

# Request for Proposal

Digital Banking Revamp for Conventional and Islamic Banking

| Field         | Details                                                              |
|---------------|----------------------------------------------------------------------|
| Institution   | AB Bank PLC                                                          |
| Project       | Digital Banking Revamp for Conventional and Islamic Banking          |
| Document Type | Request for Proposal (RFP)                                           |
| Version       | 1.8                                                                  |
| Date          | 05 October 2026                                                      |
| Prepared For  | Digital Banking, Islamic Banking and Information Technology Division |

**Confidentiality Notice:** This document contains confidential information intended for use by invited vendors and the issuing financial institution only. Vendors shall not disclose, reproduce or distribute this document without prior written authorization.

## 1. Introduction

### 1.1 Purpose

This Request for Proposal (RFP) invites qualified vendors to submit technical and commercial proposals for the design, development, integration, implementation, deployment, support and continuous enhancement of a modern digital banking platform for AB Bank PLC, covering Conventional and Islamic banking services across mobile, web, branch-assisted, back-office and kiosk channels.

### 1.2 Background

AB Bank PLC intends to modernize and reposition its digital banking ecosystem to move beyond common banking functions and deliver a differentiated, intelligent and lifestyle-led banking experience. The initiative should increase digital adoption, deepen customer engagement and financial literacy, improve credit accessibility and financial inclusion, strengthen operational controls with enhance security and support secure, scalable and regulatory-compliant services across customer-facing and internal channels.

The Bangladesh financial services market is characterized by high mobile internet penetration, Android-led usage, strong MFS adoption for daily transactions and continued reliance on banks for savings, trust and formal credit. The strategic opportunity for AB Bank is to combine bank-grade trust with MFS-like convenience, contextual intelligence, accessible credit and lifestyle ecosystem integration with modern AI and ML based system and services.

### 1.3 Objectives

- Enhance digital customer experience through intuitive, accessible and consistent mobile and web journeys.
- Enable end-to-end digital banking services including onboarding, account management, fund transfers, bill payments, deposits, loans, card services, service requests and account closure workflows.
- Improve operational efficiency through automated workflows, maker-checker approvals, branch-assisted service delivery, back-office dashboards with insightful report and service request tracking.
- Strengthen security, fraud prevention, access control, auditability, data protection and Bangladesh Bank regulatory compliance.
- Introduce intelligent banking capabilities including AI chatbot, smart financial insights, predictive analytics, personalized offers and AI-based fraud detection.
- Support lifestyle banking features such as merchant offers, loyalty rewards, subscriptions, travel/booking, Bangla QR, NFC/tap-to-pay and partner marketplace integrations where commercially and regulatorily feasible.
- Provide analytics, reporting and campaign management capabilities for customer engagement, product adoption, branch performance and digital channel performance.
- Establish a scalable architecture that supports future fintech partnerships, open APIs, digital product expansion and continuous improvement.

## 2. Scope of Work

### 2.1 Functional Requirements

The proposed solution shall include, but not be limited to, the following functional scope. Vendors must provide a compliance response against each requirement using FC, PC or NC as defined in the attached requirement workbook and response legend.

The functional scope of the Digital Banking Platform is organized into key domains covering conventional and Islamic banking journeys. A concise summary of each domain is provided below. For the full, granular functional requirements and compliance checklist, please refer to the attached requirement workbook.

- **Mobile Banking App:** Comprehensive mobile experience for banking services featuring digital onboarding (NID OCR/Liveness), secure biometric authentication, multi-rail fund transfers (Internal, NPSB, BEFTN, RTGS, MFS, etc.), bill payments, and lifestyle integration.
- **Internet Banking Web App:** A responsive web-based counterpart providing consistent banking journeys, advanced statement management, and secure browser-based access to all core retail, corporate and SME, banking services.
- **Back Office Portal:** Centralized administrative hub for user management (RBAC), customer lifecycle approvals, product management, real-time transaction monitoring, risk configuration, and regulatory reporting.
- **Branch Portal / Assisted Digital Banking:** Specialized interface for branch staff to assist customers with onboarding, complex service requests, and end-to-end digital loan and savings and LC origination workflows.
- **Self-Service Kiosk Portal:** Secure, session-based kiosk interface for independent customer use within branches, supporting onboarding, transfers, and service tracking with automated privacy resets.

### 2.2 Advanced & Lifestyle Banking Features

The platform shall support modern digital and lifestyle banking capabilities, organized into the following functional domains, subject to business prioritization, regulatory approval, and implementation roadmap:

#### Lifestyle, Engagement & Ecosystem

- API-based partner onboarding and in-app marketplace for merchant offers, vouchers, and services such as travel, hotel booking, OTT, and telecom.
- Social and scheduled banking features including bill splitting, request money, recurring payment automation, and streak-based engagement rewards.
- Investment and credit products including digital gold, Smart EMI, Buy Now Pay Later (BNPL) capabilities, and location-based merchant discovery.

- Contactless and digital payments including NFC/tap-to-pay, Bangla QR, and virtual card issuance with personalized cashback and refer-and-earn campaigns.

### **Intelligent Banking & PFM**

- AI-powered virtual assistant and chatbot supporting voice commands for inquiries, transaction guidance, and smart bill capture via OCR.
- Personal Financial Management (PFM) featuring automated spending analysis, budgeting tools, savings goals progress, and a customizable widget-based dashboard.
- Contextual intelligence providing proactive financial tips, salary cycle alerts, and personalized product recommendations based on spending behavior.
- Advanced AI-based fraud detection analyzing device telemetry, behavioral patterns, and abnormal locations to prevent high-risk activity.

### **Data Analytics & Insights**

- Real-time operational dashboards for digital adoption, campaign performance, customer behavior, and branch performance tracking.
- Predictive analytics for churn risk, portfolio health, NPL indicators, and customer segmentation to optimize engagement.
- Compliance-ready reporting and audit dashboards supporting AML monitoring, regulatory activity tracking, and masked data exports.

