Incident Management

Tuesday, 15 June 2021

Version 1.4

**Document Number**

|  |  |
| --- | --- |
| **Document Reference** | **Date Created** |
|  |  |

**Contact Information**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Organization** | **Tel** | **Email** |
|  |  |  |  |
|  |  |  |  |

**Document Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Author** | **Date** | **Changes** |
| 1.0 |  | 29 October 2020 | Initial Release |
| 1.4 |  | 29 November 2020 | Updated based on Ooredoo & DP Comments |

**Document Distribution**

|  |  |  |
| --- | --- | --- |
| **Recipients** | **Position** | **Organization** |
|  |  |  |

**Reference Documents**

|  |  |  |
| --- | --- | --- |
| **Document ID** | **Title/Description/Link** | **Name & Version** |
|  |  |  |

**Disclaimer:**

Please note this is an iterative document and will be continuously updated during the course of the program. This is owing to the methodology adopted for project delivery. In other words, this document will be live and updated with additional details as new scenarios are taken up for implementation through future Sprints.

**Abbreviations and Terms**

| **Acronym** | **Term** | **Definition** |
| --- | --- | --- |
| CCC | Customer Contact Center | Teams responsible for processing and coordination of appropriate timely responses to service consumers. |
| CI | Configuration Item | A component that needs to be managed to deliver an IT service |
| CMDB | Configuration Management Database | An ITIL database used by an organization to store information about hardware and software assets |
| CMS | Configuration Management System | A set of tools and databases that are used to support service assets and manage IT Service Provider's Configuration data |
| CSF | Critical Success Factor | Areas in which steps are taken where high performance or success is important—the areas that determine the success of a business |
| CSI | Continual Service Improvement | Aims to deal with measures to be adopted to improve the service quality by learning from past successes and failures |
| IM | Incident Management | Process is to restore a normal service operation as quickly as possible and to minimize the impact on business operations |
| ISD | Integrated Service Desk | Processing and coordination of appropriate and  timely responses to service consumers Resolving issues within the SLA timelines |
| IT | Information Technology | An information system including all hardware, software and peripheral equipment – operated by a limited group of users |
| ITIL | IT Infrastructure Library | A set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. |
| ITSM | IT Service Management | Activities that are performed by an organization to design, plan, deliver, operate and control information technology (IT) services offered to customers |
| KB | Knowledge Base | Repository of knowledge and information of an organization |
| KPI | Key Performance Indicator | A measure of performance that enables organizations to obtain information about many relevant factors such as the effectiveness and efficiency of their processes. |
| RASCI | Responsible, Accountable, Supported, Consulted, Informed | A matrix highlighting roles & responsibilities corresponding to activities involved. |
| SLA | Service Level Agreement | A documented agreement between a service provider and a customer that identifies both services required and the expected level of service. |
| SMO | Service Management Office | Office Accountable for ensuring the service management processes governance and integrations for the quality service delivery. |
| SOP | Standard Operating Procedure | A set of instructions that describe the processing of given work tasks and are process, service or workplace driven |
| SPOC | Single Point of Contact | A Single Point of Contact (SPOC) to meet the communication needs of both users and IT staff, and to satisfy both Customer and IT Provider objectives |
| SQCC | Smart Qatar Control Center | Operational user groups |
| SQCP | Smart Qatar Central Platform | Central platform that offers host of platforms products and TASMU services |

**Table of Contents**

[**Table of Contents** 5](#_Toc55517892)

[1. Process Overview 8](#_Toc55517893)

[**1.1** Purpose of the document 8](#_Toc55517894)

[**1.2** Scope & Target Audience 8](#_Toc55517895)

[**1.3** Process Definition 8](#_Toc55517896)

[**1.4** Goal 8](#_Toc55517897)

[**1.5** Process Objectives 8](#_Toc55517898)

[**1.6** Process Trigger 8](#_Toc55517899)

[**1.7** Interfaces with other Processes 9](#_Toc55517900)

[2 Incident Management Policies 11](#_Toc55517901)

[3 Incident Management Process Overview and Level 2 Process Description 12](#_Toc55517902)

[**3.1** Incident Management Process Overview 12](#_Toc55517903)

[**3.2** Detection and Recording Sub-process 16](#_Toc55517904)

[**3.3** Classification and Initial Support Sub-process 18](#_Toc55517905)

[**3.4** Investigation and Diagnosis Sub-process 22](#_Toc55517906)

[**3.5** Resolution and Recovery Sub-process 25](#_Toc55517907)

[**3.6** Confirmation and Closure Sub-process 27](#_Toc55517908)

[**3.7** Major Incident Management Sub-process 29](#_Toc55517909)

[4 Roles and Responsibilities 32](#_Toc55517910)

[**4.1** RASCI Chart 32](#_Toc55517911)

[**4.2** Roles and Responsibilities 35](#_Toc55517912)

[4.2.1 Requestor 35](#_Toc55517913)

[4.2.2 Service Desk 35](#_Toc55517914)

[4.2.3 Resolver group L2/L3 36](#_Toc55517915)

[4.2.4 Operation Manager 36](#_Toc55517916)

[4.2.5 Incident Manager 36](#_Toc55517917)

[4.2.6 Major Incident Manager 36](#_Toc55517918)

[**4.3** Risk & Dependencies 37](#_Toc55517919)

[5 Key Performance Indicators 38](#_Toc55517920)

[6 Handling Guidelines 39](#_Toc55517921)

[**6.1** Exception Handling Process 39](#_Toc55517922)

[**6.2** Escalation Handling 39](#_Toc55517923)

[7 Appendix 40](#_Toc55517924)

[**7.1** Appendix A – Incident Priority Matrix 40](#_Toc55517925)

[**7.2** Appendix B – Incident Priority Change Approver Template 40](#_Toc55517926)

[**7.3** Appendix C – Major Incident Management Template 40](#_Toc55517927)

[**7.4** Appendix D –Ticket Status 40](#_Toc55517928)

[**7.5** Appendix E – Escalation Matrix 40](#_Toc55517929)

[**7.6** Appendix F – Vendor Contact Details 40](#_Toc55517930)

[**7.7** Appendix G – Notification 40](#_Toc55517931)

[**7.8** Appendix H – Sample IM Data Gathering Template 41](#_Toc55517932)

[**7.9** Appendix I – TASMU User Persona mapping 41](#_Toc55517933)

[**7.10** Appendix J – Recommended Best practices 41](#_Toc55517934)

**List of Tables**

[Table 1: Description of Incident Management Process Overview 11](#_Toc54800328)

