ADIB – Standard

Database Security Standard

STD-ITD-553

Date: 30th January 2024

Version: 6.2

Version Control & Change Management

Version	Issue Date	Details of Change	Reason for change
6.2	January, 2024	Document reviewed no change required	Full review
6.1	June 2023	Annual Review NO Change	Annual Review
6.0	June 2022	Removed below examples from document e.g. Database administrators with access to development and SIT database should not have privileges to administer UAT or production databases. Similarly, database administrators responsible to administer UAT and production database should not have privilege to administer development and SIT database.	To align with current TechOps structure.
5.0	January, 2022	- Updated document to ensure adequate Database security controls are up to date.	Process annual review
4.0	Publishing Date	- Added cloud base database solutions must be approved by DRB - Added Database Authentication related controls - Added Database Activity Monitoring	Align with best practices of Database security
3.0	Publishing Date	Process Optimization	Naming convention for database users
2.0	Publishing Date	GARR points addressed	Creation Streamlining of complete Standard
1.2	Publishing Date	Streamlining of complete Standard	Process Optimization

Prepared by	Approved by	Reviewed by
Governance Team	Head of IT Compliance and Security Architecture Head of Technology GRC	IT Security Engineer, Applications IT Governance Manager

Contents

1 Overview

The purpose of this standard is to ensure adequate security controls are defined, developed, and implemented to secure acquisition, maintenance, and operation of databases at ADIB ITD.

2 Applicability

This standard is applicable to ADIB ITD.

3 Process Owner

Head of Technology GRC

4 Data Base Security

4.1 Installation and Configuration

1. During installations or on-cloud implementations, databases should be configured with secure baseline of the configurations and best practices features necessary for performing business operations.
2. The database must be installed on non-default ports.
3. All databases should be configured as per the respective database security checklist. All non-relational database implementation must be approved by Enterprise Architecture team to follow technology stack of ADIB.
4. All cloud base database solutions must be reviewed and approved by Design Review Committee (DRB).
5. The default database user accounts and passwords which are not required for normal operations should be disabled.
6. If a default user account is required on the database, necessary approvals from the Head T&Cs/Designate and the IT GRC Head/ Designate should be obtained. Records of all such exceptions should be maintained by the database administrators.
7. Remote connection to the database server should be through secure channels.
8. Applications as mentioned below shall connect to their respective databases (i.e. the connection strings) in a secure manner such as use HTTPS/SSL/TLS for establishing connections. If using ODBC, the connection parameters should be stored in a way so that they are not accessible for reading:
   - Application databases hosted on the cloud
   - On-premises applications falling under the ADIB PCI scope

4.2 Network Placement of Database

1. All critical databases should be placed in dedicated network segments, secured by a firewall and strong network access lists in network devices.
2. There should be no direct communication between the web server and database server. Web server should communicate with an intermediate application server which in turn should communicate with the database server.
3. The critical application and the database server should be hosted on separate physical servers.
4. Critical databases should have fault tolerance, high availability, and scalability.

4.3 File System Security

1. Sensitive database files should be protected against unauthorized access by configuring appropriate OS level permissions on these files. Such files include home directories of the database system, secure settings of registry keys etc.

4.4 Database Authentication

1. User ids which give an indication of the privilege level of the user, or which can be easily guessed should not be used. For instance, user ids such as administrator, DBA, supervisor etc. should be discouraged.
2. Database user IDs or passwords should not be hard coded in clear text into application source code.
3. The database passwords should be configured to adhere to the Password Standard.
4. Individual user account must be under PAM control with must be granted by authorized PAM approvers.
5. All individual access to databases must be related to with change request or incident ticket through the PAM.

4.5 Database Account

1. All user accounts and privilege management for the databases should be done in accordance with the User Access Management Procedure.
2. There should be a standard naming convention followed for administrator and user accounts created on the database.
3. Application user account should have access to required database objects only.
4. User accounts used for database access should be reviewed and approved by the IT System Owner:

   a. Applications should not use built-in or generic account IDs for database access.
   b. Applications which can use dedicated database user IDs for every user should ensure access rights to the database are provided on a need to know basis.

