Incident Management Process

Standard Practises Document

GAVS Technologies N.A., Inc

116 Village Blvd, Suite 200, Princeton,

New Jersey 08540, USA.

http://www.gavstech.com/

Document Version

Document Revision Number	2.3
Effective Date	22-Jan-24
Owner	GAVS Quality Team
Modified by	Gouri Mahendru
Approved by	Sekar T

Document Revision History

Version No.	Release date	Summary of changes	Prepared by	Approved by
1.0	30-Jan-20	Initial Document	Rama Vani Periasamy	Sekar T
2.0	19-Mar-20	Updated Section E-2 Templates	Rama Vani Periasamy	Sekar T
2.1	1-Jun-20	Updated as per ISO 20000-1:2018 reference	Santhiya P	Sekar T
2.2	26-Jan-23	Annual Review	Gouri Mahendru	Sekar T
2.3	22-Jan-24	Updated the process workflows in Section B (1)	Gouri Mahendru	Sekar T

Contents

Section A: Introduction

1. Overview

The following Incident Management Process has been designed for the GAVS IT Service Management program. It will be used as a reference for the implementation and use of the Incident Management process on an ongoing basis. This process document is based on the best practices described in the Information Technology Infrastructure Library (ITIL®) Framework.

It includes Incident Management goals, objectives, scope, policies, key terms, roles, responsibilities, authority, process diagrams and associated activity descriptions. This Process will have relationships with other Processes and those documents should be read and understood along with this, the primary related processes being Problem and Change Management.

2. Definition

ITIL® defines an **Incident** as an unplanned interruption to or quality reduction of an IT service. Incidents can include failures or degradation of your services reported by users of those services; by your own technical staff; or automatically from monitoring tools.

Incident Management is the process responsible for managing the lifecycle of all Incidents irrespective of their origination.

The Incident Management process is triggered in three ways:

- End user contacts the Service Desk Single Point of Contact (SPOC) to report service disruption.
- Auto-detected events generate an incident in the Management tracking tool.
- Internal support groups identify a service disruption (or potential disruption) on their managed systems and generate an incident.

3. Process Objective

The primary objective of the Incident Management process is to restore services as soon as possible and communicate the solution or workaround to the end user.

The goals for the Incident Management process are to:

- Restore normal service operation as quickly as possible.
- Minimize the adverse impact on business operations.
- Ensure that agreed levels of service quality, standardized methods and procedures are maintained.
- Effectively and efficiently use resources to support the Business during service failures or disruptions.

4. Scope

The scope of the Incident Management process refers to the extent or boundaries to which the Incident Management process is applied.

- 24*7 Incident Management is available for all IT Service Providers, End user issues, internal and third parties, service failures and security incidents, which impact IT performance and the agreed Service Levels.
- It includes events resulting from failures, queries reported through the Service Desk or alerts generated through monitoring tools.
- The recorded incidents are categorized, prioritized, owned, and followed through to service recovery and incident resolution.
- It encompasses call management, communication, and efficient support.

Incident Management will be deployed and applicable to:

- Customers covered by Service Level Agreements (SLAs) specifying service targets for resolution of Incidents.
- Service Providers adopting the Incident Management responsibilities outlined by Service Level Agreements, Operating Level Agreements (OLAs), and Underpinning Contracts (UCs),
- Services to which Incident Management Resolution Targets agreed in Service Level Agreements apply.

4.1. Out of Scope

Incident Management does not fix the underlying problem (Root Cause) of the incident. Finding the Root Cause is a function of Problem Management and is fixed either through Change Management or Service Request Fulfillment.

5. Policy

The policies defined for Incident Management process are listed as follows:

- There will be one common process to manage all types of incidents across the organization.
- Authorized end users should contact the Service Desk SPOC to report all incidents.
- All incidents must be logged and tracked within a centralized database.
- The end user will receive status information on incidents throughout the incident lifecycle, at appropriate or agreed time intervals.
- There will be clear linkages between Incident records, Problem records, Known Errors, and Requests for Change (RFC).
- Closure of incidents is subject to successful resolution and restoration.
- There will be a defined escalation process to ensure timely resolution of incidents within agreed

SLA.

6. Benefits

There are several qualitative and quantitative benefits that can be achieved, for both the IT service providers and the customers by implementing an effective and efficient Incident Management process.

6.1 Benefits to the IT Service Provider

- Improved ability to identify potential improvements to IT services.
- Better prioritization of efforts
- Better use of resources, reduction in unplanned labor and associated costs
- More control over IT services
- Better alignment between departments
- More empowered IT staff
- Better control over vendors through Incident Management metrics

6.2 Benefits to the Users

- Higher service availability due to reduced service downtime
- Reduction in unplanned labor and associated costs
- IT activity aligned to real-time business priorities.
- Identification of potential improvements to services
- Identification of additional service or training requirements for the business or IT

Section B: Process Flow

1. High-level Incident Management Process

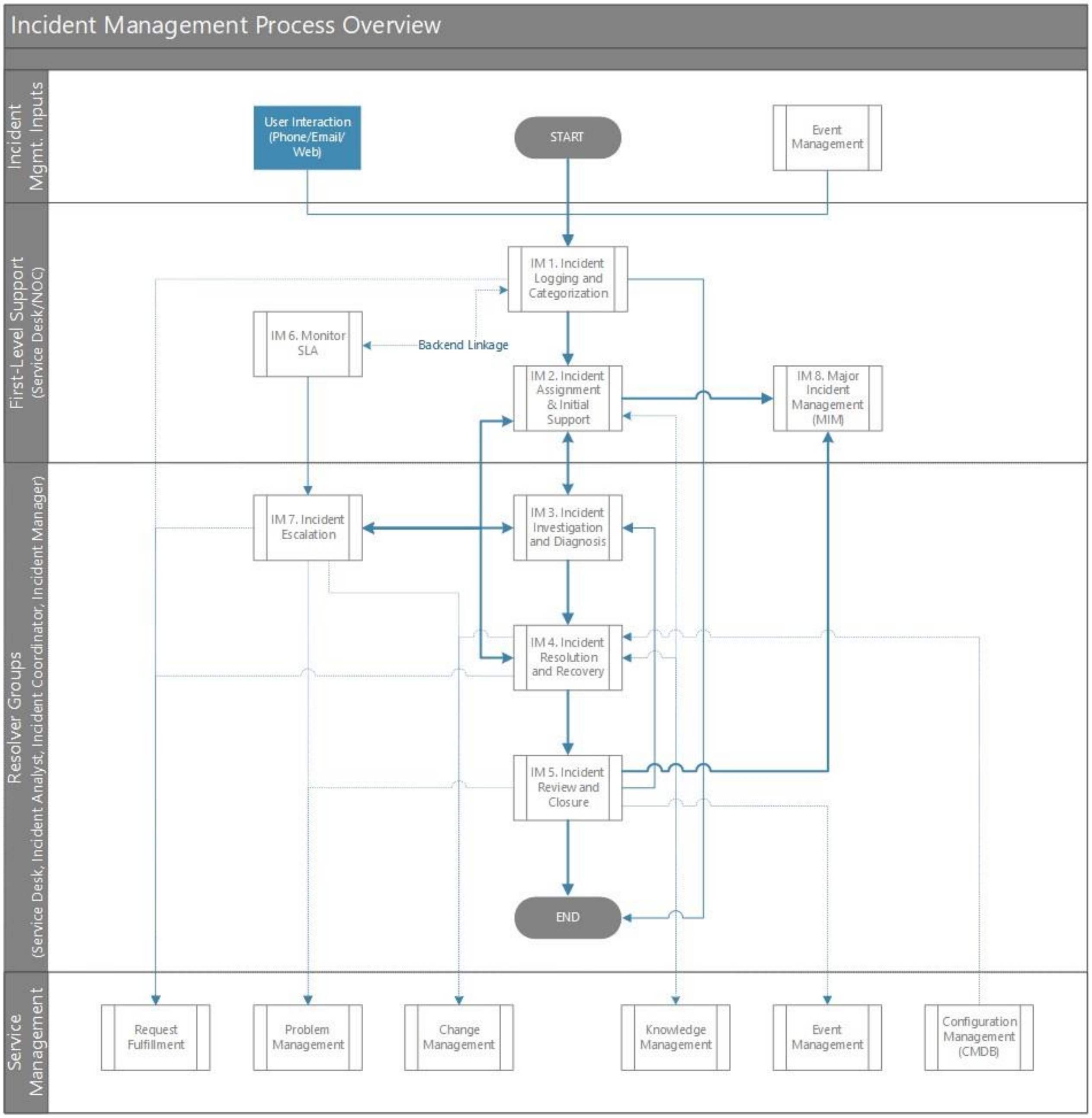

Incident Management Process Overview
Incident Mgmt. Inputs
First-Level Support (Service Desk/NOC)
Resolver Groups (Service Desk, Incident Analyst, Incident Coordinator, Incident Manager)
Service Management
User Interaction (Phone/Email/ Web)
START
Event Management
IM 1. Incident Logging and Categorization
IM 6. Monitor SLA
Backend Linkage
IM 2. Incident Assignment & Initial Support
IM 8. Major Incident Management (MIM)
IM 7. Incident Escalation
IM 3. Incident Investigation and Diagnosis
IM 4. Incident Resolution and Recovery
IM 5. Incident Review and Closure
END
Request Fulfillment
Problem Management
Change Management
Knowledge Management
Event Management
Configuration Management (CMDB)

