REQUEST FOR PROPOSAL (RFP)

# Core Banking System Infrastructure and Cloud-Native Platform Upgrade

Generic, vendor-neutral technical specification, evaluation and bill of quantities

| Item | Detail |
|---|---|
| RFP reference | RFP-CBS-INFRA-2026 |
| Issued by | The Premier Bank PLC, Information Technology Division, Head Office, Dhaka |
| Document | Master tender document: technical specification, evaluation criteria and bill of quantities |
| Environments | Production Data Centre (DC) & Disaster Recovery (DR) |
| Price basis | All prices shall be quoted in BDT, inclusive of applicable taxes, VAT, and duties, and shall include three (3) years of support.<br>Bidders shall also provide indicative renewal prices for Years 4 and 5, which shall be for reference only. |
| Bid Submission | Oracle Database Appliance (ODA) may be proposed separately. The remaining solution components shall be offered as a complete package. Bidders may submit proposals for (i) the complete solution, (ii) ODA only, or (iii) the complete solution excluding ODA.<br><br>Partial proposals covering only selected components of the remaining solution shall not be accepted. |
| Classification | Confidential. Issued to invited Bidders for this RFP only. |

## Document control

| Issue | Date | Prepared by | Description |
|---|---|---|---|
| 1.0 | November 2026 | Information Technology Division, Infrastructure Unit | Issued with the RFP |

| Role | Name | Designation | Signature / date |
|---|---|---|---|
| Prepared by | Foiz Mohammed Rashed | Head of IT Infrastructure | Rashed 12.11.26 |
| | Motashim Billah | Database Administrator | 12.11.2026 |
| Approved by | Abu Md. Sabbir Hassan Chowdhury | Head of Information Technology Division | 12.11.26 |

# Table of Contents

## Contents

**1. Introduction** ..... **3**
1.1 Purpose ..... 3
1.2 Objectives ..... 3
1.3 Brand and platform neutrality ..... 3
1.4 How to respond ..... 3
**2. Scope, Environments and Sizing Basis** ..... **3**
2.1 Environments and minimum servers [Applications, Database and Storage] ..... 3
2.2 Bank volumetrics ..... 4
2.3 Availability and resilience ..... 5
2.4 Recovery Objectives ..... 5
**3. General Requirements** ..... **5**
**4. Technical Specification** ..... **5**
4.1 Database tier: Oracle Database on ODA ..... 5
4.2 Compute servers and storage (cloud-native platform nodes) ..... 6
4.3 Operating system and cloud-native platform ..... 6
4.4 Environmental software (Equivalent commercial or Community version with managed service) ..... 7
4.5 Network ..... 8
4.6 Security tooling and observability ..... 8
**5. Microservice and service-to-service protection** ..... **9**
**6. Pod, container and node protection** ..... **9**
**7. Data protection & Backup** ..... **10**
**8. Monitoring, detection and response** ..... **10**
**9. Licensing, Warranty and Commercial Terms** ..... **10**
**10. FAR DR PROVISION** ..... **11**
**11 Services** ..... **11**
11.1 Implementation and microservices onboarding ..... 11
11.2 Training ..... 11
11.3 Comprehensive support and maintenance (3 years) ..... 12
**12. Bidder Qualification** ..... **12**
**13. Evaluation and Selection** ..... **13**
13.1 Evaluation steps ..... 13
13.2 Technical scoring ..... 13
13.3 Financial evaluation and award ..... 14
**14. Bill of Quantities and format** ..... **14**

# 1. Introduction

## 1.1 Purpose

The Premier Bank PLC (the Bank) invites proposals from qualified system integrators to supply, install, commission, support and train its staff on the infrastructure that will host an upgraded Core Banking System (CBS) and its channel and integration services. The scope covers hardware, operating systems, middleware and environmental software for the Production Data Centre (DC), the Disaster Recovery site (DR) and the Testing / UAT environment.

The database tier is fixed: Oracle Database on Oracle Database Appliance (ODA). All other tiers are specified by function and capacity, so any supplier that meets the requirements may bid.

## 1.2 Objectives

- The proposed CBS shall support deployment on enterprise-grade, scalable, and highly available physical, virtualized, HCI, containerized, or cloud-native infrastructure, with centralized management, automated deployment, and controlled release mechanisms.
- Recover production at DR by operator-initiated failover within the recovery objectives in Section 2.4.
- Keep all data, logs, backups and secrets on Bank-controlled infrastructure in Bangladesh, and operate fully without an Internet connection.
- Support compliance with the Bangladesh Bank ICT Security Guideline, PCI DSS and ISO/IEC 27001.
- Protect microservices, pods and data inside the platform while keeping the Bank's MZ–DMZ firewalls, zoning and load balancers as the control point (Section 5 ,6) .

## 1.3 Brand and platform neutrality

Product names mentioned in this document (e.g., Redis, Kafka, Nexus, MinIO, Vault, etc.) are indicative only and represent the required functionality, API or protocol compatibility. Bidders may propose OEM-licensed, commercially supported, community/open-source or hybrid (OEM + Community) solutions, provided they ensure **three (3) years of managed services, technical support, maintenance and knowledge transfer** with full responsibility for solution performance, security, and operational continuity.

