ADIB – Standard

IT Control Assurance Standard
STD-ITD-016

Date: 28th Feb 2023
Version: 9.0

Version Control & Change Management

Version	Issue Date	Details of Change	Reason for change
9.0	28th Feb, 2022	Added IT Compliance Guidelines section Added IT Compliance implementation section Added compliance tools Added control for logging Non-Compliance issues in Risk mgmt. tool	To align with best practices based on the current need
8.0	30th June, 2022	Cloud CSP and Azure Advisor and Azure security centre controls added Cloud adoption changes incorporated	Cloud adoption changes
7.0	30th March, 2022	Merged Compliance Assessment process with Control Assurance docs.	
6.1	September, 2021	Document reviewed. No change required	Process annual review
6.0	Publishing Date	- Control Modified: Deviation or Change in the original plan shall be informed to higher management - Control Modified: The revised report should be sent to Head of IT GRM - Control Modified: Standard Execution Timelines - ASAP or 5 Business Days at max or as agreed / ASAP or 15 days before target date or as agreed.	To align with best practices based on the current need
5.0	Publishing Date	Added control under section: IT Control Assurance Reviews meeting: "Deviation in original plan during Control Review Meeting, would be made only on direction of Higher Management"	To align with current practice.
4.0	Publishing Date	Added: - identify suitable risk and rating for the finding/ issue based on the ADIB Operational Risk Framework - In case of any deviation in timelines, re-targeting of issues should follow Issues and Actions Management procedure defined by ORM	To align with current practice
3.0	Publishing date	Reviewed & updated document	To align with current practice
2.0	Publishing date	Standard Update	Reflecting recent improvements in the standard along with the changes
1.0	Publishing date	New standard on regulatory advisory / requirement management.	New Document

Prepared by	Approved by	Reviewed by
Governance Team	Head of Technology GRC Head of IT Compliance and Security Architecture	Assistant IT Vulnerability Manager Head of Reg and Compliance Assurance

Document Contents

1. Overview

The objective of this document is to delineate the standards for ITD reviews to ensure that ADIB's ITD is functioning as intended and to enhance existing controls and security posture.

2. Applicability

IT Controls assurance would cover reviews covering people, processes, and systems hosted on prem as well as cloud across ADIB ITD.

This procedure document is applicable to UAE, Qatar, Iraq, Sudan, UK

3. Standard Owner

Head of IT Compliance & Security Architecture

4. Standard Statements

4.1. Types of Findings

A finding is deemed as such if any of controls is found absent or ineffective. Findings are based on the below categories depending on the rating of the risk:

- Critical
- High
- Medium
- Low

4.2. IT Control Assurance Reviews Meeting

1. ITCA annual plan should be formulated for ITD departments and shall be shared for BRCC review and with Head of IT GRC approval.

   The plan is built after taking into consideration multiple inputs. Inputs include:
   - ITD Departmental Objectives.
   - ITD Process documents.
   - IT RCSA, past issues and actions.
   - GARR or external audit calendar.
   - Regulatory and compliance requirements
   - Azure advisor and security center (Microsoft Defender for Cloud) - Security recommendations
   - Internal review and validation of vendor provided/third party independent assessment reports on CSP

2. ITCA reviews should be executed according to the annual plan. Ad-hoc reviews might be initiated, as necessary, to address an immediate requirement or request in case of any changes, updated ITCA plan shall be shared with BRCC and Head of IT GRC for review and approval. In case, ad hoc review needs priority, annual plan may be re-visited to add the ad-hoc review and make any change if required.
3. Periodic IT Control Assurance Assessment reviews on existing production IT systems shall be performed as per Appendix A.
4. Deviation or Change in the original plan shell be informed to higher management (Head of IT GRC and BRCC).

5. Technical Control Assurance checking shall be performed manually by practiced system engineers, or through automated tools.

4.3. Conducting ITCA Reviews

1. ITCA Reviews should be conducted according to the annual plan.
2. A memorandum shall be formulated by illustrating the objective, background, scope of work, approach, and timelines for the reviews (if required).
3. The review shall re-visit closed findings in the Risk and Controls register. Findings in “Open” state should not be mentioned in the reports.
4. Issue and action priority for the findings should be in accordance with ADIB Operational risk framework.
5. The review upon conclusion should be followed with a discussion for the initial findings recorded with the stakeholders of the review. This discussion is meant to:
   - Present the findings and its matters.
   - Get a confirmation that findings recorded are factual or not.
   - If the findings recorded aren’t factual, the responsible stakeholder should present the evidence.
6. Final Report should be prepared based on the following inputs received from the stakeholders for the findings confirmed to be factually correct
7. Action plan to bridge the gap (including milestones if required). In case of a dispute, the dispute to be raised to Head of GRC.
   - Target date.
   - Responsible person and organizational entity.
8. The reviews upon conclusion should outline in a revised report with details as below:
   - The findings matter in detail.
   - The findings category and risk rating (As per department RCSA).
   - Risk of not addressing the findings’
   - Root Cause of the finding (if possible / applicable)
   - Actions required for addressing the findings risk
9. The revised report should be sent to Tech GRC management and BRCC for their review and logged into ORM Tool for monitoring and tracking.
10. Standard Execution Timelines

