HICSE IT Incident Management Process

|  |
| --- |
| **Document Author: Tony Butler** |
| **Document ID:**  |
| **Document Version: 0.15** |
| **Date: 21th February 2024** |
| **Approved By: Paul Clancy** |

**Revision History**

| **Issue** | **Date** | **Author** | **Description**  |
| --- | --- | --- | --- |
| 0.01 | 2/11/2023 | Tony Butler | First Draft |
| 0.04 | 2/1/2024 | Paul Clancy | Review |
| 0.08 | 15/2/2024 | Tony Butler | Redesign |
| 0.09 | 15/2/2024 | Paul Clancy | Review |
| 0.10 | 19/2/2024 | Tony Butler | Revisions |
| 0.11 | 20/2/2024 | Paul Clancy | Review |
| 0.12 | 20/2/2024 | Tony Butler | Revisions |
| 0.13 | 20/2/2024 | Paul Clancy | Review |
| 0.14 | 20/2/2024 | Tony Butler | Revision |
| 0.15 | 8/3/2024 | Tony Butler | Revision |

Reference Documents

|  |  |
| --- | --- |
| **Parent Document** |  |
|  |  |
|  |  |
| **Offspring Document(s)** | 1. Request Fulfilment Process
 |
|  |  |
|  |  |
| **Reference Document(s)** |  |
|  |  |

Glossary

|  |  |
| --- | --- |
| Call | A telephone call to the IT Service Desk from a Customer. A Call could result in an Incident, or a Service Request being logged. |
| Category | Categories and subcategories are used to specify (i.e. breakdown) tickets in the Service Management tool for dispatching and/or reporting purposes. |
| Classification | Process of defining labels to tickets for the Management of ITIL Incidents. Classification encompasses two factors:1. **Category:** Defines the type of item that the Incident affects, for example: Is the hardware or the software presenting problems?
2. **Priority:** Define service priority. To do so, you should analyse two other factors:
	* **Impact:** What consequences can this Incident have on the company’s operations?

**Urgency:** What is the estimated time to solve this Incident? |
| Configuration Item (CI) | Any component that needs to be managed to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the CMDB. 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 SLOs. |
| Configuration Management Database (CMDB) | A Configuration Management Database (CMDB) is a database that contains all relevant information about the hardware and software components used in an organisation's IT services and the relationships between those components. A CMDB provides an organised view of configuration data and a means of examining that data from any desired perspective. |
| Customer | Someone who receives goods or services from IT. The customer of IT is the person or group that defines and agrees the Service Level Targets. The term Customer is also informally used to mean users. |
| First Time Fix (FTF) | First Time Fix, also called First Call Resolution (FCR), is the percentage of calls in which the caller gets an answer to his question immediately. It can also mean that the requested action is performed without any additional initiative from the caller or that somebody needs to call back. |
| Fit for Purpose | Fit to purpose, or utility, means that Service must fulfil customer needs. |
| Fit for Use | Fit for use, or warranty, means that service is available when a user needs it. |
| Impact | Measure of the business criticality of an Incident. Often equal to the extent of a deviation of agreed or expected Service Levels |
| Incident | An unplanned interruption to an IT service or a reduction in the quality of an IT service. Failure of a CI that has not yet affected a service is also an Incident. |
| Incident Owner | Incident Owner is the person to whom the Incident is assigned. |
| Incident Record | A record containing the details of an Incident. Each Incident record documents the lifecycle of a single Incident. |
| Incident Recovery | The implementation of the resolution and the confirmation of restoration of Service from the Customer. |
| Incident Resolution | Action that will resolve an Incident. This may be a Workaround. |
| Key Performance Indicator (KPI) | A Key Performance Indicator is a measurable value that demonstrates how effectively a company is achieving key business objectives. Organisations use KPIs at multiple levels to evaluate their success at reaching targets. High-level KPIs may focus on the overall performance of the business, while low-level KPIs may focus on processes in departments such as sales, marketing, HR, support, and others. |
| Major Incident | Incidents with Priority 1 (or Priority 2). A Major Incident results in significant disruption to the business. They must be solved with greater urgency than normal Incidents. |
| Priority | A label used to identify the relative importance of an Incident, Problem or Change. Priority is based on impact and urgency and is used to identify required times for actions to be taken. |
| Problem | A cause of one or more Incidents. The cause is not usually known at the time a Problem record is created. When IT does not use a formal Problem Management process it is often done within resolving an Incident causing the SLO being breached. |
| Problem Management | The process responsible for managing the lifecycle of all Problems. The primary objectives of Problem Management are to prevent Incidents from happening, and to minimise the impact of Incidents that cannot be prevented. |
| Procedure | A procedure is a series of (work)instructions that must be executed in a specific order. |

