### EVENT MANAGEMENT PROCESS

<table>
<thead>
<tr>
<th>Code:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Version:</td>
<td></td>
</tr>
<tr>
<td>Date of version</td>
<td></td>
</tr>
<tr>
<td>Created by:</td>
<td></td>
</tr>
<tr>
<td>Approved by:</td>
<td></td>
</tr>
<tr>
<td>Confidentiality level:</td>
<td></td>
</tr>
</tbody>
</table>

*Comment [BV1]:* All fields in this document marked by square brackets [] must be filled in.

*Comment [BV2]:* If you want to find out more about the Event Management process see [http://www.20000academy.com/Blog/July-2013/Events-a-flood-or-mountain-creek](http://www.20000academy.com/Blog/July-2013/Events-a-flood-or-mountain-creek)

*Comment [BV3]:* The document coding system should be in line with the organization’s existing system for document coding; in case such a system is not in place, this line may be deleted.
Change history

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Created by</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>xx/xx/2013</td>
<td>0.1</td>
<td>Branimir Valentic</td>
<td>Basic document template</td>
</tr>
</tbody>
</table>

Table of contents

1. PURPOSE, SCOPE AND USERS.............................................................................. 3
2. REFERENCE DOCUMENTS ...................................................................................... 3
3. POLICY .............................................................................................................. 3
   3.1 EVENT MANAGEMENT ................................................................................... 3
   3.2 TOOL INTEGRATION ..................................................................................... 3
   3.3 EVENT HANDLING ....................................................................................... 4
4. PROCESS ACTIVITIES ............................................................................................ 5
   4.1 EVENT NOTIFICATION ................................................................................ 6
   4.2 EVENT DETECTION ..................................................................................... 6
   4.3 EVENT FIRST-LEVEL CORRELATION, FILTERING AND LOGGING .................... 6
   4.4 SIGNIFICANCE .......................................................................................... 6
   4.5 SECOND-LEVEL EVENT CORRELATION ........................................................ 6
   4.6 FURTHER ACTION REQUIRED / RESPONSE SELECTION ................................ 6
   4.7 REVIEW ACTIONS ..................................................................................... 6
   4.8 CLOSE EVENT ............................................................................................ 7
5. ROLES AND RESPONSIBILITIES ........................................................................... 7
   5.1 EVENT MANAGER ..................................................................................... 7
   5.2 TECHNICAL AND APPLICATION MANAGEMENT STAFF .............................. 7
6. MEASUREMENT AND METRICS .............................................................................. 7
   6.1 MEASUREMENT ........................................................................................ 7
   6.2 METRICS ................................................................................................ 8
   6.3 CRITICAL SUCCESS FACTORS (CSF) AND KEY PERFORMANCE INDICATORS (KPI) 8
7. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT......................... 9
8. VALIDITY AND DOCUMENT MANAGEMENT ....................................................... 9
9. APPENDICES ..................................................................................................... 9
1. Purpose, scope and users

The aim of this document is to define the purpose, scope, principles and activities for the Event Management process.

This document is applied to the entire IT Service Management (ITSM) organization.

Users of this document are all employees of [organization name], as well as all external parties who have a role in the ITSM.

2. Reference documents

- Incident Management Process
- Problem Management Process
- Change Management Process
- Technical Management Function
- Application Management Function

3. Policy

3.1 Event Management

The purpose of the Event Management process is to manage events from their detection, through making sense of them to determining an appropriate control action.

The scope of Event Management covers:

<table>
<thead>
<tr>
<th>Type</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Items (CIs)</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>Daily activities:</td>
<td></td>
</tr>
<tr>
<td>- Perform a review</td>
<td></td>
</tr>
<tr>
<td>- Identify impact</td>
<td></td>
</tr>
<tr>
<td>- Ensure applications</td>
<td></td>
</tr>
<tr>
<td>[...etc.]</td>
<td></td>
</tr>
</tbody>
</table>

3.2 Tool integration

Events are detected by [monitoring tool].

[tool name] is a tool that supports the Event Management process and activities. [role description] is responsible to manage tool usage and integration with other tools. [Technical operator] is responsible to manage operational handling of [tool name].

[tool name] is integrated with the following monitoring tools:

- [tool name]
3.3 Event handling

The event catalogue (see Appendix) presents the event classification scheme and defines the distribution of events. [Event manager] is responsible for establishing of event catalogue.

[organization name] utilizes the following categories of significance for events:

- Informational events
- Warning events
- Exceptional events

[Event Manager] defines the following as [organization name]'s rule set to process, evaluate and respond to events:

- Event is resolved inside Event Management process.
- Event is escalated to Problem Management process for all exceptional events.
- [Technical or Application Management staff] escalates warning events that are not escalated automatically.
- Event is escalated to Change Management process – for events that indicate that changes on existing CIs are needed.
4. Process activities

[Diagram of Process Activities]

Comment [BV22]: This is a high-level process description. It should be adapted depending on the actual situation.

Figure: Event Management process activities
Copyright© AXELOS Limited 2014. All rights reserved. Material is produced under license from AXELOS
4.1 Event notification

[Event Manager] is responsible to:

- Define with [IT Operations Manager] categories of events are entered into Event Catalogue (see Appendix).
- Coordinate with [IT Operations Manager] collection of input data which are entered into [Event Management tool].

4.2 Event detection

Events are received and [role description] returns information to requester if it is not an event.

4.3 Event first-level correlation, filtering and logging

[Event Manager] is responsible to define which events will be [tool name].

