ADIB –Procedures

Security Log Management Procedure
PRC-ITD-536

Date: 30th January 2024
Version: 5.1

Version Control & Change Management

Version	Issue Date	Details of Change	Reason for change
5.1	30th January,2024	No change required	Annual Review
5.0	December, 2022	Annual review	Incorporate GISD requirement
4.0	January, 2022	Added cloud related controls	Cloud adoption
3.0	July, 2021	NTP Service Administration has been handed over to IT SecOps team	Align with current organization structure
2.1	Publishing Date	Annual Review, no change required.	Reviewed as per annual cycle.
2.0	Publishing Date	Modified responsibilities for "Audit Loggings" Modified KPIs	Alignment with best practices
1.0	Publishing Date	New document	NESA Compliance Requirement

Prepared by	Approved by	Reviewed by
Governance Team	Head of IT Compliance and Security Architecture	IT Governance Manager ArcSight Consultant GISD

Contents

1. Purpose & Scope

The objective of this document is to establish a practice in developing, implementing, and effectively maintaining log management practices across ADIB IT environment. This procedure is applicable to UAE, Qatar, Iraq, UK & Sudan ITD environment

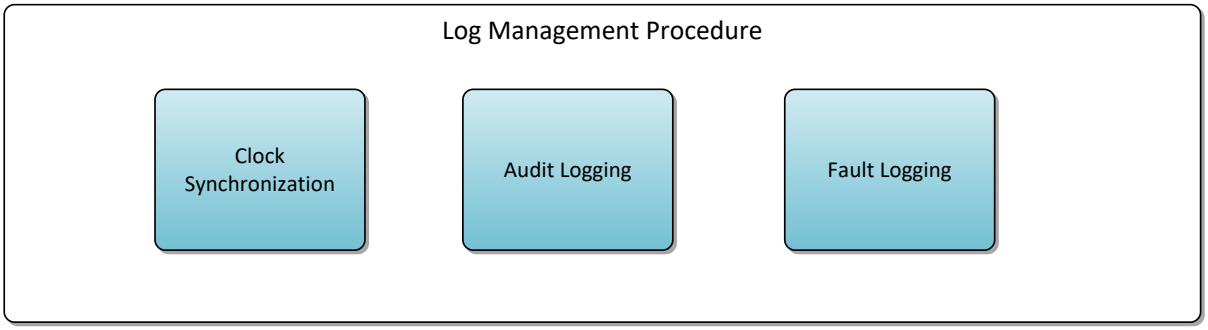
2. Process Owner

Head of IT Compliance and Security Architecture

3. RACI Matrix

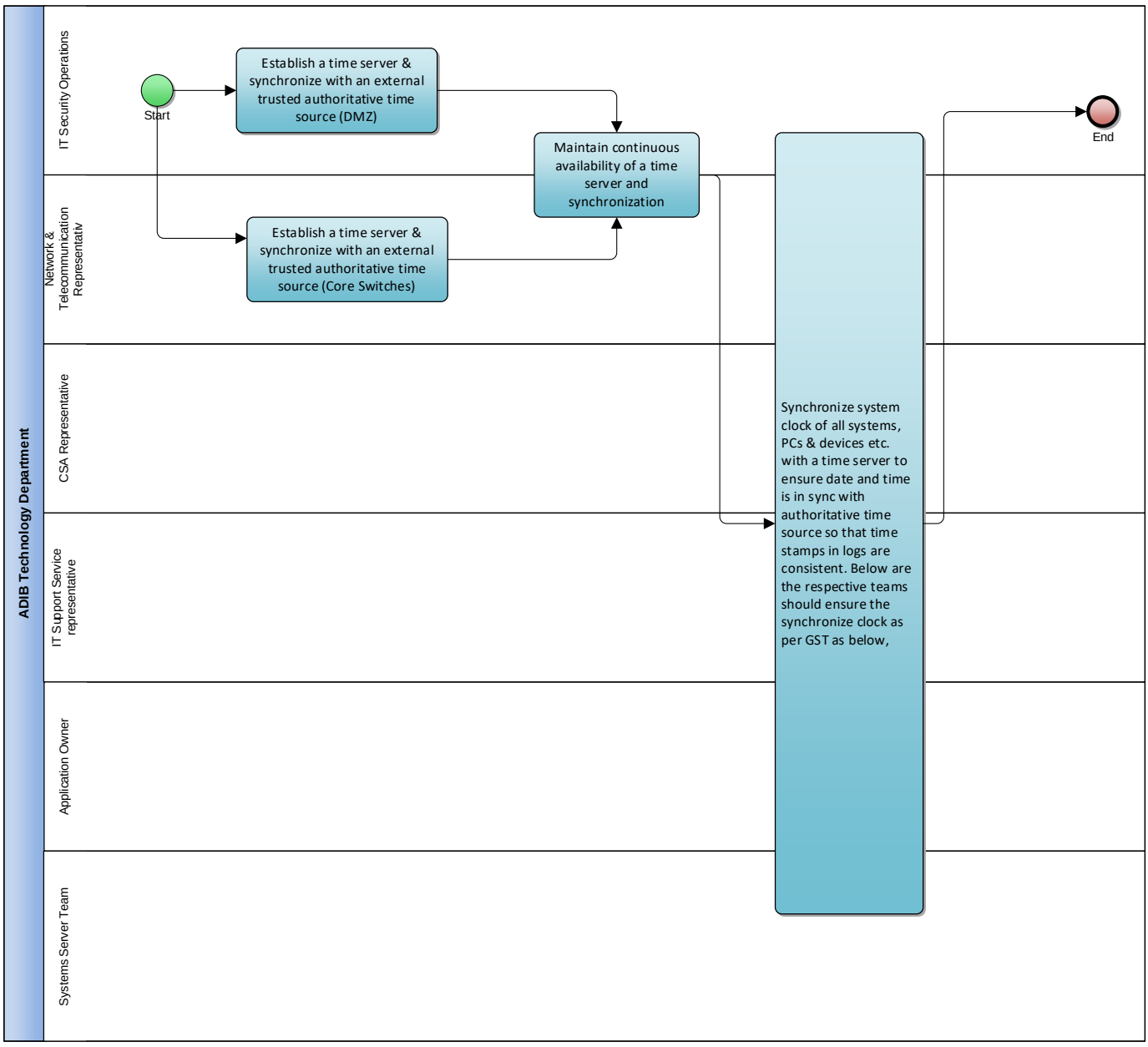
Roles / Activity	Network Team	Systems Team	IT SecOps Team	User Support	SIEM Admin (IT CSA)	IT CSA	GISD	IT Application Owner	Business Owner	CCoE
Clock Synchronization	R	R	A	R	I	C	I	I	I	C
Audit Logging	R	R	R	I	R	C	R	A	C	C
Fault Logging	I	I	I	I	I	I	R	A	C	C