Contents

[1. Introduction 8](#_Toc159236876)

[1.1 Definition of Incident Management 8](#_Toc159236877)

[1.2 Purpose of Incident Management 8](#_Toc159236878)

[1.3 Objectives of Incident Management 8](#_Toc159236879)

[1.4 Benefits of Incident Management 9](#_Toc159236880)

[1.5 Requirements of Incident Management 9](#_Toc159236881)

[1.6 Incident Management Scope and Tooling 10](#_Toc159236882)

[1.7 Incident Management versus related processes 11](#_Toc159236883)

[1.7.1 Event Management 11](#_Toc159236884)

[1.7.2 Problem Management 11](#_Toc159236885)

[1.7.3 Request Fulfilment 11](#_Toc159236886)

[1.7.4 HICSE Incident Management versus Supplier Incident Management 12](#_Toc159236887)

[2. Roles and Responsibilities 13](#_Toc159236888)

[3. Incident Prioritisation 15](#_Toc159236889)

[3.1 Urgency 15](#_Toc159236890)

[3.2 Impact 15](#_Toc159236891)

[3.3 Priority 15](#_Toc159236892)

[3.4 Priority adjustment 16](#_Toc159236893)

[3.5 Operational Guidelines 16](#_Toc159236894)

[4. SLO’s, KPI’s and Reporting 17](#_Toc159236895)

[4.1 Service Levels 17](#_Toc159236896)

[4.2 Key performance Indicators and Metrics 18](#_Toc159236897)

[4.3 Reporting 19](#_Toc159236898)

[4.3.1 Major Incidents 19](#_Toc159236899)

[4.3.2 Daily report 19](#_Toc159236900)

[4.3.3 Monthly report 19](#_Toc159236901)

[5. Incident Process description 20](#_Toc159236902)

[5.1 Process Flow diagram. 20](#_Toc159236903)

[5.2 Detailed process steps 21](#_Toc159236904)

[5.3 RACI Matrix 24](#_Toc159236905)

[6. Governance 25](#_Toc159236906)

[6.1 Meeting Structure 25](#_Toc159236907)

[7. Appendix Error! Bookmark not defined.](#_Toc159236908)

[7.1 Incident states **Error! Bookmark not defined.**](#_Toc159236909)

# Introduction

Incident Management is a critical process that provides organisations with the ability to first detect Incidents and then to target the correct support resources to resolve the Incidents as quickly as possible.

The process also provides management with accurate information on the Incidents impacting the organisation, so that they can identify the required support resources and plan for their provision. By utilising the Incident Management process, organisations can ensure that their support resources are focusing on the issues that have the greatest Urgency and potentially the greatest Impact on the business.

## Definition of Incident Management

In ITIL terminology, an Incident is defined as unplanned interruption to an IT Service, reduction in the quality of an IT Service, or failure of a Configuration Item (CI) that may potentially impact an IT Service.

Incident Management is defined as “the process responsible for managing the life cycle of all Incidents”. Incidents can be detected by the end users impacted by the Incident, support teams, event monitoring tools or third-party suppliers.

## Purpose of Incident Management

The Incident Management process is in place to restore normal service operation as quickly as possible, minimising adverse impact on business operations. While ensuring that agreed service and operational levels are maintained.