[Table 2: Description of Detection & Recording Sub-process 15](#_Toc54800329)

[Table 3: Description of Classification & Initial Support Sub-process 17](#_Toc54800330)

[Table 4: Description of Investigation & Diagnosis Sub-process 21](#_Toc54800331)

[Table 5: Description of Resolution & Recovery Sub-process 24](#_Toc54800332)

[Table 6: Description of Confirmation & Closure Sub-process 26](#_Toc54800333)

[Table 7: Description of Major Incident Management Sub-process 28](#_Toc54800334)

[Table 8: Responsibility Matrix for Process 31](#_Toc54800335)

**List of Figures**

[Figure 1: Incident Management Process Overview 11](#_Toc54800336)

[Figure 2: Detection & Recording Sub-process 15](#_Toc54800337)

[Figure 3: Classification & Initial Support Sub-process 17](#_Toc54800338)

[Figure 4: Investigation & Diagnosis Sub-process 21](#_Toc54800339)

[Figure 5: Resolution & Recovery Sub-process 24](#_Toc54800340)

[Figure 6: Confirmation & Closure Sub-process 26](#_Toc54800341)

[Figure 7: Major Incident Management Sub-process 28](#_Toc54800342)

# Process Overview

This section provides the details such as the purpose, scope, process definition, objectives of the document.

## Purpose of the document

This document describes the Incident Management (IM) process to be followed. This will be used as a reference for the implementation and use of Incident Management process on an on-going basis. This process document is based on the best practices described in the Information Technology Infrastructure Library (ITIL) framework.

## Scope & Target Audience

The scope of incident management process applies to all the services provided by TASMU SQCC’s IT Operations. This will also include the incidents reported by users or customer.

The target audience for this document includes all IM process roles and relevant TASMU user persona, the Service Desk Agents, other IM process owners, IT Resolver Group Members, Application Support Staff involved in IM.

## Process Definition

The incident is an unplanned interruption to a service or reduction in the quality of service. Incident management is a defined mechanism for logging, recording and resolving incidents. IM aims to restore the service or process as quickly as possible, often through a workaround or temporary fixes, rather than through trying to find a permanent solution.

Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service is an ‘incident’.

## Goal

The primary goal of the IM process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations.

The primary purpose of the Incident Management is to restore normal service/ or operations as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of quality and availability are maintained

## Process Objectives

The objectives of the IM process are to:

* Provide a channel for users to raise incidents and receive solutions for which a predefined authorization and qualification process exists
* Increase visibility and communication of incidents to business and IT support staff
* Enhance the business perception of IT using a professional approach in quickly resolving and communicating incidents when they occur
* Provide information to users and TASMU representative about the procedure for raising Incidents
* Align Incident Management activities and priorities with those of the business
* Maintain user satisfaction with the quality of IT services

## Process Trigger

The process triggers for IM process are as follows:

* Incident raised automatically through the Event Management system
* IT Operations/ Security Operations/ Resolver Groups staff raise an incident ticket
* Technology Operations staff (IT Service and Asset Management staff – L2/L3) may notice a potential failure and raise an incident

## Interfaces with other Processes

The details of the interfaces and other processes are as follows:

| **Relationship with Other Processes** | | | |
| --- | --- | --- | --- |
| **Process** | **Relationship Description** | **Input** | **Output** |
| Problem Management | Problem resolution will trigger Incident resolution of associated incidents | ✔ |  |
| Incidents are often caused by underlying problems, which must be solved to prevent the incident from recurring.  The major incident will also trigger the Problem Management process for root cause analysis |  | ✔ |
| Configuration Management | Configuration Management provides the data used to identify and progress incidents. One of the uses of the CMS is to identify faulty equipment and to assess the impact of an incident. | ✔ |  |
| Incident Management can maintain the status of faulty CIs. It can also assist Configuration Management to audit the infrastructure when working to resolve an incident. |  | ✔ |
| Change Management | Where a change is required to implement a workaround or resolution, this will need to be logged as a Request for Change and progressed through Change Management | ✔ |  |
| IM can detect and resolve incidents that arise from failed changes. |  | ✔ |
| Capacity Management | The performance issue will form the input for Incident Management | ✔ |  |
| IM can trigger input to Capacity Management in case if capacity ramp-up is required |  | ✔ |
| Availability Management | The unavailability of service or component will form the input for Incident Management | ✔ |  |
| Event Management | The Events generated through the monitoring tool will trigger Incident | ✔ |  |
| Information Security | IM team will inform Information Security Team in case if any Security Incidents are raised | ✔ |  |
| The guidelines laid down by the Information Security team will be referred by IM team in case of Security related incidents |  | ✔ |
| Service Request Management | Many service requests may come in through the CCC/ISD and may be initially handled through the IM process before being identified as a SR. | ✔ |  |
| Incidents that are erroneously initiated as service requests must be rerouted to the service desk for appropriate incident handling  Also, incidents that require a service request to be logged in to resolve incidents, will serve as an input to SRM |  | ✔ |
| Service Level Management (SLM) | IM provides historical data that enables SLM to review Service Level Agreements (SLAs) objectively and regularly | ✔ |  |
| SLM defines the targets for the response and resolution of incident. |  | ✔ |
| Knowledge Management | The incident resolution will trigger the creation, modification, or retirement of the Knowledge article. |  | ✔ |
| Existing knowledge will be used during the resolution of the incident. | ✔ |  |
| Release Management | Issues occurring during releases will act as a trigger to create incidents | ✔ |  |

# Incident Management Policies

The policies defined for IM process are as follows:

* All incidents must be logged and tracked within a centralized ITSM tool
* All IT Incidents across the organization should follow the defined incident management process
* The requestor/ user will create the interactions by contacting the Service Desk team through call/email/Marketplace portal/Mobile application
* The priority of the incidents is based on impact and urgency definitions
* All incidents will be prioritized between Critical and Low
* All the Incident Management Process reviews and governances will be chaired by SMO
* Major Incidents should be handled and addressed as per the defined Major Incident Management Sub-Process
* The security-related incidents will be handled separately as a part of the Information Security Incident handling process
* Agreed escalation process shall be followed to ensure timely resolution of incidents
* Clear linkages between incident records, service requests, problem records, known errors and requests for change should be documented as and when applicable
* Resolver should ensure timely updates of the incident in Incident Work log with appropriate status
* Resolver shall ensure timely resolution of the incident within agreed SLA
* Incidents will be resolved following a 3-strike policy in case the user does not respond after three follow-ups in eight business days
* The Requestor can reopen a resolved Incident if the user is not satisfied with the resolution within three business days
* User should provide feedback once the issues are resolved
* If user do not provide the feedback on incident resolution or reopen the incident, then the incident will be auto hard closed after three business days

# Incident Management Process Overview and Level 2 Process Description

This section describes the details of the IM process overview and its Level 2 sub-processes details.

