ADIB – Standard

Security Log Management Standard
STD-ITD-562

Date: 20th January 2024
Version: 5.0

Version Control & Change Management

Version	Issue Date	Details of Change	Reason for change
5.0	January 2024	Updated log retention from 2 year to 3 years. Added cloud resources.	Align with current practice
4.0	January 2023	Updated log retention from 1 year to 2 years Added: only authorized staff shall maintain and review audit logs Added: Access/review request for any log file shall be approved by log owner	GISD requirement
3.0	January, 2022	Added cloud related controls	Cloud Adoption
2.0	Publishing Date	Added "Note: More detailed device category wise logs to be enabled is mentioned in 'Security Log Baseline Checklist'.	Assist the respective support teams to perform the tasks related to security log management
1.2	Publishing Date	Annual Review, no change required.	Reviewed as per annual cycle.
1.1	Publishing Date	No change required	Ensure document effectiveness
1.0	Publishing Date	New document	NESA Compliance Requirement

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

Document Contents

1 Overview

The objective of this standard is to monitor and log various events associated with the access of banks information resource, IT systems and facilities at all sites (including Cloud System's). To provision a mechanism, on retrieving and reporting information on logged events and to measure the effectiveness and compliance with various bank policies and standards.

2 Applicability

This standard is applicable to ADIB ITD environment.

3 Standard Owner

Head of Technology GRC

4 Standard Statements

4.1 General Guidelines on Security Log Management:

1. All the endpoints, servers, network devices shall be synchronized to the centralized internal time server.
2. Logs as mentioned in the table below shall be diverted and stored securely at a centralized location for monitoring and correlation. Appropriate technologies shall be adopted while storing the logs. Logs shall be retained for an agreed time period.

System	Environment (On-premises/Cloud)	Log Types Collected
Windows Production Servers	Primary & DR	Security
Unix Production Servers	Primary & DR	System / Audit
Windows non-production DMZ Servers	Primary (QA/QC/DEV)	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	Primary & DR	Audit
Cloud Resources	Primary & DR	Azure Activity Logs / Azure Diagnostics Logs / Azure Security Alerts
Critical Applications (Customer Facing / 3 Party Vendor Applications)	Primary & DR	Audit Trials

Note: More detailed device category wise logs to be enabled is mentioned in 'CL-ITD-551 - Security Log Baseline Checklist Document'.

3. Automation of audit trails for all system components to reconstruct enlisted events shall be implemented:
    a. Activities of users, root, or administrative privileges
    b. Access to all audit trails
    c. Invalid logical access attempts
    d. Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges
    e. Initialization, stopping, or pausing of the audit logs
    f. Creation and deletion of system-level objects

~~4.~~ Logging shall not record sensitive information (such as passwords) which would present a substantial risk if accessed by unauthorized parties.

5. Access to sensitive logs need to be managed by automated system like IDAM/PAM.
6. Access/review requests for any log files need to be approved by the log owner. Log owner is the application or database owner as the log will contain data from the application or database. Same apply for IT devices and systems.
7. When allocating the responsibility for log review, a separation of roles shall be implemented between the individual(s) undertaking the review and those whose activities are being monitored or reviewed. A list of authorized staff to review the logs shall be developed, maintained, approved by management, and regularly updated.
8. Auditing shall be enabled on all IT-Infrastructure Assets as listed in point 2 for recording exception and other security-related events.
9. Audit trail history for at least three years shall be retained or as per the guidelines set by the regulatory body, with a minimum of three months immediately available for analysis
10. The audit log at a minimum shall record the details regarding user account name, date, time, and Origination of event, success/failure indication, device name, device IP address,
11. Audit logs shall be protected from unauthorized access and only authorized administrator / auditor shall have access to the logs.
12. Audit trails shall be secured so that they cannot be altered by ensuring following measures:
    a. Access to audit trails to on need basis and limiting to the required log information's only.
    b. Protect audit trail files from unauthorized modifications.
    c. Promptly back up audit trail files to a centralized log server or media that is difficult to alter. Backed-up audit log files shall have the same or more but not less than security controls applied to the original audit logs. -
    d. Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.
13. Audit logs shall be backed up regularly as per backup policy and standards
14. Audit log shall be real-time analyzed by GISD SOC for security incidents, policy violation, fraudulent activity and reports shall be prepared based on the stakeholder requirement.
15. Access to system audit tools, i.e., software or data files, shall be protected to prevent any possible misuse or compromise. Such tools shall be separated from the development and production systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection.
16. All bank systems and network devices shall be monitored to ascertain security of the information assets and systems-and detect any malicious activities.
17. At minimum following reviews shall be conducted:
    a. All security events shall be analyzed real-time.
    b. Logs of all system components that store, process, and/or Sensitive Authentication Data - daily basis.

c. Logs of all critical system components - daily basis.
d. Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.) - daily basis.
e. Review logs of all other system components periodically based on the bank's policies and risk management strategy, as determined by the organization's annual risk assessment.
f. Follow up exceptions and anomalies identified during the review process.

18. Events shall be categorized based on the severity and shall be reported appropriately based on the stakeholder requirement.
19. Incident management process shall be followed when an incident is detected while monitoring.
20. Result of the monitoring activities shall be reviewed (regularly) for exceptions. The frequency of the review shall be based on the risks involved.

4.2 Cloud systems Logging and Monitoring

1. Configure logging and monitoring solutions in the cloud services.
2. Configure the information system, protects audit records from unauthorized access, modification, deletion, and retention of audit logs with right RBAC in place.
3. Implement monitoring solution in security audit logs to detect activity outside of typical or expected patterns. Establish cloud services to review and take appropriate and timely actions on detected anomalies.
4. Implement a reliable time source across all relevant information processing systems to ensure clock synchronization.
5. Implement logging scope which information meta/data system events should be logged.
6. Configure the cloud services to generate audit records containing relevant security information about the username, email, and system IPs.
7. Configure audit logging for key vault and key usages for all the systems, services, and Cloud API accesses to ensure transaction/activity logging
8. Establish an agreement with cloud service provider that we receive report for access control logs to ensure auditable access control system in place.
9. Implement cloud solution for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.

5 Appendixes

5.1 Annex I: Internal References

Doc. Ref. No.	Name	Type of Document (Policy / Standard)
PRC-ITD-536	Security Log Management Procedure.	Procedure
CL-ITD-551	Security Log Baseline Checklist	Checklist