A Bidder whose product deviates from a requirement shall state the deviation and the equivalent it offers. The Bank will not favor any supplier, platform or brand.

## 1.4 How to respond

- Answer every numbered requirement with C (comply), PC (partially comply) or NC (not comply) and give verifiable evidence: OEM datasheet and section, a documentation link or a demonstration. A "C" without evidence is scored as NC.
- M = mandatory; D = desirable. Any NC, or any PC that is not justified, on an M requirement makes the bid technically non-responsive.
- Every figure is the Bank's minimum. Bidders may offer more and shall state the offered value.
- Attach OEM authorization letters for all hardware and software, the platform vendor's hardware compatibility statement, and the OEM sizing reports requested in this document.

# 2. Scope, Environments and Sizing Basis

## 2.1 Environments and minimum servers [Applications, Database and Storage]

The Bank will operate the proposed solutions across two sites: the Data Center (DC) and Disaster Recovery (DR). The UAT environment shall be hosted at the DC, and DR failover shall be manually initiated by authorized personnel, without automatic site-level failover.

**Application Servers Sizing:**

| Environment | Minimum servers | Physical cores (Usable) | Platform Topology |
|---|---|---|---|
| DC (primary, active) | 5 | 480 | The proposed solution shall comprise a minimum of five (5) nodes or equivalent infrastructure capacity, ensuring full production workload availability under N+1 redundancy during a single-node failure or maintenance. The architecture shall support virtual machines (VMs) or containerized workloads or combining both through an integrated, scalable, and highly available infrastructure platform, without mandating any specific technology or OEM. |
| DR (passive) | 3 | 288 | The architecture shall support virtual machines (VMs) or containerized workloads or combining both through an integrated, scalable, and highly available infrastructure platform, without mandating any specific technology or OEM. |
| Test / UAT | 1 | 96 | Single-node, no HA. |
| **Total** | **9** | **864** | Each server: 2 sockets, 96 physical cores,1 TB memory. (Minimum) |

The server counts above are minimums. A Bidder shall offer more servers wherever its sizing, the CBS vendor's guide or the N+1 requirement needs them, at no extra cost to the Bank. A Bidder proposing a different architecture may offer equivalent capacity if it meets the same performance, resilience and failure-tolerance targets and attaches the OEM sizing report.

**Applications/Others Storage Sizing:**

| Description | DC | DR |
|---|---|---|
| Usable NVMe per site (Minimum) | 45 TB | 45 TB |
| Usable storage (S3/ NAS/SAN/equivalent or software-defined storage compatible) (Minimum) | 30 TB | 30 TB |

The proposed solution shall provide a minimum aggregate capacity storage across both DC and DR sites, deployable through dedicated storage systems, integrated cluster-node storage or equivalent enterprise-grade storage architecture, ensuring high availability, performance and redundancy.

Bidders size every tier from the volumetrics, state their assumptions and confirm that the offered capacity meets the CBS vendor's sizing guide. Capacity needed beyond the minimums to meet it is supplied at no extra cost to the Bank.

**Database Servers and storage Sizing:**

| Environment | Minimum servers | Physical cores/RAM | Storage |
|---|---|---|---|
| DC (primary, active, HA) | Oracle Database Appliance HA | Total Core 128 & Total RAM 3 TB | 138 TB raw SSD |
| DR | Oracle Database Appliance HA | Total Core 128 & Total RAM 2 TB | 46 TB raw SSD + 396 TB raw HDD |

## 2.2 Bank volumetrics

| Parameter | Value |
|---|---|
| Active customers | 2,500,000 (25 lakh) |
| Branches and sub-branches | 500, nationwide |
| Growth over the contract term | 30% per year (planning figure) for storage, memory and throughput |
| Peak TPS, batch window, database size and change rate, cache dataset, message volumes, log volume, DC–DR link | Released at the pre-bid meeting by addendum. |

### 2.3 Availability and resilience

Production at the DC shall be designed for at least 99.95% monthly availability, excluding agreed maintenance windows. Loss of one server, disk, network card, switch, controller or power feed shall not interrupt service.

### 2.4 Recovery Objectives

| Objective | Target |
|---|---|
| RPO, persistent volumes and VM data | 0-15 minutes. |
| RTO, production CBS cluster at DR (running at 60% capacity) | 4 hours or better |
| RTO, management plane | 2 hours or better |
| Database tier RPO / RTO | Near-zero |

