ADIB – Procedure

Incident Management Procedure
PRC-ITD-516

Date: 30th March 2023

Version: 14.2

Version Control & Change Management

Version	Issue Date	Details of Change	Reason for change
14.2	30th March, 2023	Document reviewed and no change required	Document annual review
14.1	30th November, 2022	1. Modified: Customer impacting P1 priority incidents and customer impacted incidents must be reported to Technology risk representative within 48 hours from the date of discovery. in order to log it in ORM tool. 2. Modified frequency for weekly Incident meeting for P1 Customer impacting.	1. Escalation Criteria update for Customer Impacting Incidents. 2. Frequency cannot be defined since this is covered in RCA meetings which happen after a P1 Incident, and we cannot anticipate the frequency
14.0	30th August, 2022	Added KRI table	Align with ORM Documentation Template
13.0	30th January, 2022	Added Cloud Incident Management process flow	Cloud adoption
12.0	Publishing Date	Updated as per current structure of organization, incidents related to security has been shifted to GISD	Organization restructuring
11.0	Publishing Date	Offshore Site / Vendor Site Critical Incident Handling tasks added	Provision Incidents arising out of Offshore Service Provider
10.0	Publishing Date	RCA to be reported within 14 days of incident logging Postproduction Incident and Support Control is added	Postproduction Incident Control
9.0	Publishing Date	Incident validation and escalation process updated for P1/P2 incidents. Updated Reporting of incidents having financial loss Included new channels of Incident reporting. Process design changed.	Process optimization and alignment of process as per current practices.
8.0	Publishing Date	Updated KPIs	
7.0	Publishing Date	Procedure & Process reviewed and has been revamped to meet the correctness of activities currently followed	Process enhancement
6.0	Publishing Date	Incident Management Process Revamped BPMN diagrams updated according to iServer Format	To accommodate current practice. Initiated by Process Owner
5.0	Publishing Date	Corrected condition in diagram for Incident Detection (4.2.1.2) Corrected reference to Major Incident Procedure step to 4.2.2.1.2	Initiated by Process Owner

Prepared by	Approved by	Reviewed by
Governance Team	IT Change Manager	IT Governance Specialist

Documents Contents

1. Purpose & Scope

The purpose of this document is to capture the activities to address the Incident Management process lifecycle requirements according to the best practices and enable personnel to follow this procedure consistently.
This procedure is applicable to the following IT related incidents, in ADIB UAE, Qatar, Iraq, Sudan and UK, that affect:

1. IT Services (cloud & On-premises infrastructure/Applications) Availability.
2. End User Support
3. Offshore Service Providers.

2. Process Owner

IT Change Manager

3. Other stakeholders/ IT Incident Focal Points

1. Operations Command Centre – IT Operations Manager
2. IT Services (infrastructure) Availability -Head of TechOps
3. IT Services (Applications) Availability – Head of Business Platform
4. IT support – Team Leader, L1 User Support
5. IT Support - Desktop Management Team Leader

4. RACI

Roles / Activity	IT Operation & Command Centre Team	IT Service support team	IT Incident Manager	IT Incident Focal Points	IT GRM Designate	Resolver Team	ADIB Employee
Monitoring of IT system alerts (OBM)	R		A	R	I	R	
End User Incident Reporting		R	AR	R	I	R	R
Review and Monitoring			AR	R	R		

5. Incident Management Procedure

5.1 Monitoring of IT Systems Alerts

Monitor the availability of IT systems Incidents through monitoring tool:

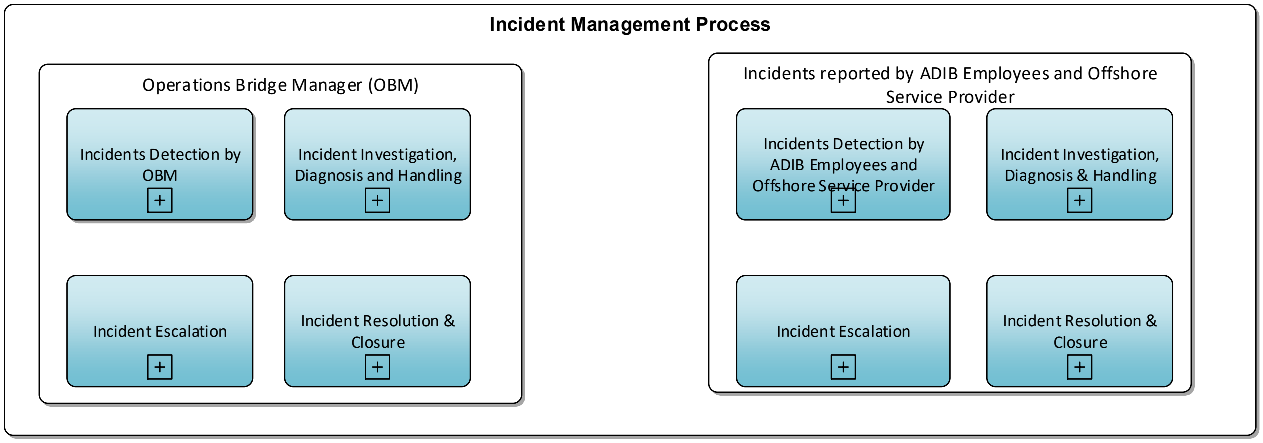
Operations Bridge Manager (OBM): Monitor & alert events related to Network, System and Business/IT Application performance and availability.

