



BAHRAIN DEVELOPMENT BANK BSC(c)

DIGITAL LENDING & ONBOARDING
BUSINESS REQUIREMENTS DOCUMENT
VERSION 1.0

BUSINESS REQUIREMENT DOCUMENT

Table of Contents

Glossary	2
1. Introduction	3
1.1. Purpose	3
1.2. Scope	3
1.3. Business Objectives	3
2. Process Overview	4
2.1. Customer Onboarding	4
2.2. Lending Application	4
2.3. Common Functional requirements	5
2.4. Client Onboarding & Account Opening Requirements	8
2.5. Digital Lending Requirements	9
2.6. Bank Administration Requirements	10
3. Non-Functional Requirements	11
3.1. Architecture	11
3.2. Performance & Availability	11
3.3. Scalability	12
3.4. Compliance	12
3.5. Usability	12
3.6. Infrastructure	13
3.7. Integration Capabilities	13
3.8. Audit Trails	14
3.9. Reporting Requirements	14
4. Integration requirements	15
5. Product Roadmap Requirements	16
6. Data privacy & Security Requirements	16
7. Deliverables	17
8. Training	17
9. Stakeholders	18

BUSINESS REQUIREMENT DOCUMENT

Glossary

This following table highlights and explains all key terms and abbreviations used in the document.

Term	Definition
MOIC	Ministry of Industry and Commerce
WATHIQ	The System of Benefit Company that holds the individual's information
KYC	Know Your Customer
SLA	Service Level Agreement
Sijilat	The system of MOIC that holds the information of Commercial entities
SME	Micro, small and medium enterprises as defined by the MOIC
AI	Artificial Intelligence
ID&V	Identification & Verification
CRM	Customer Relationship Management
AML	Anti Money Laundry
ETB	Existing To Bank
NTB	New To Bank
PEP	Politically Exposed Person
CSR	Customer Service Representative
EDD	Enhanced Due Diligence
LOS	Loan Origination System
CBS	Core Banking System
CIF	Customer Information File (Customer Reference on CBS)
BCRB	Bahrain Credit Reference Bureau
CR	Commercial Registration (Business Identifier)
TAT	Turnaround Time

BUSINESS REQUIREMENT DOCUMENT

1. INTRODUCTION

1.1. Purpose

This document outlines the business requirements for the development and deployment of digital lending and onboarding solutions that will serve both retail and corporate customers of BDB. The platforms will allow individuals and businesses to onboard and apply for financing securely and efficiently online, and through the branches.

1.2. Scope

The solution will include the below functionalities for retail (individual) and corporate customers:

- Onboarding new customers online
- Onboarding new customers through the branch
- Account opening for new and existing customers
- Lending application online

Lending applications through branch & lending approval process will be out of this scope and should be covered in the LOS (Lending Origination System) implementation scope.

1.3. Business Objectives

By implementing digital onboarding and lending, BDB can achieve a competitive edge, improve customer satisfaction, and drive sustainable growth in an increasingly digital financial landscape.

- Enhance Customer Experience: Reduce the time required for onboarding and loan approval, and enable customers to complete their applications from anywhere, anytime via digital platforms.
- Transparency: Provide real-time updates on application status and loan terms, building trust with clients.
- Operational Efficiency: Minimize manual intervention in onboarding, credit assessment, and loan processing, reducing errors and delays.
- Cost Saving: Lower operational costs by digitizing processes and reducing reliance on physical branches and paperwork. Digital platform also handles a higher volume of clients and applications without significant increases in staffing or resources.
- Boost Revenue Generation: Accelerate the time to revenue by quickly processing loans application and attract more clients by offering seamless and innovative digital services.
- Strengthen Brand Image: Position the bank as a forward-thinking, tech-savvy institution. Build trust with clients by providing secure, efficient, and transparent services.
- Regulatory and Compliance Alignment: Ensure full compliance with financial regulations, including KYC, AML, and data privacy laws. Fraud prevention using advanced security measures like biometric verification and AI-driven fraud detection.
- Support Strategic Goals: Align with BDB's broader digital transformation initiatives, customer-centric approach and boost the revenue generation.