## 3. General Requirements

| ID | Requirement | Type |
|---|---|---|
| G-01 | One accountable Bidder acts as single point of contact for all lots and owns every incident end to end, including OEM coordination. | M |
| G-02 | Every component shall install, run, upgrade and stay licensed with no Internet connection, using the Bank's private registry and repositories as the only artifact source. No mandatory telemetry, call-home or online license activation. | M |
| G-03 | All data, metadata, logs, metrics, backups and secrets stay on Bank infrastructure in Bangladesh. No SaaS component may be required. | M |
| G-04 | Orchestration shall be CNCF-certified Kubernetes conformant with a published vendor lifecycle. No end-of-life shall be announced within 24 months of go-live; each release is supported for at least 12 months. | M |
| G-05 | Rolling upgrades of OS, platform and middleware with pre-upgrade checks and rollback or a documented recovery procedure, without service interruption. | M |
| G-06 | Platform administration shall be accessible through REST APIs and/or CLI, while cluster and application configurations preferable declaratively through GitOps. | M |
| G-07 | Support for OCI, CSI, CNI, Kubernetes Ingress and Gateway API, OpenTelemetry, OIDC, SAML 2.0, X.509 PKI, TLS 1.2/1.3, and syslog and/or CEF standards. | M |
| G-08 | The proposed platform and operating system shall support FIPS 140-2 and/or FIPS 140-3 validated cryptographic modules operating in an approved configuration. The Bidder shall provide applicable CMVP certificate details and evidence of compatibility with the proposed software versions. Modules undergoing validation may be proposed with documented status and prior certification evidence, subject to the Bank's acceptance. | M |
| G-09 | Control-mapping statement to the Bangladesh Bank ICT Security Guideline (current version), PCI DSS v4.0.1 and ISO/IEC 27001:2022. | M |
| G-10 | NTP synchronization with the Bank's sources; logs and dashboards in Asia/Dhaka time. | M |
| G-11 | Hardware shall be on the certified hardware lists of the offered platform and OS vendors. | M |

## 4. Technical Specification

### 4.1 Database tier: Oracle Database on ODA

The proposed solution shall include Oracle Database Appliance (ODA) in a High Availability (HA) configuration at both Data Center (DC) and Disaster Recovery (DR) sites. Oracle Real Application Clusters (RAC) shall be implemented both at the DC & DR. Database replication and synchronization between DC and DR through Oracle Data Guard to ensure data consistency, business continuity and disaster recovery readiness.

| ID | Requirement | Type |
|---|---|---|
| DB-01 | Integrated, pre-built Oracle Database Appliance supplied and supported by the database vendor: two server nodes and shared storage per system. | M |

| ID | Requirement | Type |
|---|---|---|
| DB-02 | Per node: 2 x 64-bit x86 processors with at least 32 cores each (128 cores per system), 2.6 GHz base or higher; at least 1.5 TB memory per node (DC), 1 TB memory per node (DR) expandable without replacing modules. | M |
| DB-03 | Capacity-on-demand licensing of processor cores: the Bank enables and licenses only the cores it needs and adds cores later without hardware change. | M |
| DB-04 | Storage: DC all-flash, at least 138 TB raw (at least 36 TB usable after ASM mirroring, expandable to 70 TB without downtime); DR at least 46 TB flash plus 396 TB HDD raw. Encrypted at rest; no single point of failure. | M |
| DB-05 | Per node: 2 x quad-port 10GBase-T and 1 x dual-port 10/25 GbE SFP28, with transceivers for the Bank's switches. | M |
| DB-06 | Vendor patch bundles at least once a year; access through the Bank's privileged access management; monitoring and logs to the Bank NOC and SIEM. | M |
| DB-07 | Three years of support from acceptance: 24x7, Severity 1 response within 1-hour, on-site parts within 4 hours at DC and next business day at DR; spares held in Bangladesh. | M |
| DB-08 | Hands-on training (RAC, Data Guard, RMAN, appliance administration), at least 5 days for 4 participants, with exam vouchers where available. | M |

## 4.2 Compute servers and storage (cloud-native platform nodes)

**The configuration is the minimum per node; Bidders may offer more or equivalent.**

| ID | Requirement | Type |
|---|---|---|
| SV-01 | Minimum 2U rack-mount enterprise server equipped with two (2) Intel Xeon 6 processors or equivalent AMD EPYC processors, providing at least 96 physical cores per server, a base clock speed of 2.5 GHz or higher, and a minimum L3 cache of 144 MB per processor. The server architecture shall support future processor upgrades or additions through an OEM-supported, compatible chipset and motherboard design. | M |
| SV-02 | Minimum 1 TB DDR5 RAM per server with all memory channels populated for full bandwidth, expandable in place to at least 2 TB without replacing installed modules | M |
| SV-03 | Controller/Boot: Hardware RAID controller with appropriate cache and data protection features, where applicable. Provide 2 × 480 GB or higher enterprise-grade NVMe boot drives configured in RAID 1 or equivalent redundancy. | M |
| SV-04 | Network: 1 x 4-port 1 GbE Base-T + 10GbE x 4 Copper Ethernet /RJ45 + 2 x 2-port 10/25 GbE SFP28 (four 25 GbE ports) with 25 GbE SR transceivers<br>*(Bidders may propose an alternative port configuration based on their proposed solution, technical architecture, and compatibility with the Bank's existing network infrastructure, provided that the overall performance and connectivity)* | M |
| SV-05 | Redundant hot-plug Titanium-class PSUs and fans; one free full-height PCIe 5.0 x16 slot; out-of-band port with enterprise license (virtual console, virtual media, Redfish); TPM 2.0, secure boot, silicon-based or equivalent hardware-anchored root of trust, signed firmware, secure erase; OEM management console with staged firmware baselines (three-year license). | M |
| SV-06 | Bastions: 1U, minimum 2 x 12-core, 128 GB, 4 x 2.4 TB SAS in hardware RAID, 2 x 25 GbE, redundant PSUs, certified for the offered enterprise Linux. [Optional, if required for proposed solution] | Optional |
| SV-07 | Minimum Usable storage: Separate Storage or Cluster Node -<br>• NVMe – 45 TB (Both DC & DR each)<br>• S3/ NAS/SAN/equivalent or software-defined storage compatible – 30 TB<br><br>Capacities are usable after all protection and replication overhead. Any additional storage required for DC-DR replication or data protection shall be declared by the OEM and provisioned by the Bidder (Section 2.1). | M |
| SV-08 | Three years of OEM warranty from acceptance: 24x7x365, parts and labour, 4-hour on-site, keep-your-drive, in-country spares depot (address stated). | M |

