ADIB – IMS/Appendix
(All ADIB international Branches)

IT Security Roles-Responsibilities
IMS-ITD-001 Appendix-G

Date: 30th April 2023
Version: 8.0

Version Control & Change Management

Version	Issue Date	Details of Change	Reason for change
8.0	April 2023	Updated mandates have been reflected for below units: - IT Control Assurance - IT Security Operations - IT Support / Site Team / IT Service Desk	Annual Review
7.0	April 2022	Updated mandates have been reflected for below units: - IT Control Assurance - IT Security Operations	Annual Review
6.0	April 2021	Added/Modified responsibilities	Annual Review
5.0	May, 2020	Modified document ownership	To align with organization structure
4.0	Publishing date	Annual Review	Reviewed document to meet annual review cycle compliance
3.0	Publishing date	Realignment of role and responsibilities of Security Operations with GISD	Annual Review and aligned with GISD Information Security Policy;
2.0	Publishing date	New Template Revalidation of the responsibilities	Process optimization GISD-ITD Transition

Prepared by	Approved by	Reviewed by
Governance Team	Head of OCIO	IT GRM Manager

Document Contents

1 Information Security Organization

ADIB ISMS implements a top-down approach in establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS). This ensures the involvement of the top management in driving the Information Security Program. Information Security Organization is a formal hierarchy of roles and responsibilities established for ADIB ISMS Framework.

ADIB Security Organization involves.

- Management Representative
- Information Security Coordinator
- IT Support / Site Team / IT Service Desk
- IOP (Network & Sys Admin)
- ITSO (IT Security Operations)

1.1 Technology Governance Section:

1. Responsible to streamline, optimize, maintain & update ITD processes and documentation.
2. Conduct awareness sessions for technology processes
3. Designs, manage, review and continually improve the Integrated Management System (IMS). Achieve satisfactory audit rating.
4. Ensure the Preparation, compilation, review, follow up and periodic reporting of IT department performance
5. Ensure self and staff members complete mandatory training

1.2 Technology Risk Management:

1. Implement ADIB's enterprise risk management objectives and mandates across the ITD.
2. Establish, manage and maintain the Risk & Control Self-Assessment process of the technology department units.
3. Provide technology leadership risk management guidance and risk treatment options to reduce technology risks.
4. Maintain the technology Risk register and map identified issues to relevant risks.
5. Monitor the performance and effectiveness of established controls and optimize them for risk reduction.
6. Manage the development and reporting of Key Risk Indicators to measure the effectiveness of technology department processes.
7. Conduct scheduled risk assessments & direct initiatives to minimize residual risk to align with the target risk appetite.
8. Interface and represent technology department in ADIB's Operational Risk Management engagements and forums.

1.3 Technology Control Assurance:

1. Monitor and Track Corrective Action plan for the issues identified through Internal/external audits, reviews and self-identified.
2. Provide periodic progress reports on the implementation of corrective actions to stakeholders and management till closure.
3. Conduct technology and process assurance reviews on regular and on-demand basis.
4. Maintain and manage the implementation of regulatory and industry compliance requirements related to ITD.
5. Coordinate and manage internal/external audits across technology department and point of contact for other departments.
6. Participate in the review of Standards and Processes to ensure required controls are addressed