5.2 Reporting of Incidents

Reporting of Incidents are made through following channels:

1. **Incidents reported by ADIB Employees and Offshore Service Providers**: Based on telephonic interactions, emails or through self-help service option from ADIB Intranet.
2. **Monitoring of IT system alerts by ADIB IT Operations & Command Centre:** Based on the alerts received through Monitoring Tools

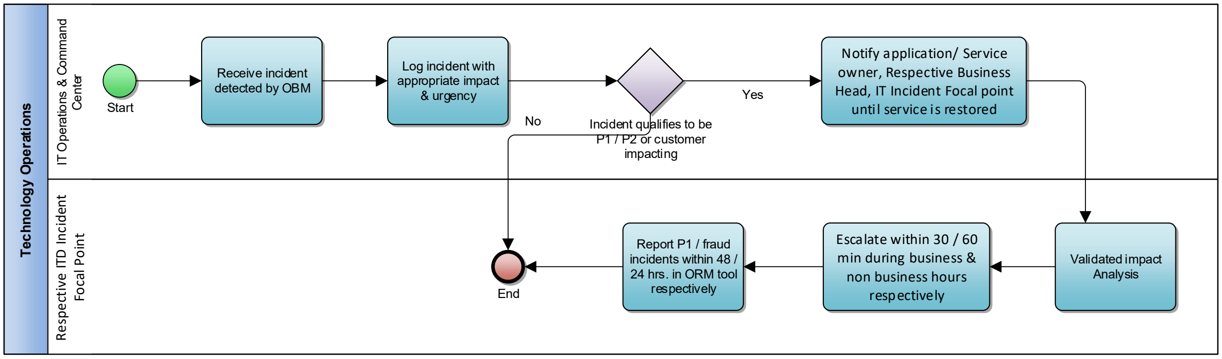
6. Detailed Process Description and Workflows


Incident Management Process
Operations Bridge Manager (OBM)
Incidents Detection by OBM
Incident Investigation, Diagnosis and Handling
Incident Escalation
Incident Resolution & Closure
Incidents reported by ADIB Employees and Offshore Service Provider
Incidents Detection by ADIB Employees and Offshore Service Provider
Incident Investigation, Diagnosis & Handling
Incident Escalation
Incident Resolution & Closure

6.1 Operations Bridge Manager (OBM)

6.1.1

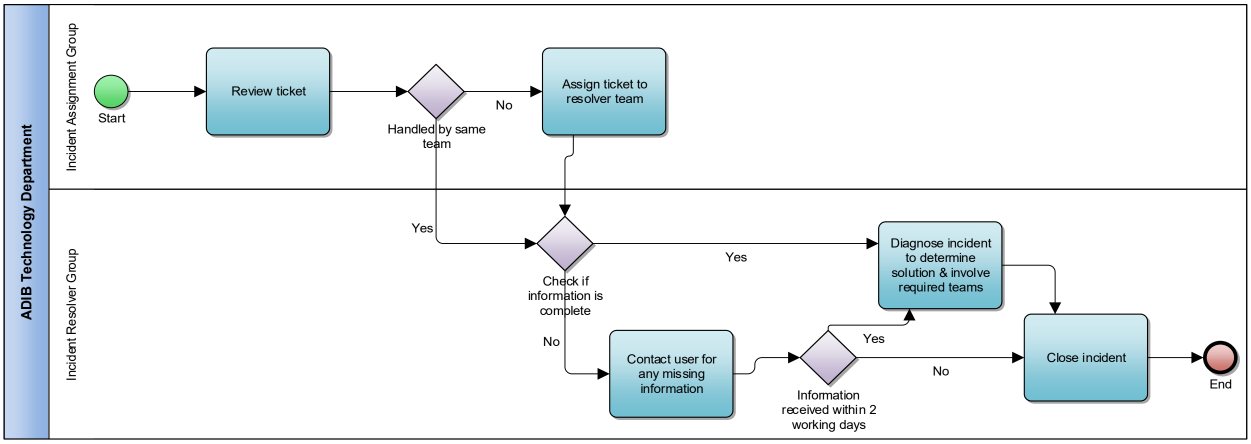
6.1.2 Incidents Detection by OBM


Technology Operations
IT Operations & Command Center
Respective ITD Incident Focal Point
Start
Receive incident detected by OBM
Log incident with appropriate impact & urgency
Incident qualifies to be P1 / P2 or customer impacting
Yes
No
Notify application/ Service owner, Respective Business Head, IT Incident Focal point until service is restored
Validated impact Analysis
Escalate within 30 / 60 min during business & non business hours respectively
Report P1 / fraud incidents within 48 / 24 hrs. in ORM tool respectively
End

Sr. No.	Process Step Description	Responsibility	Document (Record, WI) / Tool Reference
1	Alerts detected using OBM Tool are sent to IT Operation & Command Centre Team	IT Operation & Command Centre Team	OBM Tool
2	Based on the alerts, IT Operation & Command Centre logs an incident, with appropriate impact and urgency.	IT Operation & Command Centre Team	IT Service Management Tool
3	Checks if the incident qualifies to be P1/P2 or customer impacting incidents.	IT Operation & Command Centre Team	STD-ITD-542 Appendix B - Validating IT Incident Ratings Template IT Service Management Tool
3.1	**If Incident qualifies as P1/P2 category:** Notify the application/ Service owner, Respective Business Head, IT Incident Focal point by any possible means	IT Operation & Command Centre Team	IT Service Management Tool

	(Phone, Email, etc.) until the service is restored and start resource mobilization for system recovery		
3.2	Validate the impact analysis of P1, P2 and other incidents which impact customers	Respective ITD Incident Focal Point	IT Service Management Tool STD-ITD-542 Appendix B - Validating IT Incident Ratings Template
3.3	Once the issue is confirmed that there is customer impact, escalate to respective business group Incident Manager or his backup along with CIO and Head of respective department and related stakeholders within 30 minutes during Business hours or within 60 minutes during non-business hours, from time since identification	Respective ITD Incident Focal Point	E-mail
4	Customer impacting P1 priority incidents must be reported to Technology risk representative within 48 hours from the date of discovery. in order to log it in ORM tool. Fraud incidents reported within 24 hours from the date of discovery	IT Incident Manager	IT Service Management Tool ORM Tool