## 4.3 Operating system and cloud-native platform

| ID | Requirement | Type |
|---|---|---|
| PL-01 | The proposed solution shall support enterprise-grade operating systems, virtualization, container orchestration or equivalent infrastructure platforms, with appropriate licensing and 24×7 technical support covering all DC, DR and UAT environments for three (3) years. | M |

| ID | Requirement | Type |
|---|---|---|
| PL-02 | The solution shall provide secure, hardened and supported enterprise operating systems for applicable physical servers, virtual machines and management components, including security patching, vulnerability remediation and applicable industry-standard security configurations. | M |
| PL-03 | The solution shall support highly available production infrastructure at DC, resilient DR infrastructure and a dedicated UAT environment, with centralized provisioning, lifecycle management and offline installation and upgrade capabilities. | M |
| PL-04 | The solution shall provide centralized infrastructure and workload management across DC, DR and UAT, including configuration management, policy enforcement, monitoring, compliance reporting, and management recovery capabilities. | M |
| PL-05 | The solution shall provide secure software repositories or container registries, as applicable, supporting vulnerability scanning, software integrity verification, controlled distribution, offline operation and replication or recovery between DC and DR. | M |
| PL-06 | The solution shall support standardized application deployment, configuration management, version control, automated or controlled release processes and configuration-drift detection through CI/CD, GitOps or equivalent enterprise deployment mechanisms. | M |
| PL-07 | The solution shall support secure network connectivity, segmentation, access policies, encrypted communication, ingress/egress traffic control, load balancing and service-to-service protection through integrated or equivalent networking and security technologies. | M |
| PL-08 | The solution shall provide secure workload isolation, resource quotas, role-based access control (RBAC), audit logging, and centralized authentication with integration to enterprise identity services such as LDAP, Active Directory, or OIDC, as applicable. | M |
| PL-09 | The solution shall support security compliance assessment, vulnerability scanning, file-integrity monitoring, and secure software distribution, aligned with applicable CIS, NIST, PCI DSS and other recognized security standards. | M |
| PL-10 | The solution shall provide supported and regularly maintained operating system, application runtime, and container base images, where applicable, with security updates, vulnerability remediation and software integrity verification throughout the support period. | M |
| PL-11 | The solution shall support application and workload backup, restoration, snapshots and disaster recovery across physical, virtualized and containerized environments, using enterprise-grade storage and data protection mechanisms. | M |
| PL-12 | The solution should support flexible workload deployment and migration across virtual machines, containers and compatible infrastructure platforms, including workload mobility, live migration or equivalent mechanisms where supported. | D |
| PL-13 | The Bidder shall ensure coordinated lifecycle management, patching, upgrades, integration and technical support for all proposed infrastructure and platform components, including OEM-licensed, community-supported or hybrid solutions, under a single point of accountability for three (3) years. | M |

## 4.4 Environmental software (Equivalent commercial or Community version with managed service)

The proposed solution may include OEM-licensed, commercially supported, community/open-source, or hybrid technologies. All components shall support deployment on compatible physical, virtualized, HCI, or container-based infrastructure, with three (3) years of 24×7 critical-incident support, managed services, maintenance, and knowledge transfer. Components already included in the proposed platform shall be quoted at zero additional license cost.

***Note : Bidders may propose alternative capacity and configurations based on their proposed solution architecture and technical feasibility, subject to meeting the Bank's functional, performance and availability requirements of the below areas**

| ID | Function | Minimum capacity and functional requirements | Type |
|---|---|---|---|
| ES-01 | **In-Memory Cache, Session and Key-Value Store** | Provide a distributed caching, session management, and key-value storage solution with a minimum usable capacity of 100 GB at the Primary DC, equivalent replicated capacity at DR, and 10 GB at UAT. The solution must support high availability, automatic failover, data replication, encryption at rest and in transit, authentication, and compatibility with the CBS application environment. | M |
| ES-02 | **Messaging and Event Streaming** | Provide scalable messaging and event-streaming capabilities supporting minimum 200 MB/s peak and 25 MB/s sustained ingress, with adequate performance headroom. Support message persistence, retention, replication, fault tolerance, secure communication, monitoring, and DC-to-DR synchronization. Equivalent architectures are acceptable with validated sizing. | M |

| ID | Function | Minimum capacity and functional requirements | Type |
|---|---|---|---|
| ES-03 | **Artifact and Package Repository** | Provide centralized management of software packages, container images, application dependencies and deployment artifacts. Support standard repository formats, access control, version management, vulnerability-scanning integration, offline operation, backup and recovery, with HA at DC and recovery capability at DR. | M |
| ES-04 | **Secrets Management and PKI** | Provide centralized, highly available secrets, credentials, encryption-key, and certificate management across DC and DR. Support secure storage, access control, audit logging, certificate lifecycle automation, and integration with the Bank's PKI, HSM, or equivalent key-management infrastructure. | M |
| ES-05 | **Identity, API and CBS-Compatible Middleware** | Provide identity and access management, API management, authentication, authorization, and middleware integration. Support OAuth 2.0, OIDC, SAML 2.0, MFA, and directory integration. Middleware and transaction coordination components shall be compatible with and certified or approved by the CBS vendor, with DC/DR availability and recovery capabilities. | M |
| ES-06 | **DR Automation, Source Control and Deployment Management** | Provide infrastructure and application automation, source-code management, version control, controlled deployment, and disaster recovery operations. Support RBAC, audit logging, security-scanning integration, and operator-initiated DC-to-DR failover and recovery through commercially supported or equivalent open-source tools. | M |