For events that are not reported, the following rule applies: [...].

[role description] logs events; see Event Record in Appendix. Mandatory data when logging an event are:

- Topic
- Category – see Event Catalogue in Appendix
- [Network Info]
- Urgency and impact – see Event Record in Appendix

4.4 Significance

Depending on the category of significance for detected events, [IT Operations Manager] follows the response procedure according to the Event Catalogue; see Event Record in Appendix.

4.5 Second-level event correlation

[IT Operations technician] is responsible to carry out the following activities:

- Event categorization (in case re-categorization is needed)
- Event prioritization (in case re-prioritization is needed)
- Gathering of all data needed to resolve event

4.6 Further action required / Response selection

[Event Manager] is responsible to offer response to events categorized as recurring, and enter them into the Event Catalogue (see Event Catalogue in Appendix).

4.7 Review actions

Review is a mechanism to:

- Check appropriateness of event handling
- Detect trends
Check if handover procedure with other processes (i.e. Incident/Problem/Change Management process) is efficient.

Only [Warning events with alerts] will be reviewed inside the Event Management process by [event assignee].

Exceptional events and warning events which were escalated to incident/Problem/Change Management process will be reviewed inside managing process. [Event Manager] is responsible to check that this was done.

4.8 Close event

Events that were escalated to Incident/Problem/Change Management process must be handled by [event assignee].

Events handled by event management will be closed:

- By [Technical or Application Management staff] if human intervention was needed
- Automatically by tool for events handled solely by tool

5. Roles and responsibilities

5.1. Event Manager

[job title] assigns the Event Manager role.

Responsibilities of Event Manager:
- Overall responsible for carrying out activities within the scope of Event Management
- Coordinates with other Service Management roles
- Plans and manages tools needed to support Event Management process
- Responsible for reporting and management information
- Manages work of event staff
- Manages and maintains Event Management process and procedures
- Manages if events occurred throughout other processes i.e. Incident/Problem/Change Management

5.2. Technical and Application Management staff

Technical and Application Management staff manage events that will be handled by the Event Management process. Technical and Application Management staff are defined in [Document name].

6. Measurement and metrics

6.1. Measurement

[role description] is responsible to produce reports.
6.2. Metrics

Metrics reports are produced monthly, with quarterly and yearly summaries. Metrics to be reported include:

- Total number of events
- Breakdown of events by categories
- Number and percentage of events incorrectly categorized
- Number and percentage of events divided by topic
- Number and percentage of events that triggered an incident/problem/Manage Process
- Number and percentage of incidents resolved by Technical and Application Management staff
- Breakdown of events by time of day, to help pinpoint peaks and ensure matching of resources

Reports are grouped into the following categories:

- Event category
- Time
- Severity
- Location

6.3. Critical Success Factors (CSF) and Key Performance Indicators (KPI)

[role description] is responsible to define CSFs and respective KPIs. Achievements against KPIs are measured and evaluated by [role description].

<table>
<thead>
<tr>
<th>Critical Success Factor</th>
<th>Key Performance Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events are communicated in the proper way to the functions that need to be informed or take actions.</td>
<td>Number of events that need human intervention and information if this was performed.</td>
</tr>
<tr>
<td>Correct level of filtering events is set.</td>
<td>Number of incidents triggered by Event Management process without human intervention.</td>
</tr>
<tr>
<td></td>
<td>Total numbers of events.</td>
</tr>
<tr>
<td></td>
<td>Number of incidents and problems having no category, information, warning, exception.</td>
</tr>
</tbody>
</table>

Comment [BV41]: Example: Event Management, Continual Service Improvement Manager

Comment [BV42]: Or similar role. Change if needed.

Comment [BV43]: Change if needed.

Comment [BV44]: In case

Comment [BV45]: Example of CSFs and KPIs. Each organization must develop own processes and as a basis for improvement.
7. Managing records kept on the basis of this document

<table>
<thead>
<tr>
<th>Record name</th>
<th>Storage location</th>
<th>Person responsible for storage</th>
<th>Controls for record protection</th>
<th>Retention time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Record (in electronic form)</td>
<td>[tool name]</td>
<td>[job title]</td>
<td>Technical and Application Management staff have right to add/change the record</td>
<td>Event Records are kept for 5 years.</td>
</tr>
<tr>
<td>Reports</td>
<td>[tool name]</td>
<td>[job title]</td>
<td>Event Manager</td>
<td>Reports are kept for [...]</td>
</tr>
<tr>
<td>Event Catalogue</td>
<td>[tool name, i.e. data storage location]</td>
<td>[job title]</td>
<td>Event Manager</td>
<td>New version replaces old one. Old one is archived.</td>
</tr>
</tbody>
</table>

8. Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must check and, if necessary, update the document at least once a year.

9. Appendices

- Appendix 1 Event Catalogue
- Appendix 2 Event Record

[job title]

[name]

[signature]
Some other examples include:

- Omitted
- Escalated into incidents with lowest priority (5)
- Such events will be stored in log file either inside event management tool, monitoring tool or on CI.
- [City/State]

This is an example.

Optional data can be:

- Location/Room
- Description

See Event record in Appendix.

Usually, this will be done by an agent/technician or correlation engine which resides either inside the monitoring tool or event management tool (e.g. monitoring tool uses e-mail to report events as well as keywords which clearly identify category and topic)

Can be done manually, by a technician, but usually this is done inside the event management tool based on business rules. It can happen that for certain types of events, no action is required. In such case, the next step is - Close.