ADIB – Standard

Application Security Standard
STD-ITD-502

Date: 30th January 2024

Version: 10.0

Version Control & Change Management

Version	Issue Date	Details of Change	Reason for change
10.0	January 2024	Updated Symmetric encryption standard and added security testing control.	Annual review
9.0	January 2023	Added: TLS v1.2 must be used with strong cipher suite only	As per approved Network and Transport Layer Protocols
8.0	January 2022	Controls for protection against open source known vulnerabilities has been added Control has been added for native cloud applications.	Annual review
7.0	Software Escrow Criteria	Added Criteria: Software escrow agreements	CB requirement
6.0	Publishing Date	Added Control: The captcha shall add be added to public websites which has web form with input fields	to mitigate brute force attack
5.0	Publishing Date	Added controls: - Soft token, hard token or risk-based authentication should be preferred. - Industrial standards should be followed in all API implementations	Enhancements
4.0	Publishing Date	Updated encryption standard	Updated to ensure it is in line with the current process and updated in current template
3.0		Added Controls for Mobile application	Document review
2.0		Application Standard 1) Additional controls for "Mobile" applications security controls 2) Includes mobile application signing control – to be done on ADIB controlled environment	Final Version
1.3		Addition of "mobile applications" guidelines Formatting changes. References updated to ITD Policy and Security Policy	Input from process owner and department head
1.0	20/03/2017	Creation	Creation

Prepared by	Approved by	Reviewed by
IT GRM	IT Security Engineer, Applications Head of Technology GRC	IT Governance Manager

Document Contents

1 Overview

The objective of this document is to define specifications for Information security and Quality related controls of an application system to encourage pro-active approach in application development.

2 Applicability

This standard is applicable to ADIB UAE, and international ITD application systems managed from UAE.

3 Standard Owner

Head of Technology GRC

4 Standard Statements

4.1 Controls to be Incorporated

Each Application/System shall be classified for type {such as Client Server; Web application (n – tier) [accessed internally or externally]; Workflow Application; Other}. It shall be rated for criticality level as per the following:

Criticality	Criteria
High	Financial impact and/or compliance impact and/or customer impact at the front desk
Medium	Customer impact at other location than front desk
Low	Impact only on internal ADIB activities

4.1.1 General Application controls

1. Authenticated access to external entities (such as: databases, INI files, APIs, system folders, system services, Others)
2. Encryption standard shall be deployed for code, database communication, data, password, configuration information and inter module communication with minimum strength of 128 bit.
3. Method of system license/ copy protection shall not restrict use of a particular operating system, or perpetual use of hardware peripherals (such as dongle, media, etc.)
4. Authorization based on roles/groups (such as user, manager, supervisor, system administrator, groups, maintenance accounts, etc.) shall be enabled
5. Data input and output validation controls shall be applied to avoid any code injection such as SQL injection, XSS, HTML, CSS injections. Input filtering shall be applied on server-side as an input-filtering method for each http request
6. Errors/ system messages screen displays shall not disclose any information related to the installed packages, OS, Database and/or security setup.
7. Auditing mechanism deployed shall have tamper proof, continuous logging systems (one for the normal users' activities (client side), and another for administration activities). The logs shall be available in "Read Only" mode only to authorized user(s). It shall have the facility to search/ filter/ arrange/ export/ view or print audit information and log reports (such as Security Matrix, User Activity Log, Administrator Activity Log, etc.).
8. Shall have the capability to synchronize with the central time server (for Server based systems).
9. Shall have configurable user authentication measures {Capability to support single-sign on or, configurable password management [including but not limited to enforcement for length (blank not allowed, configured minimum character length for user name and password), combination, complexity, age, history, expiry reminder, lock up, changing default password, etc.], secure method of storing password data, etc.}.
10. User list shall be synchronized with the ADIB Active Directory so that configurable user access control measures such as capability to restrict user profiles to use specified workstations, within a given time range, deactivate user if inactive/ dormant for predefined period, display details of last successful login, intelligent

prompting such as 'either username or password incorrect!' at time of user login, mechanism to segregate client from the backend, etc.} can be used