## 4.5 Network

***Note: Bidders may propose an alternative port configuration based on their proposed solution, technical architecture, and compatibility with the Bank's existing network infrastructure, provided that the overall performance and connectivity**

**Tor Switch**

| ID | Requirement | Type |
|---|---|---|
| NW-01 | 48 x 10/25 GbE Copper (RJ45) and at least 4 x 40 GbE QSFP uplinks, non-blocking (Bidder to justify the uplink count from the offered design (Including necessary cables & other accessories) | M |
| NW-02 | Minimum Quantity 4: DC (2), DR (2) (Bidder Can offer as per their proposed solution) | M |
| NW-03 | 03 (Three) years OEM warranty, 24 x 7 x 365, parts and labor | M |

**Management Switch**

| ID | Requirement | Type |
|---|---|---|
| MS-01 | Managed L2, isolated management VLAN for server BMCs, storage, switch and database platform management | M |
| MS-02 | Port guide per switch: Minimum 48 x 1 GbE RJ45 and 4 x 10/25 GbE SFP28 uplinks. | M |
| MS-03 | Out-of-Band (OOB) Management Switch: 02 (Two) — DC 01, DR 01 | M |
| MS-04 | 03 (Three) years OEM warranty, 24 x 7 x 365, parts and labor | M |

**cabling & optics**

| ID | Requirement | Type |
|---|---|---|
| CO-01 | Bidder should assess the accessories as per their solution | M |

## 4.6 Security tooling and observability

Premier Bank PLC – CBS Infrastructure Security & Observability Requirements

| ID | Requirement | Type |
|---|---|---|
| SE-01 | Provide vulnerability scanning across applicable application images, software dependencies, registries, and running workloads, with offline assessment, exception management, SBOM support and software integrity verification. | M |

| ID | Requirement | Type |
|---|---|---|
| SE-02 | Provide security posture assessment, RBAC review, configurable security policies and compliance reporting aligned with applicable CIS, NIST and PCI DSS standards. | M |
| SE-03 | Provide runtime threat detection, behavioral monitoring, alerting and configurable response mechanisms for applicable VM, host and container workloads, using OEM-supported or equivalent technologies. | M |
| SE-04 | Support network segmentation, least-privilege access controls, security-policy management, configuration assessment, and policy validation across applicable workloads and infrastructure. | M |
| SE-05 | Provide centralized security-policy enforcement, role-based access control, audit logging, emergency administrative access, and integration with the Bank's SIEM, SSO and ticketing systems. | M |
| SE-06 | Provide authenticated infrastructure vulnerability assessment across DC and DR, application security testing for UAT, endpoint/workload protection, and software artifact integrity verification. | M |
| SE-07 | Support sensitive-data inspection and protection, including cardholder/account information and web application security controls through integrated or external security solutions. | D |
| OB-01 | Provide centralized infrastructure and application monitoring, alerting, logging and tracing with NOC/SIEM integration, hardware health monitoring, 90-day online log retention and 12-month total retention with immutable archival capability. | M |

## 5 Microservice and service-to-service protection

| ID | Requirement | Type |
|---|---|---|
| MS-01 | The solution shall support default-deny network security policies for inbound and outbound traffic, with centralized policy management, controlled exceptions, and enforcement of baseline security policies across applicable workloads. | M |
| MS-02 | The solution shall support secure service-to-service communication using mutual TLS (mTLS) or equivalent security mechanisms, with centralized certificate management, Bank PKI integration, and automated certificate renewal where applicable. | M |
| MS-03 | The solution shall provide identity-based service authentication and authorization, supporting industry-standard mechanisms such as OAuth 2.0, JWT, workload identity, and centrally managed access policies and credentials. | M |
| MS-04 | The solution shall provide API security controls, including authentication, authorization, rate limiting, request validation, access restrictions, and protection against applicable OWASP API Security Top 10 vulnerabilities through integrated or external security components. | M |
| MS-05 | The solution shall support controlled outbound network access using configurable IP, CIDR, FQDN, or equivalent allow-list mechanisms with centralized monitoring and enforcement of authorized external communications. | M |
| MS-06 | The solution shall support workload resource allocation, utilization limits, isolation, timeout management and failure-handling mechanisms to prevent resource exhaustion and minimize cascading service failures. | M |
| MS-07 | The solution shall prevent exposure of sensitive banking information, including account numbers, cardholder data, passwords, and authentication tokens, through appropriate log masking, data protection, encryption, and access-control mechanisms. | M |