BUSINESS REQUIREMENT DOCUMENT

2. PROCESS OVERVIEW

2.1. Customer Onboarding



Above process to allow both ETB and NTB, retail & corporate clients to apply for account opening. System to recognize the ETB clients and skip certain steps automatically to allow clients to open accounts. There are differences in the steps and requirements between retail and corporate clients onboarding.

2.2. Lending Application



Above process to allow both ETB and NTB, retail & corporate clients to apply for lending. System to recognize the ETB clients and skip certain steps automatically to allow clients to apply for lending. There are differences in the flow and requirements between retail and corporate clients' applications.

* Post application submission, applicant should be able to follow up on the application status and provide additional requirements (if any) through the platform based on the bank Backoffice team feedback.

BUSINESS REQUIREMENT DOCUMENT

Functional Requirements

2.3. Common Functional requirements

2.3.1. Business Validation

- Ability to integrate with MOIC Sijilat APIs to pull the CR information
- Business Eligibility Check: System to perform eligibility check based on rules as defined by the bank.

2.3.2. ID & Identity Verification

- Use AI online ID&V tools to verify Applicant and Shareholders identities and authenticate their IDs instantly.
- Capture the IDs scans out of the ID&V process
- Seamless integration is expected with the ID&V tool within the onboarding and lending process
- Provide option to allow Backoffice team to view the ID&V cases that failed for certain no of times and approve applications to proceed to the next step with manual approval of the identity verification.
- Individual Eligibility Check: System to perform eligibility check based on rules as defined by the bank.

2.3.3. KYC/AML Compliance

- Automate Know Your Customer (KYC) capture and online integration with eKYC Wathiq system is expected.
- Instant AML screening is required through integration with the bank AML system to ensure compliance with regulatory requirements.
- Screening against the internal and external lists is required, and alerts/actions to be taken by the platform automatically according to the rules setup supplied by the bank (e.g. blacklist, freeze and abuser lists)
- Ability to embed Compliance rules within the platform, where additional approvals are required for certain cases as per the rules.

2.3.4. Documents Upload & Management

- Platform should allow clients to upload required documents (e.g., financial statements, CR certificate, etc.) via a secure portal.
- Support saving and accessing documents from the platform back office and saving additional copies within the bank through integration with the document management system of the bank.
- Screening against viruses is required while uploading the documents into the portal.
- OCR to be enabled to extract the information of the uploaded documents and allow authorized users to review and amend as required.

2.3.5. Risk Assessment

- Support risk profiling to evaluate the corporate clients based on their entity information and AML screening results while onboarding & lending and assign the risk score on core and eKYC Wathiq system.

2.3.6. Integration with Digital Banking

- Platform should allow clients to create accounts and apply for lending through both pre-login and post-login screens of BDB digital banking platform.

BUSINESS REQUIREMENT DOCUMENT

- Certain steps of verification of the client and business to be skipped when the client tries to apply from post-login screens of BDB digital banking.
- Platform to allow both methods, to integrate through APIs to trigger the functions, or to display platform interface within frames from digital banking application.
- Platform to support the integration with both web based and mobile applications of BDB digital banking.

2.3.7. Tigger from 3rd Party

- Platform to allow triggering the processes of customer onboarding, account opening, and lending application from 3rd party platforms.
- Vendor to provide the APIs and integration requirements to enable this.
- Applications triggered from 3rd party platforms to be tracked through the dashboard and allow taking the enabled actions on them.
- Sync the status and updates on these applications with LOS.

2.3.8. Accessibility

- Platform should support accessing the services through both web interface and mobile application, and to support the view from different devices (desktop, mobile, tablets, etc.).
- Omnichannel Access: Ensure onboarding & lending are accessible by clients via web, mobile apps, and in-branch (self-service machines in future).
- Branch team to have interface for onboarding & account opening.