Fig. 1: High-level Incident Management Flowchart

In ITIL®, incidents go through a structured workflow that encourages efficiency and best results for both providers and customers. ITIL® recommends the incident management process follow these steps:

1. Incident Logging and Categorization
2. Incident Assignment and Initial Support
3. Incident Investigation and Diagnosis
4. Incident Resolution and Recovery
5. Incident Review and Closure
6. Monitor SLAs
7. Incident Escalation
8. Major Incident Management

1.0. Logging and Categorization

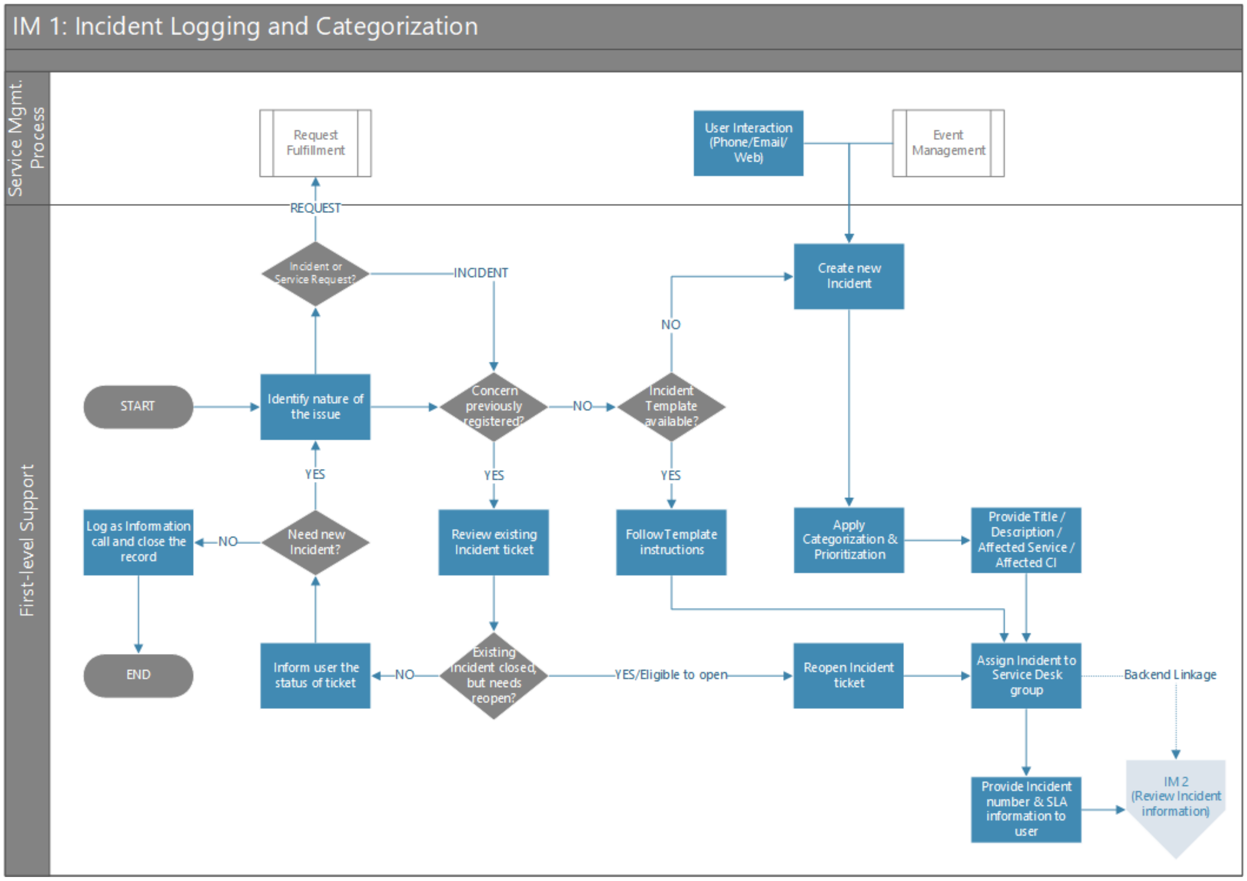

IM 1: Incident Logging and Categorization
Service Mgmt. Process
First-level Support
Request Fulfillment
User Interaction (Phone/Email/ Web)
Event Management
REQUEST
Incident or Service Request?
INCIDENT
Create new Incident
NO
START
Identify nature of the issue
Concern previously registered?
NO
Incident Template available?
YES
YES
YES
Log as Information call and close the record
NO
Need new Incident?
Review existing Incident ticket
Follow Template instructions
Apply Categorization & Prioritization
Provide Title / Description / Affected Service / Affected CI
END
Inform user the status of ticket
NO
Existing incident closed, but needs reopen?
YES/Eligible to open
Reopen Incident ticket
Assign Incident to Service Desk group
Backend Linkage
Provide Incident number & SLA information to user
IM 2 (Review Incident information)

Fig. 2: Identification and Recording Sub-process.

Procedure	Description	Input	Output
Phone / Email	▪ User identifies a disruption of a service or need for an additional service. ▪ Users can notify service desk about the incident through Phone or Email.	▪ Disruption of Service ▪ Need for additional service	▪ Contact Service Desk
Web Portal	▪ User identifies a disruption of a service or need for an additional service. ▪ Users can open incident tickets by themselves through web portal. Users need to fill basic details. ▪ If possible, the web portal should be configured to display a message about any disrupted services or scheduled disruption of services.	▪ Disruption of Service ▪ Need for additional service	▪ Incident registered through web
Monitoring Tools	▪ Incidents are also detected by a monitoring tool, a command-and-control group who manages the monitoring tools. ▪ Command and control group can also open a ticket if a monitoring condition is observed, which needs further investigation.	▪ Disruption of Service	▪ Case registered in system
Collect and record information	▪ Greet and welcome end user. ▪ Notification of any relevant known outage/problem issues would be extended to the user at this time. ▪ Information about the success or failure of releases and future release dates, from the release and deployment management process. The personnel handling this should be provided with relevant reports and data / information which provides this information from release and deployment process. ▪ Access to information like service request management procedure, known errors, problem resolutions, and the CMBD is provisioned for the Service Desk team. ▪ Service Desk Agent collects or	▪ End-user contacts Service Desk	▪ Incident registered in system. ▪ Basic Incident details recorded and verified

	verifies the basic details on a case-to-case basis. ▪ Refer Appendix A for ticket record details.		
Validate user (for internal SD Process)	▪ System performs authentication for end user, from user database. Also, SD authenticates end user for licensing, passwords, and access. ▪ If the end user is not validated, revert to user for getting necessary details. ▪ If end user is authorized, proceed with next step.	▪ Registered Incident ▪ User database	▪ User validated. ▪ Request rejected due to failure of authentication. ▪ User profile update process initiated. ▪ Populated Incident with user data
Validate issue (for Middleware – Application support)	▪ Validate the issue/complaint with respect the middleware application environment. ▪ If issue / complaint is not validated, revert to user for getting necessary details. ▪ If issue / complaint is validated with respect to environment, proceed with next step	▪ Registered Incident ▪ Issue / Complaint details	▪ Issue / Complaint validated. ▪ issue sent back to requestor due to failure of validation. ▪ Populated Incident with environment data

