ADIB – Procedure

IT Control Assurance Procedure
PRC-ITD-531

Date: 28th February, 2023
Version: 8.0

Version Control & Change Management

Version	Issue Date	Details of Change	Reason for Change
8.0	Feb, 2023	Updated the "Roles & RACI" Added IT Compliance Implementation workflow Added Head of Reg and Compliance Assurance	Added more details.
7.0	June, 2022	Cloud CSP and Azure Advisor and Azure security centre controls added Cloud adoption changes are incorporated	Cloud adoption
6.0	April, 2022	Merged Compliance Assessment process with Control Assurance docs.	
5.0	July, 2021	IT Control Assurance Manager will ensure details of methodology and testing coverage, based on the type of reviews are documented in Control Assurance report.	Control Assurance reports issued after reviews performed by ITCA team will be standardized.
4.0	Publishing Date	Control Modified: Send the ITCA annual plan for review and approval to Head of IT GRM and Head of IT GRC. Control/Responsibility Modified: - Send the Memorandum to IT GRM and GRC Head for review. Responsibility: IT Control Assurance Manager - Send the Memorandum to respective department heads for their intimation. Responsibility: Head of IT GRM	Annual Review activity and ensured process is reviewed and updated
3.0	Publishing Date	RACI Chart and KPI's	To align with current practice.
2.0	Publishing date	Moved document to new format Updated "Reporting of Findings" section Added KPIs	To align with current practice.
1.0	Publishing date	New IT control Assurance Procedure	Rectifying due to non-sync with practice.

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

Document Contents

1 Purpose & Scope

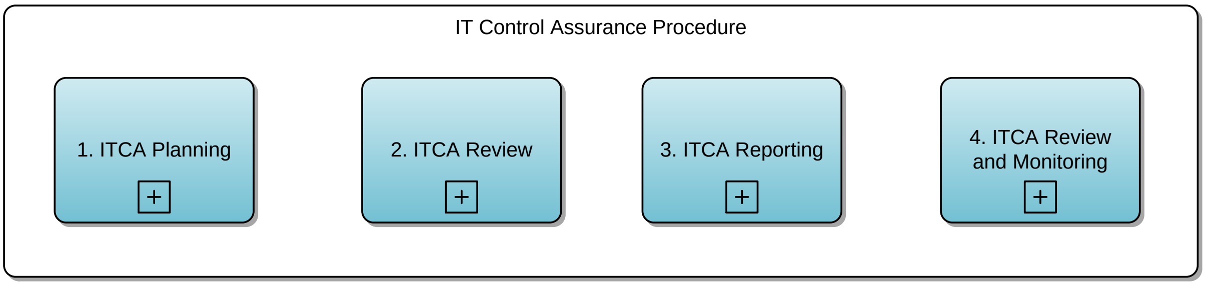
The objective of this document is to delineate the procedure for IT Control Assurance reviews to ensure that ADIB's IMS is functioning as intended.

IT Controls assurance procedure includes the reviews covering people, processes, and systems across ADIB ITD.
This procedure document is applicable to UAE, Qatar, Iraq, Sudan, UK

2 Process Owner

Head of IT Compliance and Security Architecture.

3 IT Control Assurance Process Flow - High Level Workflow



IT Control Assurance Procedure

1. ITCA Planning ⊞

2. ITCA Review ⊞

3. ITCA Reporting ⊞

4. ITCA Review and Monitoring ⊞

3.1 Roles & Responsibilities:

Head of Tech GRC	Head of Tech GRC will review the yearly control assurance plan and present to BRCC for approval.
Head of Reg and Compliance Assurance	This Unit is responsible to gather information pertaining to each area within GRC to formulate the Control Assurance Plan. Once the initial plan is drafted covering all areas not limited to Governance, Risk, Compliance and Control Assurance. It will be shared with Head of Tech GRC for his review. Later it will be presented to BRCC for ITD Leaders review for any amendment and approvals. Quarterly control assurance reports will be shared with Head of TechGRC and to all ITD Departments.
Head of Technology Control & Compliance	This Unit will ensure adequate technical controls are in place by performing compliance & control assurance reviews of Infrastructure components as per ADIB IT Policy and Standards. During the review process any operational risk is assessed, documented with mitigating controls.
Head of Technology Governance	This Unit will ensure the technology process documents are reviewed and kept up to date and approved by the process owner annually and will ensure the processes are aligned with the all issues and gaps reported by Audit and control deficiencies where applicable.
Head of Risk Management	Accountable to include ITCA issues in Risk Assessments done as part of RCSA cycles.
Head of Application Assurance	This Unit will ensure adequate technical controls are in place by performing control assurance review of Application components as per ADIB IT Policy, Application Standards and as per SDLC Process.
Head of Change Management	Performs the reviews from IT Service Management Perspectives including SLAs, Open Incidents, pending changes and problem management.