2.3.9. Backoffice View

- Platform to provide Backoffice access with live dashboard of applications created from the different channels (online & branch) for the different services, lending, onboarding, & accounts opening.
- Backoffice team to be able to extract reports from their view in different formats (Excel, PDF, etc.), and download/view the documents attached to the applications.
- Details of the captured information/documents per application to be detailed on the Backoffice view, including timestamps, TAT, channel, status of the application, exceptions and errors (if any).
- Backoffice team to be able to take actions when required e.g. to review and approve the Compliance cases that were caught based on the user role and Compliance embedded rules within the platform.
- Task Management: clear dashboard view for Bank team members to manage and execute their tasks, and for the bank management to supervise the tasks and SLAs assigned to bank teams.
- System to allow setting SLAs for the tasks and automatic notifications and reminders to be pushed by the system to the relevant user and team.

2.3.10. Email & Mobile Verification

- Verification of the provided email and mobile to be performed by the system using OTP.
- System to block automatically applications that fail to verify the OTP within certain number of trials, for certain amount of time.
- Basic validation of input format is expected.

BUSINESS REQUIREMENT DOCUMENT

2.3.11. Notifications

- Real-time notifications via email/SMS/App for all applications and updates (e.g., application created, approval received, etc.).
- Ability to capture the preferred means for communication and language for each user (e.g. e-mail, App notifications, SMS etc.)
- Notifications should be sent to both clients and bank users based on the required actions, updates, error notification, transaction execution confirmation (Success, Warning, Error, etc.)
- Report of all pushed notifications to be available for audit purposes.
- Ability to design new notifications without the involvement of the vendor.

2.3.12. Consents Capture

- Allow capturing the required consents and save tracking of them with timestamp per application, either through online or the branch.
- Allow viewing the consents for online applications as text on screen, through PDF document popup, or links to external websites as required by the bank.
- Allow viewing and granting the consents for branch applications using tablets
- Ability to upload client consent into eKYC Wathiq system through APIs integration

2.3.13. Signature Capture

- Ability to retrieve signature of an individual from eKYC Wathiq system through APIs integration and save it into the application record and core banking system
- Ability to capture e-signature and integration with DocuSign
- Ability to capture signatures through tablets or signature devices in branches with the applications

2.3.14. Customer Support

- Tutorial videos: Tutorial videos for user assistance that can be accessed through the system.
- FAQ Section: A comprehensive FAQ section that can be updated by the system admin.
- Contact us: section hold the contact information (phone no & email) to reach bank support team for help.

2.3.15. Security

- Data Encryption: Secure all customer data using end-to-end encryption.
- Two-Factor Authentication: Ensure secure login and verification processes are in line with bank guidance and requirements.
- Audit Trails: Maintain logs of all activities for compliance and internal review.
- Fraud Detection: Use AI to identify anomalies or fraudulent attempts during onboarding and lending applications.

BUSINESS REQUIREMENT DOCUMENT

2.4. Client Onboarding & Account Opening Requirements

2.4.1. Resume Application

- Applicant should be able to resume his application at any time later
- Applicant to be verified using basic information including CPR, CR, Email, Mobile, and OTPs.
- System to retrieve previous incomplete applications and allow applicant either to create new application or resume an existing one.

2.4.2. EDD Rules

- Allow embedding the EDD rules within the process implementation
- Once EDD conditions met, system should request the applicant/or CSR to input additional information

2.4.3. Registration to Digital Banking

- System to allow registration to digital banking platform as part of the onboarding.
- Client to be able configure the access parameters to digital banking platform.

2.4.4. Declarations

- Allow capturing client tax declarations for FATCA, CSR, etc.
- Allow capturing client declarations for PEP and capturing the PEP details.
- Allow capturing of additional information based on the client selection.
- Allow viewing and capturing the consents at branches using tablets

2.4.5. Manual Application

- The system should be flexible to allow CSR to process the onboarding of clients who are applying using physical forms.
- It should allow the CSR to process the onboarding without capturing the clients input through the tablets. As CSR may need to process the applications without the presence of the applicant if all forms and documents are provided.

2.4.6. Prospects from LOS

- System to allow prospects to be pushed by LOS system to the platform for clients applying for lending through branch/LOS system.
- CSR should be able to verify and turn the prospects pushed by LOS into clients. He should be able also to update the information of the prospect if any need update.