2.0. Assignment and Initial Support

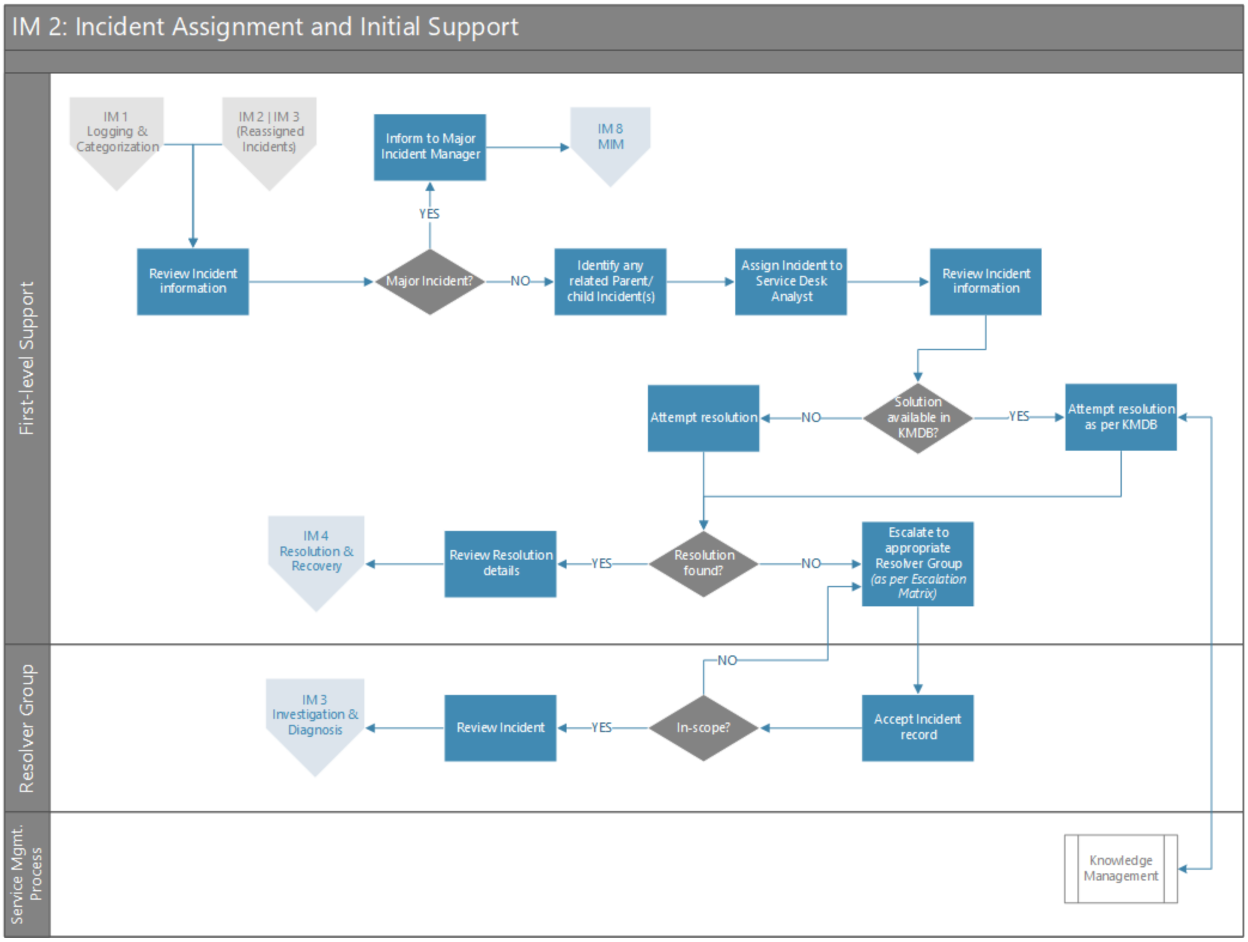

IM 2: Incident Assignment and Initial Support
First-level Support
Resolver Group
Service Mgmt. Process
IM 1 Logging & Categorization
IM 2 | IM 3 (Reassigned Incidents)
Inform to Major Incident Manager
IM 8 MIM
YES
Review Incident information
Major Incident?
NO
Identify any related Parent/ child Incident(s)
Assign Incident to Service Desk Analyst
Review Incident information
Attempt resolution
NO
Solution available in KMDB?
YES
Attempt resolution as per KMDB
IM 4 Resolution & Recovery
Review Resolution details
YES
Resolution found?
NO
Escalate to appropriate Resolver Group (as per Escalation Matrix)
NO
IM 3 Investigation & Diagnosis
Review Incident
YES
In-scope?
Accept Incident record
Knowledge Management

Fig. 3: Classification and Initial Support Sub-process

Procedure	Description	Input	Output
Assign Proper Category (SD & Middleware Apps)	▪ Every ticket needs to be assigned standard category. The same codes shall be available in ITSM tool in the form of a drop-down list.	▪ Recorded ticket with basic details	▪ Classification code assigned
Assign impact & Urgency (SD)	▪ Impact & urgency are assigned according to the criticality of the issue	▪ Classified ticket ▪ Impact and Urgency guidelines	▪ Impact and Urgency assigned
Severity automatically assigned by the system (SD)	▪ Urgency can be determined by the user and entered as part of basic details. ▪ If the ticket is a Service Request, then SR procedure is to be followed (refer to the Request Fulfilment Process). ▪ If the incident is reported by a VIP user, SD must follow the	▪ Classified ticket with Urgency and Impact code assigned. ▪ Priority matrix	▪ Priority assigned

	VIP incident management procedure if any as customized during the initial process definition activity. ▪ The tool should be configured to select the priority code automatically based on priority matrix.		
Generate Incident Record (SD & Middleware Apps)	▪ On completing all necessary details, the service desk needs to save the details and generate a ticket in the system. ▪ The system is required to generate a unique serial number for the newly generated ticket. This number can be used for all references. ▪ The incidents that are logged are verified by SD. SD gets back to user, if lack of information, categorize, assign it correctly, prioritize, and assign to proper group or solve it themselves.	▪ Tickets with all the necessary details	▪ Ticket generated into system. ▪ Ticket number
Auto – generated email to user with incident details (SD & Apps)	▪ The ticket number is to be informed to the end user using Phone, Email or Web. ▪ As a best practice it is recommended that ticket numbers should be automatically conveyed to the user by email generated by the tool. ▪ If the ticket is classified as Major Incident, go to Major Incident Management. ▪ If the ticket is classified as Security Incident, go to Security Incident Management sub-process of Information Security Management.	▪ Ticket generated	▪ Ticket number informed to the user. ▪ Major / Security Incident Management process invoked
Refer KMDB (SD)	▪ Either SD agent or resolver resource can refer to the sol DB	▪ Ticket generated	▪ Solution / Workaround identified
Take Ownership (SD & Apps)	▪ If in the previous step the solution or work around is identified, the same can be used to resolve the incident. ▪ Before proceeding for the resolution, SDA needs to take ownership of the incident. ▪ Proceed to Resolution and	▪ Solution / Workaround identified	▪ Ticket owned by SD

	Recovery		
Assign to support group / specialist (SD & Apps)	▪ If in the above step, the solution or work around is not identified or SD is not sure of the available solution, the ownership needs to be transferred to Level 2 support group for investigation and diagnosis. ▪ The assignment to the support group / specialist is to be done in accordance with the assignment procedure.	▪ Solution / Workaround not identified	▪ Ownership transferred to support group / specialist