4 Detailed Process Description and Workflows

4.1 Planning for ITCA reviews

RACI

Roles / Activity	Head of Technology Control & Compliance	Head of Reg and Compliance Assurance	Head of Technology Governance	Assistant IT Vulnerability Manager	Head of Application Assurance	IT Change Manager	Auditee Dept
Formulate Annual Plan	C, R	A, R	C	C	C	C	C
Review & approve plan	C, R	A, R	C	C	C	C	
Execute Plan	C, R	A, R	R	R	R	R	I

Sr. No.	Process Step Description	Responsibility	Document (STD, PRC, FORM, CL, TML WI) / Tool Reference
1	Formulate ITCA Annual plan for ITD departments The plan is based on the following considerations: • ITD Departmental Objectives (If available). ITD Process documents. • IT, RCSA, old issues and Actions. • GARR or external audit calendar. • Regulatory and compliance requirements • Inputs from Head of other IT functions	Head of Reg and Compliance Assurance	ITCA Annual plan
2	Send the ITCA annual plan for review and approval to Head of Tech GRC and BRCC.	Head of Reg and Compliance Assurance	ITCA Annual plan
3	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, ad hoc review needs priority, annual plan may be re-visited to add the ad-hoc review and make any change if required.	Head of Reg and Compliance Assurance	ITCA Annual plan
4	In case of any changes, ITCA plan shall be shared with Head of Tech GRC and BRCC.	Head of Reg and Compliance Assurance	ITCA Annual plan

4.2 Conduct ITCA reviews

RACI

Roles / Activity	Head of Technology Control & Compliance	Head of Reg and Compliance Assurance	Head of Technology Governance	Assistant IT Vulnerability Manager	Head of Application Assurance	IT Change Manager	Auditee Dept
Prepare Memorandum	C	A, R	C	C	C	C	
Review Memorandum	C	A, R	C	C	C	C	
Notify Identified units on audit	R	A	I	I	I	I	I
Conduct IT CA Reviews	R	A, R	R	R	R	R	I

Sr. No.	Process Step Description	Responsibility	Document (STD, PRC, FORM, CL, TML WI) / Tool Reference
1	Prepare Memorandum for selected ITD department/function / process which includes the objective, background, scope of work, exclusions (if any), approach and timelines for review.	Head of Reg and Compliance Assurance	Memorandum
2	Send the Memorandum to and Head of Tech GRC for review.	Head of Reg and Compliance Assurance	Memorandum
3	Send the memorandum to respective Departments heads for their intimation and review kick off	Head of Reg and Compliance Assurance	Memorandum
4	Conduct ITCA review based on the memorandum.	Head of Reg and Compliance Assurance	Email, Work Sheets, evidence

4.3 Reporting of findings

RACI

Roles / Activity	Head of Technology Control & Compliance	Head of Reg and Compliance Assurance	Head of Technology Governance	Assistant IT Vulnerability Manager	Head of Application Assurance	IT Change Manager	Auditee Dept
Consolidate findings for review	R	A, R	C	R	R	R	
Rate findings and map to ORM Risk	C	R	C	A	C	C	
Issue, discuss & finalize initial	C	A, R	C	C	C	C	C, I

findings with auditee.							
Prepare report with prescribed inputs	C	A	C	C	C	C	
Send revised report with imposed target date (in case of non-response)	I	A, R	I	I	I	I	I
Send report for approval	I	A	I	I	I	I	I
Send final report & log to ORM tool	I	R	I	R	I	I	I