11. Controlled (logged and monitored) secure access (if available) for vendors (onsite and off-site) shall be applied
12. Application shall be reviewed for system interdependencies (including dependencies like Proxy server connectivity, market connectivity and central bank connectivity) and connectivity (within system components and with other systems)
13. High level hardware connectivity / Component Flow Diagram (CFD) /Data Flow Diagram (DFD) highlighting the paths and storage of data, for all scenarios (Please review appendices A and B for sample of CFD and DFD) shall be maintained
14. Implementation Specification shall include all environment related details like scheduled jobs, Web Services, configuration, down times, difference reports, data, Impact of code and configuration changes for the existing systems.
15. All the project related documentation like SMR, Risk Acceptance Form (If exists), Impact Analysis, FS & IS, difference report shall be included in the implementation package as a soft copy while submitting the system/application for testing and deployment
16. Security configuration parameters shall be defined, and implementation guidance shall be maintained to ensure integration of proposed system within existing setup. It shall include details of system controls to ensure that they do not compromise working of other existing systems. It is recommended that system uses dedicated environment, but if shared environment is proposed, complete details/ description of components shall be provided as per standard templates.
17. All the services, APIs for the system shall be started automatically and no manual actions shall be allowed
18. All access to any external folder/resource shall be monitored and controlled
19. All the system parameter changes, and configuration change shall be done through an interface
20. Each application shall have Back up, roll back and Recovery Plan for the latest version of Application/system to be deployed
21. All the test data shall be cleaned from the database and applicable folders, configuration files and mosaic CDS before implementation in the productions
22. Every new system/application shall have the step-by-step user manual for better understanding and navigation of the system.
23. Client server interaction between the servers shall be thoroughly tested through simulation before system is handed over for testing.
24. All custom application code changes shall be reviewed, and code review record shall be maintained.
25. Hard coded encryption keys or storage of other secrets in the code base shall be avoided. HSM shall be used for storing encryption keys instead of hard coded storing in code base.
26. Critical business controls and calculations shall not be implemented on front end in client-side scripts.
27. All critical business controls to use in accounting such as exchange rate, anything used for calculation, account number, credit card number in front end must be re-validated to back end.
28. 2FA authentication must be implemented all payment systems and internet facing systems. Soft token, hard token or risk-based authentication should be preferred instead of using SMS OTP.
29. Industrial standards should be followed in all API implementations. In authentication, the oauth2.0 should be applied. Instead of flat file, all application logs and user activities should be logged on database.
30. The captcha shall add be added to public websites which has web form with input fields to mitigate brute force attack (wherever applicable).
31. Open-source components used in application must be free of vulnerabilities.
32. Native cloud applications must be complaint with container security standards.
33. Prior to deployment, going live, and engaging in the DRB process, all new business applications, or enhancements, encompassing additions, integrations, or modifications, must receive security testing clearance from the application security testing team through part of DRB process.

4.1.2 Additional controls for “Mobile” applications

The Bank mobile application shall:

1. Not store sensitive data in easily reachable devices such as memory card.
2. Not leak data through channels such as the application cache, logs, temporary directories etc. wherein the data is usually retained indefinitely.
3. Demonstrate, through testing, that it is not vulnerable to popular server-side attacks.
4. Demonstrate that it defends itself against the threats specified in a Threat Profile that has been developed specifically for the mobile application.
5. Not send sensitive data to external sites through tokens, the referrer etc.
6. Not share any data to any other application, other than those certified by ADIB with a secured authentication method. Any changes should require re-certification.
7. Implement mobile Operating System related features securely, without introducing vulnerabilities.
8. Re-authenticate the user before allowing the user to perform an operation involving sensitive data.
9. Ensure that non-trusted input is validated before it is used by any device resource.
10. Be protected against vulnerabilities that are directly exploitable throughout the mobile banking application, in the case of back-end services which mobile applications connect to in order to send and receive data.
11. If required, use back-end server which shall be updated and protected against known vulnerabilities.
12. Take adequate measures to protect sensitive data from being stolen over the network.
13. Not hardcode secrets like the passwords or encryption keys in the application itself. There shall be no sensitive data in the source code. Encryption keys or other secrets shall only be stored in HSM.
14. Ensure that customer is able to transact only from device registered with ADIB or other devices with such strong authentication methods.
15. Ensure that all user-initiated actions are logged along with information such as user ID, date and time. The audit trail information shall be available on demand for a certain pre-defined period following which; it shall be archived as per the retention policies.
16. Provide facility for the customer to accept application security terms and conditions (like not to use Jail-broken devices).
17. Ensure that the application setup enables ADIB to communicate with mobile application users (such as informing about new versions / updates whenever launched).
18. Not share / Private Key Certificate / Password which require privileges of ADIB Developer Account. It shall be done only through ADIB controlled IT environment/premises.
19. Not run on Jailbroken/rooted devices
20. Make use of strong SSL pinning
21. Store any sensitive information on mobile device only through secure key chain.

