Broad Scope of Work

The Bank intends to select CERT-IN empanelled Information Systems Security Audit firm/organisation to conduct comprehensive Information Systems Security Audit at Bank's DC and DR at Bangalore and Kolkata locations. The bidder has to complete the audit onsite using proven methodologies & tools for conduct of audit. The bidder has to supply all essential tools for audit and bank will only provide support for its utilization/use. The bidder has to suggest the tool to be utilised in the audit and get it approved by the Bank for its utilization.

The bidders selected by the RFP should have expertise in IT and Business understanding related to financial sector. Bidder shall be responsible to complete the allocated job and fulfilling all obligations and providing all deliverables and services required for successful completion of the project. Unless agreed to specifically by the Bank in writing for any changes in the document issued, the bidder responses should comply with the scope of work.

Unless expressly overridden by the specific agreement to be entered into between the Bank and the bidder, the bid document shall be the governing document for arrangement between the Bank and the prospective bidder in terms of this bid documents.

The bidders should take care of submitting the bids properly filled and uploaded on tendering website before closing date and time. Bidders are requested to participate in the tender process according to the time schedule mentioned above.

Scope of Comprehensive IT Audit

1. IT/Digital/Information Security Governance and Management

- IT/Digital/Information Security Policies and Procedures: Review existing IT/Digital/Information Security Policies, procedures, and standards for adequacy.
- IT/Digital/Information Security Organization Structure: Evaluate the structure, roles, and responsibilities within the IT department.
- Performance Metrics: Analyze the KPIs and metrics used to measure IT performance.
- Evaluating Bank's IT/Digital/Information Security Governance structure - which includes powers of various committees viz. IT Strategy Committee of the Board, IT Steering Committee, Information Security Committee (ISC) etc. quality of meeting deliberations, IT expertise at board level, availability of required resources, IT resource management and IT performance management,

- IT Strategy Alignment: Assess alignment of IT strategy with business objectives.
- Review the bank's policies and procedures for managing third-party risk, including vendor selection, due diligence, ongoing monitoring, and exit strategies
- Review of load testing procedures: Check whether the bank conducts performance/ load testing of new applications based on the observed trends in their previously released products.
- Assess the effectiveness of training and awareness programs for IT/Digital governance, information security, and risk management.

2. IT Risk Management

- Risk Assessment: Evaluate the currently identified IT related risks including those related to outsourced systems.
- Risk Mitigation: Evaluate the effectiveness of risk mitigation strategies & provide necessary guidance.

3. Security Management

- Access Controls: Assess the controls for physical and logical access to systems including Implementation of PIM
- Cybersecurity: Evaluate the measures in place to protect against cyber threats.
- Data Encryption: Review data encryption practices for data at rest and in transit.
- Security Monitoring: Check the effectiveness of security monitoring
- Incident Management: Review processes for handling IT incidents, incident reporting, incident response

- Security Operations Centre
  a) Audit of SOC infrastructure/implementation of Security Tools (SIEM, DAM, PIM, NBA, WAF, APT, VAS, etc.)
  b) Audit of SOC Policy/SOP Document, SOC KPI and Metrics.
  c) Cyber SOC (CSOC) has to take in to account proactive monitoring and management, capabilities with sophisticated tools for detection, quick response and backed by data and tools for sound analytic.
  d) Audit of Security Manpower, Training and Knowledge Management.
  e) People Management- Audit of Change Requests submitted for giving access in IT infrastructure including devices, applications
  f) Custom rule review and custom application integration.
  g) Incident reporting and Management.
  h) Security Analysis
  i) Audit of work authorization system between outsource service provider and Bank's team

    j) Access Control, Customer Data Privacy & Confidentiality
    k) Application security testing

4. Compliance

- Regulatory Compliance: Ensure compliance with relevant laws, regulations and Frameworks (e.g., PCI-DSS, ISO 27001, ISO9001, RBI regulation / directions including RBI's Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices dated November 7, 2023, Cert-In, Data Protection Act, IT Act etc.)
- Audit Trails: Review audit trails and logging mechanisms

5. IT Infrastructure

- Audit of IT Assets and its management.
- Network Infrastructure: Audit the design, configuration, and security of the network infrastructure.
- Data Centers: Audit data center operations, including environmental controls and physical security.