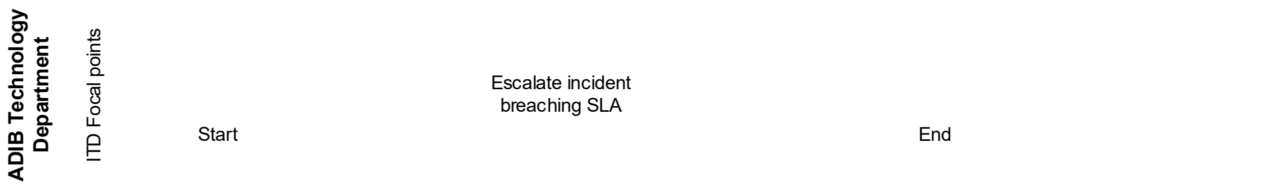
6.1.3 Incident Investigation, Diagnosis and Handling


ADIB Technology Department
Incident Assignment Group
Incident Resolver Group
Start
Review ticket
Handled by same team
No
Assign ticket to resolver team
Yes
Check if information is complete
Yes
Diagnose incident to determine solution & involve required teams
No
Contact user for any missing information
Information received within 2 working days
Yes
No
Close incident
End

Sr. No.	Process Step Description	Responsibility	Document (Record, WI) / Tool Reference
1	Review the ticket and if it is required to be handled by a different team assign/reassign the incident ticket to the relevant team **OR** Reassign the ticket to the ADIB IT Service Desk team for relevant team assignment.	Assigned Team	IT Service Management Tool
2	Contact the user once by the phone and once by the email, and the incident's status is set to be as "Pending Customer" in case of pending information.	Resolver Team	

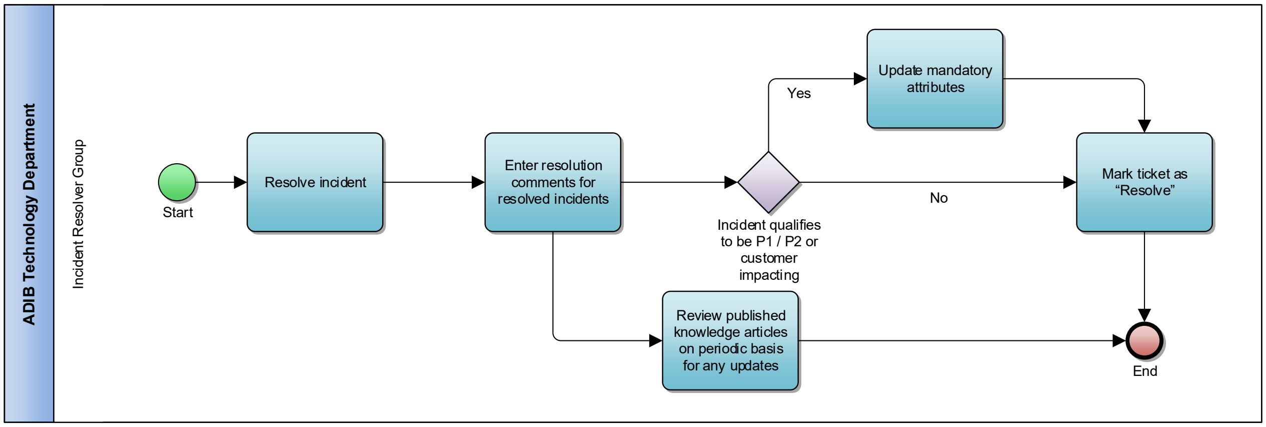
	If there is no response from the user or the user was not able to fulfil the IT representative requirements in two working days the ticket shall be closed (Status “Resolved”) providing the communication remarks & evidences between the user and IT Representative to the ticket.		IT Service Management Tool
3	With Complete information available, Diagnose the incident to determine the resolution & involve other ADIB ITD teams/ employees/ SMEs and/or external parties like Vendors, ISP etc. for resolving the incident, if required.	Resolver Team	IT Service Management Tool

6.1.4 Escalation



Sr. No.	Process Step Description	Responsibility	Document (Record, WI) / Tool Reference
1	Incidents breaching SLA’s shall be escalated.	IT Incident Focal Point	STD-ITD-575 Service & Operational Level Management IT Service Management Tool.
2	Incident should be reported and escalated as per STD-ITD-542 Incident Management Standard Appendix B: Incident Reporting & Escalation Matrix	As per STD-ITD-542 Appendix A	STD-ITD-542 Incident Management Standard Appendix A: Incident Reporting & Escalation Matrix
3	Mechanism of incident reporting and escalation should be as per STD-ITD-542 Incident Management Standard Appendix C: Reporting & Escalation mechanism	As per STD-ITD-542 Appendix A	STD-ITD-542 Incident Management Standard Appendix C: Reporting & Escalation mechanism