3.0. Investigation and Diagnosis

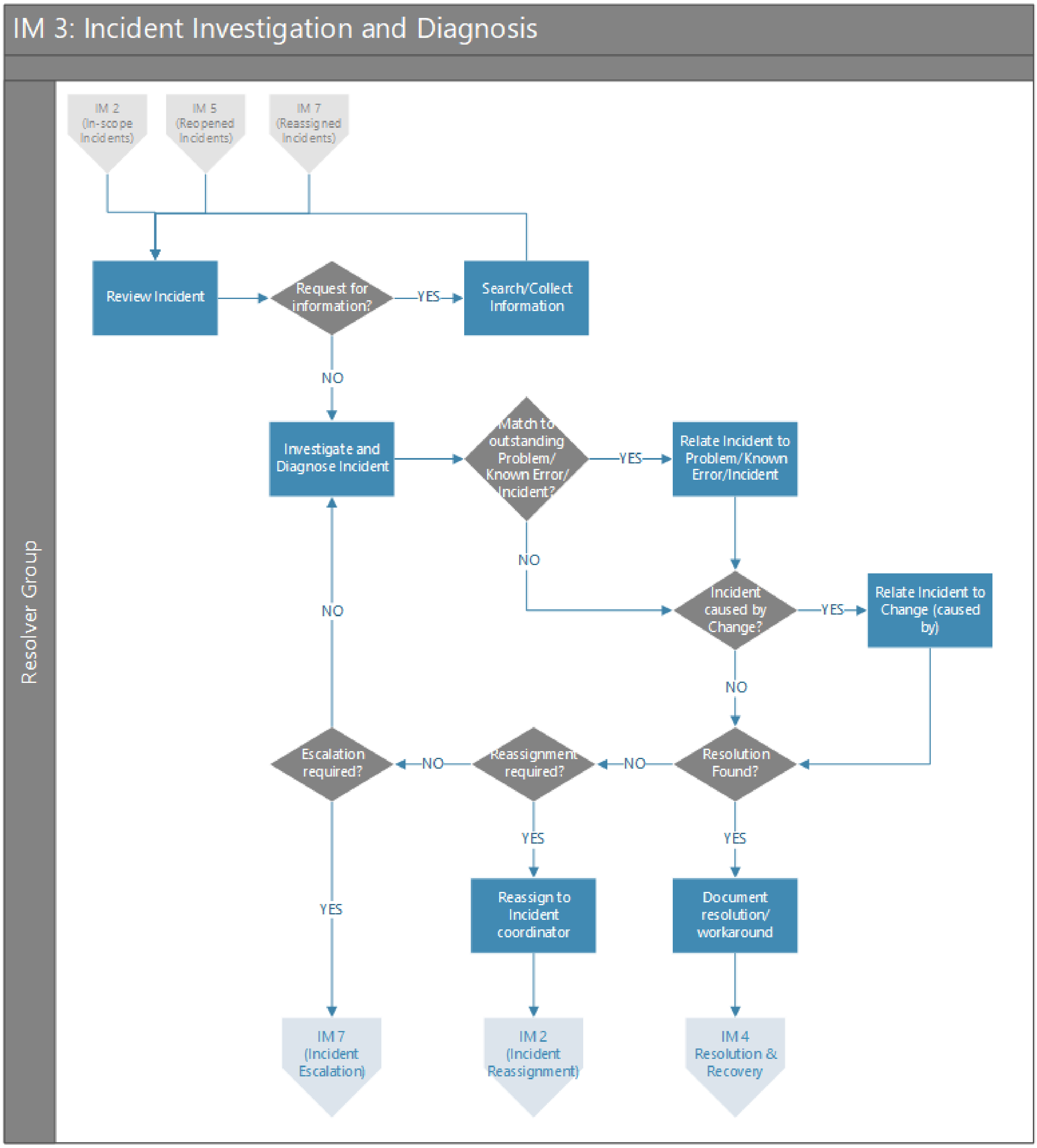

IM 3: Incident Investigation and Diagnosis
Resolver Group
IM 2 (In-scope Incidents)
IM 5 (Reopened Incidents)
IM 7 (Reassigned Incidents)
Review Incident
Request for information?
YES
Search/Collect Information
NO
Investigate and Diagnose Incident
Match to outstanding Problem/ Known Error/ Incident?
YES
Relate Incident to Problem/Known Error/Incident
NO
Incident caused by Change?
YES
Relate Incident to Change (caused by)
NO
Resolution Found?
NO
Reassignment required?
NO
Escalation required?
NO
YES
YES
YES
Document resolution/ workaround
Reassign to Incident coordinator
IM 7 (Incident Escalation)
IM 2 (Incident Reassignment)
IM 4 Resolution & Recovery

Fig. 4: Investigation and Diagnosis Sub-process

Procedure	Description	Input	Output
Initial Investigation and Diagnosis	▪ Ticket assigned to support specialist, is investigated, and diagnosed to ensure correct assignment. ▪ In case of correct assignment, support specialist must assume the ownership.	▪ Ticket assigned to support specialist	▪ Initial investigation and diagnosis performed. ▪ Ticker accepted by support.
Update work log and assign to SD or valid service group	▪ If the ticket is not routed to the appropriate specialist, or the scope of ticket is outside the technology area managed by support specialist, the same must be updated in ticket work log and reassigned to service desk.	▪ Ticket not accepted by support specialist	▪ Ticket updated and reassigned to Service Desk
Gather information from user	▪ If the details available in incident records are insufficient for detailed diagnosis, the same should be collected from the user.	▪ Ticket accepted by support specialist	▪ More information generated from user
Validate priority	▪ The priority is again to be validated based on the investigation done by a support specialist. ▪ If required, the priority needs to be changed by support specialist by changing the impact code or urgency code after consultation with user.	▪ More information on ticket available	▪ Priority validated / changed
Validate category	▪ The classification is again to be validated based on the investigation done by support specialist. ▪ If required, the classification needs to be changed by a support specialist. ▪ If the Incident is identified as Major Incident, then follow Major Incident Process.	▪ More information on ticket available	▪ Classification validated / changed
Refer KMDB for existing workaround / solution	▪ Support specialist can refer the KMDB for existing solutions or known errors.	▪ Ticket priority and classification revalidated	▪ Solution / Workaround available
Conduct detailed diagnosis	▪ If the solution is still not known, a support specialist can conduct the detailed diagnosis. During this period, it is required to update the ticket at the agreed time interval and inform the end	▪ Ticket priority and classification revalidated	▪ Solution / Workaround available

	user accordingly. ▪ If the solution / workaround is identified, the same needs to be updated in ticket work log and proceed to step – Resolution and Recovery.		
Update worklog and work with vendor(s)	▪ If still the solution / workaround is not identified, support specialist must determine whether the vendor intervention is required. If so, the ticket is updated with an appropriate work log and resolver team will collaborate with vendor. ▪ The ownership of the ticket still lies with the support specialist and is responsible for updating the status in ticket and if required to the end user.	▪ Solution / Workaround not available ▪ Vendor assignment procedure	▪ Assign to vendor
Detailed diagnosis by vendor	▪ On assignment to the vendor, the ticket needs to be updated with vendor incident details. ▪ Ticket is updated by resolver group with inputs from vendor.	▪ Ticket to be discussed with Vendor for resolution	▪ Solution / Workaround provided by Vendor
Specialists with work on issue till resolution	▪ Specialist with update the work log. ▪ Specialist will work on Incident till resolution	▪ Solution / Workaround not available	▪ Raise a Problem ticket or RCA as required. ▪ Update worklog and Incident status

4.0. Resolution and Recovery

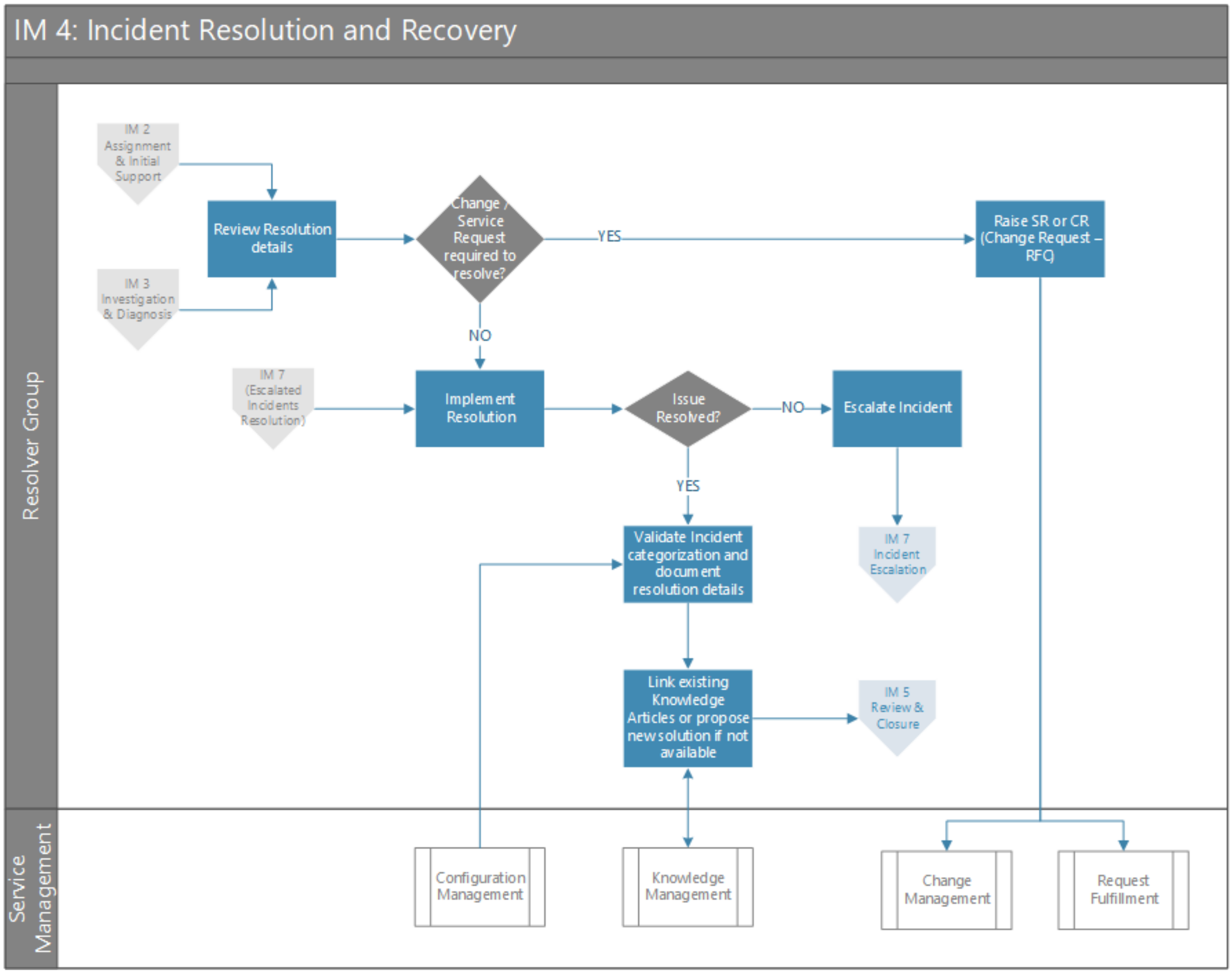

IM 4: Incident Resolution and Recovery
Resolver Group
Service Management
IM 2 Assignment & Initial Support
IM 3 Investigation & Diagnosis
Review Resolution details
Change / Service Request required to resolve?
YES
NO
Raise SR or CR (Change Request – RFC)
IM 7 (Escalated Incidents Resolution)
Implement Resolution
Issue Resolved?
NO
Escalate Incident
YES
Validate Incident categorization and document resolution details
IM 7 Incident Escalation
Link existing Knowledge Articles or propose new solution if not available
IM 5 Review & Closure
Configuration Management
Knowledge Management
Change Management
Request Fulfillment