4.1.3 Additional controls for Web/ Special purpose application

The application system shall have:

1. Architecture based on multiple tiers. In case of web application, it is preferred to have multiple web servers on front-line.
2. Web user access to the front-end web servers only.
3. Reviewed for Protection against common vulnerabilities (such as Parameter Manipulation, SQL Injection, Command Injection, Cross Site Scripting, Directory Traversal, Buffer Overflow, Cookie Snooping, Authentication Hijacking, Log Tampering, Attack Obfuscation, Error message Interception, Denial of Service, etc.)
4. Application specific controls (such as message authentication and integrity - in case of a messaging application, maintenance of privacy - in case of customer interaction, etc.)
5. In order to provide protection and monitoring with WAF and firewalls, between application tiers, all web application should be implemented three-tier architecture as presentation layer, application layer and data layer for perspective of secure application design and availability.

4.1.4 Encryption Algorithms

1. Any non-listed encryption algorithm (cipher or mode of operation) is strictly forbidden.

A.1 Approved Encryption Algorithm requirements

Symmetric encryption
Advanced Encryption Standard (AES): The Advanced Encryption Standard (AES) is a widely accepted symmetric encryption algorithm available in key sizes of 128, 192, or 256 bits, renowned for its high level of security and widespread adoption.

Asymmetric Encryption Algorithms

a. RSA (key length as per key length table below)
b. Elliptic Curve cryptography (ECC) (key length as per key length table below)
a. Identity Based Encryption (IBE) (key lengths must be assessed and agreed by IT Security to be equivalent to other approved key lengths)

Asymmetric Key Lengths

a. Given any cryptographic algorithm will only be safe to use for a period of time based on available computational power (required to feasibly cracking the encryption); wherever available higher strengths of ciphers should be used than the minimum requirements specified in Table A.2 below.
b. The selection of a key length for an asymmetric algorithm shall be based upon an expected end of life for a system in scope.
c. Where there is particular technology or industry standard constraints (for example chip cards, EMV) the smaller key lengths may be used for the periods shown.

A.2 Asymmetric key length requirements

Expected system end of life	RSA / El Gamal / DSA	ECC
End 2026	3072	256
End 2024	2048	256
End 2018	1152	224

Approved Hash Algorithms

a. For Digital Signature applications SHA-3, SHA-2
b. For another applications SHA-3, SHA-2
c. Bcrypt (for password hashing only, note that PBKDF2 with a 32-bit salt and at least 10,000 iterations is recommended)
d. SHA-2 refers to a family of hash algorithms of various hash sizes (SHA-224, SHA-256, SHA-384, and SHA-512). All these are approved for use. Where available, SHA-2 hashing algorithm is strongly recommended to be used with the SHA-256/SHA-384 being the most adopted options.
e. SHA3 is recommended to be used wherever the product supports.

Network and Transport Layer Protocols
The following Network and Transport Protocols are approved:

a. TLS Version 1.2 (v1.2 must be used with strong cipher suite only) or higher must be used where available.
b. SSL (all versions), TLS1.0 and TLS 1.1 must not be used.