6.1.5 Incident Resolution & Closure

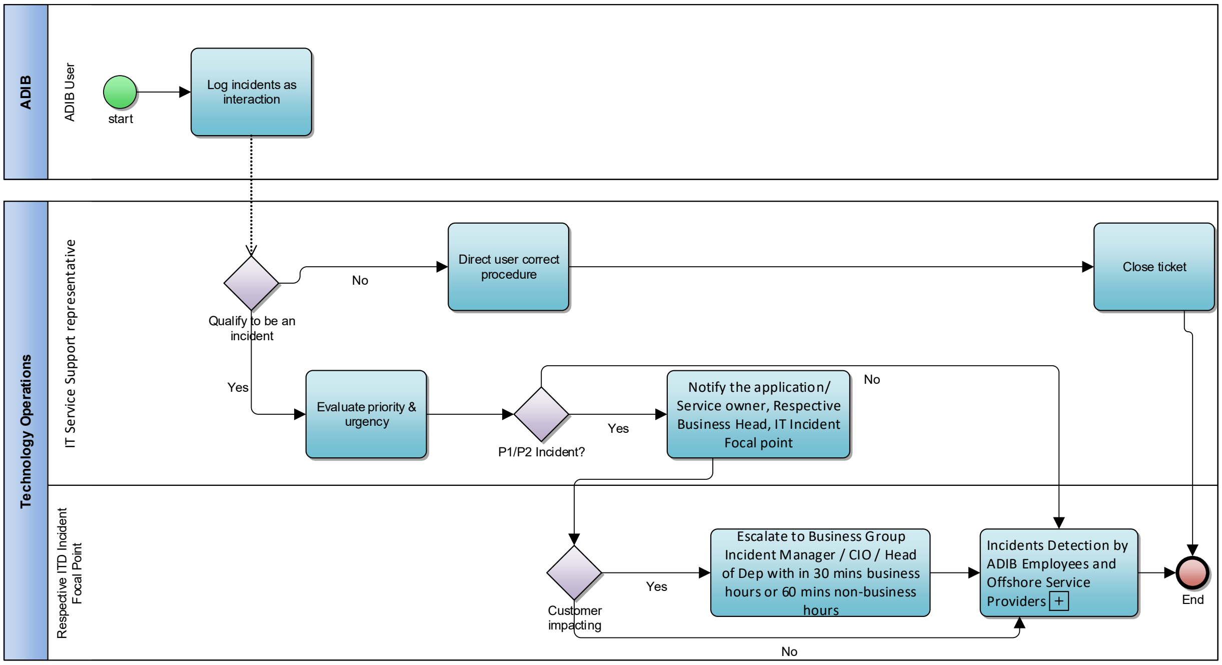

ADIB Technology Department
Incident Resolver Group
Start
Resolve incident
Enter resolution comments for resolved incidents
Incident qualifies to be P1 / P2 or customer impacting
Yes
Update mandatory attributes
No
Mark ticket as "Resolve"
Review published knowledge articles on periodic basis for any updates
End

Sr. No.	Process Step Description	Responsibility	Document (Record, WI) / Tool Reference
1	Once an incident is resolved, the resolver team enters the resolution comments & the cause of the incident ticket and marks the ticket as 'Resolved' Once the ticket is set to the 'Resolved' state, an email notification is sent to the user along with the resolution comments. The incident ticket closes automatically after a period of 5 calendar days from the date the ticket was set to the -'Resolved' state, unless it is re-opened before this 5 day period.	Resolver Team	IT Service Management Tool
2	**For P1 & P2incident:** Below details are mandatory to fill: Impact (% value and in text): Downtime (if any), Outage Start and End: Root cause: (P1 only) Root cause analysis approach (5 Whys, Fishbone etc.): (P1 only) Resolution action: Immediate Action Taken: Closure comment:	Resolver Team	Email
3	Ensure lessons learnt and guidelines as are recorded as a knowledge base (KB) article for the incident ticket before it is closed.	Tools Team	Knowledge Management Process

4	Review published knowledge articles on an on-going basis for any updates if required.	Resolver Team	IT Service Management Tool
5	Review the incident resolution to ensure appropriateness & adequacy of the incident resolution comments and instructs his/her team to update the resolution comments if he/she finds the comments to be incomplete/insufficient	Resolver Team Lead	IT Service Management Tool

6.2 Incidents reported by ADIB Employees and Offshore Service Provider

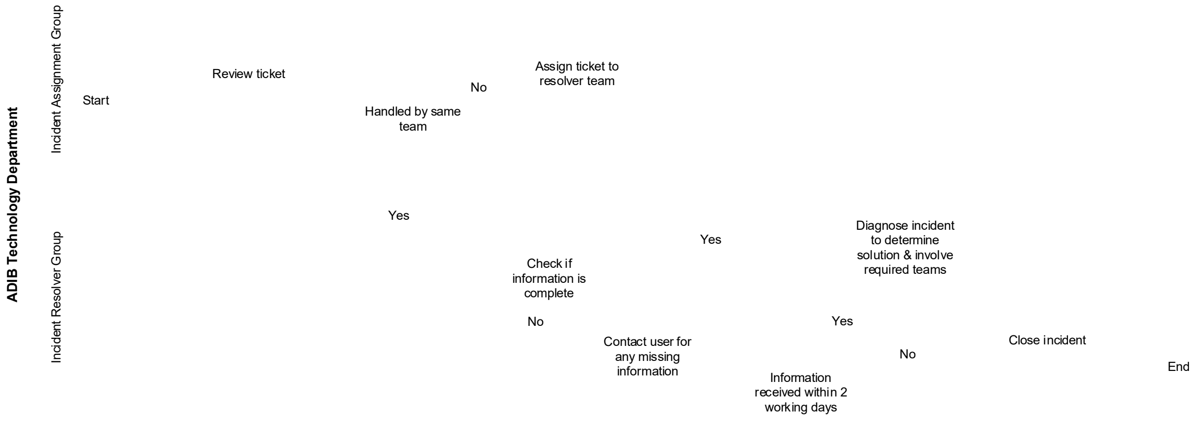
6.2.1 Incidents Detection by ADIB Employees and Offshore Service Providers


