

Service Operations Insight (SOI) Web

Standards

None Listed

More Info

None Listed

Process Activity Name: EVM-08 Is Further Action Required?

Previous Activities

EVM-07 Complete Second Level Event Correlation

Next Activities

If "Yes":

EVM-09 Response Selected

Or

If "No":

EVM-12 Close Event

Description

This Subject Matter Expert(s) (SMEs) make a determination if further action is required or if they can close the event. The SMEs may need to engage the Enterprise Command Center Monitoring Team for further response selection.

Responsible Role

Subject Matter Expert(s)

Accountable Role

Enterprise Command Center Monitoring Team

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: EVM-09 Response Selected

Previous Activities

EVM-08 Is Further Action Required?

Next Activities

EVM-10 Review Actions

Description

The Enterprise Command Center Monitoring Team working with the Subject Matter Expert(s) (SMEs) selects the response to best resolve the Event. The SMEs provide recommendations for actions to be taken to mitigate the event to the Enterprise Command Center Monitoring Team.

Input

Event Notification

Filtered Event

Output

Selected Response

Associated Artifacts

None Listed

Responsible Role

Enterprise Command Center Monitoring Team

Accountable Role

Subject Matter Expert(s)

Consulted Role

None Listed

Informed Role

Customer

Tools and Websites

Enterprise Operations (EO) Monitoring Team website

Service Operations Insight (SOI) Web

Standards

None Listed

More Info

None Listed

Process Activity Name: EVM-10 Review Actions

Previous Activities

EVM-09 Response Selected

Next Activities

EVM-11 Information Only?

Description

The Enterprise Command Center Monitoring Team reviews actions and ensures all significant events have been handled appropriately and to track trends and count of event types. In the cases where events have initiated an incident, or change, the review action should not be duplicated as part of those processes. The intention is to ensure that the hand-off between the Event Management process and other processes takes place as designed. This is to ensure that incidents or changes originating within Operations Management do not get lost between the teams or departments. The review is also used as input into continual improvement and the evaluation and audit of the Event Management process.

Input

Event Notification

Filtered Event

Output

Filtered Event Actions Reviewed

Associated Artifacts

None Listed

Responsible Role

Enterprise Command Center Monitoring Team

Accountable Role

Subject Matter Expert(s)

Consulted Role

Event Manager; Stakeholders

Informed Role

Event Management Process Owner; Customer

Tools and Websites

Enterprise Operations (EO) Monitoring Team website

Service Operations Insight (SOI) Web

Standards

None Listed

More Info

The Service Operations Insight (SOI) Web is accessed in the Operation Tools Links of the EO Monitoring Team Web Page. Access to the Service Operations Insight (SOI) event management tool requires the user to obtain access to the site. The user can gain access to the SOI Web by contacting Enterprise Operations SharePoint Site Collection Administrator.

Process Activity Name: EVM-11 Information Only?

Previous Activities

EVM-10 Review Actions

Next Activities

If "Yes":

EVM-12 Close Event

Or

If "No":

EVM-13 Incident Management

Description

The Enterprise Command Center Monitoring Team makes a decision that no further action would be required and the information from this event is tracked for future events only. If so, the Event can be closed. If however, the Enterprise Command Center Monitoring Team feels that this needs to go to the Incident Management process for further action the teams notifies the Incident Management Team.

Responsible Role

Enterprise Command Center Monitoring Team

Accountable Role

None Listed

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: EVM-12 Close Event

Previous Activities

EVM-08 Is Further Action Required?

Or

EVM-11 Information Only?

Next Activities

Process Ends

Description

The Enterprise Command Center Monitoring Team closes the Event once properly resolved and documented. If an event turns into an incident, the event can be closed or remain open until the related incident is closed. Informational events are simply logged and then used as input to other processes. In the case of events that generate an incident, problem or change, these should be formally closed with a link to the appropriate record from the other process.

Input

Event Notification

Filtered Event

Output

Closed Event

Associated Artifacts

None Listed

Responsible Role

Enterprise Command Center Monitoring Team

Accountable Role

Subject Matter Expert(s)

Consulted Role

None Listed

Informed Role

Event Management Staff; Event Management Process Owner; Stakeholders

Tools and Websites

Enterprise Operations (EO) Monitoring Team website

Service Operations Insight (SOI) Web

Standards

None Listed

More Info

The Service Operations Insight (SOI) Web is accessed in the Operation Tools Links of the EO Monitoring Team Web Page. Access to the Service Operations Insight (SOI) event management tool requires the user to obtain access to the site. The user can gain access to the SOI Web by contacting Enterprise Operations SharePoint Site Collection Administrator.

Process Activity Name: EVM-13 Incident Management

Previous Activities

EVM-11 Information Only?

Next Activities

If "Stay in EVM":

Process Ends

Or

If "Go To Incident Management":

Incident Management Process

Description

The Enterprise Command Center Monitoring Team submits and Incident Ticket to the VA Command Center if the Event requires the team to process the event through the Incident Management System.

Input

Event Notification

Filtered Event

Output

Incident Ticket

Associated Artifacts

None Listed

Responsible Role

Enterprise Command Center Monitoring Team

Accountable Role

None Listed

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Enterprise Operations (EO) Monitoring Team website

Service Operations Insight (SOI) Web

Standards

None Listed

More Info

None Listed

END OF PROCESS