### **Digital Channels & Experience**

- Omnichannel journey continuity across mobile, web, kiosk, and branch-assisted channels with draft save/resume and status tracking.
- Advanced card controls for instant temporary blocking, unblocking, and limit management.
- Inclusive design featuring multi-language support (Bangla/English), high-contrast modes, senior-friendly interfaces, and WCAG-aligned accessibility.

### **Sustainability & Green Banking**

The platform shall provide an automated carbon footprint estimation tool based on user transaction data. It shall offer contextual tips on reducing environmental impact and suggest "green" investment or savings product alternatives. The platform shall include administrative controls allowing the Bank to manage, update, and configure these tips and product offerings.

### **Financial Well-being**

The platform shall feature a proactive "Nudge Engine" that delivers intelligent, personalized financial health prompts based on predictive analytics.

### **SME & Gig-Economy Support**

The platform shall support a specialized digital dashboard for micro-entrepreneurs and gig workers, enabling separate "Business/Side-Hustle" sub-accounts, digital invoicing, payment link generation, and simplified cash-flow reporting.

## Open Banking & API Ecosystem

The Digital Banking Platform shall natively expose its APIs to support seamless integration with internal and external (third-party) systems. In parallel, the solution must support integration with an independent, enterprise-grade API Management and Gateway platform for centralized control, security, and external exposure.

The solution shall:

- The Digital Banking Platform shall include built-in API Gateway, documentation, and sandbox capabilities to enable rapid implementation of Open Banking services. At the same time, the solution architecture must remain fully gateway-agnostic to ensure future flexibility.
- Vendors are required to:
- Maintain a clear separation between the Service Layer (business logic) and the API Gateway Layer (policy enforcement and exposure).
- Provide comprehensive Open API/Swagger specifications that are independent of any proprietary or vendor-specific gateway formats.
- Clearly describe their approach for migrating API exposure from the platform's native gateway to a future enterprise-grade Central API Gateway, ensuring that such a transition can be accomplished primarily through configuration changes rather than platform re-engineering.

### 2.3 Non-Functional Requirements

| Area            | Minimum Requirement                                                                                                                                                                                                                                                                                   |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Availability    | High availability design with no single point of failure for critical customer-facing services. Vendor shall propose target uptime SLA and maintenance windows.                                                                                                                                       |
| Scalability     | Elastic scaling for mobile/web traffic, campaigns, payment spikes, salary periods and festival transaction peaks.                                                                                                                                                                                     |
| Performance     | Vendor shall provide response-time benchmarks for login, dashboard loading, transfer initiation, bill payment, OTP validation, statement generation and reporting dashboards.                                                                                                                         |
| Security        | End-to-end encryption, MFA, secure session management, transaction PIN, device binding, fraud detection, secure coding, secrets management. Vendor shall provide artifacts for security assessments (e.g., SAST/DAST/SCA) and support the bank's VAPT and SIEM/SOC integration requirements.          |
| Compliance      | Compliance with applicable Bangladesh Bank guidelines circulars and policies such as (but not limited to), ICT Security Policies, ICT Policies, Cloud Computing Policies etc. AML/CFT guidelines and policy requirements, KYC guideline, data privacy and security obligations and internal policies. |
| Audit & Logging | Complete audit trails for customers, branch users, admins, approvals, payments, data changes, API calls and privileged actions.                                                                                                                                                                       |

|                           |                                                                                                                                                                                              |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Usability & Accessibility | Responsive design, Bangla/English support, high-contrast mode, scalable fonts, simplified/senior-friendly UI, screen design suitable for visually impaired users and WCAG-aligned practices. |
| Resilience                | DR-ready deployment, data backup, recovery testing, monitoring, alerting and incident response processes.                                                                                    |
| Maintainability           | Modular architecture, documented APIs, CI/CD readiness, automated test coverage, release management and environment separation.                                                              |

## 2.4 Integration Requirements

| Integration Domain            | Expected Integration Scope                                                                                                                                       |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Core Banking System (CBS)     | Customer/account information, balance, transaction posting, account opening, deposit products, statements, service request status and account closure workflows. |
| Payment Gateways and Switches | NPSB/BEFTN/RTGS or relevant national payment rails, Bangla QR, card payment, card bill payment and interbank transfer integrations as applicable.                |
| MFS Providers                 | bKash, Nagad, Upay, Rocket, Meghna Pay, Mcash, gpay by shamdhan and additional approved MFS/PSO/PSP providers for wallet transfers and beneficiary management.   |
| Card Management System        | Card status, card bill payment, card-to-account transfer, temporary block/unblock, card limits and virtual card capability where supported.                      |
| NID/e-KYC/Liveness            | NID OCR, face verification, liveness detection, AML screening and digital consent/e-signature workflows.                                                         |
| Loan Systems / Credit Scoring | Loan application, eligibility calculator, credit bureau integration, scoring/risk grading, document checklist and disbursement/servicing workflows.              |
| Trade Finance / LC            | LC application capture, document management, validation, workflow queue, maker-checker approvals and status tracking.                                            |
| Notification Services         | SMS, email, push notification, in-app notification, login alerts, payment reminders and campaign messages.                                                       |
| Customer Support              | Chatwoot or equivalent chat/helpdesk, ticketing, callback scheduling and support workflow integration.                                                           |
| Analytics / Data Platform     | Customer behavior analytics, campaign data, adoption metrics, fraud events, reporting exports and BI/dashboard feeds.                                            |
| SIEM / SOC / Security Tools   | Security logs, events, suspicious activity alerts, user/admin activity logs and integration with SIEM/SOC tools.                                                 |
| Third-party Partner APIs      | Merchant offers, subscriptions, travel/booking, OTT, digital marketplace and approved lifestyle ecosystem services.                                              |
| LLM Integration               | For AI automation                                                                                                                                                |