Sr. No.	**Process Step Description**	**Responsibility**	**Document (STD, PRC, FORM, CL, TML WI) / Tool Reference**
1	Consolidate the findings or observations for current review. **Note**: The Open findings from previous review are not included in the current review reports.	Head of Reg and Compliance Assurance	Excel file of findings / observations
2	Identify relevant risk and rating for the finding/ issue based on the ADIB Operational Risk Framework.	Head of Reg and Compliance Assurance	Excel file of findings / observations
3	Issue and review initial list of findings with the Auditee. Revise and finalize the list based on the evidence provided by Auditee for findings claimed to be invalid (if any).	Head of Reg and Compliance Assurance Department	Excel file of findings / observations
4	Control Assurance report have the details of methodology and testing coverage, based on the type of reviews, such as infrastructure, application development, support, etc.	Head of Reg and Compliance Assurance	Report
5	Prepare the report with additional following inputs of the findings based on the responses received from the audited department: Action plans to bridge the gaps identified. Target dates to rectify the gaps. Responsible personnel. Deliverables to be provided (if required).	Head of Reg and Compliance Assurance	Report
6	If response is not received within 5 business days or as agreed from department under review, impose the set target dates and proceed with preparing revised report. Revised report includes: • The findings in detail. • Finding category and risk rating (as per department RCSA) • Risk of not addressing the findings.	Head of Reg and Compliance Assurance	

Sr. No.	Process Step Description	Responsibility	Document (STD, PRC, FORM, CL, TML WI) / Tool Reference
	• Actions required for addressing the findings risk. Expected Deliverables: Documents / evidence required to reflect action taken to rectify the root cause of the problem (if required / applicable).		
7	Send the revised report to Tech GRC management and BRCC, for their review to log the issues in the ORM tool.	Head of Reg and Compliance Assurance	Revised report
8	In case of changes / suggestions by IT GRC Management, update the final report accordingly. In case of no change suggested, or if response is not received within 5 business days, proceed with issuing of final report. The same to be logged in ORM tool.	Head of Reg and Compliance Assurance	-

4.4 Review and Monitoring

RACI

Roles / Activity	Head of Reg and Compliance Assurance	IT Control Assurance Representative	Head of Tech GRC	Auditee Department
Conduct monthly reviews of the ITD progress	A	R	I	I
On deviation obtain justification from auditee	A	R	C, I	R
Re-targeting of Issues	C	R,	C	A, R
Send monthly progress status report	A	R	I	I

Sr. No.	Process Step Description	Responsibility	Document (STD, PRC, FORM, CL, TML WI) / Tool Reference
1	Conduct monthly reviews of the ITD team progress towards fulfilment of the action plans against each finding logged in ORM tool till closure of issue	Head of Reg and Compliance Assurance	ORM Tool
2	In case of any deviation in timelines, re-targeting of issues should follow Issues and Actions Management procedure defined by ORM.	Action owner / Department Under Review (Auditee) Designate	Approvals, Justification
3	Send progress status report to~~,~~ Head of Tech GRC and respective audited departments and CIO monthly.	Head of Reg and Compliance Assurance	Progress status report/Dashboard

4.5 Non-Compliance Issues Management

RACI

Roles / Activity	Head of Reg and Compliance Assurance	IT Control Assurance Representative	Head of Tech GRC	IT System / Application Owner
Run compliance assessments to verify closure	A	R	I	**C**
Report all the Non Compliance issues	A	R	I	I

Sr. No.	Process Step Description	Responsibility	Document (Record, WI) / Tool Reference
▪ Non-Compliance Issues Management1			
1	Run compliance assessments to verify closure of all the assigned Non-Compliance issues. Note: - The assessment will be performed 30 days after assigning the assessment report and the scope of the assessment will only be restricted to the assigned Non-Compliance issues. Based on GISD inputs, IT Control Assurance Representative will perform the assessment and share the report.	IT Control Assurance Representative	IT Compliance Assessment Report
2	Report all the Non-Compliance issues which haven't been closed to Head of IT Controls & Compliance for escalation as per the matrix defined in the IT Control Assurance Standard.	IT Control Assurance Representative	Email

4.6 Cloud Security Vulnerabilities

Roles / Activity	IT Risk Management Representative	GISD Team (VAPT)	IT System \ Application Owner	ITGRC Head	IT Management
Review vulnerability reports received by GISD	R	I	-	-	-
Inform the respective ITD teams	R	-	I	I	I
Inform ITD teams & management on the closure status	R	I	I	I	I

Sr. No.	Process Step Description	Responsibility	Document (Record, WI) / Tool Reference
▪ Security Vulnerabilities			
1	Review vulnerability reports received by GISD to filter out the ones with incomplete information and/or which are not applicable and publish the report on the centralized vulnerability remediation actions tracker. Note: - GISD vulnerability reports will be published as per timelines mentioned in the IT Control Assurance Standard.	IT Risk Management Representative	Vulnerability Remediation Actions Tracker
2	Inform the respective ITD teams on the new updates made on the vulnerability remediation actions tracker.	IT Risk Management Representative	Email
3	Provide periodic report of vulnerability remediation actions closure status to ITD teams & management.	IT Risk Management Representative	Email BRCC Presentation