Audit to ensure IT Infrastructure compliance with IT / Information Security Policy of Bank and as per Data Centre Standard practices.
An indicative but not exhaustive list of activities is listed below:

a) Data Centre/Disaster Recovery Centre civil and interiors as per submitted layout
b) Adequacy of server space in view of future requirement
c) Access control facility
d) Fire detection and prevention
e) Fire protection system for server rooms
f) Very Early smoke detection /Fire alarm systems for server rooms
g) Water leak detection systems for server rooms
h) Electrical subsystem (main panel, cables, Power Distribution Unit (PDU) and earthing)
i) Review of Electrical Power requirement and availability.
j) UPS systems
k) DG sets and Control of fuel
l) Precision (computer room standard) Air-conditioning systems for server room
m) Air-conditioning system for other relevant areas of DC
n) Building management system software/hardware (should cover Access controls for Passkeys, Compartmentalization, Creation and Review of Logs, Identification and Escort Requirements, Use of Cages / Rooms & others)
o) Closed circuit television system (CCTV) area for monitoring entry/exit points and strategic locations within the server room
p) Structured cabling system for functional areas as per layout
q) Environmental threat protection (Air Purifier, Humidity Control etc.)

r) Review/Audit of operator awareness of physical security breaches
s) Review of safeguards to mitigate risks associated with earthquake and water related threats
t) Verification of Physical Security policy and review of authorization documentation on file for each individual who has card access to the data center.
u) Audit of License verification of all hardware, Software etc. on entry and exit in DC/DR
v) Review of adequacy of physical Security (Guards, arms etc.)

6. Audit of Data Centre, Disaster Recovery Centre (DRC) & Near Site

- Physical security of Data Centre, Disaster Recovery Centre and Near Site
- Access control system
- Fire / flooding / water leakage / gas leakage etc.
- Handling of movement of man /material in /out of DC / DRC
- Air-conditioning of DC / DRC
- Electrical supply to DC/ DRC, Raw power / UPS / Genset
- Surveillance system of DC / DRC
- Redundancy of power level, UPS capacity at DC, DRC
- Physical & environmental controls at DC & DRC
- Assets safeguarding
- Incident handling procedures
- Cyber Incident Response Plan

7. Audit of Database Management System and Data Security

a) Database configuration Audit/review.
b) Adequate Authorization & authentication mechanism
c) Segregation of duties & environment
d) Database integrity control mechanism
e) Data Protection & Privacy mechanism
f) Adequate Logical access controls
g) Use of Data Definition Language (DDL), Data Manipulation Language (DML).
h) Monitoring of log of changes to the Data Definitions.
i) Rotation of duties.
j) Review of controls procedures for sensitive DB passwords.
k) Review of changes to control /parameter files of database
l) Replication between DC, DR, Near DR sites
m) Review of Backup, Recovery & Restoration testing procedures
n) Review of DB links

8. Audit of Network Performance Analysis (NPA):

- Network Performance Audit analysis
- capacity planning analysis,

- LAN/WAN link utilization and quality analysis,
- Existing load pattern for network device and Uplink,
- Congestion area at various topology layer and traffic pattern analysis.

- DMZ demarcation and IP addresses present in DMZ must be identifiable.
- Review of Firewall rules as per security policy utilizing advanced security tools.
- Identification of threat path and issuance of advisories.
- Identification & suggestion of Micro segmentation of networks and analysis of such traffic.

Capacity Planning of Network

Audit shall consist of network device audit for existing capacity requirement and scalable factor, existing load and capacity of physical layer topology and logical layer architecture, audit on type of equipment required for specific task (Core Network device, Perimeter device and Aggregating devices). Following minimum should be collected during the audit.