## Incident Management Process Overview

The following flow-chart depicts the IM process:



Figure 1: Incident Management Process Overview

The overview of IM Process is as follows:

Table 1: Description of Incident Management Process Overview

| **Sr. No** | **Procedure** | **Description** | **Input** | **Output** |
| --- | --- | --- | --- | --- |
| 1.0 | Communicate Issue | Incident can be initiated through any of the following triggers:   * TASMU digital Channel (CRM portal) * SQCC Customer Contact Center - Incident reported to Service Desk by the requestor through a Phone call or email * Event Monitoring Tool - Incidents automatically logged on detecting alert by the monitoring tool | * User Request * User Information * Event from Monitoring tool | * Incident request initiated |
| 2.0 | Detection & Recording | **Incident Detection & Recording**   * Service Desk authenticates the user by verifying their identification against available user information. Subsequently, Service Desk confirms completeness of details provided and in case any more information is needed collects it from the requester, the Service Desk will refer CMDB to collect and verify the CI information. * If the incident is logged over any TASMU digital Channel and information is insufficient, the user will be asked to provide the complete information; the ticket will be kept in pending state till details are received from the user. * Incidents qualified as automatically detected events are logged in an incident management tool. * If Security related incident, follow Information Security Incident Management Process | * Interrupted service * User Information * CI (Configuration Item) Information from CMDB | * User verified as authorized user * CI verified as authorized * Incident recorded * Security Incident identified |
| 3.0 | Classification & Initial Support | **Categorize & Prioritize Incidents**  Typically, the tool will assign category and priority to an incident based on pre-defined rules or values configured in the tool.  Service Desk can change the category if necessary, for routing the incident ticket to the correct resolver group.  Service Desk can also change priority (if required). Priority is determined based on urgency and impact values provided in the ‘Incident priority matrix’ Refer – [**Appendix A**](#_Appendix_A_–)  **Initial Support** (a) Incident Matching  Resolver group/Level 1match the incident with historical data and problem database to find if any workaround or resolution is already available.  If the incident-matching is successful, provide the workaround or resolution.  Follow the incident closure procedure.  (b) Refer to the Resolver group second level (L2) support  If the incident-matching is not successful, try providing a solution quickly.  If incident is resolved, follow the closure procedure and if it is not possible to resolve quickly, route and assign the incident to the appropriate L2 resolver group.  Refer and involve the Incident Manager in cases of Major Incidents identified or where it is not possible to refer to the appropriate level. | * User Information * CI Information from CMDB * Recorded incident | * Incident(s) categorized, logged& prioritized * Incident(s) routed/assigned to the appropriate L2 * Incident(s) Resolved * Major Incident identified |
| 4.0 | Investigation & Diagnosis | **Investigation**   * The Resolver group L2 team takes charge of the incident, analyses and diagnose the incident using appropriate method and tools * On successful diagnosis, identify a solution and appropriate action to restore the services. * Involve Resolver group L3 support if required.   **Actions**   * If the solution is found, the same is updated in the ticket work log and proceed to step 5.0 – Resolution and Recovery. In case where detail Root Cause analysis (RCA) is required (Major incidents), raise problem ticket. * If the resolution requires change, raise the Change Request (CR). * In case if vendor support is needed, change the status as “pending”, contact the concerned vendor and follow-up with the vendor till resolution. | * Routed/Assigned incident | * Incident diagnosed and solution identified * Problem ticket * Change request |
| 5.0 | Resolution & Recovery | * Apply solution/appropriate break-fix * Ensure that an interrupted service is restored. * Change the incident status to ‘Resolved’ | * Identified Solution | * Restored Service * Resolved Incident |
| 6.0 | Confirmation & Closure | * Once the incident is resolved, automatic intimation through email goes to user including request for user feedback for the Resolved incidents * User is supposed to close the incident and provide feedback * In case if user is not satisfied with the solution, they will move the Incident to Assigned state, and the process repeats for appropriate resolution.   **Auto Hard Closure**   * If the incident is not reopened or closed by requestor, it will be auto hard closed as per the agreed policy | * Resolved Incident | * User feedback * Reopened incident * Closed incident |
| 7.0 | Major Incident | * When an incident is identified as the major incident, based on the ‘Major incident criteria Template’ Refer – [**Appendix C**](#_Appendix_C_–)   Following activities should be carried out:   * Validate Major Incident * Inform the stakeholders * Open Conference bridge * Involve related support groups * Invoke DR if needed * Co-ordinate resolution * Communicate status to stakeholders * Final resolution update to stakeholders * Initiate problem ticket * Major Incident manager is responsible for coordinating among various parties and communicating to stakeholders till the resolution. | * Major Incident Identified | * Major Incident Resolved * Communication to stakeholders * DR invoked * Problem record created |

## Detection and Recording Sub-process

The steps involved in Detection and Recording sub-process is illustrated in the following figure:



Figure 2: Detection & Recording Sub-process

The following table provides the description of Detection & Recording sub-process:

| **Sr. No** | **Procedure** | **Description** | **Input** | **Output** |
| --- | --- | --- | --- | --- |
| 2.1 | Collect & Record information | * If the user contacts through phone Greet and welcome end user. * Welcome may take the form of live response, email or portal personalized message depending upon the method of access the user is utilizing. * Gather User, CI and Issue details * Notify users of any relevant known outage/problem issues | * User contacts service desk * Disruption of service | * Record updated with relevant details |
| 2.2 | Validate user profile data | * Validate user referring to user information available in the system | * User information updated in the system | * User Information verification in the system |
| 2.3 | Is Data Correct | * If the user is authorized, proceed with the next step else reject the request and inform the requester to initiate user profile update and end the process. | * User information verification | * User validated * Request rejected due to failure of validation |
| 2.4 | Verify IM or SR | * Verify if the requestor is communicating issue or service request. If issue proceed to 2.5 task else follow Service Request Management process | * Incident(s) under registration | * Issue or request identified * Service Request Management |
| 2.5 | Validate CI Information | * Validate Configuration Item (CI) referring to the Configuration Management Database (CMDB). | * CI information received | * CI information verification |
| 2.6 | Is Information Correct | * If CI is not valid, initiate the CMDB update process. | * User authenticated * CMDB | * CI validated by referring CMDB |