Message Authentication Code (MAC) algorithms

a. HMAC (must use an approved hash algorithm) - OMAC/CMAC, OMAC2 – VMAC

4.1.5 Vendor Declarations

The vendor shall agree (by declarations/acceptance or contract)

1. Not to violate any Intellectual Property Rights, licensing rights, etc. while producing the system and subsequently providing it to ADIB.
2. System to be penetration tested. Further, he has to agree to provide fix for all the concerns raised and elimination of existing vulnerabilities before launching on the internet.
3. Not to deploy techniques to covertly gather information about individuals at the time of access authentication.
4. On installation according to best practices (such as remove unnecessary services, files, or programs, disable anonymous user account), free from negligence issues, not jeopardizing the security setup, and customized (if required) according to business needs of ADIB.
5. On protection against source code vulnerabilities for the system (such as hard coded passwords, time/events triggers, loops, trap doors, or any path that may circumvent security or that include special access privileges for developers).
6. Usage of mature development tools and techniques, which have the known bugs and problems corrected. Providing details of count and rating of vulnerabilities of the Operating System and coding language. It shall include the current status of system hardening and provision of future vulnerability management.
7. That all applications should fulfil security requirements as defined in RFP document (Request for Proposal document – owned by VMCP)

4.1.6 Vulnerability Risk Rating

The information security department assesses the vulnerability risk as per the following

Risk Rating	Criteria
High	loss of system or network control due to the compromise of a privileged user account
Medium	loss of system or network functions from the compromise of a normal user account or limited privileged user account
Low	loss of confidentiality and integrity of data or unauthorized access to files or other system/network resources

4.1.7 System acceptance Criteria

Final Acceptance for releasing the system to the Infrastructure and Operations environment shall be subject to:

- All the security vulnerabilities have been “**Closed**” or assigned an appropriate closing date;
- **Or risk acceptance as per the following matrix:**

		System Criticality	
		High	Medium
Risk Rating	High	System Owner (head of the concerned requesting Division)	
	Medium		

- Or risk acceptance by the System Owner (head of the concerned requesting Division) only, if other security vulnerabilities are still “**Open**”.

4.1.8 Software Escrow Criteria

Software escrow takes place in an agreement between three parties ADIB, Software supplier and Escrow solution provider to ensure availability and continuity. Applications will be required to have escrow agreement based on EA application profiling. Below are the criteria:

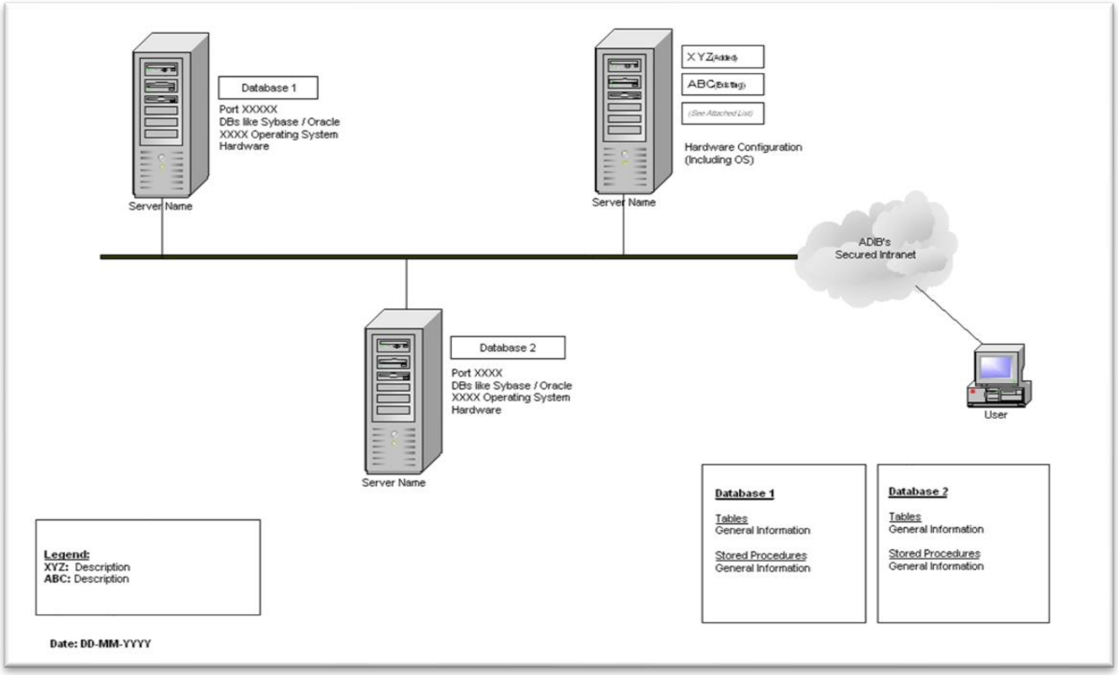
- The business applications with criticality rating of ‘High’ and above.
- The source code of the application does not belong to ADIB and does not control in ADIB premises.