## 6 Pod, container and node protection

| ID | Requirement | Type |
|---|---|---|
| PD-01 | The proposed solution shall enforce secure workload configurations, including least-privilege execution, restricted administrative access, prevention of unauthorized privilege escalation and workload isolation across applicable VM, container and node environments. Exceptions shall require documented approval and audit logging. | M |
| PD-02 | The solution shall support least-privilege access for application and service identities through role-based access control (RBAC), restricted permissions, secure authentication and controlled credential/token management. | M |
| PD-03 | The solution shall support secure software image and workload deployment through trusted repositories, vulnerability scanning, integrity verification and configurable security policies to prevent unauthorized or vulnerable workloads from running in production. | M |
| PD-04 | The solution shall provide runtime security monitoring and protection against unauthorized processes, malicious activities, and suspicious workload behavior, with controlled administrative access and auditable emergency access mechanisms. | M |

| ID | Requirement | Type |
|---|---|---|
| PD-05 | The solution shall provide secure storage, encryption, access control, and lifecycle management of application credentials, secrets, and encryption keys through integrated or external enterprise-grade secrets management solutions. | M |
| PD-06 | The solution shall support hardened operating systems and infrastructure nodes, including applicable CIS or equivalent security benchmarks, access restrictions, security patch management, vulnerability remediation, and cryptographic protection mechanisms. | M |
| PD-07 | The solution shall secure infrastructure management and orchestration components through authenticated access, least-privilege RBAC, audit logging, encrypted communication, secure configuration storage, backup protection, and restricted management-network access. | M |
| PD-08 | The solution should support enhanced workload isolation or sandboxing mechanisms for sensitive or untrusted applications through VM-based, container-based, or equivalent isolation technologies. | D |

## 7 Data protection & Backup

| ID | Requirement | Type |
|---|---|---|
| DP-01 | TLS 1.2 or higher for every path: pod to pod, application to database, DC–DR replication, storage replication and backups. Weak ciphers and protocols disabled. | M |
| DP-02 | Encryption at rest for the database (TDE), persistent volumes, object storage and backups. Keys held in an external KMS or HSM and separated from storage and platform administrators. | M |
| DP-03 | UAT receives masked data only. Production data cloned to UAT is masked before use; production secrets, certificates and identities are never used in UAT; UAT access is separate from production. | M |
| DP-04 | Secure erase or certified destruction of drives and media at repair and decommissioning, with a certificate to the Bank. | M |
| BA-01 | The Bidder shall ensure that the proposed solution is fully compatible with and supports integration with the Veeam Backup & Replication solution, including the provision of 50 appropriate Veeam licenses as part of the proposed scope. | M |

## 8 Monitoring, detection and response

| ID | Requirement | Type |
|---|---|---|
| M-01 | The proposed solution shall support centralized, tamper-evident security and audit logging across infrastructure, virtualization, containers, applications, and management components, as applicable. Logs shall be integrated with the Bank's SIEM through standard protocols, include relevant event identifiers, and be retained for a minimum of 12 months. | M |
| M-02 | The solution shall provide continuous security monitoring, threat detection and alerting for unauthorized access, privilege escalation, suspicious network activities, security-policy violations, credential misuse, and abnormal workload behavior, with integration into the Bank's 24×7 Security Operations Center (SOC). | M |
| DT-01 | The solution shall support incident detection, investigation, containment, recovery and forensic evidence collection for security incidents, including compromised workloads, infrastructure nodes, credentials, and ransomware attacks. Documented incident-response procedures shall be tested at least annually. | M |
| RS-01 | The solution shall provide vulnerability assessment, security patch management and remediation in accordance with the Bank's security policies and agreed SLAs. Critical vulnerabilities shall be mitigated within seven (7) days of an available fix. Vulnerability assessment and penetration testing shall be conducted before go-live and annually thereafter, with remediation of identified solution-related vulnerabilities at no additional cost to the Bank. | M |
| RS-02 | Equivalent security monitoring, protection, and compliance controls shall be implemented across DC, DR and UAT environments, as applicable. Quarterly compliance evidence shall be provided against Bangladesh Bank ICT Security Guidelines, PCI DSS, and applicable Bank policies, with appropriate access for internal audit and compliance teams. | M |

# 9. Licensing, Warranty and Commercial Terms

- **Term:** The support and maintenance period shall be three (3) years, commencing from the respective software go-live date and hardware installation completion/acceptance date, as applicable. Bidders must

separately quote indicative annual renewal prices for Year 4 and Year 5, including all applicable support, maintenance, AMC, taxes and duties.

- Prices: All prices shall be quoted in BDT, inclusive of applicable taxes, VAT, and duties, and shall include three (3) years of support. Bidders shall also provide indicative renewal prices for Years 4 and 5, which shall be for reference only
- Registration: every subscription and support entitlement is registered in the Bank's name in each OEM portal within 15 days of delivery, with the Bank's named administrators as owners. OEM authorization letters are mandatory for every OEM-licensed or commercially supported product.
- Warranty: each lot carries its OEM warranty or subscription support; the comprehensive support contract (Section 10.3) complements and does not replace it.

# 10. FAR DR PROVISION

The proposed solution shall support future deployment at a Far Disaster Recovery (Far DR) site using the Bank's existing hardware infrastructure, including the installation and configuration of both the CBS application and Oracle CBS database, without any additional software licensing costs. The Bidder shall provide all necessary installation, configuration, integration, and deployment support for the Far DR site.