Table **2**: Description of Detection & Recording Sub-process

## Classification and Initial Support Sub-process

The steps involved in Classification and Initial Support sub-process is illustrated in the following figure:



Figure 3: Classification & Initial Support Sub-process

The following table depicts the description of Classification and Initial Support sub-process:

Table 3: Description of Classification & Initial Support Sub-process

| **Sr. No** | **Procedure** | **Description** | **Input** | **Output** |
| --- | --- | --- | --- | --- |
| 3.1 | Assign proper category | * Service Desk validates category and if incorrect, assigns appropriate category. * Service Desk assigns proper category while registering incidents based on call/email. | * Registered incident * Incident under registration | * Appropriate Category assigned. |
| 3.2 | Assign impact code | * Service Desk validates impact code and if incorrect, assigns appropriate impact code. * Appropriate impact code will be auto assigned based on the priority of incident logged. Refer to [**- Appendix A**](#_Appendix_A_–) for Priority Matrix | * Registered incident * Incident under registration | * Appropriate Impact code assigned |
| 3.3 | Assign Priority | * Service Desk validates priority and if not correct, assigns appropriate priority. * Service Desk assigns proper priority while registering incidents based on call/email. Refer - [**Appendix A**](#_Appendix_A_–)for ‘Incident Priority Matrix’. | * Registered incident * Incident under registration * Priority matrix | * Appropriated Priority assigned |
| 3.4 | Generate Incident Record | * On completing all necessary details, Service Desk saves the details and generates a ticket in the system. * System automatically generates a unique ticket number. | * Incident(s) under registration | * Incident Registered (Logged) * Ticket Number generated |
| 3.5 | Inform Ticket number to user | * On generating incident ticket, system automatically sends mail to user giving the ticket number. * This number can be used for all references. | * Registered Incident | * Ticket number informed to the user. |
| 3.6 | Is Major Incident | * If the ticket is classified as Major Incident, Inform MI Manager. Refer to [**Appendix C**](#_Appendix_C_–) ‘Major incident criteria Template’ * If Incident is not a Major Incident move to 3.7 sub process | * MIM Criteria | * Major Incident identified * Follow resolution procedure |
| 3.7 | Match Known Error database | * Resolver group L1 will perform incident matching against KEDB to check if any solution/workaround is already available for this incident, else follow 3.13 sub process | * Check for Known errors | * Extract Resolution steps |
| 3.8 | Extract resolution or workaround action from known error database | * Extract matching solution found in KEDB extract resolution or workaround action from known error database else perform matching against problem management database. | * Registered Incident * KEDB | * Workaround/ resolution extracted |
| 3.9 | Update incident count on known error record | * Resolution group L1 will update the incident count for the already documented Known Error Record | * Registered Incident * KEDB | * Updated Incident count for Known Error |
| 3.10 | Update incident record with ID of known error | * Resolution group L1 will update the incident record with the Known Error ID | * Registered Incident * KEDB | * Updated Incident Record with Known Error ID |
| 3.11 | Update incident record with classification data | * Resolution group L1 will update the incident record with classification data as per the Known Error | * Registered Incident * KEDB | * Incident ticket updated with correct Classification details |
| 3.12 | Inform customer of workaround/Resolution | * Inform the extracted work around/Resolution to the customer | * Extracted workaround/Resolution | * Workaround or Resolution informed to customer |
| 3.13 | Match on with Problem Record | * In case incident matching against problem management database is successful, go to 3.14 else, assign to Resolver group L2 team as appropriate for investigation and diagnosis | * Problem record verification | * Problem record verified * Assignment for resolution |
| 3.14 | Update incident count on problem record | * Resolver Group L1 will update the incident count for the already documented problem Record | * Registered Incident * Problem record | * Updated Incident count on Problem record |
| 3.15 | Update Incident record with ID of problem record | * Resolver Group L1 will update the incident record with the problem record ID | * Registered Incident * Problem record | * Update Incident record with ID of problem record |
| 3.16 | Update incident record with classification data | * Resolver Group L1 will update the incident record with classification data as per the Problem record | * Registered Incident * Problem record | * Incident ticket updated with correct Classification details |
| 3.17 | IS SOP Available | * Resolution Group L1 will check for SOP for the resolution, If SOP is available, move to resolution & closure | * SOP verification | * Resolution & Recovery * Vendor intervention |
| 3.18 | Assign to L2 | * If the resolver group L1 is unable to solve the issue they will escalate the issue to L2 team for resolution | * Issue escalated to L2 | * L2 team to perform investigation & diagnosis * Assign to Vendor for resolution |
| 3.19 | Vendor intervention | * Put the ticket on hold for vendor intervention | * Registered Incident | * Vendor Ticket generated |
| 3.20 | Update worklog and raise ticket with vendor | * Raise the ticket for Vendor to resolve the issue | * Vendor intervention | * Incident generated for Vendor |
| 3.21 | Vendor support & Resolution | * Update the incident with Vendor provided resolution and proceed to 5.0 Resolution and Recovery | * Vendor Ticket | * Vendor ticket resolved |

## Investigation and Diagnosis Sub-process

The steps involved in Investigation and Diagnosis sub-process is illustrated in the following figure.



