ADIB – Standard

Incident Management Standard
STD-ITD-542

Date: 30th March 2023

Version: 14.1

Version Control & Change Management

Version	Issue Date	Details of Change	Reason for change
14.1	30th March, 2023	Document reviewed and no change required	Document annual review
14.0	November	Added: 6.6 Escalation Any unplanned impact on customer facing services exceeding 4 hrs. will be notified to "Customer Communication Group" in order to notify the customers of the service impacted and advise on alternative solutions during the interruption of the service. Any unplanned impact on customer facing services exceeding 4 hrs., with "CB – Communication Group" in order to communicate with Central Bank Added: 9.1 Appendix A Critical incident reporting group will be informed instead of COO by TRM and Service / Incident Supervisor for P1 – Critical / Very High & P2 - High.	CB UAE mandate. Enhanced Escalation Matrix.
13.0	September 2022	Demoting incident priority is subject to Incident Manager's assessment and GRC head shall be informed. Appendix B is referred in document.	To ensure management is informed for any change in incident categorization.
12.0	30th January, 2022	Updated for Cloud Incident Management	As per cloud adoption
11.0	Publishing Date	Removed Incident management processes for Security and Compliance. Added updated matrix for Priority calculation, Escalation & mode of escalation.	To align with current practice.
10.0	Publishing Date	Offshore Site / Vendor Site Critical Incident Handling tasks added Removed "Respective control(s) related to the incident shall be assessed, along-with the status of the incident, as part of IT Control assurance review calendar"	Provision Incidents arising out of Offshore Service Provider To align with current practice
9-0	Publishing Date	Change process owner and SLA for RCA defined. Post Production Incident and Support Control is added	GAAR Issue addressed
8.0	Publishing Date	Added Stakeholders/IT Incident Focal Points Added End User Support Incidents Identify channels of incidents Modified Reporting of incident section	Align with best practices
7.0	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 optimization

6.0	Publishing Date	Document reviewed and has been revamped to meet the correctness of activities currently followed	To reflect current practices in relation to Incident Management
5.1	Publishing Date	NESA Security Control update	NESA Compliance
5.0	Publishing Date	Entire Standard has been revamped	To accommodate current practice.
4.0	Publishing Date	The tables moved from procedure to Annexure in Standard	Document restructuring

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

Document Contents

1 Overview

The purpose of this document is to address the Incident Management process lifecycle requirements according to the best practices and enable personnel to follow this standard consistently.

2 Objective

The Incident Management objective is to restore service operation as quickly as possible while preserving the confidentiality, integrity & availability (CIA) elements of business operations & IT systems /applications, in the event of IT incidents that negatively impact ADIB's business.

3 Applicability

This standard is applicable to the following types of IT related incidents, in ADIB UAE, Qatar, Iraq, Sudan and UK, that affect:

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

4 Process Owner

IT Change Manager

5 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
6. Cloud Management Team
7. Cloud Incident Assignment Group
8. Cloud Incident Manager (ADIB Incident Manager)
9. Cloud COE Team
10. Technology Enterprise Architecture Team & Support Personnel

6 Standard Statements

6.1 General

IT Incidents shall be of two (2) types as follows:

1- IT Services (On-premises or Cloud infrastructure/Applications) Availability Incidents:

These are incidents where IT Services (On-premises or Cloud infrastructure/Applications) are unavailable, but not limited to following

- Environmental conditions
- Hardware/ Software Configuration Issues
- Hardware failure
- Software errors

2- End User Support Incidents

IT support incidents are end user related incidents which does not fall under other incident categories

6.2 IT Incident Prevention

- The IT Services shall be periodically reviewed by ITD concerned party to prevent IT incidents. This shall be an on-going activity and incorporates all the constantly emerging new threats & vulnerabilities relevant to ADIB ITD, Patching Database and Server Operating Systems and others. Repeated IT incidents shall be reviewed as per defined Problem management process to prevent/ reduce service unavailability / downtime.

6.3 IT Incident Detection, Reporting and Logging

- IT Incidents shall be detected through the following channels:
  - Reporting of incidents by ADIB employees.
  - Monitoring of IT system alerts by ADIB IT Operations & Command Centre.
- All IT incidents shall be logged and tracked in the IT Service Management tool.
- Incidents related to cloud CIs or cloud services will be tagged as Cloud incident.
- Users shall be informed / guided in case the incident ticket raised by them are determined to be invalid and then the incident tickets shall be closed.