5 Exceptions

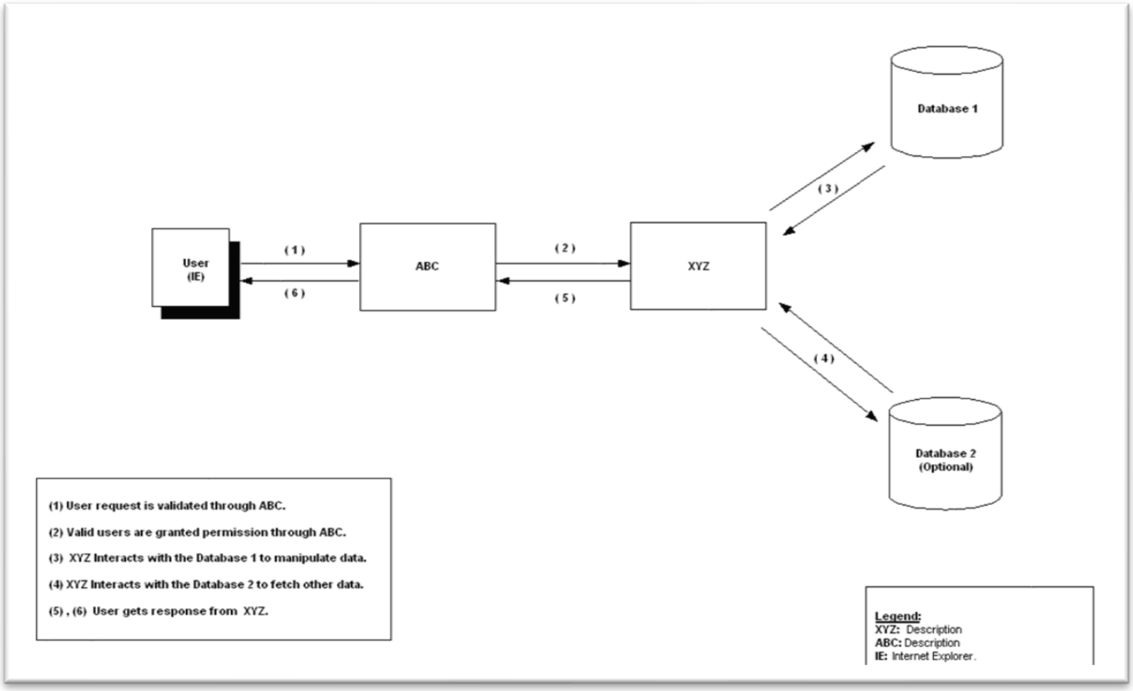
Any deviation to the standard shall be documented along-with associated risks and shall be approved

6 Appendixes

Appendix A: Component flow diagram sample



Appendix B: Data flow diagram sample



(1) User request is validated through ABC.

(2) Valid users are granted permission through ABC.

(3) XYZ Interacts with the Database 1 to manipulate data.

(4) XYZ Interacts with the Database 2 to fetch other data.

(5) , (6) User gets response from XYZ.

Legend:
XYZ: Description
ABC: Description
IE: Internet Explorer.