4. Log Management – High Level Process Diagram



5. Detailed Process Description and Workflows

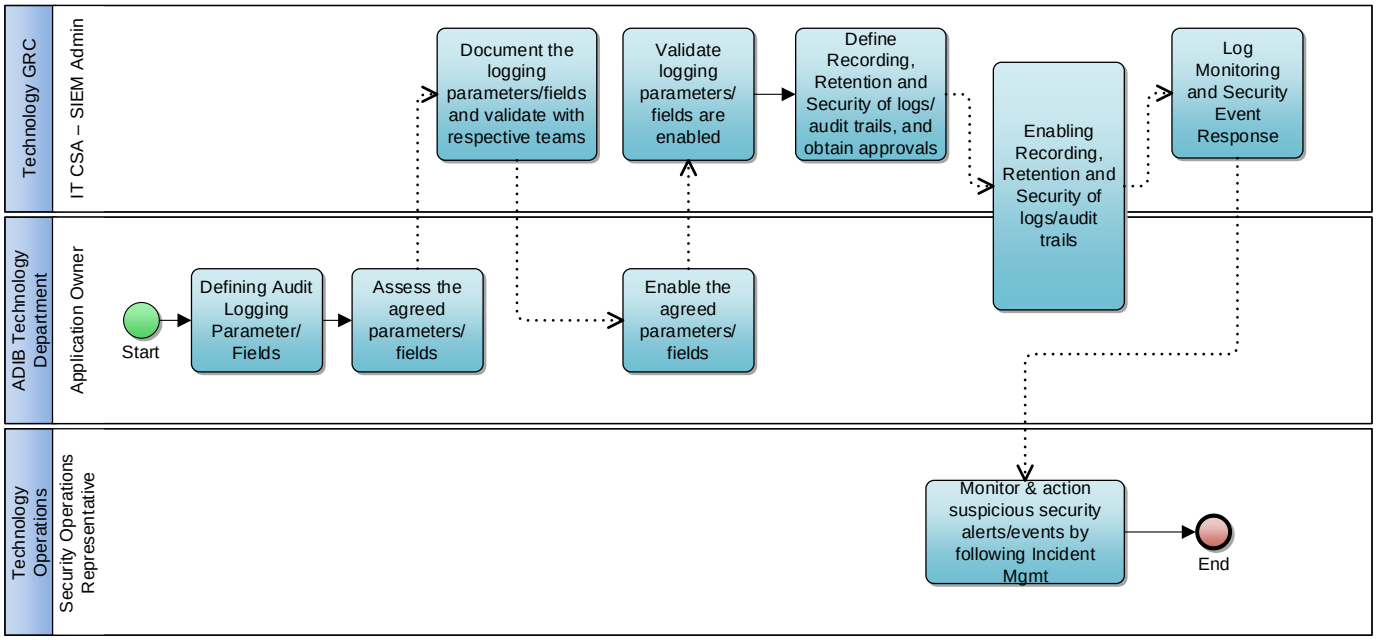
5.1.1 Clock Synchronization



Sr. No.	Activity	Responsible	Document (STD, Procedure, WI, Checklist, Forms) / Records / Tools
1	Establish a time server (NTP server) and synchronize with an external trusted authoritative time source as per Gulf Standard Time (GST).	IT SecOPs (DMZ) Network Team (Core Switches)	Central NTP Server

	Ensure stratum level of the time source should not be above level 2 or 3.		
2	Maintain continuous availability of a time server and synchronization with external authoritative time source.	IT SecOps (DMZ) Network Team (Core Switches)	Central NTP Server
3	Synchronize system clock of all systems, PCs & devices etc. with a time server to ensure date and time is in sync with authoritative time source so that time stamps in logs are consistent. Below are the respective teams should ensure the synchronize clock as per GST as below, IT SecOps – Ensure Security devices and Services ITD Network – Network devices and Services Systems team – Servers and Storage User Support – Desktop, Laptops and VDI IT Application owners – Applications services	IT CSA (Compliance & Monitoring Devices) IT SecOps (Security Devices) ITD Network (Network Devices) Systems Team (Servers) User Support (Desktops & Laptops) IT Application Owners (Applications)	IT Tool (Monitoring Devices)