# 11 Services

## 11.1 Implementation and microservices onboarding

The implementation shall be carried out in coordination with the CBS vendor, who will be responsible for providing application code, functional modifications, and necessary application-level certification.

The scope of implementation shall include:

- Installation and Deployment: Installation, rack and stack, 72-hour burn-in testing, and air-gapped deployment of the DC, DR, and UAT clusters.
- Platform Implementation: Architecture and design, containerization using supported base images, environment-specific Helm and GitOps repositories, and implementation of CI/CD pipelines.
- Security and Integration: Integration of middleware, security scanning, secret detection, SBOM generation, image signing, vulnerability assessment, observability, and platform hardening.
- Performance and DR Testing: Performance testing based on the Bank's expected peak TPS, application-level DR testing, and validation of measured RPO/RTO with DR operating at 60% of the primary capacity.
- Documentation and Knowledge Transfer: Preparation of technical documentation and necessary knowledge transfer sessions, with at least five handover sessions for each relevant technical area.
- Cutover and Post-Implementation Support: Production cutover and eight weeks of on-site hypercare support.

Indicative Implementation Timeline:

| Implementation Phase | Duration |
|---|---|
| Architecture and Design | 4 weeks |
| Containerization and CI/CD Pipelines | 8–10 weeks |
| Middleware and Application Integration | 6 weeks |
| Testing and Validation | 6 weeks |
| Production Cutover and Hypercare | 8 weeks |

Commercial and Resource Requirements:

- Implementation costs shall be quoted on a fixed-price, milestone-based basis.
- Separate man-day rates shall be provided for additional requirements and change requests.
- Key implementation engineers must hold valid Kubernetes-related certifications, and their CVs must be submitted for the Bank's review.
- Replacement of any approved key resource shall require prior approval from the Bank.

## 11.2 Training

The vendor shall arrange professional training for minimum 10 Bank participants in each of the following training areas, with the specified duration:

1. Platform Administration: 8 days.
2. Application Development: 8 days.
3. Multi-Cluster Management and Container Security: 5 days.
4. Registry, GitOps and CI/CD Pipelines: 3 days.
5. Service Mesh: 2 days.
6. Event Streaming: 4 days.
7. In-Memory Data Store: 2 days.
8. Identity and Access Management: 2 days.
9. API Management: 2 days.
10. Secrets Management and Public Key Infrastructure (PKI): 2 days.
11. CI/CD and DevSecOps Tools: 3 days.
12. Automation Platform: 4 days.
13. Observability and Monitoring: 2 days.
14. Disaster Recovery (DR) Runbooks and Drills: 2 days.
15. Microservices Patterns, Transactions and Workflow Management: 4 days.

Training Delivery and Other Requirements:

- Training shall be conducted in person within Bangladesh, at a location to be determined by the Bank after the contract award.
- All training sessions shall be delivered by certified and experienced instructors.
- Comprehensive course materials and relevant technical documentation shall be provided to all participants.

Commercial Requirement: The vendor shall quote a consolidated fixed price covering all training programs, including instructors, course materials, laboratory access, examination vouchers (where applicable), and repeat training arrangements. The pricing shall remain the same irrespective of the selected training delivery mode.

### 11.3 Comprehensive support and maintenance (3 years)

| Severity | Definition | Response | Restore | Resolution |
|---|---|---|---|---|
| 1 Critical | Production down at DC or DR, data loss, active security incident | 15 min; on site within 2 hours (24x7x365) | 4 hours | 24 hours; RCA in 5 business days |
| 2 High | Major degradation, loss of HA or DC–DR replication | 30 min; on site within 4 hours | 8 hours | 3 calendar days |
| 3 Medium | Limited impact with workaround; any UAT issue | 4 business hours | 2 business days | 10 business days |
| 4 Low | Information request, documentation, minor defect | 1 business day | n/a | 20 business days |

- **Preventive work:** Half yearly health checks with written reports; CVE assessment (critical vulnerabilities assessed within 1 business day and mitigated within 7 days of a fix); UAT-first patching; free parts replacement; support for one DR drill per year; monthly service report by the 7th working day and a quarterly service review.
- Service credits: 5% of the quarterly fee per missed Severity 1 target, 2% per missed Severity 2 target, 1% when Severity 3 / 4 compliance falls below 95%, and 2% per missed preventive visit or DR drill; capped at 20% of the quarterly fee. Three or more Severity 1 breaches in a quarter may be treated as material breach.
- **Commercial basis:** a fixed annual fee for each of the three years, quoted separately.

## 12. Bidder Qualification

The Bidder must meet the following minimum eligibility requirements:

1. Company Experience: Minimum five (5) years of business operation with at least five (5) years of proven experience in the banking and financial services sector.

2. Legal Documents: Valid Trade License, Certificate of Incorporation, e-TIN, VAT/BIN Registration Certificate and applicable Tax Return Submission Acknowledgement.

3. Financial Capability: Audited financial statements and annual turnover for the last three (3) consecutive financial years.