## Objectives of Incident Management

The objectives of Incident Management include:

* Resolving Incidents as quickly as possible
* Maintaining business satisfaction with IT Services
* Maintaining quality of IT Services
* Aligning Incident Management activities and priorities with those of the business
* To increase visibility and communication of Incidents to the business and IT support staff
* Enhancing business perception of IT through use of professional approach in quickly resolving and communicating on Incidents
* Using standardised methods and Procedures for efficient and prompt response, analysis, documentation, management, and reporting.

## Benefits of Incident Management

Benefits of Incident Management include but are not limited to:

* The ability to detect and resolve Incidents, which results in lower downtime to the business.
* The ability to align IT activity to real-time business priorities. This is because Incident Management includes the capability to identify business priorities and allocate resources as necessary (e.g., in case of a high Priority Incident)
* The ability to increase Customer satisfaction by identifying improvement opportunities via user satisfaction surveys and improving the Incident Management process accordingly.

## Requirements of Incident Management

Requirements of Incident Management include but are not limited to:

* **Clear Definition of Incidents**: Initiator is to clearly define the incident and to provide complete and accurate information of the incident. This could include security breaches, system failures, data breaches, natural disasters, etc.
* **Classification and Prioritisation**: Each incident will follow the Incident Prioritisation process to establish a classification incident based on severity and impact.
* **Notification Procedures**: The initiator will follow the process to raise an incident as clearly defined in the Roles & Responsibilities and Incident Process. Where the procedures for reporting incidents, including who to notify, how to report, and escalation paths is defined.
* **Response Times**: The expected response times for different types of incidents is defined. This helps ensure that incidents are addressed promptly to minimise damage and downtime.
* **Roles and Responsibilities**: There is a clearly define of the roles and responsibilities of individuals involved in incident management process, including incident initiators, responders, coordinators, communication liaisons, etc.
* **Documentation Requirements**: It is the initiators and responders’ responsibility to provide information that is needed for each incident, including timelines, actions taken, and resolutions. This documentation is valuable for post-incident analysis and improving incident response processes.
* **Training and Awareness**: Ensure that staff members receive adequate training on incident management procedures and are aware of their roles and responsibilities during incidents.
* **Testing and Exercises**: From time to time some testing of the solution may be required before making changes to a live system. Scheduling testing incident response procedures through tabletop exercises, simulations, or full-scale drills maybe required. This helps identify gaps in the process and allows teams to practice their response in a controlled environment.
* **Continuous Improvement**: The Incident Management Process is designed to Implement a process for reviewing and improving incident management procedures based on lessons learned from past incidents and changes in the organisation's environment.
* **Compliance Requirements**: We ensure that incident management procedures align with relevant regulatory requirements and industry standards.
* **Security Considerations**: Incorporate security best practices into incident management procedures to safeguard sensitive information and protect against further security breaches during incident response.
* **Vendor and Third-Party Management**: Establish procedures for managing incidents involving vendors or third-party service providers, including communication protocols and escalation paths. As defined in the Incident Process Flow.
* **Feedback Mechanism**: Implement a feedback mechanism for stakeholders to provide input on the effectiveness of incident management procedures and suggest improvements.

## Incident Management Scope and Tooling

The HICSE IT Service Management tool is Topdesk, which includes full Incident Management functionality.

This can be found by the following link <https://topdesk.hitachi-infocon.com/>

The scope of Incident Management includes all Incidents related to HICSE IT Services.

## Incident Management versus related processes

This section describes the relation between Incident Management and other ITIL processes. The differences between these processes and Incident Management are described below.

### Event Management

Event management concerns the detection of any change in an IT component (something has happened), this includes assurances of things ‘going right’ (e.g., information events) and things that ‘might’ need some action but do not impact a Service (e.g. warning events). Therefore, not all events become Incidents. Once an event indicates an interruption to an IT Service or reduction in the quality of an IT service, it should trigger an Incident.