Fig. 5: Resolution and Recovery Sub-process

Procedure	Description	Input	Output
Conduct the tasks for Resolution and Recovery	▪ Service Desk Agent on identifying the solution / workaround can start executing the tasks for resolution. ▪ Also, Support Specialist on identifying the solution / Workaround after detailed investigation and diagnosis can start executing the tasks for resolution. ▪ If the incident has been forwarded to the Vendor, then the resolution tasks will either be executed by the Support Specialist or Vendor after the vendor has identified the	▪ Solution / Workaround identified	▪ Resolution tasks executed

	solution/workaround.		
Update work log and resolve Incident	▪ To successfully resolve the incident, recovery steps need to be conducted if required. (Example: Restore data, configure application and so on) ▪ If incident is resolved, update the work log, and proceed to step - Confirmation and Closure. ▪ If incident is not resolved even after executing resolution tasks and performing recovery, one of the following decisions need to be taken: i) Open RCA Ticket – In case it is determined that the solution can only be achieved after performing problem analysis, open the RCA ticket. ii) Open Change Ticket - In case it is determined that the solution can only be achieved after performing a change, open the change ticket. iii) Revert to support specialist	▪ Resolution tasks executed	▪ Recovery performed. ▪ Problem ticket opened. ▪ Change ticket opened. ▪ Escalated to vendor. ▪ Work log updated and transferred to Service Desk
Update worklog for Confirmation and Closure	▪ On successful resolution and recovery, Support Specialist should update the work log and resolve the incident.	▪ Recovery performed	▪ Worklog updated and Incident resolved

5.0. Review and Closure

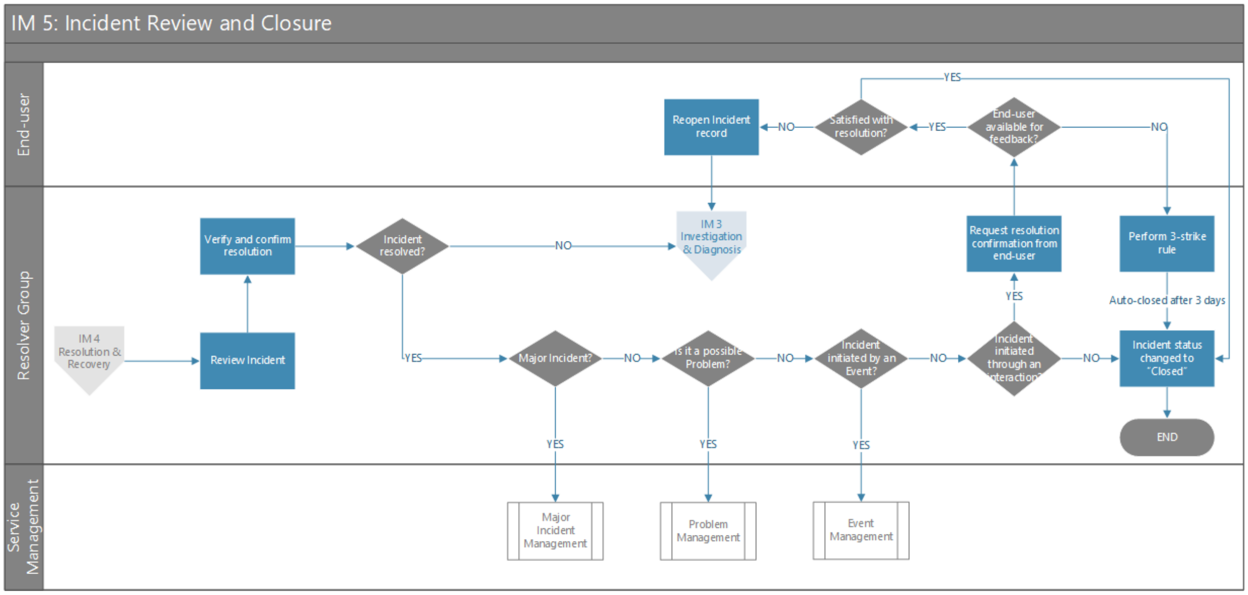
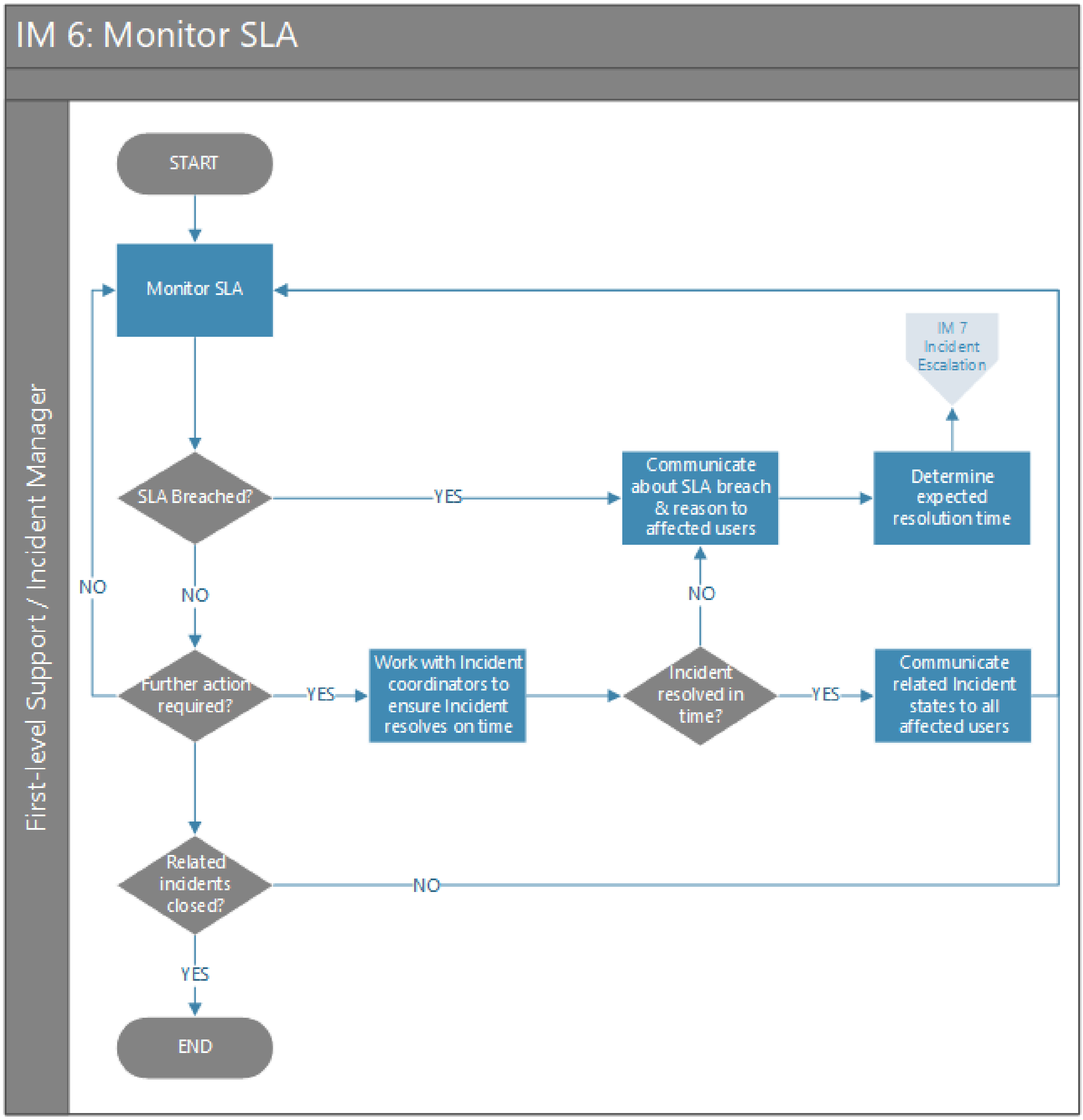

IM 5: Incident Review and Closure
End-user
Resolver Group
Service Management
Reopen Incident record
NO
Satisfied with resolution?
YES
End-user available for feedback?
YES
NO
IM 4 Resolution & Recovery
Review Incident
Verify and confirm resolution
Incident resolved?
NO
IM 3 Investigation & Diagnosis
Request resolution confirmation from end-user
Perform 3-strike rule
Auto-closed after 3 days
YES
Major Incident?
NO
Is it a possible Problem?
NO
Incident initiated by an Event?
NO
Incident initiated through an interaction?
NO
YES
Incident status changed to "Closed"
END
YES
YES
YES
Major Incident Management
Problem Management
Event Management