7. Define, establish, and maintain technology Controls for ADIB technology systems and applications.
8. Verify, report and support technology department teams in implementing technology Controls on ADIB systems prior to the go-live of new production systems and major changes on existing production systems.
9. Participate in DRB (Design Review Board) and CAB (Change Approval Board) meetings to review new ADIB business information systems changes to existing systems in order to recommend, discuss, finalize, consolidate and ensure the technology system's designed are compiled with control mandates and business requirements.
10. Perform periodic User Access review for production critical infrastructure systems.
11. Perform periodic review of technology Admin activities on critical ADIB production infrastructure systems to ensure detection & reporting of unauthorized admin activities on production systems.
12. Ensure continual enhancement, technical maintenance, fine tuning and administration of ADIB SIEM and DAM systems.
13. Define, establish, and maintain system configuration baseline controls for critical ADIB production infrastructure systems to ensure proper system security hardening and compliance with ADIB standards.
14. Perform periodic and ad-hoc technology Compliance Reviews on all production servers, client machines, security, and network devices.
15. Implement new monitoring requirements from GISD and business in ADIB SIEM and DAM systems.
16. Ensure timely license subscription & maintenance support renewals as per approved budget for all systems managed.
17. Enabling business to adopt and use the required latest emerging technologies by ensuring technology controls are in place to protect & also add value to business objectives.
18. Develop, establish and maintain technology Controls for ADIB technology systems and applications.
19. Defining & establishing technology controls to meet new ADIB regulatory and industrial standard requirements and mitigate new technology risks.
20. Protecting technology systems from known business risks by continually monitoring, reviewing & enhancing the defined technology controls to ensure they are always effective in mitigating these risks.
21. Verify, report and support IT Application teams in implementing IT Application standards prior to the go-live of new applications and major changes on existing production applications.
22. Perform periodic and ad-hoc technology Compliance Reviews on production systems & applications.
23. Track health check reports for application till closure.
24. Participate in DRB (Design Review Board) and CAB (Change Approval Board) meetings to review new ADIB business information systems change to existing systems in order to recommend, discuss, finalize, consolidate and ensure the technology system's designed are compiled with control mandates and business requirements

1.4 Information Security Co-coordinator

1.4.1 Role

Information Security Coordinators act as a point of contact for the ITD units within the scope of ISMS and is responsible for implementing and driving ISMS related activities within their ITD Units. Information Security Coordinators work with the Governance and Risk management Representative to ensure ISMS related requirements are identified, implemented, tested and maintained on an ongoing basis. Head of respective ITD unit is designated as Information Security Coordinator (IS Coordinator)

1.4.2 Task Summary

Information Security Coordinators are responsible to execute the following tasks in the ISMS framework:

1. Work with department managers to evaluate the assets based on Confidentiality, Integrity and Availability
2. Work with the Technology Governance and Risk Management Teams in implementing controls required to mitigate identified risks within respective departments
3. Assist Technology Governance and Risk Management Teams while assessing the Security implications of any technological or organizational changes within respective units.
4. Facilitate Technology Governance Team conducting periodic independent reviews of ISMS, internally or in coordination with external auditors
5. Work closely with department managers in a timely closure for any non-conformity reported during audits of the ISMS
6. Update Technology Governance Team on a periodic basis on the closure status of audit non-conformities.
7. Update Technology Governance and Risk Management Teams on any situations within their respective department that may lead to an event or any security incidents or policy violations

1.4.3 Skills & Competencies

1. Awareness about the ADIB Information Security Policies, procedures, and standards
2. In-depth understanding on ITD activities of respective Unit
3. Able to demonstrate strong analytical and decision-making skills
4. Organized and capable of coordinating to complete a task
5. Effective team management skills
6. Strong communication skills
7. Able to respond effectively to unforeseen events to support business interests.

1.5 IT Support / Site Team / IT Service Desk

IT Support / Site Team / IT Service Desk shall be responsible for:

1. Centralized technology Service Desk Management
2. UAE client hardware provisioning and support
3. Desktop management that includes Operating Systems, Client Security platforms, Client Business Apps
4. Client remote and UAE onsite Support
5. Software deployments and client patch management
6. Deployments and support of special business solutions such as Managed Printing and Imaging Solution, Digital Signage and Customer Management System
7. IT Service Request Management
8. Support of ATM/CCDM/ITM/TCRs and Sites technology setup Management
9. Image management: Managing Server and Desktop OS images in Citrix Provisioning and Machine creation services.

Citrix Team:

1. Monitoring Citrix infrastructure through Citrix Director and Cloud Studio
2. Configuration and deployment of Citrix NetScaler Classic and advance policy
3. Deployment of Citrix NetScaler for Configure and support server proxy, process SSL requests, offers VPN etc.
4. Quickly troubleshoot, analyse, and resolve issue related to Citrix XenApp and Desktop, NetScaler, Azure, Citrix Cloud and FSLogix.
5. Perform capacity planning through ongoing monitoring, alerting, and reporting of resource utilization levels and errors in the environment.