4.7 Cloud advisory recommendation

RACI

Roles / Activity	IT Risk Management Representative	Cloud Chapter Lead - CCoE	Cloud Operation engineer	Head of cloud Operations	IT System \ Application Owner	ITGRC Head	IT Management
Review vulnerability reports in Azure advisor	R	R, C	C	A	-	-	-
Inform the respective ITD cloud operations teams	R	R, C	C	A	I	I	I

Inform ITD teams & management on the closure status	**R**	**R, C**	**C**	**A**	**I**	**I**	**I**

Sr. No.	**Process Step Description**	**Responsibility**	**Document (Record, WI) / Tool Reference**
Security Vulnerabilities			
1	Assess Azure Advisor and Azure security center (Microsoft defender for cloud) recommendations	IT Risk Management Representative Cloud Chapter Lead Cloud Architect	Email
2	Address valid recommendation and update the cloud security policy in Azure	Cloud Operation engineer	Email (Export of Azure advisor and security center)
3	Inform the respective ITD teams on the new updates made on the vulnerability remediation actions tracker.	IT Risk Management Representative	Email
4	Provide periodic report of vulnerability remediation actions closure status to ITD teams & management.	IT Risk Management Representative	Email

4.8 Cloud internal review and validation of CSP assessment reports (vendor provided/third party)

RACI

Roles / Activity	**IT Risk Management Representative**	**Cloud Chapter Lead - CCoE**	**Head of cloud Operations**	**IT System \ Application Owner**	**ITGRC Head**	**ITD Management**
Review and validation of CSP assessment reports (vendor provided/third party)	**R**	**R, A**	**C**	**-**	**-**	**-**
Inform the respective ITD teams	**C**	**R, A**	**C**	**I**	**I**	**I**
Inform ITD teams & management on the closure status	**C**	**R, A**	**C**	**I**	**I**	**I**

Sr. No.	**Process Step Description**	**Responsibility**	**Document (Record, WI) / Tool Reference**
Review and validation of CSP assessment reports (vendor provided/third party)			
1	Internal review and validation of vendor provided/third party independent assessment reports on CSP	Cloud Chapter Lead Cloud Architect IT Risk Management Representative	Email
2	Consult with CSP if any clarification and deviations on provided assessment reports	Cloud Chapter Lead	Email

Sr. No.	Process Step Description	Responsibility	Document (Record, WI) / Tool Reference
3	Address valid recommendation with CSP and update the ITD management	Cloud Chapter Lead	Email

4.9 IT Compliance Implementation

RACI

Roles / Activity	Head of Tech - GRC	Technology Compliance representative	Tech Governance	Assistant IT Vulnerability Manager	TechOps
Develop the Compliance Standard	I	A, R	C	C	C
Create Compliance Profiles	I	A	I	I	C
Manage the tools	I	R, A			I
Fix Non-Compliance Issue	I	C		I	R
Reviews & Monitoring	I	R		I	C
Reporting	I	R, A	I	I	I
Exception Handling	R	A		I	C

Sr. No.	Process Step Description	Responsibility	Document (Record, WI) / Tool Reference
1	Develop the Compliance Standard	Technology Compliance representative	
2	Create Compliance Profiles tools to scan as per define compliance parameters	Technology Compliance representative	
3	Manage the tools (Tripwire CCM & Skybox) is used for configuration compliance scan	Technology Compliance representative	Standard Operating Procedure for Compliance tools
4	Fix Non- Compliance Issue – TechOps is responsible to fix all non-compliance	TechOps	
5	Reviews & Monitoring – Validate and track closure of Non-Compliance issues	Technology Compliance representative	ITCA Standard
6	Compliance report share with respective stakeholders via email communications	Technology Compliance representative	ITCA Standard
7	Exception Handling – Non-compliance issues which can't be fixed will be treated as exception approval from Head of Tech-GRC and Head of TechOps.	Head of Tech - GRC	ITCA Standard

Sr. No.	Process Step Description	Responsibility	Document (Record, WI) / Tool Reference