Figure 4: Investigation & Diagnosis Sub-process

Table 4: Description of Investigation & Diagnosis Sub-process

| **Sr. No** | **Procedure** | **Description** | **Input** | **Output** |
| --- | --- | --- | --- | --- |
| 4.1 | Initial Investigation and Diagnosis | * The Resolution group L2 takes charge of the incident, analyses and diagnose the incident | * Incident assigned to L2 | * Initial Investigation and Diagnosis done |
| 4.2 | Is Ticket Accepted | * Check if the ticket is correctly routed. If yes go to 4.4 subprocess else proceed with 4.3 | * Incident verification | * Incident Reassignment * Gather information |
| 4.3 | Update work log and re-assign to Resolution Group L1 | * If the incident ticket is routed incorrectly/ outside the technology area managed, the same is to be updated in ticket work log, and reassigned to Resolution Group L1 to assign the Incident to appropriate L2 team * Go to Task 3.18 for further action | * Initial Investigation and Diagnosis done | * Ticket updated and reassigned to Resolution group L1 |
| 4.4 | More inputs required | * If the details available in incident records are insufficient for detailed diagnosis, L2 team collects required information from the user else proceed to 4.6 | * Initial Investigation and Diagnosis | * User information |
| 4.5 | Gather information from user | * If the details available in incident records are insufficient for detailed diagnosis, L2 team collects required information from the user. * Incident will be put on-hold | * Initial Investigation and Diagnosis done | * Incident On-Hold |
| 4.6 | Validate priority | * Resolution group L2 revalidates the priority. * In case if priority must be changed, approval is necessary as per ‘Incident Priority Approver List Template’ Refer – [**Appendix B**](#_Appendix_B_–) * Priority can be changed with appropriate approval | * Updated incident ticket | * Priority validated |
| 4.7 | Is Major Incident | * If the Incident is identified as Major Incident, then follow (7.0) | * Update priority | * Major Incident |
| 4.8 | Refer KEDB for existing work around and solution | * Resolution group L2 team also refers the KEDB for existing solutions or known errors. (as required) | * Updated incident ticket | * KEDB Referred |
| 4.9 | Carry out Detailed diagnosis | * The L2 team takes charge of the incident, analyses and diagnose the incident using appropriate method and tools * On successful diagnosis, identify solution and appropriate action to repair and restore the services. | * Updated incident ticket | * Solution / Workaround identified |
| 4.10 | Is Solution/  Workaround available | * If the solution / workaround is identified, the same needs to be updated in ticket work log and proceed to 5.0 sub process for Resolution and Recovery. | * Detailed investigation & Diagnosis | * Resolution & Recovery |
| 4.11 | Need Vendor intervention | * If the solution / workaround not identified and if vendor support is required go to 4.12 * If L3 support is needed go to 4.14 else work on the solution. | * Detailed investigation & Diagnosis | * Vendor/L3 intervention |
| 4.12 | Update ticket and assign to vendor | * If the solution or workaround is not identified, Resolution group L2 team must determine whether the vendor intervention is required. If so, open a ticket with vendor or inform vendor through an email and update the work log with appropriate details. * The ownership of the ticket still lies with the support team and is responsible for updating the status in ticket and keep user inform about status. | * Vendor contact list | * Vendor incident raised |
| 4.13 | Receive Vendor support & resolution | * Update the incident with Vendor provided resolution and proceed to 5.0 Resolution and Recovery | * Vendor Ticket | * Vendor ticket resolved |
| 4.14 | Need L3 intervention | * If there is any support required from the Resolution Group L3, Incident will be routed to L3 team and follow 4.15 sub process | * Investigation & Diagnosis | * Reassignment for Resolver group L3 |
| 4.15 | Update work log and reassign to L3 | * L3 will do the necessary diagnosis and provide solution. | * Ticket assigned to L3 | * Solution/ Workaround identified. |

## Resolution and Recovery Sub-process

The steps involved in Resolution and Recovery sub-process is illustrated in the following figure:



Figure 5: Resolution & Recovery Sub-process

The following table depicts the description of Resolution and Recovery sub-process:

Table 5: Description of Resolution & Recovery Sub-process

| **Sr. No** | **Procedure** | **Description** | **Input** | **Output** |
| --- | --- | --- | --- | --- |
| 5.1 | Carry out the tasks for incident resolution | * Resolution Group L1 executes tasks for incident resolution, updates resolution code and comments, as applicable | * Identified Solution | * Incident Resolved |
| 5.2 | Resolution/  Workaround | * If the solution is a workaround go to 5.3 sub process else is it is a resolution, follow 5.4 sub process | * Identified Solution | * Resolution * Workaround |
| 5.3 | Implement Workaround | * If workaround available, Resolution group L2/ L3 team implements workaround and initiate Problem ticket and proceed to 5.4 | * Identified Workaround | * Incident Resolved * Problem management |
| 5.4 | Carry Out the Tasks for Incident Resolution | * Resolution group L2/L3 execute tasks for incident resolution, as applicable | * Identified Solution | * Incident Resolved |
| 5.5 | Carry out the tasks to recover | * On successfully resolving the incident, the recovery steps need to be carried out if required. | * Identified Solution / Workaround and recovery steps | * Recovery steps |
| 5.6 | Is Incident Resolved | * If incident is resolved, update the work log and proceed to 5.7 sub process. * If incident is not resolved even after executing resolution tasks and performing recovery, one of the following actions needs to be taken: * Open Problem Record or Open Change Record | * Identified Solution / Workaround and recovery steps | * Recovery performed * Confirmation & Closure * Problem * Change |
| 5.7 | Update work log and resolve incident | * On successful resolution and recovery, Resolution group L2 / L3 updates the work log and incident status (as resolved) and proceed to 6.0 - Confirmation and Closure. | * Solution applied * Recovery performed | * Work log updated and incident resolved * Incident status changed to “Resolved” |
| 5.8 | Is Problem Record Required | * Open Problem Ticket – In case it is determined that the solution can only be achieved after performing problem analysis, open the problem ticket and follow Problem Management | * Investigation | * Problem Record |
| 5.9 | Is Change Record Required | * Open Change Ticket - In case it is determined that the solution can only be achieved after performing a change, open the change ticket and follow Change Management | * Investigation | * Change Record |

## Confirmation and Closure Sub-process

The steps involved in Confirmation and Closure sub-process is illustrated in the following figure:



Figure 6: Confirmation & Closure Sub-process

The following table depicts the description of Confirmation & Closure sub-process:

Table 6: Description of Confirmation & Closure Sub-process

| **Sr. No** | **Procedure** | **Description** | **Input** | **Output** |
| --- | --- | --- | --- | --- |
| 6.1 | Confirm resolution with user (Auto email) | * On resolution and recovery, the incident status is changed to “Resolved” & auto email is sent to the requestor for resolution confirmation. * If user is satisfied with resolution provided, ask for user feedback and closure on Incident else go to 6.2 * If user provides feedback go to 6.3 else 6.4 | * Resolved Incident | * Resolution accepted by user * Resolution rejected by user |
| 6.2 | Is User Satisfied | * If the user is not satisfied with the resolution provided, he/she will change the status to Assigned and will follow 6.3 sub process | * User confirmation | * Re-Open Incident * Provide feedback |
| 6.3 | Re-open incident (Change status to Assigned) | * If the user is not satisfied with the resolution provided, he/she change the status of the Incident from Resolved to Assigned. * Reopen incident is automatically assigned to respective resolver group. | * Resolution rejected by user | * Incident reopened |
| 6.4 | User provide feedback | * If the User provides feedback, follow the 6.5 sub process else follow 6.6 sub process | * User feedback | * User feedback * Closed Incident |
| 6.5 | Provide feedback and close incident | * User provides the feedback on the resolution and closes the request. | * Resolution accepted by user | * User feedback * Closed Incident |
| 6.6 | Auto hard closure of the incident | * If the Incident is not closed by user, then as per the predefined auto-closure time, ticket will be auto-closed | * Pre-defined auto closure time reached | * Incident auto-closed |