### 3. Technical Requirements

#### 3.1 Architecture

| Ref.  | Requirement                                                                                                                                                                                                                                                                             |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AR-01 | The solution should preferably align with BIAN (Banking Industry Architecture Network) Service Landscape and Service Domains where applicable, and the vendor shall describe the level of alignment in the proposal.                                                                    |
| AR-02 | The preferred architecture shall be microservices-based or modular service-oriented architecture with clear separation of digital channels, orchestration/API layer, integration layer, workflow engine, data layer, event/logging layer and analytics layer.                           |
| AR-03 | The solution shall natively expose APIs while remaining fully gateway-agnostic, enabling seamless use of an external enterprise API Management/Gateway platform for centralized security, throttling, monitoring, sandbox access and lifecycle control.                                 |
| AR-04 | Business services and API management concerns must be clearly separated. The solution shall support standard Open API/Swagger definitions and allow API exposure to shift from the native gateway to an external platform through configuration and integration without re-engineering. |
| AR-05 | The vendor shall provide target architecture, logical architecture, deployment architecture, integration architecture, security architecture, data architecture and end-to-end data flow diagrams.                                                                                      |
| AR-06 | The solution shall support horizontal scaling, stateless service design where applicable, containerization, environment segregation, zero/low-downtime deployments and automated rollback strategy.                                                                                     |
| AR-07 | The platform architecture must be designed to support chaos engineering readiness, including controlled failure testing and graceful handling of service degradation without manual intervention.                                                                                       |

#### 3.2 Deployment Architecture and Environment Setup

| Ref.  | Requirement                                                                                                                                                                                                                                                                      |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DA-01 | The solution shall support cloud-based deployment on Bank-approved local cloud or private cloud infrastructure located within Bangladesh and aligned with applicable Bangladesh Bank circulars, data residency requirements and Bank policy.                                     |
| DA-02 | The proposed solution must support secure and scalable Kubernetes/orchestration-based deployment within the Bank-approved cloud environment.                                                                                                                                     |
| DA-03 | The architecture must support containerized application services, API services, background jobs, database connectivity, ingress controller/API gateway, secrets management, centralized logging, monitoring, autoscaling, backup, disaster recovery and environment segregation. |
| DA-04 | The vendor shall provide and execute a complete environment setup plan covering Development, SIT, UAT, Training where applicable, Pre-Production, Production and Disaster                                                                                                        |

| Ref.  | Requirement                                                                                                                                                                                                                                                                                                                                 |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | Recovery environments. Each environment must be segregated, secured, documented and configured according to Bank IT, security and operational policies.                                                                                                                                                                                     |
| DA-05 | Production deployment must ensure load balancing, fault tolerance, TLS encryption, role-based access control, audit logging, pod/node monitoring, vulnerability management and compliance with Bank security and regulatory requirements.                                                                                                   |
| DA-06 | The vendor must provide Kubernetes/orchestration deployment diagrams, namespace strategy, resource sizing, Helm/YAML manifests, network policies, service exposure model, CI/CD integration, security hardening, image scanning, rollback process, high availability design, blue-green/canary deployment approach and operational runbook. |
| DA-07 | Live production data shall not be used directly in Development, SIT, UAT, Training, Pre-Production or vendor-hosted environments unless the data is masked, anonymized or tokenized according to Bank information security and data privacy requirements.                                                                                   |

### 3.3 Integration and API Standards

| Ref.  | Requirement                                                                                                                                                                                                                                                                                                                  |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IN-01 | The solution shall provide a flexible integration framework capable of securely integrating with the Bank's internal systems and approved external/third-party applications.                                                                                                                                                 |
| IN-02 | Supported integration methods shall include REST/JSON and SOAP APIs, event-based integration, message queues, secure file exchange/SFTP, webhooks, database views where approved and other Bank-approved protocols.                                                                                                          |
| IN-03 | The integration scope shall include, but not be limited to, CBS, payment rails, card systems, MFS providers, e-KYC, NID OCR, liveness detection, AML screening, notification gateways, support/helpdesk systems, analytics platforms, regulatory reporting systems, third-party service providers and approved partner APIs. |
| IN-04 | The solution must be ready for integration with Bangladesh's local payment and financial ecosystem, including NPSB, BEFTN, RTGS, Bangla QR issuer/acquirer flows, Core Banking System, card management system, payment switch, SMS/email gateway, AML/fraud monitoring system and regulatory reporting platforms.            |
| IN-05 | The solution must provide secure REST/JSON APIs with proper versioning, complete documentation, Bank-approved authentication, configurable rate limits and defined SLA for critical APIs covering availability, response time, timeout, throughput and error threshold.                                                      |
| IN-06 | APIs must support secure logging, error handling, idempotency for financial transactions, monitoring, API Gateway integration and sandbox/readiness environment where applicable.                                                                                                                                            |
| IN-07 | The vendor shall identify all integration dependencies, data formats, protocol requirements, security controls, retry logic, reconciliation approach, failure-handling process and monitoring mechanism for each integration.                                                                                                |

### 3.4 Security, Privacy and Fraud Controls

| Ref.  | Requirement                                                                                                                                                                                                                                                                                                                      |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SE-01 | The solution shall provide security controls including MFA, encryption at rest and in transit, secrets management, secure key management, RBAC/ABAC, secure session management, transaction signing/PIN validation and configurable fraud controls.                                                                              |
| SE-02 | All sensitive data, secrets, encryption keys, certificates and credentials must be stored and managed securely using Bank-approved key management practices and must not be hardcoded in application source code, scripts or configuration files.                                                                                |
| SE-03 | The solution shall support Bank security monitoring through SIEM/SOC integration, forwarding security logs, audit trails, API logs, authentication logs, administrative activities, transaction anomalies and system alerts in a mutually agreed structured format.                                                              |
| SE-04 | The vendor shall follow secure SDLC practices including threat modeling where applicable, secure coding standards, code review, security testing, VAPT remediation, vulnerability management and security hardening guidelines.                                                                                                  |
| SE-05 | The vendor must provide a defined cyber incident response process covering detection, escalation, containment, investigation, recovery and post-incident reporting, including response SLA and breach notification timelines agreed with the Bank.                                                                               |
| SE-06 | The vendor must provide a clear fraud liability framework defining responsibility split between the Bank and the vendor for fraud prevention, detection, investigation, reporting and loss recovery.                                                                                                                             |
| SE-07 | The Bank shall remain responsible for business policy decisions, customer approval, transaction authorization rules and final customer communication; the vendor shall be responsible for ensuring the solution operates securely, correctly and in line with agreed controls, configurations, audit trails and SLA commitments. |