- Bandwidth utilization at links
- Availability of bandwidth
- Current utilization levels (normal and non-peak hours)
- Scalability of bandwidth & utilization
- Network device performance related to CPU and memory utilization of devices During peak traffic Memory
- Performance (Ping response time)
- Queue/buffer drops
- Broadcast volumes, Collisions, Giants, Runts, traffic-shaping parameters
- NetFlow statistic
- Remote Network Monitoring (RMON)
- End of Life/End of Support network devices

Capacity planning of Infrastructure

- Capacity planning of servers
- EOS/EOL servers and replacement plan
- Past trends/analysis may also be included along with current utilization and future projection under Capacity planning.

Performance Audit

- **Link Level**

  A detailed analysis of link usage patterns is to be prepared. This should include, for each link, average and peak utilization over the time period. Latency (round-trip response time) of each link at various load conditions should also be obtained. Throughput also to be measured (using dummy applications- such as ftp for example) for as many critical segments as possible.

- **Application level**

  A break down by each category of traffic (i.e., which application is generating how much data) should be obtained for as many links as possible. This should be analyzed for any anomaly and suggestions given for reducing/controlling any unnecessary traffic.

  Review the deployment architecture of the Applications in scope,

  Review of testing process conducted for all digital applications before Go-Live and for major changes.

  review on the adequacy of test environment.

  Review of potential impact of interface related capacity & performance issues on the application

Sufficiency and coverage of UAT test cases, review of defects & tracking mechanism, re- testing & acceptance, before Go-Live of the deployment of in-house developed/outsourced applications.

Real-Time Monitoring/Analysis/Control Mechanisms

An exhaustive list of reports to be generated regularly (every few minutes, hourly, daily, weekly) such as the following:

- Degradation in performance of any link below a threshold.
- Health of services and generate alarms on failures.
- Usage patterns (number of transactions) per application should be prepared.
- Suggestions for suitable state-of-the art tools for pro-active real time monitoring, analysis and control of the network traffic should also be given.
- Process Management Audit Review of key processes related to the Network
- Configuration Management Process
- Change Management Process
- Backup
- SLA Management

9. Business Continuity and Disaster Recovery

To audit BCP/DRP in terms of its adequacy, effectiveness, efficiency, activation ability and reliability taking into consideration.

a) Review of BCP & DRP Processes
b) Business Flows
c) Review of recovery time objectives
d) Review of Recovery Point Objective
e) Review of Business Continuity Strategy
f) Review of submission of DR test result to IT Steering Committee or higher authority.
g) Identify Individual Point of failures

h) Doing assessment and providing observations on DR Drill (Frequency of DR Drill, Scope of DR Drill, Method of DR Drill, addressing the findings of DR Drill, Reporting the findings of drills, Reviewing the DR Drill conducted and its effectiveness. The audit may also comment on lapses and corrective action taken) conducted for all four quarters.

i) Identification of downtime, reporting of the downtime and Root Cause Analysis of the downtime process to identify the root cause, lessons learnt and corrective actions/ measures initiated/ implemented – its appropriateness and sufficiency, escalation to Board/ Board level committee, stakeholders etc. Among other things comment on planning, coordination, timely escalation, coordination and communication, roles and responsibilities of various teams, media engagement and mitigation measures.

j) If DR strategy is dependent upon vendors: -

    a) Review of arrangements available with vendors to enable the DR exercise function successfully and necessary infrastructure thereof.

    b) Where the continuity of critical business operations is dependent on vendor, review, whether the bank has taken/ checked the assurance from service providers for continuance of critical operations by having BCP in place at service providers' end.

10. Audit of System Development and Change Management

- System Development Life Cycle (SDLC): Review the SDLC processes for developing and deploying IT systems.
- Change Management: Assess the processes for managing changes to IT systems and infrastructure.
- Configuration Management: Evaluate the configuration management practices.
- Evaluate the version management practices to ensure proper controls are in place in the area of System development, programming management, data management, security management, operations management and quality assurance management. Industry Best Practices are observed wherever possible.
- Review of principles adopted by the bank to adhere to secure by design.
- Review of Security Assessment Mechanisms before development of any
  new/regular change or for new product.
- Review API design, Review on API secure SDLC, Review on how API usage and performance metrics, Review on API security.