2.4.7. Prospects from Digital Lending

- System to allow prospects to be pushed by the digital lending module to the platform for clients applying for lending online through the same platform.
- CSR should be able to verify and turn the prospects pushed by the online lending module into clients. He should be able also to update the information of the prospect if any need update.

BUSINESS REQUIREMENT DOCUMENT

2.5. Digital Lending Requirements

2.5.1. Application Management

- Provide clients with a dashboard to monitor the applications, their status, and account activities.
- The applicant should be able to take certain actions on the applications, e.g. to provide additional requirements and information based on bank team feedback on LOS.
- Applicants should be able to save the applications and resume it later at any time.

2.5.2. Application Requirements & Flow

- Dynamic Forms: Ability to customize application forms and checklist requirements based on client type and finance product type.
- Ability to configure different flow steps for application per client type and finance product type.

2.5.3. Credit Scoring

- Ability to set up credit scoring rules to calculate initial credit score for the application based on the application parameters automatically.
- Ability to integrate with the BCRB for obtaining credit scores and histories to support credit risk assessments.

2.5.4. Loan Calculator

- Provide clients with a loan calculator to allow them to try different scenarios input calculation.
- The system should allow the bank to configure the financing rates and credit rating based on the client type, financing product, finance amount, etc.

2.5.5. Real-Time Decisioning

- AI-based Risk Assessment based on the credit scoring and rules setup for the credit facilities applications.
- Ability to configure decision rules to decline or accept applications instantly based on application parameters and risk assessment results.

2.5.6. Application Follow up

- Applicant should be able to track the status of the submitted applications
- Applicant to be notified by the system in case any update on the application appeared or in case any action required from his end on the application
- Applicant should be able to upload and provide additional requirements based on the bank Backoffice team updates that are done on LOS.
- System to sync the application status with LOS system of BDB.

BUSINESS REQUIREMENT DOCUMENT

2.5.7. Documentation Review

- System to retrieve the approved documentation from LOS as per the approval process.
- System to allow client to review documentation/offer, download, and provide decision with remarks on the platform.
- System to update client updates on the application & feedback back to LOS.
- System to maintain availability of documents for client approval based on the SLA setup by the bank.

2.5.8. Applications From Other Channels

- Ability to read applications created through another channel (e.g. Branch) from LOS.
- Applicants should be able to register an access account to the platform and track the status of the submitted applications through branch.
- All features enabled on the applications created online through the platform should be enabled to the applications created through the other channels (e.g. notifications, actions, updates, etc.)
- System to sync the application status with LOS system of BDB.

2.6. Bank Administration Requirements

2.6.1. Configuration

- System Parameters - System should support add/modify/delete the system parameters through Backoffice interface end
- System should support maker and checker authority concept for all configuration and actions executed by the bank staff and administrators.
- Support configuring different admin fees, profit rates, product types etc
- Availability of Process Management tool is preferred, where bank administrators can update and configure process flows and forms without the need for vendor support.

2.6.2. Bank Administration

- The platform provides administration functions to allow creation and management of bank users of the platform.
- Bank administrators to be able to update, manage, enable, and disable the privileges and roles assigned to user accounts of both clients and bank users.
- Support configuration of the color schemes, artwork and logos used on the platform interface.

3. NON-FUNCTIONAL REQUIREMENTS

3.1. Architecture

- The solution design should be cloud native
- The overall solution should be modular in structure, allowing the bank to easily activate / launch or even scale specific modules based on need
- The solution (including sub-components) should be based on a micro-services architecture
- The solution should be build using latest technology, leading industry standards and protocols
- The solution should be data base agnostic
- The solution architecture should allow secured extension of certain application capabilities to 3rd parties (outside of network) portal for 3rd party agents and affiliates to process information, customer self-service portal, providing restricted access to customer information to outsourced functions (such as contact center)
- The overall solution set should provide omnichannel platform capability to ensure e-channels are aligned (from a content, product, service, authentication and service flow perspective, allowing users to initiate a transaction from one channel and completing them on another)
- Mobile apps should be present on both Google Play and Appstore, supporting Android and iOS
- The system should have the capability to configure and generate ad-hoc operational reports leveraging real time data, statements and advises
- The source codes and compiler must be available in escrow and must be maintained under version control software