Activity	Std. Timeline
Requirement/Review/Response Collection (By Email, By Discussion in a Meeting, etc.)	ASAP or 5 Business Days at max or as agreed
Evidence Collection	ASAP or 15 days before target date or as agreed.

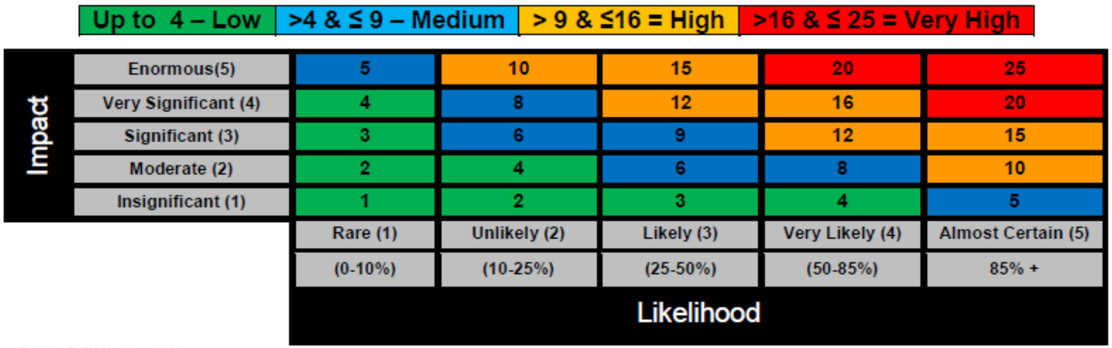
11. Head of Tech GRC and/or CIO has the authority to impose sooner deadlines as seen appropriate in-light of the findings’ risk.

4.4. Review & Monitoring

1. IT CA Representative should Review ITD team's progress toward the fulfillment of their actions plans on monthly basis.
2. IT CA Representative should Report progress status to Head of Tech GRC, and Department Heads on monthly basis.
3. In case of any deviation in timelines, re-targeting of issues should follow Issues and Actions Management procedure defined by ORM.
4. Closure of all the reported Non-compliance issues shall be managed by the respective project manager and IT Application\System owner.

4.5. Non-compliance issues

1. Compliance status of IT systems (on-premises and cloud) and applications assessed as part of periodic compliance assessments shall be reported to IT management as below:
    a. Head of IT Compliance and Security Architecture - Monthly
    b. Head of IT-GRC- Quarterly
    c. Cloud Chapter Lead – Monthly
    d. Head of Cloud operations - Quarterly
2. All Non-Compliance issues shall be reported & assigned to the respective IT system\application owner. Incidents shall be assigned to track closure of Non-Compliance issues.
3. All Non-Compliance issues with severity of Critical (Very High), High, and Medium shall be logged into Archer and assigned to respective IT system\application owner with target date.
4. All Low severity non-compliance issues shall be present to BRCC to respective unit head for their approval and target date to fix the issue.
5. All open Non-Compliance issues shall be reported and escalated based on their aging as below:
    a. Open for 30 days- Department Head of the action owner
    b. Open for 45 days- Head of Cloud Operations and Cloud Chapter Lead
    c. Open for 60 days- Head of Tech Operations



Up to 4 – Low	>4 & ≤ 9 – Medium	> 9 & ≤16 = High	>16 & ≤ 25 = Very High

Impact					
Enormous(5)	5	10	15	20	25
Very Significant (4)	4	8	12	16	20
Significant (3)	3	6	9	12	15
Moderate (2)	2	4	6	8	10
Insignificant (1)	1	2	3	4	5
	Rare (1)	Unlikely (2)	Likely (3)	Very Likely (4)	Almost Certain (5)
	(0-10%)	(10-25%)	(25-50%)	(50-85%)	85% +
	Likelihood				

Table 7 Risk Heat Map

4.6. Security Vulnerabilities

1. Vulnerabilities reports sent by GISD to ITGRC for assignment shall be verified for errors and accordingly reported to the respective ITD teams within 15 days of receiving the report.
2. Closure status of vulnerabilities on production IT systems shall be reported to the IT Vulnerability Owners and IT Management on a monthly basis.

