Application Information Security Assessment

Information System/ Service Name:	
Supplier:	
Date:	
Assessor:	

Questions			Supplier Input		
S/N	Evaluation Criteria	Description	Response (A)	Comments (B)	Evidence (C)
		A. Solution Security			
		A1. Application Security Characteristics			
A.1.1	Solution Security Certification	Is the solution's security certified? If yes under which certification?			
A.1.2	Security Assessment / Penetration Test / Code Security Review	Has a penetration test, security assessment or code review been recently performed on the solution, when and by whom?			
A.1.3	Non mitigated vulnerabilities	In case a penetration test, security assessment or code review has been recently performed, have all vulnerabilities been mitigated? If not, please specify.			
A.1.4	Software patching	Does the company provides continous software updates and fixes for security vulnerabilities?			
A.1.5	Encryption in transit	Are data encrypted during transmission? Describe encryption mechanisms in the comments area.			
A.1.6	Encryption at rest	Are data encrypted at rest? Describe encryption mechanisms in the comments area.			
A.1.10	Data saved / used locally at the client side	Is the application prevented from using / saving specific data locally at the client's terminal / device? If no, explain further why and how local/client data are protected.			
A.1.11	Browser security directives	Does the application enforce browser security settings (e.g. headers missing, deactivated auto complete, disabled caching) when sensitive data is provided by or sent to the browser?			
		A2. Secure Authentication and User Management			
A.2.1	Integration with Active Directory	Does the solution support all types of accounts to be managed through a centralized User Repository (e.g. Active Directory / other LDAP directory for on premise implementation OR Authentication with Microsoft 365 for cloud implementation)? Please explain in the comments column			
A.2.2	Strong and Two-Factor Authentication mechanism support	Does the application support MFA authentication?			
A.2.3	User administration environment	Does the application offer an appropriate environment (e.g. GUI) so that users and roles (Groups or Profiles) can be managed (e.g. user and roles creation, access rights assignment, setting password policy)?			
A.2.4	User segregation	Are the solution's administrative interfaces segregated from users' functionality? Please elaborate how the segragation is accomplished.			
A.2.5	Four-eye Principle for specific transactions	Does the application enforces dual control in the form of maker and checker of changes/transactions to ensure these activities before they are accepted by the system?			
A.2.6	Four-eye Principle for administrative actions	Does the application enforces dual control in the form of maker and checker of administrative actions to ensure these activities before they are accepted by the system?			
A.2.8	Number of Concurrent Sessions	Does the application offer the ability to set the maximum number of concurrent sessions per user?			
A.2.9	Sessions and Idle timeout	Does the application offer the ability to set the maximum session time-out and inactivity time?			
A.2.11	Secure Password creation	Is the creation of initial passwords performed automatically? If yes, how are they provided to the user?			
A.2.12	Password change enforcement	In case the creation of initial password is not performed automatically, does the solution enforce password change at the first login?			
A.2.13	Password protection	Are the passwords protected from being visible to anyone (including the administrator) through the GUI?			
A.2.14	Default accounts management	Does the application offer an option to disable or rename default accounts?			
A.2.15	User Account (ID) Parameters	Does the solution support manual configuration of minimum username length?			
A.2.16	User Account (ID) Parameters	Does the solution support automatic user accounts disabling when a wrong password is given for X consecutive times (where X the number of failed attempts set by the Administrator)?			
A.2.18	Password Parameters	Does the solution support password complexity rules customisation for the following: minimum password length of 12 characters contain at least one character from 3 out of 4 categories: capital, lowercase, numbers and symbols, no more than X consecutive characters of the same category are used Password lifetime Password history that forces new passwords to differ from the old ones.			
A.2.18	Password Parameters	Does the solution support password complexity rules customisation for the following: minimum password length of 12 characters contain at least one character from 3 out of 4 categories: capital, lowercase, numbers and symbols, no more than X consecutive characters of the same category are used Password lifetime Password history that forces new passwords to differ from the old ones.			
A.2.19	CAPTCHA	Does the solution support CAPTCHA or device fingerprinting for suspicious flows or after several failures.			
		A3. Logging & Auditing			
A.3.1	User and Administration actions Logging	Does the solution record (log) all actions performed by the users (e.g. logins, inquiries, transactions)? • Transaction date and time • User ID (username) • Type of Transaction • Source and Destination IP Address • Transaction/Action Data • Transaction/Action result (successful, unsuccessful) and reason of failure • Transaction/Action number			
A.3.2	Logging Data (System Level)	Does the solution record (log) the following actions performed into the system? • Date and time of events • User ID (username) • Unsuccessful attempts to access system and/or application data • Unsuccessful attempts to access critical system folders and files • Use of external/peripheral devices • System start up and shut down • System/Application Failures			
A.3.3	Log Retention	Are there any restrictions on the log retention (e.g. time-based or storage-based)?			
A.3.4	Log Protection	Are logs protected from tampering in order to ensure their data integrity?			