## Major Incident Management Sub-process

The steps involved in Major Incident Management sub-process is illustrated in the following figure:



Figure 7: Major Incident Management Sub-process

The following table depicts the description of Major Incident Management sub-process:

Table 7: Description of Major Incident Management Sub-process

| **Sr. No** | **Procedure** | **Description** | **Input** | **Output** |
| --- | --- | --- | --- | --- |
| 7.1 | Is Major Incident? | * If the identified issue is a major Incident follow 7.2. * If not qualified it is routed back to 3.7, 4.8 and stakeholders are informed about rejection. | * Major Incident identification | * Major Incident identified * Reassignment as normal incident |
| 7.2 | Accept Major Incident | * On receiving Major Incident Confirmation Refer – [**Appendix C**](#_Appendix_C_–) * If qualified as a major incident go to 7.3 | * Incident identified as Major Incident * MIM Criteria | * Major Incident accepted by Major Incident Manager |
| 7.3 | Review incident details | * On accepting the ownership of the Incident, the Major Incident Manager reviews incident details. | * Major Incident accepted by Major Incident Manager | * Major Incident reviewed |
| 7.4 | Inform the Stakeholders | * Inform all the stake holders about the major incident | * Reviewed Major Incident | * All concerned stakeholders informed |
| 7.5 | Open Conference Bridge | * Major Incident Manager opens a conference bridge. | * Major Incident | * Conference bridge opened |
| 7.6 | Involve related support groups | * All related Resolution groups are informed about the Major Incident and asked to join the Conference Bridge. | * Conference bridge opened | * Respective support groups informed and joined on bridge |
| 7.7 | Determine additional /specific stakeholders | * Stakeholders for communication are determined by Major Incident Manager in consultation with support groups & customer | * Major Incident * Additional/specific Stake holders identified | * Additional/specific Stake holders identified |
| 7.8 | Need to invoke DR | * Check if DR needs to be invoked, If yes go to DR Process else follow 7.7 | * Major Incident | * DR Invoked (if needed) |
| 7.9 | Co-ordinate resolution | * Major Incident Manager will coordinate with the support groups till the resolution of the incident | * Conference bridge opened * Related support groups informed and joined on bridge | * Co-ordination for resolution |
| 7.10 | Is MI Resolved | * In case, if the incident is resolved, then follow task 7.13 for initiating Problem ticket if applicable. * If incident not resolved, then follow task 7.11 for further investigation | * Incident resolution | * Incident resolved * Incident not resolved |
| 7.11 | Coordinate to update incident record | * Major Incident Manager will coordinate with support team for due update of incident record | * Coordination for resolution | * Updated incident record |
| 7.12 | Communicate status to stakeholders | * Major Incident Manager updates the status to the identified stakeholders as per the communication plan. | * Status update | * Communication to stake holders |
| 7.13 | Final Resolution update to Stakeholders | * Obtain service resolution confirmation and send the final resolution update to respective stakeholders. | * Major Incident Resolved | * Final email notification to stakeholders |
| 7.14 | Initiate problem ticket | * Major Incident Manager will coordinate with the problem manager for creating the problem ticket | * Major Incident resolved | * Problem ticket created |

# Roles and Responsibilities

This Section describes the details of RACSI chart and Roles and Responsibilities

## RASCI Chart

|  |  |  |
| --- | --- | --- |
| **Legend:** |  | R= Responsible for a particular action, but not necessarily authority |
|  |  | A = Accountable for the action. There is only one person accountable for any given action. |
|  |  | S =Support, the person is supposed to support in resolution |
|  |  | C= Consulted before the action (but not necessarily agree with it) |
|  |  | I= Informed after the action (need to know basis) |