3.2. Performance & Availability

- System Availability: The platform should guarantee 99.9% uptime. The system should be available 24/7, with scheduled maintenance windows announced in advance.
- Response Time: User actions should receive a response time of less than 3 seconds for most functionalities.
- support for automated backups and easy failover mechanisms.
- The solution must be configured and implemented with high availability and load balanced architecture
- Archived data must be available within a maximum of 5 minutes
- The system is expected to have the following performance characteristics for transactions per day:
- 90% of all user transactions should be completed in 2 seconds
- The remaining 10% of user transactions (inquiry and batches) should be completed in 5 seconds
- The system should not degrade less than 95% during peak times
- Support SLA requirement from solution vendors (Please refer Appendix-1 for the priority definitions)
 - For Priority 1 issues, the response time should be within 10 Minutes and the resolution time should be less than 2 hours
 - For Priority 2 issues, the response time should be within 10 Minutes and the resolution time should be less than 4 hours
 - For Priority 3 issues, the response time should be within 10 Minutes and the resolution time should be less than 8 hours
 - For Priority 4 issues, the response time should be within 10 Minutes and the resolution time should be less than 16 hours

BUSINESS REQUIREMENT DOCUMENT

- For Priority 5 issues, the response time should be within 10 Minutes and the resolution time should be less than 24 hours

3.3. Scalability

- The system must support increasing numbers of retail and corporate users, with seamless scalability for transaction volume growth.
-

3.4. Compliance

- Real-time Screening: applications created through the platform should go through real-time screening with various systems (internal or external) such as Black-list, World-check, diseased list, AML lists etc.
- Compliance rules: System should allow embedding compliance rules within the processes. System to assign to BDB teams, cases that were triggered by the compliance rules according to the approval authority matrix and allow BDB team to take actions on them.

3.5. Usability

- The platform should have a user-friendly interface, with clear navigation and minimal steps for completing key tasks
- An experienced UI/UX designer to be allocated by the vendor for the project implementation for all interfaces within the scope of the project.
- UI/UX design to be approved by the bank and customization to be allowed as per the bank branding, requirements, and team revision output.
- Supports multi-lingual screens (at least English and Arabic) for all customer-facing interfaces and capture customer's language preference.
- Mobile Access: Ensure mobile-friendly interfaces for ease of access and convenience.
- The system must be able to provide comprehensive on-screen help facilities
- Report formats must allow for dynamic formatting of columns
- The system must be intuitive and easy to use by users with limited training
- Comprehensive system documentation should be made available in both English and potentially also in Arabic
- System should allow data entry must in English and Arabic
- The solution must support export of on-screen data to MS Office applications
- The solution must use descriptive error messages to inform users where errors have occurred and how to correct these.
- Works well with office productivity suites such as MS Office, PDF reader and others.
- The system must have the minimal number of screens the user needs to navigate through to complete an action (screen navigation should be configurable and easy to define and modify). Screens must allow the user to complete the work without excessive scrolling down. The system must be able to define read only fields at runtime.

BUSINESS REQUIREMENT DOCUMENT

- The system must provide the option to copy from excel and paste in UI screen. This would be useful when creating objects with many line items.
- The system must ensure that all reports be printable in pdf and MS excel
- The system user interface must be easily customizable
- Prevent users from entering data in the wrong format and perform data validation such as:
 - Presence check (i.e. all of the mandatory information has been provided)
 - Allowed character check (e.g. a numerical field contains only one decimal point)
 - Data type check (e.g. a numerical field does not contain alpha characters)
 - Format check (e.g. checks that dates are entered in the correct format)
 - Logic check (e.g. checks that a date entered is within certain parameters)
 - Duplication check (i.e. checks that an identical Registration application has not been previously submitted).
 - Dedupe check, to prevent creating multiple CIF for same client, or multiple accounts for restricted products.
- Compatible with all web browsers such as Chrome, IE, Edge, Safari, Firefox etc.