### 3.5 Observability, Logging and Audit Trail

| Ref.  | Requirement                                                                                                                                                                                             |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OB-01 | The solution shall provide comprehensive, centralized log management covering system/infrastructure logs, application logs, integration/API logs, transaction logs and security/audit logs.             |
| OB-02 | All logs shall be aggregated to a central log-management platform integrable with the Bank's SIEM, captured in structured machine-readable format with synchronized timestamps through NTP.             |
| OB-03 | Logs shall uniquely identify the originating user, role, session, source IP/device/channel, service/component, request ID, transaction/reference/correlation ID and outcome status wherever applicable. |
| OB-04 | Logs shall be protected against tampering, unauthorized access and deletion through role-based access, integrity controls, retention controls, encryption and administrative audit trails.              |

| Ref.  | Requirement                                                                                                                                                                                                                                                              |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OB-05 | Audit logs shall capture security-relevant and transaction events, including authentication, authorization, privilege changes, configuration changes, privileged/administrative actions, customer-impacting actions and financial transactions.                          |
| OB-06 | Log retention, online searchable availability and long-term archival periods shall be configurable and compliant with Bangladesh Bank ICT Security Guidelines and the Bank's retention policy.                                                                           |
| OB-07 | The vendor shall describe retention tiers, online versus archived availability, archival and retrieval mechanisms, storage encryption and secure disposal of logs at end of life.                                                                                        |
| OB-08 | The solution shall provide full observability through centralized metrics, structured logs, distributed traces, health checks, dashboards, alerting, API monitoring, transaction monitoring and incident correlation using unique transaction/reference/correlation IDs. |

### 3.6 Data Architecture, Governance and Reporting

| Ref.  | Requirement                                                                                                                                                                                                   |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DG-01 | The proposed solution must provide a secure, scalable and well-governed data architecture aligned with the Bank's operational, regulatory, reporting, analytics and future AI/ML requirements.                |
| DG-02 | All data shall remain the property of the Bank. The vendor must not use, copy, transfer, store or process Bank data outside approved environments without prior written approval from the Bank.               |
| DG-03 | The vendor must define data ownership, source-of-truth systems, data flow, logical and physical data model, metadata, data lineage, data quality controls, retention, archival, backup and recovery approach. |
| DG-04 | The solution must support role-based data access, audit trails, data classification, data masking, retention policies and secure data extraction when required by the Bank.                                   |
| DG-05 | The solution should integrate with the Bank's source systems for customer, account, product, branch, user, role, limit, fee and transaction rule data. Duplication of master data should be minimized.        |
| DG-06 | The vendor must clearly identify the source of truth for all key data entities and define how data will be synchronized across systems.                                                                       |
| DG-07 | The solution must support integration with the Bank's data lake, data warehouse, BI, MIS, regulatory reporting, fraud monitoring and analytics platforms.                                                     |
| DG-08 | The solution should support standard data export formats such as CSV, JSON, XML, database views, APIs or other agreed formats.                                                                                |
| DG-09 | Reporting and analytics must not adversely affect production performance. The architecture should support reporting replicas, data marts, scheduled data feeds or other approved approaches.                  |

| Ref.  | Requirement                                                                                                                                                                                                                                              |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DG-10 | Sensitive data must be encrypted at rest and in transit. Sensitive data must be masked, tokenized or anonymized where applicable, especially in non-production environments.                                                                             |
| DG-11 | The solution must support configurable data retention, archival and purging based on the Bank's policy and regulatory requirements.                                                                                                                      |
| DG-12 | The architecture should support future AI, machine learning, personalization, customer segmentation, fraud detection and predictive analytics use cases through clean, structured, governed and accessible data.                                         |
| DG-13 | The proposed solution must support Bangladesh Bank and BFIU regulatory reporting requirements, including applicable CTR, STR, AML/CFT, transaction monitoring, audit and compliance-related reports, within prescribed regulatory timelines and formats. |

### 3.7 Performance, Scalability and Operational KPIs

| Ref.  | Requirement                                                                                                                                                                                                                                              |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PF-01 | The proposed solution must meet minimum performance benchmarks under normal, peak and stress-load conditions. The vendor must validate benchmarks through performance, load, stress and concurrency testing before production go-live.                   |
| PF-02 | The vendor shall define and demonstrate performance benchmarks for login, dashboard loading, fund transfer, bill payment, QR payment, statement generation, report generation, notification delivery, API response and peak-load transaction processing. |
| PF-03 | The vendor must define supported concurrent users, transactions per second, API throughput, queue processing capacity, batch processing windows, timeout thresholds and graceful degradation behavior.                                                   |
| PF-04 | The vendor must define and commit to measurable operational KPIs covering system availability, transaction reliability, performance and stability.                                                                                                       |
| PF-05 | The production system should maintain minimum 99.9% uptime, at least 99% transaction success rate, agreed API/page response latency within SLA and low application crash/error rate across web and mobile channels.                                      |
| PF-06 | Performance test reports, test scripts, test data profile, test environment sizing, bottleneck analysis and remediation evidence shall be submitted before go-live approval.                                                                             |

### 3.8 DevSecOps and CI/CD

| Ref.  | Requirement                                                                                                                                                                                                   |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DS-01 | The proposed solution should preferably support a GitLab-centric DevSecOps and CI/CD process for secure, controlled and auditable software delivery across Dev, SIT, UAT, Pre-Prod, Prod and DR environments. |

| Ref.  | Requirement                                                                                                                                                                                                                                                               |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DS-02 | The vendor must define the branching strategy, merge request approval process, build pipeline, automated testing, code quality checks, security scanning, artifact management, release tagging, deployment approval, rollback process and environment promotion workflow. |
| DS-03 | DevSecOps controls shall include source control, CI/CD pipeline, automated unit testing, integration testing, security testing, code quality gates, SAST, DAST, dependency scanning, container/image scanning, secrets scanning and vulnerability management.             |
| DS-04 | Each deployment shall maintain an auditable trail covering source version, build version, artifact checksum, approval record, deployment date/time, approver, environment, release note and rollback point.                                                               |
| DS-05 | The vendor shall support automated rollback and controlled release strategies such as blue-green, canary or phased deployment where technically applicable.                                                                                                               |