3. Vulnerabilities identified & reported on existing ADIB production IT systems as part of GISD periodic security testing; shall be remediated as per timelines agreed upon by ITD action owner. Note: - These shall exclude Operating System and application runtime components patching related vulnerabilities reported by GISD as part of ITD's production systems patching cycles as they shall follow the timelines mentioned in the Patch Management Standard.
4. Azure Advisor and Azure security center (Microsoft defender for cloud) recommendations shall be assessed and remediate as per the timelines agreed upon by Cloud action owner. Cost management recommendation shall be treated in FinOps controls.

4.7. IT Compliance Implementation

1. Technology Compliance representative develops standards and create profile in compliance tools as per approved baselines/standards.
2. Below is the list of compliance tools:

- Tripwire CCM Tool for System Configuration Compliance: This tool is used to scan Network Devices, System Platforms, Databases, etc.
- Skybox: This tool is used to perform Firewall Assurance including Firewalls Configuration and Rules Compliance

3. Technology compliance unit perform the scan of infrastructure components and share the scan results with Technology operation team to fix the non-compliance items. Once the issues are fixed another scan is performed to ensure the compliance as per defined KPIs. Non-compliance issues are reported, monitored, and tracked.

4.8. IT Compliance Guidelines

Technology compliance Team shall follow below guidelines to report compliance status to the respective stakeholders:

1- Perform review as per ITCA Standard Appendix A
2- Compliance report shall be shared with respective stakeholders via email communications
3- Track the reported discrepancies with respective stakeholders for validation
4- Non-compliance issues which can't be fixed will be treated as exception approval from Head of Tech-GRC and Head of TechOps.
5- Non-compliance issues will be logged into Archer

5. Exceptions

Any deviation to the standard shall be documented along-with associated risks and shall be approved

6. Appendixes

Appendix A

#	Description	Frequency	Time Frame
1	Operating Systems Configuration Compliance for Internal Servers	Semi annual	Mar-April / Sep-Oct

#	Description	Frequency	Time Frame
2	Operating Systems Configuration Compliance for DMZ Servers	Quarterly	Successive month after end of each quarter
3	Operating Systems Configuration Compliance for Swift Servers	Semi Annual	Mar-April / Sep-Oct
4	Configuration Compliance for DMZ Network Devices	Quarterly	Successive month after end of each quarter
5	Configuration Compliance for Internal Network Devices	Semi annual	Mar-April / Sep-Oct
6	Configuration Compliance for Internal Databases	Annual	Jan-April
7	Configuration Compliance for DMZ Security Devices	Quarterly	Successive month after end of each quarter
8	Configuration Compliance for Cloud DMZ Security Devices	Quarterly	Successive month after end of each quarter
9	Configuration Compliance for Internal Security Devices	Annual	Jan-April
10	Configuration Compliance for Cloud Internal Security Devices	Annual	Jan-April
11	Servers Share Review	Semi annual	Mar-April / Sep-Oct
12	Servers' Local admin Review	Semi annual	Mar-April / Sep-Oct
13	Client Share Review	Semi annual	May-June / Nov-Dec
14	Client Local admin Review	Semi annual	May-June / Nov-Dec
15	Client Blacklist SW review*	Annual	May-June / Nov-Dec
16	Server Blacklist Software Review	Annual	May-June / Nov-Dec
17	Review of application services running with elevated OS privileges on DMZ application servers.	Annual	Oct-Dec
18	Azure Advisor and Azure security center (Microsoft defender for cloud) recommendations and assessment	Quarterly	Successive month after end of each quarter
19	Internal review and validation of vendor provided/third party independent assessment reports on CSP	Quarterly	Successive month after end of each quarter

*Server installed software or application will be marked as blacklisted if they fall under any of the below software categories or functions:

- Social Networking
- Packet Capture\Traffic Analysis
- Email Client
- Software Development kits\tools
- Security Testing Tools
- Un-Approved Freeware Software
- Un-Approved Open-Source Software

Annex B: Acronyms

Abbreviation	Acronym
ADIB	Abu Dhabi Islamic Bank
ITD	Information Technology Division
Non-Compliance	Failure of an IT system to comply with a mandate(s) as per a published ADIB ITD Standard document.

Annex C: References

Doc. Ref. No.	Name	Type of Document (Policy / Standard)
IMSM-ITD-001	IMS Manual	Manual
STD-ITD-502	Application Standard	Standard
STD-ITD-517	Server Standard	Standard
STD-ITD-533	Database Standard	Standard
STD-ITD-507	Patch Management Standard	Standard
	ADIB ORM Process	Policy
	Security Baseline for Azure Cloud Resources	Baseline