ADIB
ADIB User
start
Log incidents as interaction
Technology Operations
IT Service Support representative
Qualify to be an incident
No
Direct user correct procedure
Close ticket
Yes
Evaluate priority & urgency
P1/P2 Incident?
Yes
Notify the application/ Service owner, Respective Business Head, IT Incident Focal point
No
Respective ITD Incident Focal Point
Customer impacting
Yes
Escalate to Business Group Incident Manager / CIO / Head of Dep with in 30 mins business hours or 60 mins non-business hours
Incidents Detection by ADIB Employees and Offshore Service Providers +
End
No

Sr. No.	Process Step Description	Responsibility	Document (Record, WI) / Tool Reference
Incident Reported by ADIB Employee			
1	All incidents detected by ADIB Employee are reported to ADIB IT Service Desk via phone, email or directly logged as complain /issue in the Service Manager tool.	ADIB Employee	IT Service Management Tool
1.1	Incidents detected by ADIB Employee and reported through ITD Service manager portal are logged as an interaction in the Service Manager tool.	All ADIB Employee & IT Service Manager	IT Service Management Tool

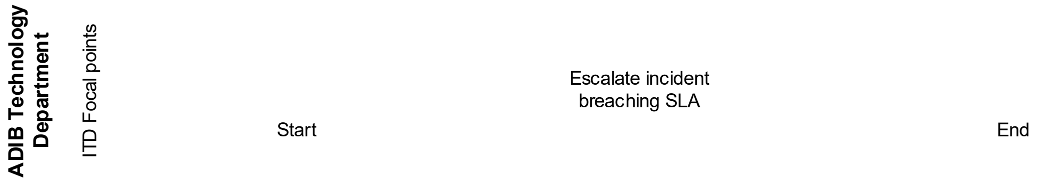
1.2	If the interaction does not qualify to be an incident, clearly indicate that in the resolution, directing the user to the correct procedure before closing the interaction. (not applicable for compliance advisories)	IT Service Support representative	IT Service Management Tool
1.3	If the interaction with ADIB employee qualifies to be an incident, an evaluation of both priority and urgency is done.	IT Service Support representative	IT Service Management Tool
Incident Reported by Offshore Service Provider			
1.	All incidents detected by Offshore Service Provider are reported in the Service Manager tool.	Offshore Service Provider	IT Service Management Tool
2	Checks if the incident qualifies to be P1/P2 or customer impacting incidents.	IT Service Support representative	STD-ITD-542 Appendix B - Validating IT Incident Ratings Template
2.1	**<u>If Incident qualifies as P1/P2 category:</u>** Notify the application/ Service owner, Respective Business Head, IT Incident Focal point by any possible means (Phone, Email, etc.) until the service is restored and start resource mobilization for system recovery	IT Service Support representative	IT Service Management Tool
2.2	Validate the impact analysis of P1, P2 and other incidents which impact customers	Respective ITD Incident Focal Point	IT Service Management Tool STD-ITD-542 Appendix B - Validating IT Incident Ratings Template
2.3	Once the issue is confirmed that there is customer impact, escalate to respective business group Incident Manager or his backup along with CIO and Head of respective department and related stakeholders within 30 minutes during Business hours or within 60 minutes during non-business hours, from time since identification	Respective ITD Incident Focal Point	E-mail

6.2.2 Incident Investigation, Diagnosis & Handling (not applicable for compliance advisories)


ADIB Technology Department
Incident Assignment Group
Incident Resolver Group
Start
Review ticket
Handled by same team
No
Assign ticket to resolver team
Yes
Check if information is complete
No
Contact user for any missing information
Yes
Information received within 2 working days
Yes
No
Diagnose incident to determine solution & involve required teams
Close incident
End

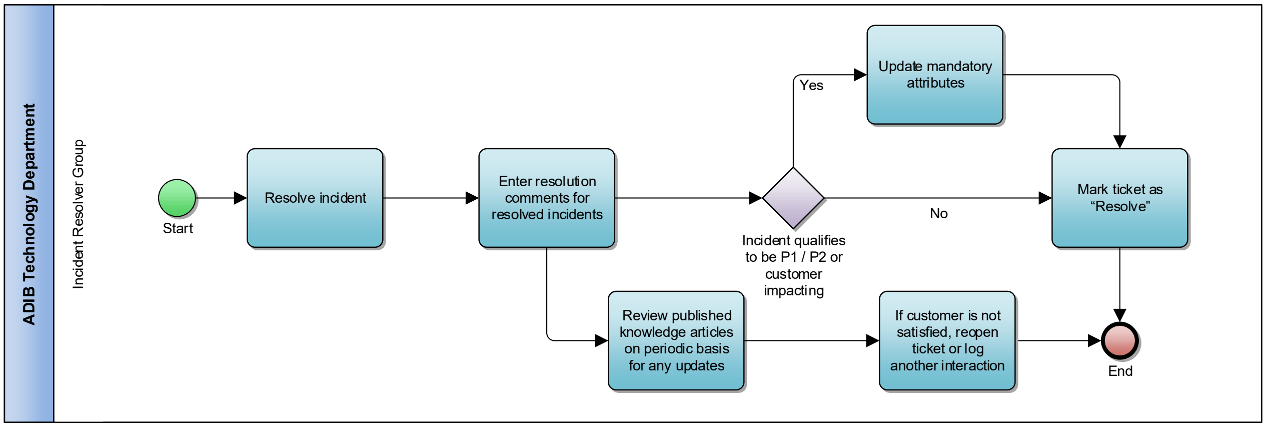
Sr. No.	Process Step Description	Responsibility	Document (Record, WI) / Tool Reference
1	Review the ticket and if it is required to be handled by a different team assign/reassign the incident ticket to the relevant team **OR** Reassign the ticket to the ADIB IT Service Desk team for relevant team assignment.	Assigned Team	IT Service Management Tool
2	Contact the user once by the phone and once by the email, and the incident's status is set to be as "Pending Customer" in case of pending information. If there is no response from the user or the user was not able to fulfil the IT representative requirements in two working days the ticket shall be closed (Status "Resolved") providing the communication remarks & evidences between the user and IT Representative to the ticket.	Resolver Team	IT Service Management Tool
3	With Complete information available, Diagnose the incident to determine the resolution & involve other ADIB ITD teams/ employees/ SMEs and/or external parties like Vendors, ISP etc. for resolving the incident, if required.	Resolver Team	IT Service Management Tool