### 3.9 Testing, Acceptance and Go-Live Readiness

| Ref.  | Requirement                                                                                                                                                                                                                         |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TA-01 | The vendor must follow a structured testing and acceptance process covering SIT, UAT, performance testing, security testing, regression testing, DR testing and go-live readiness.                                                  |
| TA-02 | The solution shall be accepted only after all agreed test cases are executed, critical/high defects are resolved, test evidence is submitted and formal sign-off is obtained from the Bank.                                         |
| TA-03 | The vendor must define go-live entry and exit criteria, including business sign-off, technical sign-off, security sign-off, performance readiness, DR readiness, operational readiness, support readiness and rollback readiness.   |
| TA-04 | Test deliverables shall include test strategy, test plan, test cases, test data approach, traceability matrix, defect log, retest evidence, performance report, security test report, DR test evidence and final acceptance report. |
| TA-05 | No production go-live shall proceed with unresolved critical/high defects unless explicitly accepted by the Bank through a documented risk acceptance process.                                                                      |

### 3.10 AI, ML and Agentic Automation Readiness

| Ref.  | Requirement                                                                                                                                                                                                                                                                                  |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AI-01 | The proposed solution should support future AI, ML and agentic automation capabilities for analytics, personalization, fraud detection, customer support, operational automation and decision support.                                                                                       |
| AI-02 | The vendor must clearly describe any AI/ML features, data requirements, model governance, explainability, human approval controls, audit logs, security safeguards and integration readiness with the Bank's data lake, warehouse, API Gateway, CRM, fraud monitoring and reporting systems. |
| AI-03 | Any AI-driven recommendation, automation or decision must be transparent, traceable, monitored and subject to Bank-defined approval, compliance and risk controls.                                                                                                                           |

| Ref.  | Requirement                                                                                                                                                                                                    |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AI-04 | The solution shall not make autonomous financial, customer-impacting or compliance-impacting decisions without Bank-approved rules, human oversight, audit trail, model monitoring and risk-control framework. |

### 3.11 Audit Rights, Compliance and Regulatory Reporting

| Ref.  | Requirement                                                                                                                                                                                                                                                        |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AC-01 | The Bank, its appointed auditors, Bangladesh Bank, BFIU and other authorized regulators shall have the right to audit, inspect, review and assess the vendor's services, systems, processes, controls, records and documentation related to the proposed solution. |
| AC-02 | Audit may be conducted through onsite visit, offsite review, remote access, document submission, interview, evidence review, system walkthrough, log review, vulnerability assessment or compliance assessment.                                                    |
| AC-03 | The solution and vendor operations shall support compliance evidence requirements related to ICT security, information security, audit, AML/CFT, data residency, ISO/IEC 27001, PCI-DSS where applicable, and other regulatory or contractual obligations.         |
| AC-04 | The vendor shall support regulatory reporting, audit evidence extraction, report generation, log retrieval and compliance responses within timelines defined by the Bank and applicable regulators.                                                                |

### 3.12 Documentation, Training and Knowledge Transfer

| Ref.  | Requirement                                                                                                                                                                                                                                                                                   |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DK-01 | The vendor must submit complete, accurate and updated project documentation throughout the project lifecycle.                                                                                                                                                                                 |
| DK-02 | Documentation shall include architecture documents, API specifications, deployment guide, integration guide, operations runbook, administration guide, user guide, security configuration guide, backup/restore guide, troubleshooting guide, DR guide, release notes and training materials. |
| DK-03 | All documents must be provided in editable format such as MS Word, Excel, Visio/draw.io or equivalent, and final signed PDF format where applicable.                                                                                                                                          |
| DK-04 | Documentation shall be considered accepted only after review, required corrections, version control and formal sign-off by the Bank.                                                                                                                                                          |
| DK-05 | The vendor must provide structured knowledge transfer and training to the Bank's business, IT, operations, security and support teams before go-live and during the handover period.                                                                                                          |
| DK-06 | Training must cover functional usage, administration, configuration, integration, reporting, troubleshooting, monitoring, backup/restore, incident handling and basic technical support. Training completion records and materials shall be submitted to the Bank.                            |

## 4. Implementation Plan

### 4.1 Project Timeline

Vendors shall submit a detailed project plan. The following indicative phased roadmap may be used for proposal planning and shall be refined during contract finalization.

| Phase                                             | Indicative Duration | Key Activities                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Phase 0: Mobilization                             | 2 weeks             | Project kickoff, governance setup, team onboarding, access planning, environment planning and detailed discovery.                                                                                                                                                                                      |
| Phase 1: Requirement Validation & Solution Design | 4-6 weeks           | Business requirement workshops, process mapping, architecture, UX journeys, integration design, security design, project backlog finalization, and API Design & Gateway-Agnostic Strategy: Definition of service-to-gateway interface, Open API standard compliance, and enterprise migration roadmap. |
| Phase 2: Core Digital Channels MVP                | 12-16 weeks         | Mobile/web foundational journeys: onboarding, login, account view, account linking, fund transfer, bill payment, recharge, statements, service tracking and notifications.                                                                                                                             |
| Phase 3: Back Office, Branch & Kiosk Enablement   | 10-14 weeks         | Admin portal, branch-assisted flows, kiosk flows, maker-checker, service request workflows, reports and audit trails.                                                                                                                                                                                  |
| Phase 4: Advanced Banking & Integrations          | 12-20 weeks         | Loans, LC workflows, merchant/lifestyle marketplace, AI chatbot, analytics, fraud detection, QR/NFC/virtual card capabilities as prioritized.                                                                                                                                                          |
| Phase 5: Testing, UAT, Security & Compliance      | 6-8 weeks           | SIT, UAT, Pre Prod, regression test, performance testing, VAPT, DR test, compliance review, operational readiness and sign-off.                                                                                                                                                                        |
| Phase 6: Go-Live & Stabilization                  | 4-8 weeks           | Production deployment, migration/cutover, hypercare, issue resolution, monitoring and post-implementation review.                                                                                                                                                                                      |
| Market Roadmap Focus: Phase 1 - Adoption Engine   | 0-6 months          | Prioritize acquisition and usage drivers: BNPL/pay-later readiness, rewards and loyalty, bill splitting/request money, smart push notifications, default account, autofill/quick actions and customizable dashboard.                                                                                   |