Fig. 8: Review and Closure Sub-process

Procedure	Description	Input	Output
Confirm resolution and User	▪ On resolution and recovery, the incident status is to be changed to "Resolved." At this point, the Resolution SLA clock should stop. Service Desk Agent need to confirm with the user whether the resolution provided is satisfactory. ▪ At least in XX % of incidents, Service Desk Agent should personally solicit the closure from User. ▪ SDA also needs to confirm that the Normal Service Operations are restored. If the service operations are not restored, the incident cannot be closed, and the status needs to be changed as "Pending" along with the reason. In this case, sub-process - Resolution and Recovery will be continued till the Normal Service Operations are restored.	▪ Incident resolved	▪ Resolution accepted by User. ▪ Resolution rejected by User
Reopen the Incident	▪ If the user is not satisfied with the resolution provided, the Incident is to be reopened in the system, by any one of the	▪ Resolution rejected by User	▪ Incident reopened

	below steps: ▪ By one-click automated option within the ticketing system ▪ Requester can contact Service Desk ▪ Requester can contact Resolver resource. ▪ The sub-process Escalation is to be followed from this point.		
Close the Incident record	▪ Service Desk to close the incident record, on successful resolution of the incident.	▪ Incident resolution	▪ Incident record closed
Auto close the Incident after hard closure limit	▪ Incident auto closed as per the predefined auto-closure time, ticket shall be closed by SD or auto-closed.	▪ Auto-closure time or close by Service Desk	▪ Incident record hard closed
User receives auto closure message	▪ User receives a closure message after the above step is completed	▪ Closure of the Incident	▪ Auto-closure message

6.0. Monitor SLA


IM 6: Monitor SLA
First-level Support / Incident Manager
START
Monitor SLA
SLA Breached?
YES
Communicate about SLA breach & reason to affected users
Determine expected resolution time
IM 7 Incident Escalation
NO
NO
Further action required?
YES
Work with Incident coordinators to ensure Incident resolves on time
Incident resolved in time?
NO
YES
Communicate related Incident states to all affected users
Related incidents closed?
NO
YES
END

7.0. Escalation

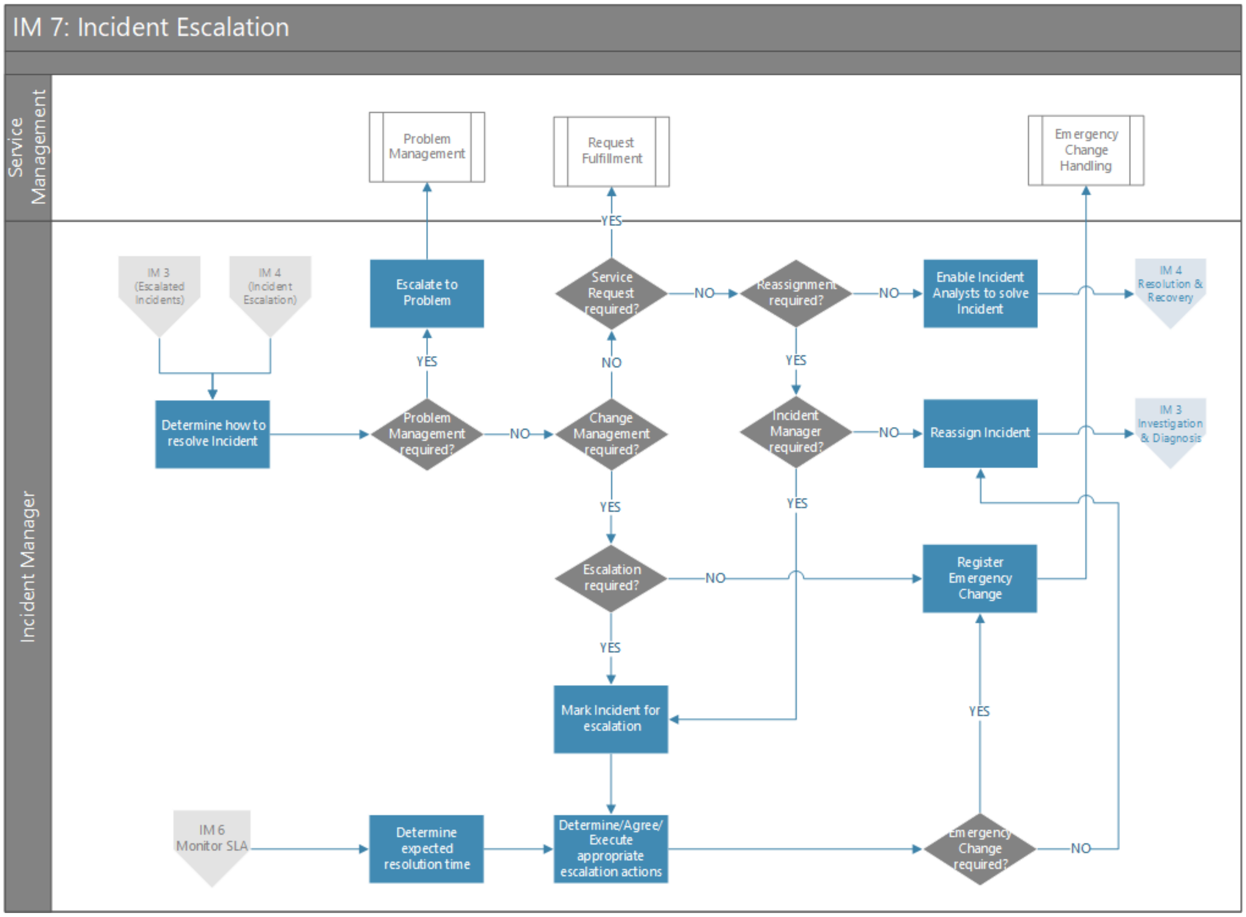

IM 7: Incident Escalation
Service Management
Incident Manager
Problem Management
Request Fulfillment
Emergency Change Handling
IM 3 (Escalated Incidents)
IM 4 (Incident Escalation)
Escalate to Problem
Service Request required?
Reassignment required?
Enable Incident Analysts to solve Incident
IM 4 Resolution & Recovery
Determine how to resolve Incident
Problem Management required?
Change Management required?
Incident Manager required?
Reassign Incident
IM 3 Investigation & Diagnosis
Escalation required?
Register Emergency Change
Mark Incident for escalation
IM 6 Monitor SLA
Determine expected resolution time
Determine/Agree/ Execute appropriate escalation actions
Emergency Change required?
YES
NO

Fig. 6: Escalation Sub-process

Procedure	Description	Input	Output
Receive notification	▪ During incident lifecycle, Service Desk can receive the notification from various sources. This notification shall be used to trigger functional and hierarchical escalation. ▪ Service Level Triggers ▪ User Escalation ▪ Reopened Incidents ▪ Escalated tickets from support specialists / group	▪ Notification from tool ▪ User escalation ▪ Reopened Incidents ▪ Escalated Incidents from support specialists	▪ Notification received by Service Desk
Get update from Incident owner	▪ Service Desk needs to contact the incident owner and get the status.	▪ Notification received by Service Desk	▪ Updates received
Update / Review Incident Record	▪ The status information received is reviewed and updated in incident along with other required information	▪ Updates received	▪ Incident updated and reviewed

Inform stakeholders based on availability and impact of system	▪ Service desk needs to inform the stakeholders based on availability & impact of system.	▪ Incident reviewed	▪ Appropriate escalation done
Inform Incident manager	▪ The Service Desk must inform the Incident Manager as agreed upon. ▪ Incident Manager shall investigate the Incident and shall determine the next course of action: ▪ If the incident is progressing, no specific action is required. ▪ If the incident is not progressing, Incident Manager shall engage additional support.	▪ Action plan prepared	▪ Action taken on Incident
Determine next action	▪ As a combined effort among service desk, incident owner and stakeholder should determine the next action plan.	▪ Appropriate escalation done	▪ Action plan prepared
Inform User / Customer	▪ • Inform User / Customer about the next actions planned.	▪ Action plan prepared	▪ Information to User / Customer
Engage additional support	▪ If the action plan determined above is to engage additional support, the same must be done (functional escalation).	▪ Action plan prepared	▪ Functional escalation done
Update Incident record	▪ Incident work log must be updated to track incidents to closure.	▪ Action plan prepared	▪ Updated worklog