A.3.5	Log search mechanism	Does a search mechanism exist for logs providing sort and presentation capabilities (e.g. selection of entries based on date range)?			
A.3.6	Log Management	Is the export or automatic transfer of logs to a third party Log Management/SIEM solution supported, using a standard log format (e.g. syslog, WMI)?			
		A4. Secure SDLC and Data Validation Controls			
A.4.1	Secure SDLC	Is information security assessed in every stage of Software Development LiveCycle (secure SDLC)?			
A.4.2	Secure Software Development Standards/Guidelines	Does the supplier follow secure coding standards/guidelines (e.g. OWASP, NIST, SANS)?			
A.4.3	Security testing	Does the company perform Static and Dynamic Application Security testing (SAST and DAST) during SDLC? Will the tests results provided to Tirana bank before go live? Please explain tools used for SAST and DAST.			
A.4.4	No hard-coded accounts/passwords	Are all hard coded and/or shared User IDs and passwords excluded from application's source code?			
A.4.5	Input Validation (format)	Are the input values validated as to their type or format (e.g. a numeric value is entered in a numeric field)?			
A.4.6	Input Validation (invalid characters/strings)	Does the application check inputs for non-expected or forbidden characters, parameters or strings (e.g. special characters, meta code, metacharacters, HTML code, direct SQL queries) to protect from malicious input?			
A.4.8	Uploaded Files Validation (File inclusion vulnerability)	If the application supports file uploading, is it possible to scan files in real-time with antivirus/malware, limit size, block executables, store outside document root, validate any uploaded files in real-time, in order to prevent arbitrary execution (e.g. php JavaScript files)?			
A.4.10	Bounds Checking – unacceptable values	Does the application validate input values against specific bounds (e.g. length, acceptable values, business rules, double/null records) to manage related threat cases (e.g. buffer overflow, heap overflow, memory corruption)?			
A.4.11	AutoComplete	Does the solution disable autocomplete(Ex users usernames/passwords are not stored in the input fields?)			
A.4.12	Separation of untrusted data from busines	Do you avoid using an interpreter (by using a safe API or providing a parameterised interface)?			
		A5. Error Handling			
A.5.1	Error Handling Mechanism	Does the application have appropriate error handling mechanisms to ensure a secure continuation of operation or secure termination, for cases of errors or execution problems?			
A.5.2	Error Information Restriction	Is the application's error handling information and/or detailed data hidden from the user?			
A.5.3	Error Logging	Are problems and errors recorded in a dedicated log (e.g. system log, application log)?			
		B. Mobile Security Characteristics (in case of a mobile application)			
B.1	Platform Usage & Permissions	Ensure proper use of platform-specific security features (e.g., iOS Keychain, Android Keystore). Only request the minimum necessary permissions (e.g., location, camera, etc.). Prohibit access to sensitive APIs (e.g., device fingerprint, clipboard) unless absolutely necessary.			
B.2	Data Storage	All sensitive data (e.g., user credentials, tokens, PII) must be securely stored using encryption in iOS Keychain or Android Keystore. Do not store sensitive data in unprotected areas (e.g., external storage, cache). Implement encryption using AES-256 for data at rest. Store session tokens and authentication credentials securely, and automatically clear them when users log out.			
B.3	Secure Communication	Enforce TLS/SSL (HTTPS) for all network communications. Implement certificate pinning to protect against man-in-the-middle (MITM) attacks. Avoid transmitting sensitive data via insecure channels (e.g., HTTP, SMS).			
B.4	Authentication	Implement strong authentication using multi-factor authentication (MFA) where applicable. Enforce secure password policies (e.g., complexity, expiration, length). Session tokens should expire after a predefined period of inactivity and should be securely stored.			
B.5	Cryptography	Use strong, up-to-date cryptographic algorithms (e.g., AES-256, RSA-2048) for encryption. Avoid using deprecated algorithms (e.g., MD5, SHA1). Ensure all cryptographic keys are securely stored and managed using platform-specific secure storage.			
B.6	Authorization	Implement role-based access control (RBAC) to restrict access to features based on user roles. Ensure server-side checks for authorization in APIs; do not rely on client-side authorization.			
B.7	Client Code Quality	Conduct code reviews and security testing to identify and eliminate bugs or vulnerabilities. Handle exceptions securely to avoid application crashes or data leaks. Ensure that no debug code, test data, or verbose logging is present in the production build.			
B.8	Code Tampering Prevention	Implement code obfuscation techniques to make reverse-engineering more difficult. Use runtime detection for app tampering (e.g., checksum verification, integrity checks). Detect and prevent modification or tampering of app code and resources.			
B.9	Reverse Engineering Protection	Obfuscate the application's code to hinder reverse engineering (e.g., using ProGuard for Android, iOS obfuscation tools). Encrypt sensitive parts of the app's configuration files and resources. Use tools to detect debuggers or emulators during runtime.			
B.10	Extraneous Functionality	Ensure that no development/debugging functionalities (e.g., admin modes, test functions) are included in the production version. Perform a full review of the app's functionality and remove any unused or unnecessary code before release.			