|                                                              |              |                                                                                                                                                                               |
|--------------------------------------------------------------|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Market Roadmap Focus:<br>Phase 2 - Engagement Layer          | 6-12 months  | Introduce daily-use and retention capabilities: smart financial insights, subscription management, travel and booking integration, Smart EMI and shared wallet/family wallet. |
| Market Roadmap Focus:<br>Phase 3 - Intelligence & Stickiness | 12-18 months | Introduce AI and ecosystem stickiness: Bangla/voice-led smart financial assistant, credit and growth products, daily-life integration and location-based ecosystem discovery. |

## 4.2 Deliverables

- Inception report and detailed project plan.
- Business Requirement Document (BRD), Functional Specification Document (FSD) and requirement traceability matrix.
- UX/UI design, clickable prototypes and design system for mobile, web, back office, branch and kiosk channels.
- Solution architecture, technical architecture, integration architecture, deployment architecture and security architecture documents.
- Developed and configured digital banking solution, including source code where contractually applicable. Source code ownership, escrow, repository access and handover terms shall be clearly defined in the contract. Source code walkthrough and Knowledge Transfer (KT) workshops shall be conducted.
- Production-ready Android (APK) and iOS (IPA) builds.
- API specifications, integration documents, developer documentation and test stubs/sandboxes.
- Any reusable SDK developed for third-party or partner integration, delivered with API reference documentation, sample code, licensing terms and sandbox access.
- Test strategy, SIT/UAT scripts, test results, defect logs, performance test reports, VAPT closure evidence and security hardening report.
- Data migration/cutover plan, rollback plan, release plan and operational readiness checklist.
- Training materials, user manuals, admin guides, operations runbooks and support knowledge base.
- Production deployment, post-go-live support, warranty support, AMC/SLA documents and final handover.
- API Strategy Document: Comprehensive API Strategy Document detailing the separation of service and gateway layers, ensuring compliance with the Bank's Gateway-Agnostic requirement.
- Enterprise Gateway Migration Roadmap: A clear configuration-based guide on how to migrate API exposure from the platform's native gateway to a central enterprise gateway in the future.
- Open API/Swagger Definitions: Vendor-neutral Open API/Swagger definitions that are decoupled from the platform's native gateway format.

### 4.3 Project Governance

| Governance Layer                 | Expected Responsibility                                                                                            |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Steering Committee               | Executive oversight, strategic decisions, budget approvals, major risk resolution and milestone acceptance.        |
| Project Management Office        | Plan tracking, dependency management, communication, issue/risk registers, change control and reporting.           |
| Business Workstream              | Requirement validation, process ownership, UAT execution, acceptance criteria and business sign-off.               |
| Technology Workstream            | Architecture, integration, environment, infrastructure, DevSecOps, technical standards and deployment readiness.   |
| Security & Compliance Workstream | Security design, regulatory compliance, VAPT, audit evidence, data privacy, AML/CFT alignment and risk acceptance. |
| Operations & Support Workstream  | Operational processes, SLA setup, monitoring, incident management, service desk and training.                      |

Vendors shall submit a communication plan, escalation matrix, RACI matrix, meeting cadence, reporting format, issue/risk management approach and change request process.

### 5. Source code ownership and exit

The complete source code and all Bank-specific customizations developed under this project shall be owned by AB Bank PLC. The vendor shall hand over source, customizations, build and deployment scripts, database schema and scripts, configuration, API and integration specifications, architecture and deployment documents, administration and technical manuals, security configuration, and relevant project artefacts. No proposed proprietary exception may dilute that ownership; list licensed third-party components, licensee terms and replacement options separately.

The vendor should commit code to a Bank-accessible version-controlled repository throughout delivery, provide tagged releases at each milestone and go-live, document reproducible builds and dependencies, conduct code and operations walkthroughs, and assist an agreed exit/transition period. Repository hosting, access controls, cadence, escrow if requested, and transition duration: To be confirmed by the vendor.

### 6. Prototype and local market evidence

At clarification stage, the shortlisted vendor should demonstrate, in a segregated test environment with synthetic or Bank-approved test data, digital onboarding, conventional and Islamic account journeys, an Islamic contract-stage rejection, SSC approval reference, donation journey, transfer and reconciliation, admin controls, audit trace, monitoring and incident suspension. Include architecture and API walkthrough, security configuration, reporting, and ATM flow only if proposed. Bank inputs: approved scenarios, sample APIs and SSC rules; duration, vendor resources, environment and deliverables: To be confirmed by the vendor.

The vendor must provide its Bangladesh legal presence, years operating, employee counts, banking and Islamic deployments, live installations, local PM and technical/support capacity, regulated-sector experience and contactable customer references where permitted. The bidder shall provide appropriate customer consent and supporting evidence for

## 7. Vendor Qualifications

- Company profile including legal entity details, ownership, years of operation, financial stability and local presence/partner arrangement in Bangladesh.
- Relevant experience implementing internet banking, mobile banking, digital onboarding, payment integrations, digital service workflows and regulatory-compliant banking platforms.
- Demonstrated experience with various internal and external system such as CBS, CMS, MFS, payment rails, KYC and AML, SIEM, reporting and analytics etc.
- Certifications and partnerships relevant to security, cloud computing, DevSecOps, database, mobile development, API management and digital banking will be an added advantage..
- Product roadmap, upgrade policy, release cadence, support organization and long-term sustainability model.
- Implementation team CVs for project manager, solution architect, security architect, business analyst, integration lead, mobile/web leads, QA lead and compliance specialist.
- Evidence of secure SDLC, ISO 27001/SOC 2 or equivalent controls, data protection controls and incident response capability.