8.0. Major Incident Management

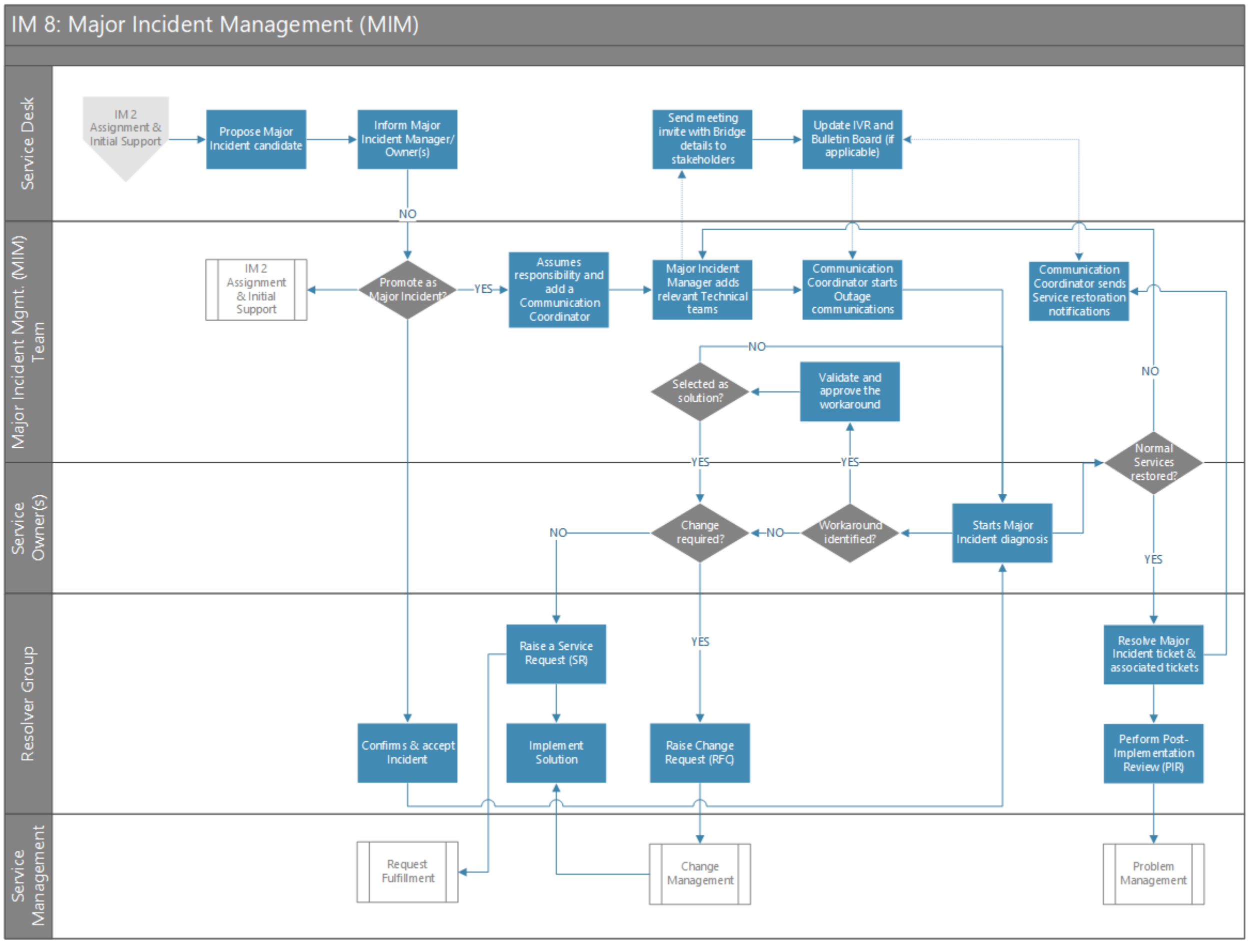

IM 8: Major Incident Management (MIM)
Service Desk
Major Incident Mgmt. (MIM) Team
Service Owner(s)
Resolver Group
Service Management
IM 2 Assignment & Initial Support
Propose Major Incident candidate
Inform Major Incident Manager/ Owner(s)
Send meeting invite with Bridge details to stakeholders
Update IVR and Bulletin Board (if applicable)
NO
IM 2 Assignment & Initial Support
Promote as Major Incident?
YES
Assumes responsibility and add a Communication Coordinator
Major Incident Manager adds relevant Technical teams
Communication Coordinator starts Outage communications
Communication Coordinator sends Service restoration notifications
NO
Selected as solution?
Validate and approve the workaround
NO
Normal Services restored?
YES
YES
NO
Change required?
NO
Workaround identified?
Starts Major Incident diagnosis
YES
YES
Raise a Service Request (SR)
Resolve Major Incident ticket & associated tickets
Confirms & accept Incident
Implement Solution
Raise Change Request (RFC)
Perform Post-Implementation Review (PIR)
Request Fulfillment
Change Management
Problem Management

Fig. 7: Major Incident Management Sub-process

Procedure	Description	Input	Output
Assume management of Incident	▪ Major Incident Management Process can be invoked by Service Desk during step Classification and Initial Support sub process or by Support Specialist during step Investigation and Diagnosis. On identifying the Major Incident, the Major Incident Coordinator is informed immediately. ▪ Before invoking the process, the Major Incident Coordinator needs to determine	▪ Incident submitted as Major Incident	▪ Incident accepted by Major Incident Coordinator

	whether the Incident submitted is qualified as Major Incident. ▪ On qualifying the Incident as Major Incident, the Major Incident Coordinator is required to accept the ownership of the Incident.		
Review Incident details	▪ On accepting the ownership of the Incident, the same is to be reviewed by Major Incident Coordinator.	▪ Incident accepted by Major incident Coordinator	▪ Incident reviewed
Open Conference Bridge	▪ On understanding the Incident history and current situation, the Major Incident Coordinator will require to open a conference bridge.	▪ Incident reviewed	▪ Conference bridge call opened
Involve related support groups	▪ All related support groups are informed about the Major Incident and asked to be on Conference Bridge.	▪ Incident reviewed	▪ Related support groups informed
Determine stakeholders for communication	▪ Stakeholders for communication are determined by Major Incident Coordinator, along with communication plan.	▪ Incident reviewed	▪ Stakeholders identified communication plan decided
Coordinate resolution	▪ All efforts are put forward by Major Incident Coordinator in coordinating the different support groups to resolve the incident.	▪ Conference bridge opened. ▪ Related support groups informed	▪ Coordination for resolution ▪ Incident resolved
Collect status	▪ If incident is not yet resolved, the status is collected by Major Incident Coordinator, and incident history is updated.	▪ Coordination for resolution	▪ Status update
Communicate the status to the stakeholders	▪ Major Incident Coordinator must update the status to the identified stakeholders as per the communication plan. Communication mediums like Email, SMS, and Pager shall be	▪ Stakeholders identified. ▪ Communication plan determined. ▪ Status update	▪ Communication to stakeholders

	used for effective communication.		
Perform post-mortem and prepare Incident report	▪ On resolution, it is required to perform the postmortem of the incident and prepare an Incident Report.	▪ Incident resolved	▪ Incident report prepared and submitted
Lesson learned and follow-up	▪ Lessons learned must be recorded in Incident Report along with preventive actions. ▪ Follow-up is required by the Incident Coordinator to ensure that respective stakeholders complete preventive action items. On completion of the same the incident can be moved further for Confirmation and Closure.	▪ Incident resolved	▪ Lessons learned / preventive actions documented, and follow-up done

Section C: Roles and Responsibilities

1. User Roles and Functions

The responsibilities of various user roles in Incident Management are listed as follows:

Roles	Responsibilities
Authorised End Users	▪ Provide detailed description of issue. ▪ User will remain engaged with the resolver group until the issue is mitigated.
Incident Manager	▪ Reviews effectiveness and efficiency of the process. ▪ Creates procedures for Incident Management. ▪ Reviews escalated incidents and takes appropriate action if it is a major incident, not for normal incidents. Incident manager would also function as the incident Owner. ▪ Ensures that Incident Management processes and tools are integrated with other processes. ▪ Is responsible for the success or failure of the process. ▪ Ensures that the process is defined, documented, maintained, and communicated to appropriate parties within the organization. ▪ Establishes and communicates the process roles and responsibilities. ▪ Establishes and communicates the process, service levels. ▪ Ensures that the process documentation is recorded. The same is also recorded in CMDB only for Network Components. ▪ Identifies and communicates opportunities for process improvement. ▪ Initiates and sponsors projects to improve or reengineer the process. ▪ Manages changes to the process. This includes reviewing and approving all proposed changes and communicating changes to all participants and affected areas.
Major Incident Coordinator / Manager	▪ Assumes ownership of a major incident. ▪ Coordinates among various teams for resolution. ▪ Opens the communication channel at the time of crisis. ▪ Determines stakeholders for communication updates. ▪ Determines contents of the communication. ▪ Reviews and postmortems the incident. ▪ Prepares Major Incident Report and presents it to the management. ▪ Proposes improvements in service delivery, processes, and infrastructure.
Service Desk (First-Level Support)	▪ Acts as the Single Point of Contact for all end user incidents. ▪ Creates a record for new incidents in the system. ▪ Categorize the incident.