### Problem Management

A Problem is the underlying cause of one or more Incidents and remains a separate entity. Problem Management proactively prevents Incidents from happening and minimises the impact of Incidents that cannot be prevented. Where Incident Management is focused on restoring the Service as soon as possible, potentially with a Workaround; Problem Management is focused on structurally solving the issue and thus preventing Incidents.

Incident review and Root Cause Analysis are separate activities and part of separate processes: The Incident review activity is part of Incident Management and serves to recap and evaluate the Incident flow and communication. This review is used as input for process improvement, input to Problem Management and uniform communication on Incidents towards stakeholders.

Root Cause Analysis activity is part of Problem Management and serves to find the root cause and define corrective actions (structural solution) for the issue.

### Request Fulfilment

Request Fulfilment process provides a channel for users to request and receive standard Services for which a pre-defined approval and qualification process exists.

Service Requests do not represent a disruption to agreed Service. Therefore, they will not be treated as Incidents.

### HICSE Incident Management versus Supplier Incident Management

HICSE Incident Management process (i.e., this document) defines the overall framework, guidelines and touch points which applies to all IT Services.

Suppliers can additionally have their own Incident Management process and procedures containing specific details for a certain Service or activity in more detail for their specific scope, especially when working with internal tooling, if these do not conflict with the HICSE Incident Management process.

# Roles and Responsibilities

|  |  |
| --- | --- |
| **Role** | **Responsibility** |
| Incident Initiator (i.e. end user) | * Report an Incident, via <https://topdesk.hitachi-infocon.com/>
* when it occurs and provide complete and accurate information to the best of their knowledge.
* Respond to mails or Calls related to the initiated Incident.
 |
| Service Desk(IT support) | * First point of contact for the user.
* Incident identification.
* Incident logging, including categorisation, prioritisation, and assignment.
* Initial investigation & diagnosis and first actor that starts resolving the Incident.
* Incident escalation and monitoring.
 |
| Support group (IT Team support group)(Second- and third-line support group: specialist support groups and external suppliers) | * Investigating and diagnosing the Incidents.
* Providing resolution and recovery of the assigned Incidents.
* Communication with the Incident Initiator required for resolving the Incident.
* Suggest possible Problems and initiate the Problem Management process for resolution.
* Identification and (automated) logging of technical monitoring Incidents.
* Ticket closure (resolution verification with Initiator for Incidents)
* Closing of Incidents (performed automatically within the SMT)
 |
| Incident Process Manager | * End-to-end Service monitoring and escalation of Incidents across domains and suppliers.
* End-to-end coordination of Major Incidents.
* Business Service Level (KPI) reporting and (KPI) reporting based on supplier Underpinning Contract.
* Process review and improvements across domains.
* Ensuring the process is performed as designed and Fit for Purpose.
* Ensuring process description meets objectives and process KPIs.
* Sponsorship, design, and continual improvement of the process and its metrics. – e.g., designing Incident models and workflows.
* Ensures that the process is regularly reviewed and updated.
* Ensure there is an integrated approach on the design and implementation of the Incident and Problem Management.
 |
| Process Owner | * Sponsorship and acceptance of the process design and its metrics.
 |

# Incident Prioritisation

The Incident prioritisation determines the Priority by using information on Urgency and Impact. The below tables detailing Urgency, Impact and Priority, gives IT employees guidelines to assess incoming Incidents on priority.

## Urgency

The following table provides guidelines for determining Urgency.

|  |  |  |  |
| --- | --- | --- | --- |
| **Urgency** | **High** | **Medium** | **Low** |
| **Workaround****available** | No WorkaroundAvailable. | Workaround availableand functional loss. | Workaround availableand no functional loss. |

## Impact

The following table provides guidelines for determining Impact. The criteria with the highest Impact will be used in the Priority matrix.

|  |  |  |  |
| --- | --- | --- | --- |
| **Impact** | **High** | **Medium** | **Low** |
| **Number of users** | Entire Location\* | Department/site. | Single user. |
| **Business Impact** | High availability application supporting primary SA operating process is down. | Medium availability application is down. | Low availability application is down. |
| **Reputation Impact** | Multiple customers, regulators, media are impacted. | Single customer. | Only internal. |

\* Small offices are considered as a department/site. These offices hold between 1-15 employees.