B.11	Additional Security	A penetration test, security assessment and a code review must be performed on the solution by external company not related to the one developing the application and all vulnerabilities must be been mitigated prior of go live. Ensure the app is compliant with platform-specific app store security guidelines (Google Play Store/Apple App Store). Implement security logging for tracking suspicious activity, but avoid logging sensitive data (e.g., passwords, PII).			
B.12	Testing Requirements	Conduct Static Application Security Testing (SAST) to identify vulnerabilities in the source code. Perform Dynamic Application Security Testing (DAST) to detect vulnerabilities during runtime. Ensure compliance with the latest OWASP Mobile Security Testing Guide (MSTG).			
		C. PCI-DSS requirements (in case the service/application contains cardholder data)			
C.1	Data Flows	Can the supplier provided a diagram that shows all cardholder data flows across systems and networks?. Please provide the diagram			
C.2	Cardholder data retention and disposal	Does the application provide automated mechanisms for cardholder data retention and disposal that can easily be customized to cover business needs?			
C.3	Cardholder data storage	Does the application store sensitive authentication data (full magnetic stripe and/or chip data, CAV2/CVC2/CVV2/CID and PIN/ PIN Block) after authorization (even if encrypted)? If sensitive authentication data is received, does the system/application render all data unrecoverable upon completion of the authorization process?			
C.4	PAN display	Does the application mask PAN when displayed or printed? Please describe masking mechanism.			
C.5	PAN storage	Does the application mask (the first six and last four digits are the maximum number of digits to be stored) or encrypt PAN when it is stored? Please describe the methods used.			
C.6	PAN transmission	Does the application use strong cryptography or masking (the first six and last four digits are the maximum number of digits to be displayed) to safeguard sensitive information during transmission (Network, email, SMS, FTP, etc)?			
C.7	Cryptographic keys management	Are procedures to protect keys used to secure stored cardholder data against disclosure and misuse, documented and implemented?			
		D. In case of Cloud Hosting			
D.1	Does Cloud hosting provider hold a valid information security/cybersecurity third-party attestation or certification (e.g., ISO 27001, SOC 2 Type 2, CSA STAR for Cloud services, Cloud Controls Matrix (CCM) etc.)? *If "yes", please state the program and date that was certified, and provide a copy of the certification*				

D.2	Are data segregation controls in place in case of a multi-tenant enivornment? If Yes, please explain the controls in place.			
D.3	Does the service provide Multiple data centers in different geographical loctions, allowing a switch to a data center in another physical locations? Please provide the location of the data centers.			
D.4	Does the organisation have a Disaster Recovery and/or Business Continuity Plan? If yes, explain in the comment session if the service provided to Tirana Bank are covered in BCP plans? Please provide in the comment session, the list of scenarios covered by BCP and a copy of plan if possible.			
D.5	Does the organisation periodically test its Recovery Plans? If yes, state how frequently and list the disaster recovery scenarios covered during DRS tests (ex. Full site loss, component failure, loss of a region, partial failures etc)			
D.6	Do you have a Recovery Time Objective (RTO) and Recovery Point Objective (RPO) defined for the cloud service provided to Tirana Bank? If yes, please provide the RPO and RTO.			
D.7	Do you perform backups of the services provided to Tirana Bank? Does the backup frequency covers the defined Recovery Point Objective. Please provide details and state where are the backups stored.			
D.8	Is Tirana Bank data encrypted during transmission? Please detail encryption mechanisms.			
D.9	Is Tirana Bank data encrypted at rest, including backups? Please detail encryption mechanisms.			
D.10	Are measures in place to pseudonymize or anonymize personal data? Please describe mechanisms used.			
D.11	Does the service provided to Tirana Bank, allows Geolocation (whitelisting of IPs from which the service can be accessible)?			
D.12	Please describe retention policy and backup policy for Tirana Bank data			
D.13	Does the company provides an Exit Strategy for Tirana Bank in case of contract termination? Please describe in the comment session			
D.14	Does the company supply verification/proof that Tirana Bank's data has been securely deleted?			
D.15	Please state if the bank has the right to audit the service provider? Additionally, is bank permitted to perform an audit of the service provider on short notice due to an emergency or crisis situation? Please note as per Bank policies, the Bank should have the right to audit.			
D.16	Is the technological stack updated continously to latest versions? State the maximum timeframe in which the company guarantees to patch open vulnerabilities, dependent on category (critical, high, moderate, low, etc.) and how this is guaranteed/proven			
D.17	Does the company provides application security in the production environment. Please describe (e.g. application-level firewall, database logging / auditing, etc.)?			
D.18	Does the company provides network segmentation (Isolate critical systems from public facing services)?			
D.19	Does the company provide a zero trust model verifying every connection internally and externally?			
D.20	Does the company provide a DDoS mitigation in case of a public facing web solution for TiranaBank?			
D.21	Does the services provided to Tirana Bank have a malware protection software installed?			