### 7.1. Support & Maintenance

| Support Area       | Expected Requirement                                                                                                                                             |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Support Model      | 24/7 local on-site and remote support for production incidents, with severity-based coverage for critical, high, medium and low incidents as defined in the SLA. |
| SLA Commitments    | Severity-based response and resolution times; root cause analysis for major incidents; service credits or penalties may be included in contract.                 |
| Issue Resolution   | Clear incident classification, escalation matrix, workaround process, permanent fix process and customer communication protocol.                                 |
| Monitoring         | Application, infrastructure, integration, API, transaction, security and user-experience monitoring.                                                             |
| Release Management | Patch management, version upgrades, release notes, regression testing and deployment approval workflow.                                                          |
| Knowledge Transfer | Training for business, operations, branch, contact center, back office, IT, security and compliance teams.                                                       |
| BCP/DR             | Support for DR drills, backup verification, failover/failback testing and RPO/RTO compliance.                                                                    |

|                        |                                                                                                                 |
|------------------------|-----------------------------------------------------------------------------------------------------------------|
| Continuous Improvement | Enhancement backlog management, change request process, quarterly roadmap review and adoption analytics review. |
|------------------------|-----------------------------------------------------------------------------------------------------------------|

## 8. Evaluation Criteria

Proposals will be evaluated based on the criteria below. Vendors should provide sufficient evidence and references for each criterion.

| Criteria                             | Weight | Evaluation Considerations                                                                                                                                                                                                                                    |
|--------------------------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Functional Fit                       | 25%    | Coverage across mobile, web, back-office, branch, and kiosk channels, including onboarding, payments, deposits, loans, letters of credit, Islamic banking journeys, service tracking, lifestyle features, AI, customer adoption, and market differentiation. |
| Technical Architecture & Integration | 20%    | Scalable, API-first architecture; CBS, payment, MFS, and card integrations; DevSecOps maturity; maintainability; and deployment flexibility.                                                                                                                 |
| Security, Risk & Compliance          | 20%    | Compliance with Bangladesh Bank ICT requirements; robust security architecture; MFA and encryption; audit logging; VAPT; fraud monitoring; data privacy and residency; and AML/CFT support.                                                                  |
| Vendor Experience & Capability       | 15%    | Relevant banking references, proven implementation experience, local support capabilities, project team expertise, certifications, and product maturity.                                                                                                     |
| Implementation Approach              | 10%    | Quality of the project plan, delivery methodology, governance, testing, migration and cutover, change management, and training.                                                                                                                              |
| Commercial Competitiveness           | 10%    | Overall value based on total cost of ownership, transparent licensing and AMC terms, optional module pricing, and contract flexibility.                                                                                                                      |

## 9. Submission Guidelines

### 9.1 Proposal Format

- Executive summary.

- Understanding of requirements and proposed solution overview.
- Detailed functional compliance matrix using FC/PC/NC.
- Technical architecture, integration architecture, security architecture and deployment model.
- Implementation methodology, project plan, governance, team structure and assumptions/dependencies.
- Regulatory, security, data privacy, data residency and audit compliance response.
- Support model, SLA, warranty, AMC and roadmap.
- Vendor qualifications, case studies, references and certifications.
- Commercial proposal in a separately sealed/marked file or section.
- Deviation statement and clarification list.

### **Submission Requirements**

Proposals must be submitted in two separate envelopes:

1. Functional and Technical Proposal
2. Commercial Proposal

### **Submission Schedule**

Proposal submission deadline: 02 November 2026, 4:00 PM

Deadline for submitting queries or requests for clarification: 18 October 2026, 12:00 PM

Clarification response date: 26 October 2026, 4:00 PM

Submit all queries and clarification requests by email to [rfp@abbl.com](mailto:rfp@abbl.com). A soft copy of the Functional and Technical Proposal must also be emailed to [rfp@abbl.com](mailto:rfp@abbl.com) and clearly identify the vendor's name and the designated contact person's name, title, and email address.

Submit hard copies of the Commercial Proposal to the Point of Contact listed in Section 10, "Contact Information."

## **9.2 Commercial proposal in BDT**

The vendor must submit a priced BDT bill of quantities. Every optional, conditional or third-party charge must be flagged and priced separately, and the payable amount must reconcile to one-time, annual and applicable tax lines.

| Cost component                  | CAPEX / OPEX | One-time BDT | Annual BDT | Basis / optionality |
|---------------------------------|--------------|--------------|------------|---------------------|
| Software license                |              |              |            |                     |
| Infrastructure / Cloud Services |              |              |            |                     |

| Cost component                        | CAPEX / OPEX | One-time BDT | Annual BDT | Basis / optionality |
|---------------------------------------|--------------|--------------|------------|---------------------|
| Implementation and project management |              |              |            |                     |
| Subscription                          |              |              |            |                     |
| Customization                         |              |              |            |                     |
| Integration                           |              |              |            |                     |
| Professional services                 |              |              |            |                     |
| Data migration                        |              |              |            |                     |
| Training                              |              |              |            |                     |
| Security and VAPT                     |              |              |            |                     |
| Third-party licensing                 |              |              |            |                     |
| Cloud and infrastructure services     |              |              |            |                     |
| 24x7 local support                    |              |              |            |                     |
| Maintenance and annual maintenance    |              |              |            |                     |
| Other applicable charges              |              |              |            |                     |

| Commercial reconciliation            | Amount (BDT) |
|--------------------------------------|--------------|
| Quoted price before taxes and duties |              |
| VAT                                  |              |
| Tax and withholding treatment        |              |
| Duties and other statutory charges   |              |
| Amount payable by AB Bank PLC        |              |

Price validity, payment milestones tied to M1–M5 acceptance, warranty, annual uplifts, license metrics, volume bands, foreign exchange conversion risk, optional ATM charges, out-of-scope rates, exclusions and assumptions shall be clearly stated by the bidder.