6.4 Incident Classification and Prioritization

- IT Incidents shall be classified as availability or end-users related.
  - The initial prioritization of an incident shall be derived as specified in **STD-ITD-542 Appendix B - Validating IT Incident Ratings Template**
  - Demoting incident priority is subject to Incident Manager's assessment and GRC head shall be informed

6.5 IT Incident Handling

- The time limit to respond & resolve incidents shall be based on the respective SLA for the assigned priority level (P1 to P4) of the incident
- There shall be linkages between incident records and known errors, whenever new IT incidents are handled, the action taken to resolve the incident & the lessons learnt from the same shall be used to develop guidelines as a source of reference for handling future occurrences of the same or similar incidents and test its effectiveness.
- For Incidents recorded by the monitoring tools and if they are of National & Public Importance (like advisories from C.B.-UAE, NESA and such others), shall be coordinated with GISD as per the prescribed Threat Intelligence process, as it deem fits.
- All cloud related incidents should be initially assigned to cloud management team for investigation & diagnosis. For further investigation, incident can be assigned to cloud COE. If CSP support is required, then an incident needs to be opened on Vendor portal.
- For P1 incidents relevant assignment teams shall be alerted by any possible means or mode (mobile, email, in-person, etc.) to highlight its importance.
  - Respective ITD Incident Focal Point shall validate the impact analysis of P1/ P2 and other incidents with customer impact, as per **STD-ITD-542 Appendix B - Validating IT Incident Ratings Template** and refer **'EA Application portfolio'** with attributes of Application criticality.
- P1 priority incidents and customer-impacted incidents should be reported in ORM tool within 48 hours from the date of discovery. Fraud incidents should be reported within 24 hours from the date of discovery.
- Recording and reporting incidents must ensure compliance with existing data confidentiality guidelines and regulations (as applicable in the particular business / jurisdiction). Necessary guidance from Compliance or Legal department shall be obtained if there is any doubt. .
- RCA shall be reported within in 14 Business days from the date of logging

6.6 Escalation

- Respective ITD team shall be informed about the P1 incidents and Customer impacting incidents which are not closed in 15 minutes during business hours or 30 minutes during non-business hours from the time of identification and start resource mobilization for system recovery
  - Respective ITD Incident Focal Point shall validate the impact analysis of P1, P2 and other incidents which impact on customers refer to **STD-ITD-542 Appendix B - Validating IT Incident Ratings Template**
  - Once the issue is confirmed that there is customer impact, escalate and report to respective stakeholders within 30 minutes during Business hours or within 60 minutes during non-business hours, from time since identification. Incident should be reported and escalated as per STD-ITD-542 Incident Management Standard Appendix A: Incident Reporting & Escalation Matrix. Mechanism of incident reporting and escalation should be as per STD-ITD-542 Incident Management Standard Appendix C: Reporting & Escalation mechanism.
  - Incident breaching SLAs as defined in **STD-ITD-575 Service Level Management**, shall be escalated.
  - Any unplanned impact on customer facing services exceeding 4 hrs. will be notified to **"Customer Communication Group"** in order to notify the customers of the service impacted and advise on alternative solutions during the interruption of the service
  - Any unplanned impact on customer facing services exceeding 4 hrs., with **"CB – Communication Group"** in order to communicate with Central Bank
  -

6.7 Incident Closure

- Closure of incidents shall be subject to successful resolution and restoration of the IT Service impacted by the incident.
- Workarounds and measures adopted to mitigate the incident shall be recorded & documented in the incident ticket, as well.
- Incidents of P1 and P2 categories shall be recorded as knowledge assets in accordance with the knowledge management process.
- All the relevant parties shall be informed about the closure of incidents & they shall subsequently be provided with the option of reporting their satisfaction with the resolution of the incident.
- Problem Ticket shall be raised for repetitive incidents as per the problem management standard.
- If the IT incident has not been completely resolved due to missing information, the user shall be contacted once by phone and once by email, and the incident's status is to be set to "Pending Customer". If no response received or the user was not able to fulfil the requirements in two working days, the ticket shall be closed provided that communication remarks & evidence are added to the ticket.
- The user shall be informed about the closure of incidents & shall subsequently be provided with the option of reopening it within 5 calendar days and reporting his/her satisfaction with the resolution of the incident
- Incidents shall be directly re-assigned to the resolver group, instead of returning it to the Service Desk.
- A thorough root cause analysis shall be conducted for P1 incidents to ensure root causes are identified and remediated with proper action plan.
- Below details are mandatory for the resolution of P1 incidents:
  - Impact (% value and in text):
  - Downtime (if any), Outage Start and End:
  - Root cause:
  - Root cause analysis approach (5 Whys, Fishbone etc.):
  - Resolution action:
  - Immediate Action Taken:

