**Contents**

[**1. Overview 5**](#_Toc98752867)

[**2. Purpose 5**](#_Toc98752868)

[**3. Scope 5**](#_Toc98752869)

[**4. Tool Integration 5**](#_Toc98752870)

[**5. Event Management Examples 5**](#_Toc98752871)

[**5.1 Event manager responsibilities 5**](#_Toc98752872)

[**6. Measurement and metrics 6**](#_Toc98752873)

[**6.1. Metrics 6**](#_Toc98752874)

[**6.2. Key performance Indicators 6**](#_Toc98752875)

[**7. Responsibility matrix 6**](#_Toc98752876)

[**8. Event Management Matrix 6**](#_Toc98752877)

[**9. Event Categories 7**](#_Toc98752878)

[**10. Record Management 7**](#_Toc98752879)

[**11. Validity 7**](#_Toc98752880)

**DOCUMENT REVISION CONTROL**

REVISION HISTORY

| **Date** | **Author** | **Version** | **Change Reference** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

REVIEWERS

| **Name** | **Position** | **Date** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

DISTRIBUTION

| **Date** | **Distributed to** | **Version** | **Distribution Format** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

APPROVALS

| **Date** | **Approved by** | **Version** | **Designation** | **Approval remarks** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**LIST OF ABBREVIATIONS**

|  |  |  |
| --- | --- | --- |
| **Index** | **Abbreviation** | **Stands For** |
| I | IT | Information Technology |
| 2 | SLA | Service Level Agreement |
| 3 | IOT | Internet of things |
| 4 | IAS | International Accounting Standards |
| 5 | FDP | Finance Department |
| 6 | ITSM | Information Technology Service Management |
| 7 | NDA | Non-Disclosure Agreement |

**Event Management Process**

Event monitoring and notification

**Event**

**Event Notification**

**Event Detection**

**Event Filtered**

**Informational Exception**

Event filtering

**Significance**

⚫ **Warning**

**Event correlation**

**Alert**

**Auto Response**

**Event Logged**

**Trigger**

**Type**

Response selection

**Problem management**

**Problem management**

**Incident management**

**Human Intervention**

Event closure

**Event closure**

**Event review**

**Resolved**

Yes No

# Overview

This document specifies how to plan and implement an effective event management system. It provides best practices on how to build your team, communicate with stakeholders, manage expectations, create a timeline for the project from start to finish, and execute the project’s events.

# Purpose

The purpose of the Event Management Document is to provide a detailed history of events which have taken place in an organization. It also needs to specify when and how these events are being tracked, recorded, monitored, or evaluated. The document should be updated whenever any changes are made to the processes that are described in it.

# Scope

This document applies to all **<Company Name>** staff.

# Tool Integration

Events are detected by **[monitoring tool].**

**[tool name]** supports event management processes and activities. **[operator name]** is responsible for managing the operational handling of **[tool].**

Resources in charge of monitoring the tool are:

* **[tool name]- ‘xxxx’**
* **[tool name]- ‘xxxx’**
* **[tool name]- ‘xxxx’**

# Event Management Examples

Events belong to one of three categories:

* Information – a successful task, like a user login or an email being received by the participant.
* Warning – when a device or service is reaching a threshold limit, like a scheduled backup not running or a server’s memory within 10% of its usable memory.
* Exception – an error given off when a component of the system acts abnormally, such as a server going down or a backup failing.

## **5.1 Event manager responsibilities**

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

* Event needs to be resolved in the event management process
* Provide warning and escalates events when not escalated automatically.
* Manages the work of event staff

# Measurement and metrics

**[designation]** is responsible to produce reports and forward it to service manager on quarterly basis.

## **6.1. Metrics**

Metrics reports are produced monthly or quarterly. They include

* Number of events
* Number of events categorized
* Breakdown of events and match the availability of resources.

## **6.2. Key performance Indicators**

**[role description]** is required to produce critical success factor and key performance indicators.

# Responsibility matrix

| **Process** | **Operations manager** | **IT operator** | **Event monitors** | **Other roles** |
| --- | --- | --- | --- | --- |
| **Maintenance of event monitoring and rules** | **R** | **A** |  | **I** |
| **Event filtering and 1st level correlation** | **A** | **C** | **R** |  |
| **2nd level correlation and response selection** | **RA** | **C** | **I** |  |
| **Event review and closure** | **AR** | **R** |  | **A** |

# Event Management Matrix

| **Events by category** | **Number or % of events that require human intervention** | **Number or % of events that were caused by existing problem** |
| --- | --- | --- |
| **Unauthorized access** | **60%** | **0** |
| **Slow servers** | **30%** | **10%** |
|  |  |  |

# Event Categories

| **Successful Events** | **Warning events** | **Exception events** | **Responsible** | **Escalation** |
| --- | --- | --- | --- | --- |
| Cyber-attack prevented | Storage level reached 80% capacity | Program disintegrated while running the code | Stark Holland | NA |
|  |  |  |  |  |
|  |  |  |  |  |

# Record Management

| **Record name** | **Storage location** | **Storage responsibility** | **Controls for record protection** | **Retention time** |
| --- | --- | --- | --- | --- |
| **Even record (in digital form)** | **Server room** | **Security analyst** | **Technical staff can change the record** | **Records are retained for 5 years** |
| **Reports** | **Accounts room** | **Account manager** | **Event manager** | **3year retention** |
| **Event catalogue** | **Pen drives** | **IT administrator** | **Event manager** | **1 year** |
|  |  |  |  |  |

# Validity

This document is valid till **[date].**

The ownership of this document is assigned to **[job role]** who must review and update it on quarterly basis.