All prices must be quoted in BDT. Commercial proposal and technical proposal must be submitted separately as two separate documents.

## 10. Contact Information

| Item                  | Details                                                                                                                            |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Primary Contact       | Head of Administration                                                                                                             |
| Address               | AB Bank PLC, Corporate Head Office, Skymark, 18 Gulshan Avenue, Dhaka 1212, Bangladesh                                             |
| Clarification Process | All clarification queries must be submitted in writing. Responses may be shared with all participating vendors to ensure fairness. |

## 11. Terms & Conditions

- The Bank reserves the right to accept or reject any proposal, cancel the RFP, modify scope or negotiate with one or more vendors without obligation to award.
- All information shared under this RFP shall be treated as confidential. Vendors shall sign NDA where required.
- Vendor shall comply with applicable laws of the land, regulations, Bangladesh Bank circulars/guidelines and internal policies of the Bank.
- Vendor shall disclose all assumptions, dependencies, exclusions, third-party components and license restrictions.
- The Bank shall retain ownership of its data, configurations, customer information, reports, integrations and custom-developed artifacts as defined in the contract.
- Vendor must support and attend audit, inspection, regulatory review and evidence submission related to the proposed solution.
- Subcontracting shall require prior written approval from the Bank. Vendor remains fully responsible for subcontractor deliverables and compliance.
- Vendor must provide exit support, data export, source/configuration handover where contractually applicable and transition assistance to avoid vendor lock-in.
- Any cloud, offshore support, remote access or data processing arrangement must be explicitly disclosed and approved by the Bank and regulator where applicable.
- The final contract shall include SLA, penalty/service credit, warranty, intellectual property, data protection, breach notification, liability, termination and dispute resolution clauses.

## 12. Regulatory & Compliance Requirements

Vendors must ensure that the proposed solution fully complies with all applicable laws, regulations, circulars and guidelines issued by Bangladesh Bank and other relevant authorities. The solution shall be designed to support internal audit, external audit, regulatory inspection and security review requirements.

## **12.1 Bangladesh Bank Compliance**

- Adherence to Bangladesh Bank ICT Security Guideline requirements applicable to banks and financial organizations, including governance, risk management, information security, operations, outsourcing, business continuity and audit controls.
- Compliance with digital banking, e-KYC, payment systems, AML/CFT, cybersecurity, outsourcing and data/reporting requirements where applicable.
- Support for audit, regulatory reporting, transaction monitoring, suspicious activity reporting and evidence generation.
- Maker-checker controls, segregation of duties, privileged access controls and approval workflows for sensitive operations.
- Vendor shall identify any regulatory approval or notification required for proposed modules such as open banking APIs, partner marketplace, NFC/tap-to-pay, virtual cards, BNPL/pay-later, digital gold/investment, escrow marketplace and cross-border/third-party integrations.

## **12.2 Data Privacy & Protection**

- Customer data confidentiality, privacy-by-design and minimum necessary data collection.
- Consent capture and audit trail for data usage, third-party sharing, marketing, analytics, AI personalization and open API access.
- Role-based access, data masking, encryption, retention policy, data deletion/anonymization where applicable and secure data export controls.
- Breach notification, incident response and forensic support obligations must be documented.
- Training and controls for vendor personnel handling bank or customer information.

## **12.3 Data Residency & Localization**

- All customer, account, transaction, authentication, audit and regulatory data must be stored within Bangladesh unless otherwise approved by the bank and applicable regulator.
- Vendor must provide clear hosting architecture including primary site, DR site, backup location, log location, analytics data location and remote support model.
- Backups, DR replicas and log archives must remain within approved regulatory locations unless explicit written and regulatory approval is obtained.
- Any cloud service provider, SaaS component, AI service, analytics engine or third-party API that processes customer data must be disclosed in the proposal.

## **12.4 Security & Risk Management**

- End-to-end encryption for data at rest and in transit.
- MFA/2FA, biometric support, secure OTP, transaction PIN, device fingerprinting, session control and login alerts.
- Maintain a secure-by-design architecture. Provide artifacts of secure coding and automated testing. Support periodic VAPT and security assessments commissioned by the bank, ensuring readiness to address findings in alignment with agreed remediation timelines.

- Support the bank's security operations by providing hooks and integration capabilities for the bank's SIEM/SOC platforms, enabling real-time monitoring, threat detection, and incident response orchestration.
- Risk controls for lifestyle marketplace, partner APIs, AI features, voice banking, NFC, virtual card and pay-later modules.
- Administrative and branch access shall be tightly controlled, logged and monitored.

### **12.5 Audit & Compliance Reporting**

- Complete audit trails for customer actions, branch-assisted actions, back-office actions, maker-checker approvals, profile changes, user administration, security events and API activity.
- Report generation and export for compliance, internal audit, external audit, Bangladesh Bank reporting and operational management. Report changes and enhancements shall be covered under AMC, subject to the agreed change-control process.
- Immutable or tamper-evident audit logging approach for sensitive events
- Regulatory reports, AML dashboards, suspicious transaction flags, failed transaction analysis and activity tracking must be available to authorized users.

### **12.6 Business Continuity & Disaster Recovery**

- Vendor shall provide a comprehensive BCP and DR architecture framework and operational runbooks, enabling the bank to align with regulatory requirements. The vendor shall provide technical support and configuration assistance during the bank's execution of DR drills and failover/failback procedures.
- Defined RPO/RTO for critical services, databases, integration queues, logs and reporting services.
- Periodic DR drills, backup restoration tests, failover/failback testing and evidence reports.
- Operational runbooks for major incident, cyber incident, payment switch outage, CBS downtime, MFS outage, notification failure and data synchronization issues.
- Graceful degradation strategy for non-critical modules and customer communication during service disruptions.

Detailed functional, technical and general requirements have been mentioned in the attached Microsoft Excel workbook file. Meeting the requirements mentioned in the said workbook is mandatory for all bidding vendors.