Table 8: Responsibility Matrix for Process

| **Process / Task Level** | **Task Description** | **User** | **Service Desk** | **Resolver Group L1** | **Resolver Group L2/L3** | **Incident Manager** | **Operational Manager** | **Major Incident Manager** | **Problem Manager** | **Vendor** | **Change**  **Manager** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Sub Process - 1.0** | **Initiate Incident** | **R** | **R** | **R** | **-** | **A** | **-** | **-** | **-** | **-** | **-** |
| **Sub Process - 2.0** | **Detection & Recording** | **I** | **R** | **R** | **-** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 2.1 | Collect & Record Info | **C** | **R** | **-** | **-** | **I** | **-** | **-** | **-** | **-** | **-** |
| Task 2.2 | Validate User Profile Data | **C** | **R** | **-** | **-** | **I** | **-** | **-** | **-** | **-** | **-** |
| Task 2.3 | Is Data correct? | **I** | **R** | **-** | **-** | **I** | **-** | **-** | **-** | **-** | **-** |
| Task 2.4 | Is IM/ SR | **I** | **R** | **-** | **-** | **I** | **-** | **-** | **-** | **-** | **-** |
| Task 2.5 | Validate CI Information | **C** | **-** | **R** | **-** | **I** | **-** | **-** | **-** | **-** | **-** |
| Task 2.6 | Is information correct | **I** | **I** | **R** | **-** | **I** | **-** | **-** | **-** | **-** | **-** |
| **Sub Process - 3.0** | **Classification and Initial Support** | **I** | **R** | **R** | **S** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 3.1 | Assign Proper Category | **-** | **R** | **R** | **-** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 3.2 | Assign Impact Code | **-** | **R** | **R** | **-** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 3.3 | Assign Priority | **-** | **R** | **R** | **-** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 3.4 | Generate Incident Record | **-** | **R** | **R** | **-** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 3.5 | Inform Incident Reference to user | **I** | **R** | **R** | **-** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 3.6 | Is Major Incident | **I** | **I** | **I** | **-** | **A** | **C,I** | **C,I** | **-** | **-** | **-** |
| Task 3.7 | Match Known Error Database | **-** | **I** | **R** | **-** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 3.8 | Extract resolution or workaround action from known error database | **I** | **-** | **R** | **-** | **A** | **-** | **-** | **I** | **-** | **-** |
| Task 3.9 | Update incident count on known error record | **-** | **-** | **R** | **-** | **A** | **-** | **-** | **I** | **-** | **-** |
| Task 3.10 | Update incident record with ID of known error | **-** | **-** | **R** | **-** | **A** | **-** | **-** | **I** | **-** | **-** |
| Task 3.11 | Update incident record with classification data | **-** | **-** | **R** | **-** | **A** | **-** | **-** | **I** | **-** | **-** |
| Task 3.12 | Inform customer of workaround / Solution | **I** | **-** | **R** | **-** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 3.13 | Match Existing Problem Record | **-** | **-** | **R** | **-** | **A** | **-** | **-** | **I** | **-** | **-** |
| Task 3.14 | Update incident count on problem record | **I** | **-** | **-** | **R** | **A** | **-** | **-** | **I** | **-** | **-** |
| Task 3.15 | Update Incident record with ID of problem record | **-** | **-** | **-** | **R** | **A** | **-** | **-** | **I** | **-** | **-** |
| Task 3.16 | Update incident record with classification data | **-** | **-** | **-** | **R** | **A** | **-** | **-** | **I** | **-** | **-** |
| Task 3.17 | Is SOP Available | **-** | **-** | **R** | **C** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 3.18 | Assign to Level 2 | **-** | **-** | **R** | **C** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 3.19 | Vendor intervention | **I** | **I** | **R** | **R** | **A** | **I** | **-** | **I** | **-** | **-** |
| Task 3.20 | Update Worklog and raise incident for Vendor | **I** | **I** | **R** | **R** | **A** | **-** | **-** | **-** | **I** | **-** |
| Task 3.21 | Vendor Resolution available | **I** | **I** | **R** | **R** | **A** | **-** | **-** | **I** | **C** | **-** |
| **Sub Process - 4.0** | **Investigation and Diagnosis** | **I** | **I** | **-** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 4.1 | Initial Investigation and Diagnosis | **-** | **I** | **-** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 4.2 | Is Ticket Accepted | **-** | **I** | **-** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 4.3 | Update Working & Reassign to SD | **I** | **I** | **-** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 4.4 | More Inputs required | **I** | **I** | **-** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 4.5 | Gather information from User | **R** | **R** | **-** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 4.6 | Validate Priority | **-** | **I** | **-** | **R** | **A** | **C** | **-** | **-** | **-** | **-** |
| Task 4.7 | Is Major Incident | **I** | **I** | **I** | **R** | **A** | **C,I** | **C,I** | **I** | **-** | **-** |
| Task 4.8 | Refer KEDB for Existing Workaround / Solution | **-** | **I** | **-** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 4.9 | Carry out Detailed Diagnosis | **-** | **I** | **-** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 4.10 | Is solution/workaround available | **-** | **I** | **-** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 4.11 | Need Vendor intervention | **-** | **I** | **-** | **R** | **A** | **I** | **-** | **-** | **I** | **-** |
| Task 4.12 | Update Working and Assign to Vendor | **-** | **I** | **-** | **R** | **A** | **I** | **-** | **-** | **-** | **-** |
| Task 4.13 | Receive Vendor Support & Resolution | **I** | **I** | **-** | **R** | **A** | **I** | **-** | **I** | **C** | **-** |
| Task 4.14 | Need L3 intervention | **-** | **I** | **-** | **R** | **A** | **I** | **-** | **-** | **-** | **-** |
| Task 4.15 | Update Worklog and reassign to L3 | **I** | **I** | **-** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| **Sub Process- 5.0** | **Resolution & Recovery** | **I** | **I** | **-** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 5.1 | Carry out the tasks for incident resolution | **-** | **-** | **R** | **-** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 5.2 | Resolution/Workaround available | **-** | **I** | **-** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 5.3 | Implement Workaround | **I** | **I** | **-** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 5.4 | Carry Out the Tasks for the Incident Resolution | **-** | **-** | **R** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 5.5 | Carry out the tasks to recover | **-** | **-** | **R** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 5.6 | Is Incident Resolved | **-** | **I** | **-** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 5.7 | Update work log and resolve incident | **I** | **R** | **-** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 5.8 | Is Problem Record Required | **I** | **I** | **-** | **R** | **A** | **-** | **-** | **C, I** | **-** | **-** |
| Task 5.9 | Is Change Record Required | **I** | **I** | **-** | **R** | **A** | **-** | **-** | **-** | **-** | **C, I** |
| **Sub Process - 6.0** | **Confirmation & Closure** | **I** | **I** | **-** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 6.1 | Confirm resolution with user (Auto email) | **I** | **R** | **R** | **R** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 6.2 | Is User Satisfied | **R** | **I** | **R** | **R** | **A** | **I** | **-** | **-** | **-** | **-** |
| Task 6.3 | Re-open incident | **A, R** | **R** | **-** | **I** | **I** | **I** | **-** | **-** | **-** | **-** |
| Task 6.4 | Ask user to provide feedback & close the incident record | **I** | **R** | **-** | **-** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 6.5 | Provide feedback and close incident | **R** | **R** | **-** | **I** | **A** | **-** | **-** | **-** | **-** | **-** |
| Task 6.6 | Auto hard closure of the incident | **I** | **-** | **-** | **-** | **A,R** | **-** | **-** | **-** | **-** | **-** |
| **Sub Process - 7.0** | **Major Incident** | **I** | **I** | **-** | **R** | **S, C** | **C** | **A** | **I** | **-** | **-** |
| Task 7.1 | Is Qualified case | **I** | **I** | **-** | **R** | **S, C** | **I** | **A, R** | **-** | **-** | **-** |
| Task 7.2 | Accept Major Incident | **I** | **I** | **-** | **R** | **S, C** | **I** | **A, R** | **-** | **-** | **-** |
| Task 7.3 | Review incident details | **I** | **I** | **-** | **R** | **S, C** | **I** | **A, R** | **-** | **-** | **-** |
| Task 7.4 | Inform the Stakeholders | **-** | **I** | **-** | **R** | **S, C** | **I** | **A, R** | **-** | **-** | **-** |
| Task 7.5 | Open Conference Bridge | **-** | **-** | **-** | **C** | **S, C** | **I** | **A, R** | **-** | **-** | **-** |
| Task 7.6 | Involve related support groups | **-** | **-** | **-** | **C** | **S, C** | **I** | **A, R** | **-** | **-** | **-** |
| Task 7.7 | Determine additional /specific stakeholders | **I** | **-** | **-** | **C** | **S, C** | **C** | **A, R** | **-** | **-** | **-** |
| Task 7.8 | Need to invoke DR | **I** | **I** | **I** | **R** | **S, C** | **C** | **A** | **-** | **-** | **-** |
| Task 7.9 | Co-ordinate resolution | **I** | **-** | **-** | **R** | **S, C** | **I** | **A, R** | **-** | **-** | **-** |
| Task 7.10 | Is Incident Resolved | **I** | **I** | **I** | **R** | **S, C** | **I** | **A** | **-** | **-** | **-** |
| Task 7.11 | Coordinate to update incident record | **-** | **I** | **-** | **R** | **S, C** | **I** | **A, R** | **-** | **-** | **-** |
| Task 7.12 | Communicate status to stakeholders | **I** | **I** | **-** | **C, I** | **S, C** | **I** | **A, R** | **-** | **-** | **-** |
| Task 7.13 | Final Resolution update to Stakeholders | **-** | **-** | **-** | **C, I** | **S, C** | **I** | **A, R** | **-** | **-** | **-** |
| Task 7.14 | Initiate problem ticket | **I** | **-** | **-** | **R** | **R** | **I** | **A, R** | **I** | **-** | **-** |