## Priority

The following table provides guidelines for determining Priority.

|  |  |
| --- | --- |
|  | **Urgency** |
| **Derived from Urgency and Impact** | **High** | **Medium** | **Low** |
| **Impact** | **High** | Emergency (P1) | High (P2) | Medium (P3) |
| **Medium** | High (P2) | Medium (P3) | Low (P4) |
| **Low** | Medium (P3) | Low (P4) | Low (P4) |

## Priority adjustment

IT Service Desk may adjust the Priority if Urgency and/or Impact are shown to be different than originally mentioned by the Initiator. IT Service Desk (IT Support) is obligated to report in the ticket because Priority has been adjusted.

## Operational Guidelines

The roles and responsibilities have been communicated to and fully understood by the appropriate process stakeholders.

All Incident documentation including Incident Tickets must be written in English to ensure the materials are understood in a common language due to the nature of the business.

Incident Management is operational for the following operational hours:

* From 08:00 AM to 17:00 PM (Monday to Thursday), 08:00 AM to 13:00 PM (Friday)
* Operational hours exclude corporate and public holidays.
* Separate agreements can be made per jurisdiction with respect to opening hours and availability of IT staff.
* This is then recorded in a Service Level Objective.
* After-hours: The IT Service Desk will address emergencies/urgent matters raised via the Incident Procedure and system (the IT portal). After-hours support can be contacted by phone for those questions that require quick follow up and cannot wait until the next business day.

The Customer may contact the IT department via following channels to submit their Incident:

* Ticket portal(https://topdesk.hitachi-infocon.com) – Preferred method to raise tickets with full information.
* Mail – Send an email to Support, IT.
* Telephone – when immediate attention is required.
* **Priority 1 incidents must always be reported via Topdesk to the IT Support Desk and followed by a call to the IT Support Team.**

# SLO’s, KPI’s and Reporting

## Service Levels

The below Service Levels are designed as a guide to the minimum level of service IT aim to provide and are detailed in the table below:

* The response time is calculated from when the Incident is initially logged to when the Incident is assigned by the IT Service Desk and updated with a communication to the Incident initiator.
* The resolution time is defined as when the Incident is deemed resolved by the Incident assignee. The Incident initiator is updated with the resolution or Workaround and the Incident state is set to ‘closed’.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Emergency (P1)** | **High (P2)** | **Medium (P3)** | **Low (P4)** |
| **Response time** | 0.5 Hour | 4 Hours | 8 hours | 8 hours |
| **Resolution Time** | 90% 4 Hours99% 8 Hours | 90% 8 hours99% 2 working days | 90% 2 working days.99% 5 workingdays | 90% within 5 working days 99% within 10working days |

The following guideline applies for calculating these KPI’s:

* In clock hours (may extend beyond user support window) for Incidents with Priority P1. In all other cases the times are expressed in working hours within the user support window (see opening hours IT department).
* Incidents pending Customer input will pause the SLO, until the moment action is pending IT ServiceDesk again.

## Key performance Indicators and Metrics

The below table details the relevant performance metrics which are measurable against Incident Management. These are listed as Result KPI’s, Influencing KPI’s and Metrics.