4. Relevant Project Experience:

- At least one (1) successfully completed Cloud-Native, Kubernetes/Container Platform, Microservices, or comparable enterprise infrastructure implementation project within the last five (5) years, preferably in the banking or financial sector.
- At least one successfully completed Oracle Database Appliance (ODA) deployment and implementation project within the last five years is required, preferably in the banking or financial services sector.

5. OEM Authorization: Valid OEM partnership and authorization letters for all proposed OEM-licensed hardware and software products.

6. Technical Certification: At least two (2) full-time certified technical engineers on the Bidder's payroll for the proposed solutions, supported by CVs and valid certifications.

7. Implementation Capability: Proven experience in enterprise infrastructure deployment, virtualization, containerization, system integration, migration, and DC/DR implementation.

8. Local Technical Support: Availability of qualified technical resources and a dedicated support team in Bangladesh.

9. OEM and Open-Source Support: OEM support commitments for commercial products and a formal support undertaking for all proposed community or open-source components.

10. Support Commitment: Capability to provide 24×7 technical support, maintenance, security updates, and SLA-based services throughout the contracted support period.

11. Project References: Submission of relevant work orders, completion certificates, client references, and supporting evidence of previous projects.

13. Regulatory Compliance: Compliance with applicable Bangladesh Bank guidelines, information security requirements, and the Bank's internal policies.

14.General Eligibility: The Bidder must have a minimum of five (5) years of relevant experience in the banking and financial services sector and must not be blacklisted, debarred, insolvent, or subject to any conflict of interest that may affect the execution of the project.

# 13. Evaluation and Selection

## 13.1 Evaluation steps

1. **Administrative eligibility** (pass / fail): complete documents, bid security, OEM authorizations, legal standing.
2. **Mandatory technical gates** (pass / fail): every M requirement in Sections 3 to 8 answered C with evidence, or PC with a justified equivalent accepted by the Bank.
3. Technical Evaluation: **Bids obtaining a technical score of less than 70 marks shall be disqualified.**
4. Financial Evaluation: Financial proposals of only technically qualified bidders shall be evaluated.
5. Contract Award: The contract shall be awarded to the bidder achieving the highest evaluated combined technical and financial score, subject to fulfilling all eligibility requirements and the Bank's approval.

## 13.2 Technical scoring

| Criterion | Points | Evaluation focus |
|---|---|---|
| A. Architecture and solution fit | 20 | Quality of the high-level design, DC–DR alignment, N+1 proof at 100 / 60 / 40%, storage and database integration. |
| B. Capabilities beyond the minimum | 10 | Desirable requirements met, scored proportionally. |
| C. Security and compliance | 10 | Zero-trust enforcement, depth of controls, alignment with the Bangladesh Bank guideline and PCI DSS. |
| D. OEM support and lifecycle | 10 | Published lifecycle, in-country support presence, regulated-sector references. No analyst-ranking points. |
| E. Bidder capability and local track record | 15 | Comparable deployments in Bangladesh, certified engineers, support center. |

| Criterion | Points | Evaluation focus |
|---|---|---|
| F. Implementation approach | 10 | Phased onboarding, risk plan, cut-over and rollback. |
| G. Support and service model | 10 | SLA commitments, escalation, staffing, knowledge-transfer plan. |
| H. Proof of concept | 10 | Points earned in scored scenarios divided by points available, times 10. |
| I. Training and documentation | 5 | Syllabus, lab access, sample operational documents. |
| **Total** | **100** | |

### 13.3 Financial evaluation and award

The Bank uses quality-and-cost-based selection with a technical weight of 70% and a financial weight of 30%:

The evaluated price is the grand total of the Bill of Quantities excluding options, inclusive of all taxes, VAT and duties. The Bidder with the highest combined score is recommended for award.

## 14. Bill of Quantities and format

Bidders shall complete the following schedule in BDT, inclusive of all applicable taxes, VAT and duties. The quantities and configurations specified in the BoQ represent the Bank's baseline requirements.

**Note: Bidders may propose alternative quantities or configurations based on their proposed solution architecture, technical feasibility, and compatibility with the Bank's existing infrastructure, provided that all functional, performance, capacity, and connectivity requirements are fulfilled. Overhead, additional-provisioning and DC-DR replication capacity supplied under Section 2.1 (Usable capacity basis) shall appear as separate, clearly labelled lines. and justified in the technical proposal.**

| Sl. No. | Item / Component Description | Qty/lot | Unit Price (if Applicable) | Total Product Price | Total 3 Years AMC Price | Total Price |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| | TOTAL | | | | | |

| Sl. No. | Item / Component Description | Qty/lot | Unit Price (if Applicable) | Total Product Price | 1st Years AMC Price | 2nd Years AMC Price | 3rd Years AMC Price | Total Price |
|---|---|---|---|---|---|---|---|---|
| 1 | | | | | | | | |
| 2 | | | | | | | | |
| 3 | | | | | | | | |
| 4 | | | | | | | | |
| | TOTAL | | | | | | | |

| Sl. No. | Item / Component Description | Qty/lot | Unit Price (if Applicable) | 4th Year AMC Price | 5th Year AMC Price |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| | TOTAL | | | | |

**Note: The bidder shall provide pricing in both (i) a bundled three (3)-year package and (ii) a year-by-year pricing breakdown. The AMC prices for Year 4 and Year 5 shall be quoted separately.**