6 Risks and Controls

Related Risks	Risk Description	Business Unit Name - Control Owner	Control Register Tracking ID	Control Subject
R-326481	Risk of business disruption & reputation loss when ADIB client machines are compromised by exploiting their known security vulnerabilities; due to inadequate identification & reporting of security vulnerabilities on ADIB client machines	Technology GRC	C-336475	Reporting & Tracking of non-compliant client machines non-compliant client machines are reported and tracked.
R-326481	Risk of business disruption & reputation loss when ADIB client machines are compromised by exploiting their known security vulnerabilities; due to inadequate identification & reporting of security vulnerabilities on ADIB client machines	Technology GRC	C-336471	Client Share Review production windows client machines are scanned for shares and identified findings are raised as incidents & assigned to the respective ITD team(s).
R-326480	Risk of business disruption & reputation loss when ADIB internal applications & IT systems are compromised by exploiting their known security vulnerabilities; due to inadequate identification & reporting of security vulnerabilities on ADIB internal applications & IT systems	Technology GRC	C-336467	Server Share Review Internal production windows servers are scanned for shares with unrestricted permissions.
R-326479	Risk of business disruption when ADIB internet facing applications & systems are compromised by exploiting their known security vulnerabilities; due to inadequate identification & reporting of security vulnerabilities on ADIB internet facing applications & systems	Technology GRC	C-336457	ADIB internet facing applications & systems Vulnerabilities and non-Conformities are assigned and tracked for closure.
R-326475	Risk of loss of confidentiality and availability due to unauthorized remote external access from third parties to ADIB IT infrastructure	Technology GRC	C-336433	Site to Site VPN Security Configuration Access control is provided as per need-to-know basis and as per business requirement
R-326475	Risk of loss of confidentiality and availability due to unauthorized remote external access from third parties to ADIB IT infrastructure	Technology GRC	C-336432	All site-to-site remote external access of third parties to ADIB infrastructure are reviewed and approved.
R-326474	Risk of loss of data that is stored locally on mobile devices in the event of device lost or theft	Technology GRC	C-336429	Preboot authentication for Laptop ADIB laptops require preboot authentication prior to loading of Operating system.

Related Risks	Risk Description	Business Unit Name - Control Owner	Control Register Tracking ID	Control Subject
				ADIB laptops lockout after 5 attempts for 30 minutes
R-326473	Risk of business disruption and financial loss when ADIB IT Administrators perform fraudulent activities on IT systems; due to inadequate monitoring & review of IT Administrator activities	Technology GRC	C-336425	IT Administrator activities Non-Conformities (NCs) are assigned and tracked for closure
R-326473	Risk of business disruption and financial loss when ADIB IT Administrators perform fraudulent activities on IT systems; due to inadequate monitoring & review of IT Administrator activities	Technology GRC	C-336423	IT Administrator Activity Review Changes made by IT administrator(s) on the following production systems are reviewed on a weekly basis for approval & authorization
R-326473	Risk of business disruption and financial loss when ADIB IT Administrators perform fraudulent activities on IT systems; due to inadequate monitoring & review of IT Administrator activities	Technology GRC	C-336422	IT Administrator Activity Monitoring mechanism is established Changes made by IT administrator(s) on the following production systems are continually monitored
R-326472	Risk of information leakage, operational and financial loss when ADIB client machines are compromised via malware programs/software; due to inadequate identification & reporting of insecure ADIB client machines.	Technology GRC	C-336419	Client Software Review
R-326472	Risk of information leakage, operational and financial loss when ADIB client machines are compromised via malware programs/software; due to inadequate identification & reporting of insecure ADIB client machines.	Technology GRC	C-336417	ADIB Endpoint Security Compliance
R-326471	Risk of information leakage, operational loss & financial loss due to ADIB IT systems being accessible to unauthorized privileged users	Technology GRC	C-336415	IT Privileged User Access Review Non-Conformities (NCs) are assigned and tracked centrally for closure.
R-326471	Risk of information leakage, operational loss & financial loss due to ADIB IT systems being accessible to unauthorized privileged users	Technology GRC	C-336414	Review of privileged user accounts for network devices is performed and findings are reported to respective teams
R-326471	Risk of information leakage, operational loss & financial loss due to ADIB IT systems being accessible to unauthorized privileged users	Technology GRC	C-336412	Client Local Admin Review Local admins on all production client machines are reviewed for authorization.