Endpoint Security Team:

1. Endpoint Security manages day to day operations of Endpoint Security
2. Manage & Maintain Endpoint security infrastructure (Forcepoint DLP, TrendMicro, ATM Security)
3. Maintenance & Administration of Azure AIP, MDATP, Defender, Bit locker, MS device control, Avecto (Beyond Trust)
4. Maintain and manage Antimalware console(s) (Deep Security Manager, Smart Protection servers, TrendMicro Control Manager)
5. Perform upgrade(s), Apply Hotfix for above solutions
6. L2/L3 support to internal Team for issues related to above solutions.
7. Implement configuration changes related to Endpoint Security including above mentioned technologies.
8. Manage and maintain High Availability of implemented endpoint security solutions across the Data Centers
9. Provide 24/7 on-call support for Command Centre /Security Monitoring and initiate response in case of any Security Incident.
10. Engineer, implement and monitor security measures for the protection of endpoints, such as endpoint Anti-Virus, Host IPS, Hard Disk encryption tools, Endpoint Privilege Management & troubleshoot technical issues related to it
11. Managing admin access on endpoints through Avecto with only restricted access as per requirement.
12. Engineer, implement, manage and monitor Antimalware solution for Servers running Windows and Linux OS across physical and Virtual machines
13. Implement and manage DLP solutions & provide technical support on end-point and network DLP platforms
14. Maintain compliance level of endpoints and monitor controls
15. Ensure that DLP system is efficiently integrated with data classification and SIEM solutions for better visibility and control over data leakage
16. Maintain and manage ATM security Management tools (iSuite, McAfee ePO, HDE console)
17. Maintain and manage Cloud Security Tools such as Intune, AIP, CASB, EDR
18. Managing Email Gateway related BAU including releasing analyzing and troubleshooting incoming email issues. Blacklisting/Whitelisting email domains/ID's based on SOC recommendations.

1.6 IOP (Network & Sys Admin)

IOP (Network & Sys Admin) shall be responsible for:

1. Administration of Storage & Backup, Virtualization, server hardware.
2. Administration & Management of Microsoft Exchange, RightFax and Active Directory
3. Network Management, Administration, Maintenance & Support for network devices and data links
4. Managing voice network including PRIs, voice gateways, unified communication, video and call recording

1.7 ITSO (IT Security Operations)

1. IT Security Operations manages day to day operations of Network Security, Managed File Transfer, IDAM, and IT Access Tools management (IT Security Admin) units.
2. Implement security device configuration changes
3. Manage and maintain High Availability of implemented security solutions across the Data Centers

4. Provide 24/7 on-call support for Command Centre /Security Monitoring and initiate response in case of any Security Incident.
5. Perimeter/Core security: Providing administration/consultation on high end firewalls – Perimeter, VPN, Core and DMZ hosted across multiple Data centers and International Branches.
6. Secure DNS: Administration of DNS security for ADIB publicly hosted records
7. Intrusion prevention: Network IPS management for inline prevention of intrusion. AV solutions in tandem with email/web security appliances.
8. Sandboxing: Administration of Malware Analysis / Sandboxing services for unknown threats integrated with Email and NIPS
9. ADIB Email security: Securing ADIB's inbound/outbound Emails undergoing multiple checks for known and unknown threats
10. User Internet Access security: Web and Content Administration of Internet gateway for secure access to users Internet access inclusive of DLP, CAS and SSL offload integrations
11. Perimeter Threat Protection: Configure Perimeter devices to protect from Targeted DOS/DDOS attacks
12. Maintain High Availability, Manage & troubleshoot two factor authentication servers used for VPN users, ADIB Securities and ADIB Direct.
13. Maintain and manage SIEM and SOAR solution and other monitoring tools.
14. Maintain and manage Cloud Security Tools.
15. Managing and administration of IAM, PAM Applications and tools.
16. Administer, manage & troubleshoot legacy Identity Management System (IDM)