- Closure comment:

6.8 Incident Review & Monitoring

- P1 & P2 Incidents shall be discussed and reviewed in management meetings to increase awareness about causes of incidents, lessons learnt etc.
- Periodic IT incident reports shall be provided to ITD management for review and monitoring the incident resolution. Such reports shall include:
  - Incident tickets (P1, P2, P3 & P4) which had their SLA breached
  - Incident tickets which have remained open for long durations of time
  - Critical Service Availability Reports
- Conduct weekly RCA meetings for the P1 incident tickets with all the IT Incident Focal points and IT Incident Manager (process owner).
- Ensure that the Incidents notified to ITD management are logged in IT Services Management Tool and are in sync with their date and time.
- Ensure incidents which are identified to be impacting customer and have not closed within 15 minutes during standard working hours and 30 minutes during non-working hours are logged as incident tickets, subsequently ensure it is intimated to the business team and ticket re-rated as P1 and a corresponding ORM tool Incident ticket been logged as per ORM Incident management process.
- Validate against Prioritization guideline (STD-ITD-542 Appendix B - Validating IT Incident Ratings Template) P1 and other incidents with customer impact.
- Any incident identified during *"Post Production Incident and Support" period (1 month from roll-out)* shall be logged, investigated, tracked on priority basis, and reported to Project Steering Committee or Project Sponsor's.
- During *"Post Production Incident and Support" period* the Project Manager or Application Owner shall report updates on progress made towards resolving these issues.
- ITD Loss incidents (P1 tickets in SM9) which are logged by the Incident Owner in ORM tool; are linked to the existing risk and control if already identified in the Risk and Control Self-Assessment (RCSA) of the respective ITD unit. If not, recommend relevant risk and control to be updated in the process documents of the respective ITD process.

7 Cloud Roles & Responsibilities

7.1 Cloud Management Team

Role Summary

- Supports & Operates the Cloud Incident Management process to restore normal cloud service operation as quickly as possible to minimize the impact to business operations.

Responsibilities

- Responsible for operating all the Cloud Incident Management activities required to perform, monitor, and to restore normal cloud service operation as quickly as possible and provide inputs for the reports of the cloud process and in-scope of Cloud Management Team.

7.2 Cloud COE Team

Role Summary

- The Cloud COE team is an authoritative and consulting Team for all, or any cloud related technical and architectural decision.

Responsibilities

- Cloud COE team will support the Incident Management process as Next Level of Escalation for Cloud Management Team.

- Responsible for engaging the CSP during implementations or for investigations needs as part of incident resolution.
- Actively contributing to continual service delivery improvement.
- Close participation in defining the infrastructure portfolio and design across the business, including applications, networks, security and hosting.
- Ensuring active participation in the Design/Architecture Review Board.
- Managing and developing a highly skilled team of Cloud SMEs and/or architects.
- Ensuring the Cloud architecture design is aligned with the wider IT and business's goals

8 Exception

- Exceptions to this Policy must be approved by the CIO in advance based on the risk ratings of the exception. This needs to be formally documented. All approved exceptions will be recorded and cross-checked for appropriate approval.
- The IT Incident types such as Disaster Recovery / BCM incidents are out of the document scope.
- Activities of Incidents related to human resource incidents are excluded from compliance to this standard

9 Appendix

9.1 Appendix A: Incident Reporting & Escalation Matrix

	Technology Relationship Manager (TRM)	Service / Incident Supervisor	Operation Team	Service Lead
P1 – Critical / Very High	Critical Incident Reporting Group" , CIO & Business Heads	Critical Incident Reporting Group" , CIO & ITD Management	Application Lead & Support teams	Engaged Vendor
P2 – High	Critical Incident Reporting Group" , CIO & Business Heads	Critical Incident Reporting Group" , CIO & ITD Management	Application Lead & Support teams	Engaged Vendor
P3 – Medium	ITD Management	ITD Management	Application Lead & Support teams	Engaged Vendor
P4 - Low	NA		NA	NA

9.2 Appendix C: Reporting & Escalation mechanism

Impact	Reporting and escalation mechanism			
	Phone Calls	Email notification	WhatsApp / Teams Message	Regular Update - 30mins
P1 – Critical / Very High	Yes	Yes	Yes	Yes
P2 – High	Yes	Yes	Yes	Yes
P3 – Medium	No	Yes	No	Where applicable
P4 – Low	No	Yes	No	No

10 Reference

- STD-ITD-542 Appendix B - Validating IT Incident Ratings Template