|  |  |  |
| --- | --- | --- |
| **Type** | **Incident** | **Description of KPI** |
| **Result KPI** | Response/Resolution SLO % met. (target 90% within target) | The number of Incidents responded to and resolved within the agreed SLO. |
| New P1 Incidents per month | The number of P1 (Emergency) Incidents logged per month. |
| **Influencing KPI** | Number of Incidents raised peremployee | The number of Incidents logged per employee per month. |
| Number of new Incidents (perCategory and Priority) | The number of Incidents logged per month against each available Category and Priority. |
| Number of resolved Incidents | Total volume of Incidents resolved in the past month/week. |
| Number of open Incidents (backlog) | The number of Incidents which remain open in Topdesk on the reporting date. |
| Number SLO Response / Resolution overdue Incidents backlog (per assignment group) | The number of Incidents which have not been responded to or resolved within the agreed SLO. This provides an overview of the number of overdue backlog Incidents per assignment group on the reporting date. |
| Customer Satisfaction rating | Customer Satisfaction is measured by asking the Customer to rate their experience and/or the completion of a customer survey. |
| **Metrics** | Oldest open Incident in days | The number of calendar days the oldest Incident has been open for. |
| % Incidents resolved by ITsupport | Provides the percentage of Incidents, resolved by the Service Desk. |
| % Incidents reassigned | The percentage of Incidents which have been reassigned. |
| % Incidents reopened | The percentage of Incidents which have been reopened after the Incident state has been set to resolved. |
| Overdue Incidents total | The total number of Incidents where the Due Date has passed on the reporting date. |

## Reporting

### Major Incidents

For each resolved emergency (P1 & P2) Incident there is a mandatory Major Incident Report (MIR) created and shared within all parties concerned. This report describes the following aspects: scope, business impact, timeline, people involved, solution, measurements, actions lists and decisions.

The Infrastructure or Application Manager troubleshooting and resolving the emergency Incident will fill in this report. Once the report is finalised, it’s sent to Head of IT & HICSE IT for filing. This report can be shared with the Business if requested.

### Daily report

A daily report is extracted from Topdesk detailing:

* Backlog open Service Requests & Change Requests categorised by date.
* Backlog of open Incidents per resource categorised by date.

### Monthly report

Every month a KPI report is created providing details on all Incidents. This report is then used for the IT Services Dashboard and is available to the Senior Leadership Team.