6.2.3 Escalation



Sr. No.	Process Step Description	Responsibility	Document (Record, WI) / Tool Reference
1	Incidents breaching SLAs shall be escalated.	IT Service Support Team	STD-ITD-575 Service & Operational Level Management IT Service Management Tool.
2	Incident should be reported and escalated	IT Incident Focal Point	STD-ITD-542 Incident Management Standard Appendix A: Incident Reporting & Escalation Matrix
3	Mechanism of incident reporting and escalation should be as per STD-ITD-542 Incident Management Standard Appendix C: Reporting & Escalation mechanism	IT Incident Focal Point	STD-ITD-542 Incident Management Standard Appendix C: Reporting & Escalation mechanism

6.2.4 Incident Resolution & Closure


ADIB Technology Department
Incident Resolver Group
Start
Resolve incident
Enter resolution comments for resolved incidents
Incident qualifies to be P1 / P2 or customer impacting
Yes
Update mandatory attributes
No
Mark ticket as "Resolve"
Review published knowledge articles on periodic basis for any updates
If customer is not satisfied, reopen ticket or log another interaction
End

Sr. No.	Process Step Description	Responsibility	Document (Record, WI) / Tool Reference
1	Once an incident is resolved, the resolver team enters the resolution comments & the cause of the incident ticket and marks the ticket as 'Resolved' in the Service Manager tool. Once the ticket is set to the 'Resolved' state, an email notification is sent to the user along with the resolution comments. The incident ticket closes automatically after a period of 5 calendar days from the date the ticket was set to the -'Resolved' state, unless it is re-opened before this 5-day period.	Resolver Team	IT Service Management Tool
2	**For P1 & P2 incident:** Below details are mandatory to fill: Impact (% value and in text): Downtime (if any), Outage Start and End: Root cause: (P1 Only) Root cause analysis approach (5 Whys, Fishbone etc.): (P1 only) Resolution action: Immediate Action Taken: Closure comment:	Resolver Team	Email
3	Ensure lessons learnt and guidelines as are recorded as a knowledge base (KB) article for the incident ticket before it is closed.	Tools Team	Knowledge Management Process
4	Review published knowledge articles on an on-going basis for any updates if required.	Resolver Team	IT Service Management Tool

5	If the end-user is not satisfied with the incident resolution, he / she submits another interaction for the same incident in the Service Manager tool or calls the IT Support Services team for registering another interaction for the same incident. If the related incident ticket found to be closed, then a new ticket is opened or else the same old ticket is reopened and re-assigned for the resolution.	IT Service Support Team	IT Service Management Tool
6	Review the incident resolution to ensure appropriateness & adequacy of the incident resolution comments and instructs his/her team to update the resolution comments if he/she finds the comments to be incomplete/insufficient	Resolver Team Lead	IT Service Management Tool