3.6. Infrastructure

- The solution should be compliant to AWS cloud
- The solution (all components) should be deployable on IaaS or SaaS on AWS cloud
- The proposed solution set must have a minimum of 4 environments - 1 Production (With Failover), 1 Production Replica, UAT and Dev environments. Please note that these are the minimum set of environments that would need to be in place. The bank should have the flexibility to create / set-up additional environments based on need (such as additional environment for testing or development or pre-production), which can be used for specific timeframes. The cloud native model should allow pricing for the additional environment only for timeframes utilized.
- All environments must be hosted on AWS cloud, locally in Bahrain (or in rare scenarios any other location approved by and CBB)
- The solution should support automatic scalability on cloud based on need
- The system should support real time replication between the two production environments (or prod and DR installations)
- The system must provide automatic failover between the two production installations

3.7. Integration Capabilities

- All solution components should expose standard functionalities as APIs that can be readily detected / made available and consumed by other (internal) application components as well as external / 3rd party applications
- The enabled APIs should be based on leading practices (e.g. REST APIs) and leverage standard communication / extension protocols
- The system should have the provision to define and maintain all APIs and robust API management capabilities
- The solution should be able to define authentication, authorization permissions for APIs in a configurable manner
- The solution should have the flexibility to define orchestration and routing rules for APIs

BUSINESS REQUIREMENT DOCUMENT

- The solution should support standard API gateway capabilities across - Routing, Mediation (e.g. transformation, validation, caching) and Throttling (e.g. supporting throttling policies based on certain time-frames, transaction volumes etc.)
- The solution should support API analytics (examples)
 - Monitoring usage limits
 - SLA Monitoring
 - debugging / error reports etc.
 - API performance and KPIs
 - monitoring operational aspects of API
 - Trend analysis / simulation
- The solution must use industry standards to authenticate and authorize web service requests

3.8. Audit Trails

- Each application and major data entity (e.g. Task, Action, User, application, etc.) should have an audit trail feature.
- Platform to keep track of which user made changes (including automated actions by the system) to which entity and at what time, in case bank admin need to review changes that have been made through the platform.

3.9. Reporting Requirements

3.9.1. Usage & Transactions Reports:

- Daily/Monthly/Quarterly Activities Summary: Details of applications and activities done on the platform, segregated by application type and client type. Including but not limited to:
 - All Successful applications (lending, account opening, client onboarding) on quarterly basis.
 - All applications failed or rejected with reasons.
 - All applications submitted with different status
 - TAT for all applications (complete, pending, rejected/cancelled).
- Daily/Monthly/Quarterly Failed Activities Report: Logs of errors encountered during applications and activities or logins executed on the platform.
- Device and Channel Analysis: Access through Device types (desktop, mobile, tablet), Operating systems, Browser preferences and app vs. web usage.

3.9.2. Compliance Reports:

- Daily/Monthly Compliance Rules Report: Details of compliance rules triggered during the applications and actions taken against them.

BUSINESS REQUIREMENT DOCUMENT

3.9.3. Engagement Metrics

- Active Applications: Number of completed/incomplete, approved/rejected applications over monthly, quarterly, and yearly intervals, segregated by client type (Corporate and Retail) and application type.
- Login Report: Number of successful/unsuccessful clients login over monthly, quarterly, and yearly intervals segregated by client type (Corporate and Retail) and application type.

3.9.4. Ad-Hoc Reports/Dashboard

It will be an advance if the platform provides Reporting tools for bank users where we can create, customize, and schedule our own reports from generic data universes/schemes without reliance on the vendor.

4. INTEGRATION REQUIREMENTS

- CBS Core Banking Systems: Real-time integration with core banking systems for data retrieval and transaction execution (CIF creation, account opening, etc.)
- LOS Banking System: To create lending applications and trigger the approval process on LOS. And to get the updates on the active applications, update the documents, and feed the client decision.
- CRM Integration: Support integration with CRM system to log the leads for certain products selected by client at the onboarding process.
- Ecosystem Data Integration:
 - WATHIQ & MOIC Sijlat: Required for authentication and KYC update purposes
 - SharePoint: to integrate with BDB SharePoint for document management
 - ID&V Tool: Integration with ID&V online tool, to verify user identity and IDs instantly.
- Compliance Screening: Support integration (real time) with various systems (internal or external) such as Black-list, World-check, diseased list, AML lists etc.
- Digital Banking: To allow clients to apply for account opening or lending from digital banking interface, pre-login and post-login.
- 3rd party platforms: To allow triggering the processes/applications from 3rd party platforms and tracking their status/updates through the platform.
- BCRB for Credit Scoring: Integration with the BCRB is crucial for obtaining credit scores and histories to support credit risk assessments.