# Incident Process description

## Process Flow diagram.



## Detailed process steps

|  |  |
| --- | --- |
| **Trigger** | **An Incident for has been identified** |
| **Activity #** | **Description** | **Executed by** |
| **1.1** | **Identify Incident / Log Incident** | **Incident Initiator****/ IT Operations** |
|  | The Incident Initiator logs an Incident via the IT Self Service portal, mail to the IT Service Desk. |  |
| **1.2** | **Decision whether this is an Incident or a Service Request** | **IT Operations** |
|  | After the user has contacted the IT Service Desk, the Service Desk determines whether an Incident has occurred based on theinformation they received from the user. |  |
| **1.3** | **Start Request Fulfilment Process** | **IT Operations** |
|  | If no Incident can be identified, IT Service Desk will determine if the Incident should be converted into a Service Request. If converted to a Service Request, then the Request Fulfilment process is triggered via the SMT. Service Desk follows the Request Fulfilment process once it has been identified. |  |
| **1.4** | **Categorise Incident** | **IT Operations** |
|  | Once the Incident is logged it must be categorised to specify the Service or equipment it relates too. Once the correct Category has been selected, the IT Service Desk can identify the resolver. |  |
| **1.5** | **Prioritise Incident** | **IT Operations** |
|  | Incident must be prioritised considering both the level of Impact and the Urgency of the Incident. The Priority of the Incident can be determined based on the Impact and Urgency matrix. |  |
| **1.6** | **Major Incident?** | **IT Operations** |
|  | When the Incident is prioritised as P1 or P2 it can be Classified as an Emergency/Major (P1 or P2) Incident. In this case the Major Incident procedure must be followed and the IT Operationsmanager is notified. |  |
| **1.7** | **Contact IOM – Start Major Incident Procedure.** | **Incident Coordinator** |
|  | Major Incident procedure is started. And moved to diagnose the incident.  |  |
| **1.8** | **Diagnose Incident** | **IT Operations** |
|  | The IT Service Desk must discover and document the full symptoms of the Incident to determine what exactly has gone wrong and how to correct it. Matching the symptoms of the Incident to a known error database or to previous occurred Incidents may help to get an understanding of what to do. If it is something new, further investigation and diagnosis is needed. |  |
| **1.9** | **Escalation Needed?** | **IT Operations** |
|  | Once the IT Service Desk has carried out the initial diagnoses they decide if the Incident requires escalation to the IT Operations Manager or 3rd party support or more management attention based on the Incident Category, Priority, and other Incident details. |  |
| **1.10** | **Functional Escalation** | **IT Operations** |
|  | Following the decision to escalate the Incident the IT Service Desk assigns the Incident to an IT Support team engineer.  |  |
| **1.11** | **Notify Manager** | **IT Operations** |
|  | If management- or Service owner support is required, the Incident may be escalated to the IT Operations Manager / team leads. (Hierarchical escalation). When a decision has been made to escalate the Incident to Service owner or manager. TheIT Operations Manager must be notified. | IT Operations Manager |
| **1.12** | **Investigate and Resolve** | **IT Operations** |
|  | On basis of diagnosis and investigation the IT Service Desk finds and implements the solution or Workaround to resolve. |  |
| **1.13 / 2.3** | **Resolution Identified?** | **IT Operations** |
|  | The Incident assignee seeks confirmation from the Incident Initiator that service has been restored sufficiently. If theInitiator confirms, the Incident is set to “Solved”. Otherwise, it will return for further investigation. See 1.8/2.1.  |  |
| **1.14 / 2.4** | **Resolve Incident & Confirm to Initiator** | **IT Operations** |
|  | If the resolution is identified, then it must be applied, and the service must be recovered. The Incident record is updated with the resolution and set to “Complete”. The Support group may refer to a knowledge article to indicate how the Incident was resolved. |  |
| **1.15 / 2.5** | **Knowledge Management** | **IT Operations** |
|  | If no Knowledge article exists on how to resolve this Incident, it may be decided to create a new one, following the Knowledge Management Process. |  |
| **2.1** | **Investigate & Resolve** | **IT Operations** |
|  | Once the IT Service Desk escalates the Incident within IT Support team to an individual engineer, the engineer/s are then responsible for carrying out investigation and resolving the Incident. |  |
| **2.2** | **Escalation Needed?** | **IT Operations** |
|  | Once the IT Support team has carried out further investigation they decide if the Incident requires escalation to 3rdparty support based on the Incident Category and Priority. |  |
| **3.1** | **Vendor Incident Procedure** | **3rd Party Support** |
|  | If the decision is made to escalate the Incident further theIncident is assigned to a 3rd party (external) support group and the vendor specific Incident procedure is started. |  |
| **4.1** | **Confirm Closure** | **Incident Initiator** |
|  | As a final check, the Incident Initiator is informed about thestatus change to “Closed”. If the Initiator replies, the Incident moves back to the status “in progress” with the last IT Support group as the assignee. (Process step 1.13/ 2.1 - Investigate and Resolve). If no response is made after further requests to the initiator from the service desk within 21 business days, the Incident can be closed by the IT Service Desk. |  |
| **Output:** | **Documented ticket with solution or recovery** | **Completed ticket** |

## RACI Matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Incident Initiator** | **IT Operations Team** | **3rd Party Support** | **IT Operations Manager** |
| **1.1: Identify / Log Incident** | R | I |  | A |
| **1.2: Incident?** | I | R |  | A |
| **1.3: Start Request Fulfilment Process** | I | R |  | A |
| **1.4: Categorise Incident** |  | R |  | A |
| **1.5: Prioritise Incident** |  | R |  | A |
| **1.6: Critical Incident?** |  | R, C |  | R, A |
| **1.7: Contact IOM – Start Major****Incident Procedure** | I | R |  | R, A |
| **1.8: Diagnose Incident** |  | R |  | A |
| **1.9: Escalation Needed?** | I | R |  | A, C |
| **1.10: Functional Escalation** | I | R |  | A |
| **1.11: Notify Manager for Hierarchical****Escalation** |  | R |  | A, C |
| **1.12: Investigate and Resolve** | I | R |  | A |
| **1.13: Resolution Identified?** | C | R |  | A |
| **1.14: Resolve Incident and confirm to****initiator** | I | R |  | A |
| **1.15: Knowledge Management** |  | R |  | R, A |
| **2.1: Investigate and Resolve** |  | R |  | A |
| **2.2: Escalation Needed?** |  | R |  | A |
| **2.3: Resolution Identified?** | C | R |  | A |
| **2.4: Resolve Incident & Confirm to****Initiator** | I | R |  | A |
| **2.5: Knowledge Management** | I | R, A |  | I |
| **3.1: Vendor Incident Procedure** | I | C | R | A |
| **4.1: Confirm Closure / auto close** | R | I | (I) | A |