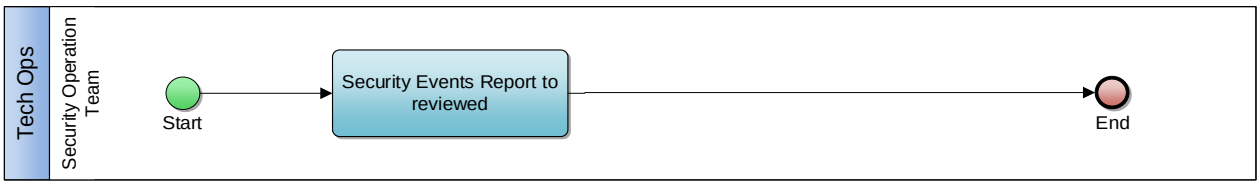
5.2 Audit Logging



Sr. No.	Activity	Responsible	Document (STD, Procedure, WI, Checklist, Forms) / Records / Tools
Defining Audit Logging Parameter/Fields			
1	Define parameters for audit logging, refer: **Appendix / Annexure reference section** for security & IT Infrastructure devices as identified in Security Log Management Standard	Application Owner (Security logs)	STD-ITD-562 Security Log Management Standard
2	Assess the logging parameters/fields as defined in **Appendix / Annexure reference section** which can be enabled for logging for the assets and identify exceptions Identify additional parameters/fields if any that are required to be captured as part of audit log/audit trail	Application Owner (Security logs)	SIEM Tool
3	Document the "logging parameters/fields" including exceptions (if any) and validate it with Head of IT CSA and respective IT System / Application Owner	SIEM Admin (IT CSA)	SIEM Tool
Enabling Audit Logging			
1	Enable logging parameters/fields as per the agreed parameters/fields	Application Owner (IT CSA)	SIEM Tool
2	Validate logging parameters/fields are enabled in accordance with agreed parameters/fields on on-prem and Cloud	ITD (Network/SecOps/System/Application owner/CSA/GISD	SIEM Tool
Defining Recording, Retention and Security requirements of logs/audit trails			
1	As per business, regulatory, and legal requirements integrate the security logs and define the recording, retention, and security requirements of logs/audit tails • Log retention period • Online storage and overwritten period of audit logs/trails • Backup schedule and purging schedule based on online storage and retention period • Access control requirement to restrict access to read only and to authorized personnel only	SIEM Admin (IT CSA)	SIEM Tool
2	Document the "recording, retention and security requirements"; In case of exceptions, approval shall be obtained from Head of CSA and respective IT / Business Owner.	SIEM Admin (IT CSA)	SIEM Tool
Enabling Recording, Retention and Security of logs/audit trails			
1	At Target IT Assets: • Implement/configure log retention period, online storage/ overwritten period of logs, backup & purging schedule, and access restrictions as per agreed recording, retention, and security requirements.	Application Owner (IT CSA)	SIEM Tool

2	At centralized logging facility: • Implement/configure log retention period, online storage/ overwritten period of logs, backup & purging schedule, and access restrictions as agreed recording, retention, and security requirements. • Record audit logs to a centralized facility in a standard format or normalize the logs to convert the logs in standard format • For International Operations of ADIB Ensure logs are aggregated to central log system of each country and synchronized to Central Log server in UAE through secure VPN connection, as per defined schedules. • Ensure encryption while log data is being stored and being transmitted over external network • Secure the backup in the backup media and storing it in a secure place as per ADIB backup standard • Ensure read only access to audit logs to authorized personnel	SIEM Admin (IT CSA)	SIEM Tool
3	Validate recording, retention and security requirements are configured in accordance with the approval and sign-off	SIEM Admin (IT CSA	SIEM Tool E-mail, IT Service Management Tool
Log Monitoring and Security Event Response			
1	Identify and document the suspicious security events to be monitored along with the respective IT Owner, Business Owner & IT CSA	SIEM Admin (IT CSA)	SIEM Tool
2	Define and enable security event monitoring rules & correlation rules to capture the required suspicious security events at central logging facility as per agreed security events requirements.	Security Operations Center Team (GISD-SOC)/SIEM Admin (IT CSA)	SIEM Tool
4	Conduct necessary testing to determine related audit logs are being captured and the related suspicious events are triggered.	SIEM Admin (IT CSA)	SIEM Tool
5	Follow STD-ITD-542 Incident Management Standard to monitor & action suspicious security alerts/events reported by central logging tool.	Security Operations Center Team (GISD-SOC)	SIEM Tool