5. PRODUCT ROADMAP REQUIREMENTS

The system should be flexible and support adding new services, products and features in later phases, including but not limited to:

- Add more accounts/products for onboarding
- Add more schemes/products for lending
- Apply for retail/corporate cards
- AI based instant risk assessment and approval
- Enable card issuance within onboarding
- Trade Financing
- Integration with Supply Chain Finance Platform
- Integration with Payment Gateways (for initial deposits & charges)
- Blockchain-Based Documents & Contracts

6. DATA PRIVACY & SECURITY REQUIREMENTS

The platform and products should support the below listed technical requirements:

- Adherence to NIST Cyber Security Framework as required by Central Bank of Bahrain(CBB), and Secure standards, development lifecycle and coding practises (e.g. OWASP).
- Should adopt secure code analysis during development (i.e., static, dynamic or hybrid).
- Should have ISO 270001, ISO 22301, SOC2(for SAAS offerings) to demonstrate strong IT and Cyber Security processes.
- Should have strong identity, authentication, authorization, access control and auditing mechanisms.
- Should have comprehensive logging, monitoring and alerting/trigger features such as of user and systems activities, object calls, requests, responses etc. as well as security events with support for log forwarding.
- Should support Role Based Access Control and delegated/segregated/granular administration to support strict access controls and to restrict access to authorized individuals and parties.
- Implement rate limiting and throttling to protect against abuse and Denial of Service Attacks.
- Adheres to privacy by design principles (e.g. PDPL) with support for data masking/obfuscation and tokenization to protect/restrict sensitive data. Also, should support data anonymization for analytics or testing purposes.
- Easy, trackable and customizable explicit user consent management for data collection and processing.
- Should provide independent penetration testing certification semi-annually covering the CBB requirements.
- Support for encryption of all sensitive and confidential data at rest and in motion with industry recognized secure algorithms.
- Supports mobile device security such as tamper detection and detection of jailbroken/rooted devices restricting app functionality.
- Supports application code obfuscation to prevent reverse engineering and provides regular updates to address vulnerabilities in application and integrated third-party components/libraries/frameworks.
- Secure OTP delivery support for sensitive actions.
- Supports data retention requirements such as those defined by the Central Bank of Bahrain.

BUSINESS REQUIREMENT DOCUMENT

- Easy to understand error messages without revealing sensitive information.
- User access, roles, privileges and activity details extractable/viewable as a report is recommended.
- Strong security integration in the case of APIs through strong authentication and audit logging.
- Clear and comprehensive API documentation for security testing.
- There should be an option to default all sensitive and confidential documents with password protection for different customers.
- The system shall implement a secure CAPTCHA mechanism to prevent automated attacks on the online user onboarding/registration and login functionalities.

7. DELIVERABLES

- Detailed delivery plan with timeline
- Experienced & Dedicated Project Management Services
- Supply and installation of System Software(s)
- Implementation of Software covering:
 - Deployment and hosting of overall solution
 - Configuration and customization, in accordance with the Bank Requirements
 - Integration development, in accordance with the Bank Requirements
 - UI/UX design customization, as approved by the Bank
 - Aligning the solution security and network design as per security policies of the Bank
 - Perform QA testing on the Software
 - Support for all functional and non-functional testing by the Bank
 - Development of operational, analytical and MIS reports
 - Providing Solution design and architecture documentation
 - Providing training sessions and materials to bank staff
 - Providing detailed documentation and user manuals
 - Providing Tutorial videos
- Go live, rollout
- Post-Implementation Support

8. TRAINING

Training sessions to cover the below*:

- Training to System testing teams (including Pilot Clients)
- Training to System Administrators
- Training to Back-office teams
- Training to Customer facing teams
- Training to Support teams

Comprehensive User Manuals for both bank users and clients to be prepared and provided by the vendor and recorded demo videos are expected to guide the users on how to use the platform.