4.6 Database Naming Convention

1. All new databases should follow a standard naming convention for easy identification. The database names should not give a direct indication to the type and version of database used
2. For Database user account (individual);

   - create the id following ‘ Staff id’

3. For Service user accounts:

   - create the id following ‘ Application name’
   - For multiple service accounts for similar application shall be distinguished by ‘App name1’ & ‘App name 2’

4.7 Data Integrity

1. The databases should ensure integrity of the data in concurrent user mode.
2. Referential integrity of data should be maintained in database design and should include cascading update and cascading delete, to ensure that changes made to the linked table are reflected in the primary table.

4.8 Storage and Replication

1. All database tables containing customer and other personal information should be stored in a secure format.
2. Production database servers should not be used in UAT, SIT and development for testing purposes.
3. If UAT environment requires production data, such data should be masked or scrammed adequately to avoid any misuse.
4. All databases supporting critical applications should have adequate data replication arrangement to a secondary site.

4.9 Data Transmission

1. Data transferred for database replication between multiple sites should be secured using encrypted channels.

4.10 Database Administration

1. All database administrators and users should have a unique user-id to authenticate to the database server.
2. There should be proper segregation of duty for database administrator in terms of different levels of access Patches
3. The database server should be regularly updated with latest security patches and hot fixes for the operating system and database files.
4. The patch management team is responsible for tracking newly released patches and ensuring installation of these patches after sufficient testing as per the Patch Management standard

4.11 Backup

1. IT System Owners should ensure the backup and retention periods defined for the databases are in line with the Backup Procedure.
2. IT System Owner should define the backup and retention period for all data stored in database server

- The backup and retention periods should consider relevant statutory and regulatory requirements.

4.12 Logging and Monitoring

1. The database should have the facility to log all critical activities to provide audit trail and help tracking malicious users and their activities in the event of a fraud. Dedicated logging devices could be used for logging purposes to decrease the load on the Database server.
2. Database should be able to log all security related events including the following

   - User account management
   - User Privilege changes
   - User login/logout time
   - Authentication failures
   - Changes in database configuration
3. All critical logs from the database server should be moved to a central storage on a real time basis. Controls should be implemented to secure logs maintained in a central storage to avoid unauthorized access by the database administrators
4. Appropriate logs should be monitored and reviewed on a periodic basis.
5. Proper reporting mechanism should be implemented to generate reports from the logs. Access to logs and reports should be restricted on need to know basis.

4.13 Change Management

1. All changes to the database should be assessed, approved, implemented, and reviewed in accordance with the Change Management Standard.

   - All changes to the database should be tested before deployment.
   - Any deviations from the original plan should be documented.
2. The test data should be adequately protected from unauthorized access.
3. Requirements and criteria for acceptance of new database or upgrades should be defined, agreed, documented, and tested.

4.14 Database Activity Monitoring

The monitoring strategy is following below requirements:

- PCI Compliance Policy/Rules/Reports to monitor PCI Servers
- Whitelist the Service accounts that are originating from the authorized application client IP address
- Capture/Monitor the traffic initiating from Database Administrator and a normal DB user accessing the database.

Sensitive Object Access

- Access to the sensitive objects by Database Administrator and a normal DB user by approved or unapproved source programs.
- Bulk changes using DML, DDL on sensitive objects of the database.
- Access to sensitive objects by users other than privilege users and application schema users
- Access to sensitive objects by application schema users not originating from Application client IP addresses.
- Enabling and accessing to the database using any default DB users should be restricted.

Category	Area	Alert Severity	Requirement Description
Sensitive Objects	Privilege User	High	Privilege User Access to Card Tables/Sensitive Tables (Card Data, Password, and any Salary etc.) via interactive login. Privilege user across Sybase, MSSQL & Oracle. Approved channels include, TOAD, SQL Developer, SQL Plus, MSSQL MGMT Studio, DBisql, DBArtisan.
	Privilege User	High	Privilege User Access to Card Tables/Sensitive Tables (Card Data, Password, and any Salary etc.) via unauthorized channels (Source Programs)
	Privilege User	High	Large SELECT, UPDATE, INSERT, DELETE(DML) queries on the Card Holder object by Database Administrators or normal DB users.
	Privilege User	High	Access to sensitive/card database tables by application schema user NOT originating from application servers.
	Privilege User	High	Access to sensitive/card database tables by ANY user other than privilege user or application users.