7. Cloud Incident Management Process Flow & Description

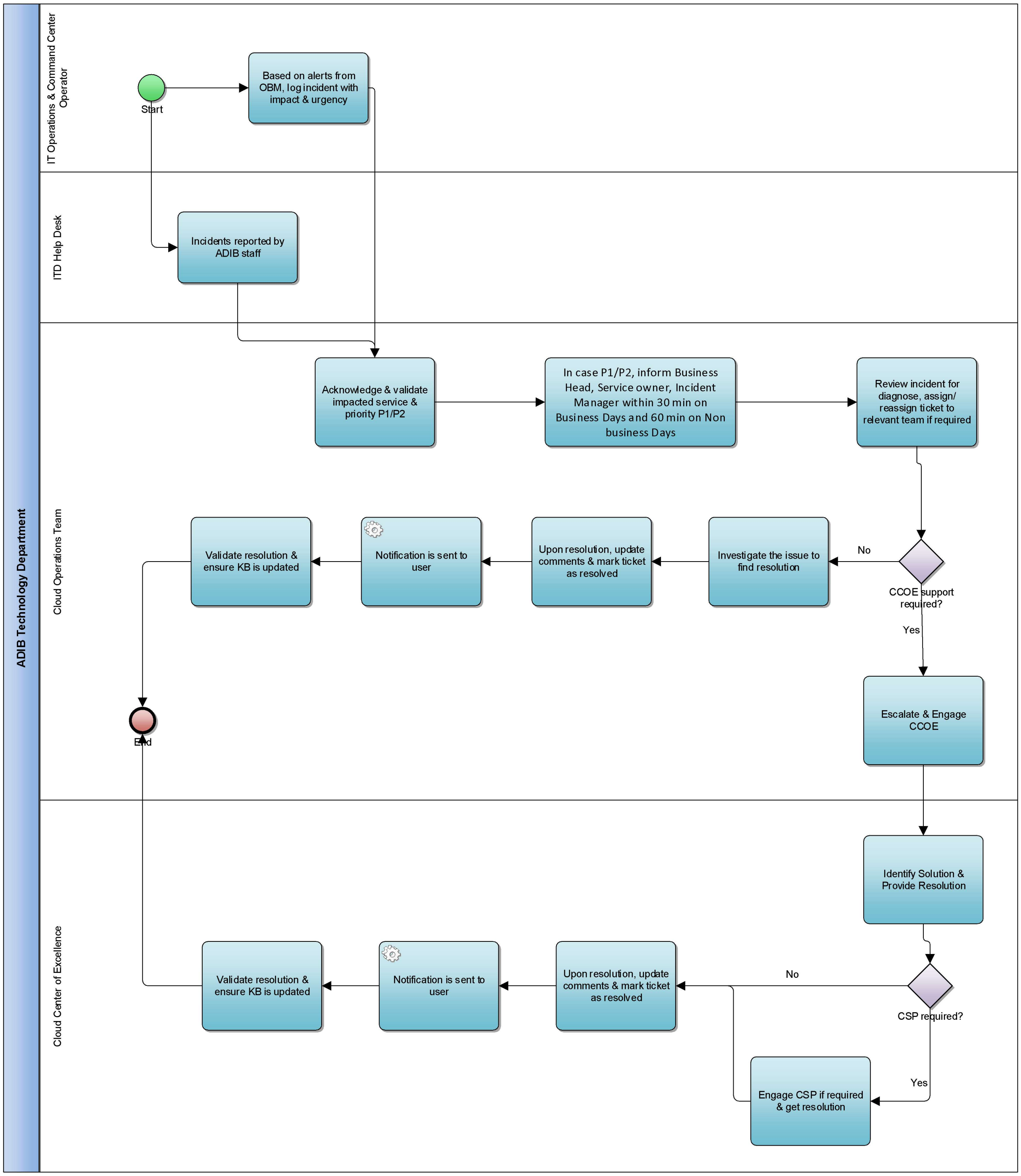
7.1 Target Audience for Cloud

- Cloud Operations Team
- Cloud Incident Assignment Group
- Cloud Incident Manager (ADIB Incident Manager)
- Cloud COE Team
- Technology Enterprise Architecture Team & Support Personnel

7.2RACI Matrix for Cloud Incident Management

Roles / Activity	OCC/Helpdesk	Incident Manager	Cloud Operations Team	Cloud COE Team	CSP
Detection & Classification	A/R	C	I		
Initial Support	I	I	A/R	C	
P1/P2 Incident and Customer Impacted?	I	I	A/R	C	
Inform Business Head, Service owner, Incident Manager	R	I	A	C	
Investigation & Diagnosis			A/R	C	
Need Elevated support	I	I	A/R	C	
Further investigate			A/R	C	
Resolution and Recovery	I	I	A/R	R	
Escalate & Engage Cloud COE Team	I	I	A/R	C	
Identify Solution & Provide Resolution	I	I	A	R	C
CSP Required?	I	I	I	A/R	C
Engage CSP		I	I	A	R
Validate Resolution	R	I	A/R	R	C

7.3 Cloud Incident Management - Process Flow


ADIB Technology Department
IT Operations & Command Center Operator
ITD Help Desk
Cloud Operations Team
Cloud Center of Excellence
Start
Based on alerts from OBM, log incident with impact & urgency
Incidents reported by ADIB staff
Acknowledge & validate impacted service & priority P1/P2
In case P1/P2, inform Business Head, Service owner, Incident Manager within 30 min on Business Days and 60 min on Non business Days
Review incident for diagnose, assign/ reassign ticket to relevant team if required
CCOE support required?
No
Yes
Investigate the issue to find resolution
Upon resolution, update comments & mark ticket as resolved
Notification is sent to user
Validate resolution & ensure KB is updated
End
Escalate & Engage CCOE
Identify Solution & Provide Resolution
CSP required?
No
Yes
Engage CSP if required & get resolution
Upon resolution, update comments & mark ticket as resolved
Notification is sent to user
Validate resolution & ensure KB is updated

Sr. No.	Process Step Description	Responsibility	Document (Record, WI) / Tool Reference
1	**Detection & Classification**		
1.1	**Incidents detected by OBM** Alerts with cloud related CIs are detected using OBM Tool which is monitored by IT Operation & Command Centre Team Based on the alerts, IT Operation & Command Centre logs an incident, with appropriate impact and urgency.	IT Operation & Command Centre Team	
1.2	**Incidents related to Cloud services reported by ADIB staffs**	ITD Helpdesk Team	
2.0	**Initial Support**		
2.1	Acknowledge and validate impacted Service and Priority	Cloud Operations Team	
2.2	To check if Incident is P1/P2 or customer impacting	Cloud Operations Team	
2.3	In case of P1/P2 or customer impacting incident, inform Business Head, Service owner, Incident Manager within 30 min on Business Days and 60 min on Non business Days	Cloud Operations Team	
3.0	**Investigation & Diagnosis**		
3.1	Review the ticket and if it is required to be handled by a different team assign/reassign the incident ticket to the relevant team else diagnose the incident to determine the resolution	Cloud Operations Team	
3.2	To check if elevated support is required from Cloud COE team.	Cloud Operations Team	
3.3	Further investigate the issue and find solution based on KB articles	Cloud Operations Team	
4.0	**Resolution and Recovery** Once an incident is resolved, the resolver team enters the resolution comments & the cause of the incident ticket and marks the ticket as 'Resolved' Once the ticket is set to the 'Resolved' state, an email notification is sent to the user and Cloud Operations Team/COE team along with the resolution comments. The incident ticket closes automatically after a period of 5 calendar days from the date the ticket was set to the - 'Resolved' state, unless it is re-opened before this 5-day period.	Cloud Operations Team Cloud COE Team	
5.0	**Escalate & Engage Cloud COE Team** If incident escalated to Cloud COE team, then they will investigate and diagnose the incident.	Cloud COE Team	
6.0	**Identify Solution & Provide Resolution** Cloud COE team will work to get the solution and restore the incident.	Cloud COE Team	
6.1	If CSP is required, then Cloud COE team will engage them to get the solution.	CSP	