# Governance

## Meeting Structure

The below governance has been agreed and will follow the outlined meeting structure below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Meeting** | **Chair** | **Frequency** | **Participants** | **Agenda Subjects** |
| **Incident Service Delivery****meeting** | IT Operations Manager | Daily | All HICSE IT Support team members | * Outstanding tickets status.
* KPI and SLO’s.
 |
| **Vendor Operational Meeting (JML)** | IT Operations Manager | Bi-weeklyTo Be scheduled with the supplier and service. | Vendor Service Delivery/Level Manager | * Discuss KPI and results.
* Inflow, outflow, and backlog of Incidents.
* Process issues & escalations.
* ITSM tool.
* related issues.
 |
| **Vendor Service Review Meeting (HEU)** | Head Of IT | Depends on supplier | Depends on domain, Service Delivery Manager | * Customer satisfaction and general business alignment for the supplier.
* Vendor performance with regards to Incident KPIs and SLOs and Incident trends.
* Output: Improvement suggestions for the Incident Management

process or Services provided by the supplier which can be input for continual service improvement or Problem Management. |
| **Business Domain meeting** | Head of IT | Depends on domain, geography | Operations Head, Regional Directors Local Business reps of smaller Offices | Operational progress per business process.Discuss all Priority 1 and 2 Incidents.Discuss the detected trends to initiate (proactive) Problem creation.Discuss the trend for all Incidents including Priority 1 and 2.Input: Overall Service Level performance per application and Incident trends.Output: Improvement suggestions for Incident Management process or business processes where continual service.* Improvement opportunities are identified based on Incident trends.
 |

# Appendix

## Incident States

The below table shows the states which can be assigned to an Incident during its lifecycle, each state has an impact on the SLO and can be starters, paused or stopped depending on the Incident state.

|  |  |  |
| --- | --- | --- |
| **State** | **Description** | **SLO and notifications** |
| **New (Logged)** | * + - * Incident is newly created.
 | * + - * SLO is started – A notification is sent.
 |
| **Assigned** | * + - * Incident is picked up by IT Service Desk and “Assigned to” the IT support, and first assessment is made. When Incident is escalated to L2/L3 support, it moves back to this state.
 | * + - * The response time is automatically calculated from the point the Incident is assigned.
 |
| **In Progress** | * + - * Incident is actively being worked on by assignment group.
 | * + - * The Response Time SLO should be stopped as the Incident moves to “In progress. (not implemented in Topdesk yet)
 |
| **Pending Customer (User)** | * + - * Incident is awaiting input from Incident initiator/business representative.
 | * + - * The SLO should be paused when the Incident state is set to on hold. The due date is automatically recalculated.
 |
| **Pending Vendor (Supplier)** | * + - * Incident is awaiting input from 3rd party vendor.
 | * + - * The SLO is not paused when the Incident state is set to “on hold” pending vendor.
 |
| **Closed** | * + - * Incident is deemed resolved by the assignee.
 | * + - * The Resolution time SLO is paused when the Incident state is set to complete, and notification is sent
 |
| **Completed** | * + - * Incident is confirmed by Initiator issue is resolved and can be closed.
 | * + - * The SLO is stopped. In this state the Incident can no longer be edited.
 |