## Roles and Responsibilities

The Roles & Responsibilities of various major roles are listed below:

### Requestor

Responsibilities include:

* Raise / Report Incident
* Provide detailed description of issue
* Provide feedback and close the incident
* Reopen the incident if the resolution is unsatisfactory

### Service Desk

Responsibilities include:

* Log, categorize and prioritize incident(s) based on the details of the Incident description and impact / merit
* Relates new incidents to existing ones when applicable (maintain Child Parent Incident Relationship)
* Transfers the incident to relevant / appropriate support team
* Tracks the incident till closure to ensure incidents are resolved within agreed SLAs
* Keep the user informed of the incident status
* Provide First call resolution for agreed First Call resolvable categories

### Resolver group L2/L3

Responsibilities include:

* Resolve incidents within agreed service levels
* Escalate the unresolved incidents to higher support levels at the appropriate time (Vendor, Product Owner / Third Party Technology Provider etc.)
* Make appropriate use of available resources to resolve incidents (people, tools and processes)
* Communicate the Incident status internally and externally as applicable
* Interface with other process as required to resolve incident
* Maintain up-to-date knowledge database / Known error database
* Update Incident Work log with updated status
* Forward / Assign Incident to appropriate CCC/ISD incase if the resolution does not lie with the currently assigned group

### Operation Manager

Responsibilities include:

* Monitors the service delivered by the team
* Assist the support staff through the process within their domain
* Analyses performance, delivery metrics and KPIs
* Identify improvement areas
* Ensure effective coordination of support activities within groups and across groups as and when needed
* Manage support staff performance and adherence to process
* Create and execute action plans when necessary to ensure resolution
* Ensure appropriate skills are available within the team / group to perform day to day operations

### Incident Manager

Responsibilities include:

* Reviews escalated incidents, and takes appropriate action such as assigning an incident owner
* Track and follow up on Open, Pending incidents with various teams for timely closure
* Generate Incident Report and share with relevant stakeholders
* Ensures that incidents are resolved through the standard Incident Management process

### Major Incident Manager

Responsibilities include:

* Opens the communication channel at the time of crisis
* Determines appropriate stakeholders and contents for communication updates
* Provides Major Incident Report

## Risk & Dependencies

The risks mentioned below are few of the examples, and not limited to those mentioned -

| **#** | **Risk/ Dependency** | **Controls** | **Treatment Plan** |
| --- | --- | --- | --- |
| 1 | Being inundated with incidents that cannot be handled within acceptable timescales due to a lack of available or properly trained resources | Adequate Resource Availability  Trained and skilled resources to be on-boarded | Frequent training and knowledge sharing session to ensure that resources are up-to-date with the required skills |
| 2 | Incidents are blogged down due poor event correlation through monitoring tool | Proper Event correlation to be configured to ensure unwanted events are not logged as incidents | Periodic reviews to ensure proper functioning of Event correlation |
| 3 | Unavailability of information about problems and known errors resulting in delayed resolutions | Ensure proper integration with Knowledge Management systems | Timely updates to the knowledge articles are KEDB will ensure quicker resolutions of incidents |
| 4 | All the incidents are not logged / recorded | Policies to ensure that all the incidents are logged / recorded in central ITSM tool | User Requestor needs to be encouraged to log the incidents through the ITSM portal or CCC/ISD to raise the incidents on behalf of user |

# Key Performance Indicators

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sr. No** | **Process/ Tower** | **Metric Name** | **Metric Description** | **Formula** | **Target %** | **Reporting Frequency** |
| 1 | Incident Management | Response SLA compliance | Percentage of Response SLA fulfillment | (No. of Incidents with response SLA met/ Total No. of Incidents) \* 100 | >90% | Monthly |
| 2 | Resolution SLA Compliance | Percentage of Resolution SLA fulfillment | (No. of Incidents with resolution SLA met/ Total No. of Incidents) \* 100 | >90% | Monthly |
| 3 | Re-Opened Incidents | Percentage of Re-Opened Incidents | (No. of Incidents Re-opened/ Total No. of Incidents) \* 100 | <5% | Monthly |

# Handling Guidelines

## Exception Handling Process

* In case if the ticketing tool is not accessible/ unavailable, the incidents will be registered manually in Excel sheet
* Priority of an incident should only be modified post proper approval
* In case if Incidents are reported for items / CI which are mentioned in the Operational Risk Register and miss the SLA, then SLA exception will be approached for such incidents

## Escalation Handling

* During incident lifecycle, CCC/ISD can receive the notification from various sources. This notification shall be used to trigger escalation of an incident. For Escalation to be followed Refer [**Appendix E**.](#_Appendix_E_–)

Note**:** 3 strike processes will follow for Incident resolution of pending cases or for incidents where resolver teams are not able to contact the Incident Requestor (User Action Required)

# Appendix

|  |
| --- |
| Appendix A – Incident Priority Matrix |



|  |
| --- |
| Appendix B – Incident Priority Change Approver Template |



|  |
| --- |
| Appendix C – Major Incident Management Template |



|  |
| --- |
| Appendix D –Ticket Status |



|  |
| --- |
| Appendix E – Escalation Matrix |



|  |
| --- |
| Appendix F – Vendor Contact Details |



|  |
| --- |
| Appendix G – Notification |

act Details



|  |
| --- |
| Appendix H – Sample IM Data Gathering Template |



|  |
| --- |
| Appendix I – TASMU User Persona mapping |

act Details



|  |
| --- |
| Appendix J – Recommended Best practices |

act Details