7.0	**Validate Resolution** Cloud Operations Team and COE team will validate the resolution. For P1 & P2incident, below details are mandatory to fill: • Impact (% value and in text): • Downtime (if any), Outage Start and End: • Root cause: (P1 only) • Root cause analysis approach (5 Whys, Fishbone etc.): (P1 only) • Resolution action: • Immediate Action Taken: • Closure comment: Ensure lessons learnt and guidelines are recorded as a knowledge base (KB) article for the incident ticket before it is closed.	Cloud Operations Team Cloud COE Team	

Cloud Service Provider Engagement:

Activity Number	Engage Cloud Service Provider - Process Description	Roles Responsible
A	Identify if CSP support is required	Cloud COE Team
B	Engage CSP- Call/mail CSP and get Incident reference number from CSP	Cloud COE Team
C	Track CSP resolution progress/ communications and update ADIB Incident ticket	Cloud Operations Team / Cloud COE Team
D	CSP resolve Incident	Cloud Service Provider
E	Validate Resolution if required logs/information is provided or if CSP provided solution works.	Cloud Operations Team/ Cloud COE Team

8. Review and Monitoring

Sr. No.	Process Step Description	Responsibility	Document (Record, WI) / Tool Reference
1.	Send a routine escalation for any service outage or downtime to ITD leaders.	IT Operations representative	E-mail
2.	A summary report of the critical IT services related to P1 & P2 incident handling & resolution shall be sent to IT Governance for CIO reporting	ITD Incident Manager	Weekly ITD Report
3.	Send a department wise report of all the incident tickets (P1, P2, and P3, P4) which had their SLA breached, to the respective ITD Unit Heads and IT Governance Manager on a monthly basis.	ITD Incident Manager	Monthly ITD Report

Sr. No.	Process Step Description	Responsibility	Document (Record, WI) / Tool Reference
4.	An automated department wise report of all the incident tickets which have remained open for long shall be sent by email to IT Governance Manager and enlisted stakeholders: • Respective ADIB ITD Managers on a weekly basis (tickets open for 60 days) • Respective ITD Unit Heads on a monthly basis (tickets open for 90 days)	ITD Incident Manager	IT Service Management Tool E-mails
5.	Monthly critical service availability report to IT Governance.	IT Operations representative	Monthly ITD Report
6.	Quarterly trend analysis report will be provided to ITD management for repetitive incidents.	IT Problem Manager	Quarterly ITD Report
7.	Automated P1 incident alerts are reviewed and all relevant evidence leading to closure which are provided by the incident owner would be reviewed.	IT Risk Management representative	ORM Tool.
8.	Conduct incident meetings with IT Incident Focal points, IT Governance Manager, and IT Risk Manager to review and assess the following: 1. Root Cause Analysis (RCA) for P1 impacting incidents and reported within 14 days of incident logging. 2. Ensure that the Incidents notified to ITD management are logged in service management tool and are in sync with their date and time. Ensure P1 and customer impacting incidents which have not been closed within 15 minutes during standard working hours and 30 minutes during non-working hours are logged as incident tickets	IT Incident Manager	TML-ITD-103 Root Cause Analysis (RCA) Template
9.	Report and monitor all new issues logged within one month *(Postproduction Incident & Support)* after Go Live or rollout of a major update in project steering committee or bring in project sponsor's attention.	Project manager or Application owner	IT Service Management Tool Email Management reporting

9. Key Performance Indicators (KPI)

Sr. No.	Key Performance Indicator	Target	Source	Reporting to	Frequency	Formula
1	Incidents resolved with in SLA	90%	IT Service Management Tool	ITD Leaders	Monthly	(Number of incidents resolved within SLA /Total number Incidents) *100
2	Percentage of Incidents re opened	<5%	IT Service Management Tool	ITD Leaders	Monthly	(Number of reopened incidents /Total number of incidents) *100

10. Risk and Control

Risk ID	Risk Name	Control ID	Controls	Control Reference (section number in the procedure)
R-326651	Failure to comply with IT incident Management procedure	C-336844	All incidents detected by ADIB users are reported to IT service desk and are logged as complaint/ issue in Service Manager (SM9) These complaints/ Issues are verified to be qualified as incidents or not by IT service desk	6.1.1
		C-336842	Alerts detected by NSM tool are reported to IT operation & Command Center Team and are logged in the service manager tool (SM9) as an incident with appropriate impact and urgency.	6.1.1
		C-336843	Alerts detected by BSM tool are reported to IT operation & Command Center Team and are logged in the service manager tool (SM9) as an incident with appropriate impact and urgency.	6.1.1
R-326625	Failure to monitor and report IT capacity requirements (Capacity Management)	C-336806	Alerts for various thresholds are in place for all infrastructure components in terms of capacity (CPU & RAM). Various capacity reports are reviewed, and corrective actions are taken where necessary to	5.1

		avoid incidents because of capacity issues.	
R-326487 Failure to adhere ORM mandate	C-336495	P1 Incidents are logged in GRC tool and updated along with root cause analysis and other required artifacts	6.1.2
	C-828173	All priority incidents "P1" and customer impacted incidents are reported to Technology risk representative by incident manager within 48 hours from the time of discovery.	6.12

11. Key Risk Indicators (KRI)

Process	Metric Name	Metric Calculation Method
Incident Management	Downtime from service outage incidents on Tier 1-3 applications exceeds the approved RTO value for the impacted service(s)	Number of service outage incidents where the service downtime exceeded the approved RTO value for the impacted Tier 1-3 application
Incident Management	P1 & P2 incidents are incorrectly categorized as P3	Count of incident tickets incorrectly categorized as P3
Incident Management	Incidents are not mapped to the impacted services	Count of P1-P3 incident tickets where the actual impacted services were not mapped to the incident ticket

12. Appendix

Appendix: Acronyms

OBM	Operations Bridge Manager