**More training sessions might be defined as required post conducting the testing.*

9. STAKEHOLDERS

- **Project Management:** Strategy and Transformation Department from the PMO perspective and IT from the project management perspective.
- **Product Owner:** Products- Digital Channels
- **Product Sponsor:** Chief Banking Officer (CBO)
- **Requirements Review & Approval:** Banking, Compliance, Legal, Risk, Information Technology, Information Security, Finance, Sharia, Operations, Credit Admin, Middle Office
- **Risk Assessment:** Risk Management Team
- **Regulators Approval:** Compliance Team
- **Shaira Compliance Approval:** Sharia Team
- **Solutions/Vendors Evaluation:** Information Technology, Strategy, Banking, Compliance, Risk, Information Security.
- **Terms & Declarations review:** Legal Team
- **Solution Testing & Signoff:** Banking, Compliance, Risk, Information Technology, Information Security, Operations, Legal, Credit Admin, Middle Office.
- **Solution UI/UX design review:** Banking, Marcom, Information Technology

BUSINESS REQUIREMENT DOCUMENT

1. APPENDIX-1: INCIDENT PRIORITY DEFINITIONS

Urgency>> Impact	Crit	Hig	Me	Lo
Critical	P1	P1	P2	P3
High	P1	P2	P3	P4
Medium	P2	P3	P4	P5
Low	P3	P4	P5	P5

U	Description		Description
C	<ul style="list-style-type: none"> - Instantaneous action required. - Catastrophic damage to essential business functions. Organization may be unable to function. - Severe financial losses for the organization. - Severe and widespread reputational damage. 		<ul style="list-style-type: none"> - Catastrophic disruption of critical business functions, rendering the organization unable to operate effectively. The impact of non-availability of the process will impact: <ul style="list-style-type: none"> - Any Reputation Impact. - Any Financial impact - Any Legal or Regulatory Impact - Service Quality / Customer Service: No service channel is available, and all customer segments are affected. - Any Critical Security Breach
H	<ul style="list-style-type: none"> - Immediate action required. - Affects essential systems or services, resulting in significant disruption or loss of functionality. - High risk of financial or operational impact. - Potential for severe reputational damage. 		<ul style="list-style-type: none"> - Severe disruption affecting essential business operations, multiple departments, or critical business processes. The impact of non-availability of the process will impact: <ul style="list-style-type: none"> - Widespread outage of critical systems or services, impacting all users or a significant portion of the organization. - Service Quality / Customer Service: A single channel of service is not available, and a single segment of customers is affected (this might VIP customers). - Any non-critical security breach
M	<ul style="list-style-type: none"> - Action required within a defined timeframe. - Affects specific departments or groups within the organization. - Moderate risk to business operations or service delivery. - Limited potential for reputational damage. 		
L	<ul style="list-style-type: none"> - Action required based on available resources and priorities. - Affects individual users or non-critical systems. 		<ul style="list-style-type: none"> - Moderate disruption affecting specific departments or groups within the organization. The impact of non-availability of the process will impact:

BUSINESS REQUIREMENT DOCUMENT

	<ul style="list-style-type: none">- Minimal risk to business operations or service delivery.- Negligible reputational impact.		<ul style="list-style-type: none">- Partial service outage or performance degradation, impacting specific business processes or user groups.- Service Quality / Customer Service: A single channel of service is not available, and a single segment of customers is affected (this might VIP customers).
			<ul style="list-style-type: none">- Minimal disruption affecting individual users or non-critical systems. The impact of non-availability of the process will impact:- Intermittent issues or minor glitches that do not significantly impact business operations.- Service Quality / Customer Service: A single channel of service is not available, and a single segment of customers are affected (this does not include VIP customers) or, customers are unlikely to be affected, but could be aware of interruption.