Schema Modifications

- Access to Administrative Objects such syslogins, sys_database, Dba_role_privilage etc
- Execution of commands such as ALTER DATABASE, ALTER SYSTEM etc.
- Execution of Account management commands such as CREATE LOGIN, ALTER LOGIN etc.

Category	Area	Alert Severity	Requirement Description
Database Modifications	Administrative Objects	Medium	Access to administrative objects (dba_privileges, Dba_role_privilage, syslogins, sp_grant etc.)
	System Schema	Medium	Access or modification to database schema such as ALTER TABLE, ALTER SYSTEM etc. by ANY user.
	User Schema	Medium	Running account management commands such as ALTER LOGIN, ALTER USER, CREATE LOGIN etc., by ANY user.

General

- This category of rules tracks execution of high privilege commands run by any user.

Category	Area	Alert Severity	Requirement Description
General	DDL Commands	Medium	Execution any DDL commands by ANY user.
	DCL Commands	Medium	Access or modification to database schema such as ALTER TABLE, ALTER SYSTEM etc. by ANY user.

4.15 Documentation

1. IT System Owner should ensure that detailed documentation is available for the following:
   - Database Installation
   - Configuration Settings
   - Back up & recovery procedure
   - Database security checklist
2. Security baseline documents should be developed and maintained by the IT GRC team for all databases deployed in ADIB ITD. All relevant security settings for database should be documented in these security baseline documents.
3. Security baseline document should be tested before applying it on the database servers.
4. Security settings which cannot be configured as per the security baseline document should be communicated to the respective department head & the IT GRC team. The IT GRC team should review the setting and provide suggestions on alternative technical controls, as may be available.

5 Exception

Any exceptions or exclusion to this Standard requires permission from the Standard Owner.
Any non-compliance to this Standard shall be considered for corrective actions and corresponding corrective action / exception has to be maintained by the Standard owner.

6 Appendixes

Annex I: Acronyms

Abbreviation	Acronym
ADIB	Abu Dhabi Islamic Bank
ITD	Information Technology Division
ITSM	IT Service Manager Tool
KPI	Key Performance Indicators
UAT	User Acceptance Test
SIT	System Integration Test
RAID	Redundant array of independent disks

Annex II: Glossary

Term	Definition
System Owner / Asset Owner	System Owner / Asset Owner is the individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the database and ensures the technical requirements of the applications are aligned to the defined business requirements. By default, respective department head shall be the system/ asset owner unless explicitly identified.
UAT- User Acceptance Test	Process to obtain confirmation from the System Owner of the application through trial and review so that modification or addition of components to the system meets all mutually agreed business requirement.
System Integration Test	Process of testing interaction between multiple modules of the application so that modification or addition of components to the individual module meets all the mutually agreed technical requirements.
Source code	Source code is any collection of statements written in human-readable computer programming language to communicate with the computer, which when converted into an executable file by a compiler, or executed on the fly by an interpreter, performs the desired functions
Need to Know	“Need to Know” refers to one’s access rights to information assets based upon one’s official roles and responsibilities.
Least Privilege	Least Privilege refers to minimum access privileges that a user needs to have by default on an information or information processing facility to conduct their day to day activities in the organization.
RAID	Redundant array of independent disks (RAID) is a technology that results in high level of storage reliability by dividing and replicating data among multiple hard disk drives.
Schema	The schema of a database system is its structure described in a formal language supported by the database management system (DBMS). In a relational database, the schema defines the tables, the fields in each table, and the relationships between fields and tables. Schemas are generally stored in a data dictionary. Although a schema is defined in text database language, the term is often used to refer to a graphical depiction of the database structure.