Related Risks	Risk Description	Business Unit Name - Control Owner	Control Register Tracking ID	Control Subject
R-326471	Risk of information leakage, operational loss & financial loss due to ADIB IT systems being accessible to unauthorized privileged users	Technology GRC	C-336410	Server Local Admin Review Local admins on all production windows servers are reviewed for authorization.
R-326470	Risk of business disruption and reputation loss when ADIB internal IT systems are compromised by exploiting their security misconfigurations; due to inadequate identification & reporting of security misconfigurations on ADIB internal IT systems	Technology GRC	C-336409	Security misconfigurations on ADIB internal IT systems Non-Conformities (NCs) are assigned and tracked centrally for closure
R-326470	Risk of business disruption and reputation loss when ADIB internal IT systems are compromised by exploiting their security misconfigurations; due to inadequate identification & reporting of security misconfigurations on ADIB internal IT systems	Technology GRC	C-336407	Secure Configuration Review of Internal Security Devices
R-326470	Risk of business disruption and reputation loss when ADIB internal IT systems are compromised by exploiting their security misconfigurations; due to inadequate identification & reporting of security misconfigurations on ADIB internal IT systems	Technology GRC	C-336405	Secure Configuration Compliance Scans for Internal Network Devices
R-326470	Risk of business disruption and reputation loss when ADIB internal IT systems are compromised by exploiting their security misconfigurations; due to inadequate identification & reporting of security misconfigurations on ADIB internal IT systems	Technology GRC	C-336404	Secure Configuration Compliance Scans for Internal DB Servers
R-326470	Risk of business disruption and reputation loss when ADIB internal IT systems are compromised by exploiting their security misconfigurations; due to inadequate identification & reporting of security misconfigurations on ADIB internal IT systems	Technology GRC	C-336402	Secure Configuration Compliance Scans for Internal Servers
R-326469	Risk of business disruption & reputation loss and financial loss when ADIB internet facing IT systems are compromised by exploiting their security misconfigurations; due to inadequate identification & reporting of security misconfigurations on ADIB internet facing IT systems.	Technology GRC	C-336400	Security misconfigurations on ADIB internet facing IT systems Non-Conformities (NCs) are assigned and tracked for closure.

Related Risks	Risk Description	Business Unit Name - Control Owner	Control Register Tracking ID	Control Subject
R-326469	Risk of business disruption & reputation loss and financial loss when ADIB internet facing IT systems are compromised by exploiting their security misconfigurations; due to inadequate identification & reporting of security misconfigurations on ADIB internet facing IT systems.	Technology GRC	C-336398	Secure Configuration Review of all DMZ Security Devices Configuration of DMZ IT Security Devices is reviewed for compliance to the respective Secure Configuration Benchmark
R-326469	Risk of business disruption & reputation loss and financial loss when ADIB internet facing IT systems are compromised by exploiting their security misconfigurations; due to inadequate identification & reporting of security misconfigurations on ADIB internet facing IT systems.	Technology GRC	C-336397	Secure Configuration Compliance Scans for DMZ Network Devices Secure Configuration Compliance scans are done for all the DMZ network devices and identified findings are raised as an incident & assigned to the respective ITD team(s)
R-326469	Risk of business disruption & reputation loss and financial loss when ADIB internet facing IT systems are compromised by exploiting their security misconfigurations; due to inadequate identification & reporting of security misconfigurations on ADIB internet facing IT systems.	Technology GRC	C-336395	Secure Configuration Compliance Scans for DMZ Servers Secure Configuration Compliance scans for the following OS platforms are done for the respective DMZ production server

7 Key Performance Indicator

Sr. Nos.	KPI	Target	Source	Reporting to	Frequency	Formula
1	IT CA review performed as per approved annual plan	90%	Approved Annual Plan and Monthly Status Reports	Head of IT Compliance and Security Architecture,	Annual	Number of Reviews completed/Total Number of reviews plan and approved* 100
2	% Of performed periodic IT Compliance Assessments as per defined schedule	95%	Semi-Annually	Head of IT Compliance and Security Architecture,	Email	(Performed IT Compliance assessment / scheduled IT compliance assessment) *100
3	% Of escalated Non-Compliance issues as per defined schedule	100%	Monthly	Head of IT Compliance and Security Architecture,	Email	(Escalated Noncompliance issues / Total of noncompliance issues identified) *100

8 Appendixes

Annex I: Acronyms

Abbreviation	Acronym
ADIB	Abu Dhabi Islamic Bank
ITD	Information Technology Division
SM9	Service Manager Tool

Annex II: References

Doc. Ref. No.	Name	Type of Document (Policy / Standard)
STD-ITD-016	IT Controls Assurance Standard	Standard