	▪ Relates new incidents to existing ones when applicable. ▪ Assigns the incident to relevant level support team. ▪ Solicits feedback from end users and conducts Customer Satisfaction Survey. ▪ SD primarily function is catch & Dispatch, except on occasions when they perform more in-depth investigation & resolution.
Service Desk Lead	▪ Invokes the appropriate support to move an incident through the process. ▪ Has the authority to identify an owner for an Incident when required. ▪ Ensures that support staff has adequate skill levels and staffing level is appropriate. ▪ Manages shift schedules and so on. ▪ Arranges for staff training and awareness sessions. ▪ Provides briefing to Service Desk staff on any changes affecting or likely to affect call volumes. ▪ Create and reviews metrics reports. ▪ Create ad hoc reports for others. ▪ Manages support staff performance of the Service Desk Function and creates and executes action plans when necessary to ensure continuous improvement. ▪ Ensures that incidents are resolved through the standard Incident Management process. ▪ Identifies those incidents where ownership is not clear and escalates it at the right time to the appropriate owner. ▪ Ensures that every incident has an owner. ▪ Collects and analyses Customer Satisfaction for process improvement.
Technical Support Specialist (Resolver Groups)	▪ Tracks the incident till closure to ensure incidents are resolved within agreed SLAs. ▪ Escalates the incidents as appropriate after predetermined threshold points are reached for unresolved incidents. This activity can also be automated. ▪ Keeps the end user informed of the incident status. Once the incident is resolved, SDA closes the incident in agreement with applicable procedures and authorized End user’s agreement. ▪ Ensures that incidents are resolved through the standard Incident Management process. ▪ Third-party performance of the Incident Management process. ▪ Resolve incidents within agreed service levels. ▪ Escalate the unresolved incidents to higher support levels at the appropriate time. ▪ 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 processes as required resolving the incident. ▪ Record events into ITSM systems as they occur. ▪ Maintain up-to-date knowledge on the relevant technical platform.

2. RACI Matrix

Sr. No.	Activity Description	End-User	First-Level Support	Resolver Groups	Incident Manager	Service Desk Manager
1	Contact Service Desk	R				
2	Initial Call Handling		R			A
3	Initial Ticket Logging and Severity	I	R			A
4	Incident Assignment	I	R		A	C
5	Incident Categorization		R		A	
6	Incident Investigation & Diagnosis (Initial Triage)		R		A	
7	Escalate/ Reassign Incident	I	R		A	
8	Perform Level 1+ Investigate & Diagnosis			R	A	
9	Submit resolution to Knowledge Base			R	A	
10	Continuous Incident Management Process Improvement	CI	CI	CI	AR	CI
11	Incident Resolution and Restoration	I		R	A	
12	Incident Closure	I		R	AI	

Section D: Governance and Process Controls

1. Controls

Process controls represent the policies and guidelines on how the process will operate along with the metrics for measuring the process and they provide direction over the operation of process by defining constraints or boundaries within which the process must operate.

Number	Name	Description
DSS02.01	Define the Incident Classification Scheme	Define the Incident classification scheme and Incident models
DSS02.02	Record, Classify and Prioritize Incidents	Identify, record, and classify Incidents, and assign a priority according to business criticality and service agreements
DSS02.04	Investigate, Diagnose and Allocate Incidents	Identify and record Incident symptoms, determine probable causes, and allocate for resolution
DSS02.05	Resolve and Recover from Incidents	Document, apply and evaluate the identified fix or workarounds and perform recovery actions to restore the IT related service
DSS02.06	Close Incidents	Verify satisfactory Incident resolution and close
DSS02.07	Track status and Produce reports	Regularly track, analyze, and report Incident trends to provide information for continual improvement

2. KPI

The following table lists the key performance indicators (KPIs) that have been selected for tracking the success of the Incident Management process. The KPIs will be measured and calculated as a percentage and reflected in the monthly SLA reports.

Sl. No.	KPI	Definition	Frequency	Target SLA	Performance SLA
1	Number of Incidents logged	per Priority, Impact, urgency			
		per Type and Category			
		per Person (i.e., top ten incidents per user)			
		per configuration item type			

Sl. No.	KPI	Definition	Frequency	Target SLA	Performance SLA
		Incidents per service			
		Incidents per Business / organizational area			
2	Average time to achieve Incident resolution	Type			
		Category			
		Priority, Impact, Urgency			
		Service			
3	Percentage of Incidents resolved by group	Service Desk			
		Tier 2 Support			
		Tier 3 Support			
		External Suppliers			
4	Number of repeated Incidents	Number of repeated Incidents with known resolution methods			
5	Number of Escalations	Number of escalations for Incidents not resolved in the agreed resolution time			
6	Average Initial Response Time	Average time taken between the time a user reports an Incident and the time that the Service Desk responds to that Incident			
7	Incident Resolution Time	Average time to resolve an Incident			
8	First time Resolution rate	Percentage of Incidents resolved at Service Desk during the first call			
9	Resolution within SLA	Rate of Incidents resolved during solution times agreed in SLA			
10	Incorrect Assignment	Number and percentage of Incidents incorrectly assigned			

3. Reports

The following table lists the Management reports that help identify trends and allow review of the health of the process. The decisive test of the relevance of a report is to have a sound answer to the question, “What decisions is this report helping management to make?”

Sl. No.	Report	Timeframe / Notes / Who
1	Major Incidents Logged and Resolved	
2	Summary of Incidents that are still to be resolved / Backlog of Incidents	
3	Open and Closed Incidents by Category / Service	
4	Reopened Incidents	
5	Incidents closed meeting SLA Target	
6	Incident Reassignment Analysis	
7	Incident Aging Report	
8	Percentage of Incidents by Priority	

3. Tools

Tool requirements specific to the Incident Management process are thus:

- Automatic Incident logging and alerting in the event of fault detection on mainframes, networks, servers and so on (possibly through an interface to system management tools) all modifications to the Incident record being registered to keep control.
- Automatic escalation facilities to facilitate the timely handling of Incidents and service requests.
- Highly flexible routing of Incidents as a basic requirement because control staff may be in multiple sites or they may be co-located in an operations bridge, and such a physical distribution may vary depending on the time of day.
- Automatic extraction of data records from the CMDB of a failed item and affected items.
- Specialised software: speed and effectiveness are major objectives of handling Incidents, and because achievement depends upon a very accurate level of Incident classification and successful matching at the point of alert, it is the classification-matching process that is an ideal application area for the use of software.
- ACD (telephone) systems integration for automatically registering names and phone numbers of Users.

- The presence of diagnostic tools/modules (i.e. Case-Based Reasoning) can help the diagnostic process.

4. Relationships with other ITIL Processes

ITIL describes an integrated set of processes which, collectively, describe an overall approach or framework to service management These interdependencies for Incident Management process are described below.

Incident Management is provided inputs from:

5.1. Service Desk

The SD routes Incidents (including automated routing) and service request fulfilment requests to the appropriate IM analyst based upon established criteria. The Service Desk ensures that routed events are within the scope of IM, authenticates the initiator, records or updates contact and infrastructure details and provides initial diagnostic information.

When an Incident is reported from many sources the SD correlates and matches reported instances of the incident against a designated Incident record. This recording may be used to indicate the magnitude or overall impact of the incident.

5.2. Problem Management

PM addresses because incidents continue to occur. PM takes the data recorded during the IM process and attempts to predict and prevent incidents from happening, especially known errors that represent common or repetitive incidents at the service desk.

5.3. Configuration Management

Incidents, as recorded by the service desk, are evaluated against the CMDB. IM may update the CMDB to show the identified incidents and affected CIs. In cases where there are similar reports of the incident, the CMDB produces information on those CIs that caused the incident and/or problem possible resolutions that were successful. If no match is found, the incident creates a new record in the CMDB to manage the current incident and provide reference for future use.

5.4. Change Management

Changes to the infrastructure are a primary source of incidents so that CM should constantly keep IM aware of changes (e.g. online provision of change schedules).

5.5. Availability Management

Because a primary concern of AM is the continued availability of systems and services, AM shares a concern with IM for early recovery from outages. Frequently, AM leads, or is integrally involved in, the restoration of high severity incidents (i.e. Situations).

5.6. Capacity Management

Optimization of service performance implies monitoring the application for end-to-end response times. In a well-run IT shop, performance levels are forecast, and the monitoring system sets threshold alarms to trigger alerts before the customer of the service is aware of an issue. It is central to alerts affecting capacity and for judging the need for contingency or service continuity measures. Operating level objectives for service capacity monitoring and control require management data views through custom or selected vendor software products. Automated monitoring tracks performance levels of an IT service. Threshold alarms allow response for out-of-range conditions.

5.7. Service Level Management

SLM negotiates and documents in SLAs the performance targets within which IM operates.

Section E: Appendix

1. References

Guidance	Section
ISO 20000-1:2018	Clause 8.6 – Resolution & Fulfilment (Incident Management)
ITIL 4	ITIL Specialist – Create, Deliver & Support

2. Templates

2.1. Major Incident Notification Template

Major%20Incident%20Notification_Temp