5.3 Fault Logging



Sr. No.	Activity	Responsible	Document (STD, Procedure, WI, Checklist, Forms) / Records / Tools
1	Security Events reported by devices and systems on SIEM tool will be reviewed and appropriate	Security Operations Center Team (GISD-SOC)	SIEM Tool

	action taken as per STD-ITD-542 Incident Management Standard		

6. Key Performance Indicators (KPI)

Sr. No.	Key Performance Indicator	Target	Source	Reporting to	Frequency	Formula
1	Percentage of reported false positives optimized and reduced by SIEM Admin quarterly	>60%	SIEM Admin/SOC Team	Head of CSA	Quarterly	(Number of false positives optimized and reduced by SIEM Admin/ Total number of false positives identified and reported by Security Monitoring Team) *100
2	Percentage of critical assets integrated with SIEM tool	>90%	SIEM Admin	Head of CSA, SOC Manager	Quarterly	(Number of critical assets integrated with SIEM / Total Number of Critical ADIB IT Assets) *100

7. Risk and Controls

Risk	**Controls**	**Reference** (section number in the procedure)
Risk of non-compliance to regulatory and compliance requirements; in the event of inaccurate log files correlation between IT systems; due to absence of time server and synchronization between IT systems.	Time server is established and is synchronized with an external trusted authoritative time source as per Gulf Standard Time (GST) with stratum level 2 or 3.	6.1 Clock Synchronization
	Time server is ensured for continuous availability and synchronization with external authoritative time source.	6.1 Clock Synchronization
Risk of confidentiality loss and service unavailability; in the event of potential IT system compromise; due to absence of defining audit logging Parameters, enabling of audit logging, Enabling Recording, Retention and Security of	Audit logging parameters are defined for security & IT Infrastructure devices. Audit log/trails are enabled for all assets. - Windows production servers (Primary & DR)- Security - Unix production servers (Primary & DR)- Security/ Audit - Windows non-production (QA, QC, DEV) DMZ servers (Primary)- Security - Network Infrastructure devices (Primary & DR)- Audit/ System - Security Infrastructure Systems (Primary & DR)- Audit/ Traffic/ System - Firewalls (Primary & DR)- Audit/ Traffic/ System - End-Point Systems (HO)- Audit - Critical Applications (Customer Facing / 3 Party Vendor Applications) (Primary & DR)- and Audit Trials	6.2 Audit Logging

logs/audit trails, Log Monitoring and Security Event Response	Audit logs recording & retention of assets classified as HIGH & CRITICAL are documented along with exceptions (if any). These are reviewed and approved by Head of IT CSA and respective IT / Business Owner.	6.2 Audit Logging
	Audit logs are recorded to a centralized facility in a standard format. For ADIB International operations, logs are aggregated to central log system of each country and synchronized securely to Central Log server in UAE.	6.2 Audit Logging
	Security event monitoring rules are defined and enabled to capture the required suspicious security events at central logging facility. Testing is performed to determine related audit logs are being captured and the related suspicious events are triggered.	6.2 Audit Logging

8. Appendixes

8.1 Annex I: Audit Logging Parameters/Fields:

Following audit logging parameters/fields should be capture as part of audit logging:
For all assets: as identified, in STD-ITD-562 Security Log Management Standard.

- Date and time stamp for all activities captured in log files
- Unsuccessful/failed logon attempts
- Originator/User id (on all applicable systems)
- Authorizer id (only for business application)
- Source IP address, if applicable (on all applicable systems) Opening modifications or closing of customer accounts, if applicable (only for business application)

For Global and Privileged Administrator PIM IDs of all assets: as identified, in STD-ITD-562 Security Log Management Standard:

- Changes to, or failed attempts to change- logging setting, system configuration, system security settings.
- Access and modifications/deletions to audit logs
- Addition or modification or revocation of access rights to privilege IDs
- Password change of privilege IDs
- Modification or revocation of access rights to user profile

8.2 Annex II: References

Doc. Ref. No.	Name	Type of Document (Policy / Standard)
STD-ITD-562	Security Log Management Standard	Standard

8.3 Annex III: External References

1. https://cloudsecurityalliance.org/research/cloud-controls-matrix/
2. CIS Microsoft Azure Foundations Benchmark v1.0.0 Now Available (cisecurity.org)