11. Audit of Data Management

- Data Quality: Assess the quality, integrity, and accuracy of data.
- Data Governance: Review data governance policies and procedures.

- Data Privacy: Ensure measures are in place to protect customer and sensitive data.
- Data Management Control: Users must be able to share data, data must be available to users when it is needed, in the location where it is needed and, in the form, in which it is needed, it must be possible to modify data fairly easily in the light of changing user requirements, integrity of data must be preserved.
- Data Localization: Data is stored in India only.

12. IT Operations

- Operational Procedures: Evaluate daily IT operational procedures and practices including EOD process
- Incident and Problem Management: Review the processes for incident and problem management.
- Service Level Management: Assess the management of service levels and third-party vendor performance.
- Review of Privileged Identity Management
- Review of adequacy of staff
- Review of reporting responsibility and periodicity of report
- Review of information sharing by bank's DC/DR team with outsourced service provider team.
- Review of work authorization system between outsourced service provider and Bank's team
- Review of Access Control, Customer Data Privacy & Confidentiality.
- Review of Media disposal

13. Audit of Applications and Software

- Application Security: Assess the security controls of critical banking applications.
- Mechanism for Source code review for critical applications. Applications security
- testing and vulnerabilities addressed may be checked
- Software Licensing: Review compliance with software licensing agreements.
- Application Performance: Evaluate the performance and reliability of applications.

The scope to further include Application Audit (covering functionality of defined rules / parameters and controls within the application) of the Applications used by the Bank. Some applications are named here below:

- Core Banking Solution (Domestic & Overseas Branches)
- Internet Banking (Domestic & Overseas)
- Loan Processing System/Loan Originating System (LOS)
- ATM Switch
- Treasury
- SWIFT

- Email System (Office and Office 365)
- Mobile Banking & UPI (Retail & Corporate) Domestic and Overseas
- Immediate Payment System (IMPS)
- Financial Inclusion (FI)
- Document Management System (DMS)
- Cheque Truncation System (CTS)
- Demit Account
- Enterprise Fraud Risk Management System (EFRMS)
- Biometric Authentication System (BAS)
- PIM solution
- Trade Finance Solution
- MIS
- HRMS
- C KYC
- Centralized FI gateway Application, including E-KYC, AEPS, etc.
- GSTN (Other applications also can be added as per Bank requirement)
- Work from Home (WFH)
- BBPS
- UCO Sarthi
- BHIM Aadhaar Pay
- Shishu Mudra
- UCO Online
- API
- Chatbot
- Prepaid Cards
- Smart Pay
- UCO Secure
- UCO Pay Plus
- NETC Fast Tag
- WhatsApp Banking
- Digilocker
- EVC Income Tax
- GeM
- SPGRS
- Meetings Management
- Public Financial Management System (PFMS)
- CBKONNECT
- Active Directory
- Enterprise Management System (EMS)
- GBM
- Patch Management Solution
- SFMS/NEFT/RTGS
- IRAAC business logic and deployment (Compliance with RBI guidelines on automation of IRACP)

14. Audit of Project Management

- Project Planning: Review the planning and management of IT projects.

- Resource Allocation: Assess the allocation of resources to IT projects.
- Project Monitoring: Evaluate the monitoring and control of ongoing IT projects.
- **Information System Acquisition, Development and Maintenance**
    - Sponsorship of senior management for development projects
    - New system or changes to current systems should be adequately specified, programmed, tested, documented prior to transfer in the live environment
    - Scrambling of sensitive data prior to use for testing purpose
- **Release Management**
    - Access to computer environment and data based on job roles and responsibilities
    - Proper segregation of duties to be maintained while granting access in the following environment
        - Live
        - Test
        - Development
- Segregation of development, test and operating (production) environments for software
- Project Management tool being used
- **Preventing Execution of Unauthorized Software:** Assess controls for preventing the execution of the unauthorized software and applications on critical end points, including the presence of mechanism to restrict and monitor remote access tools and messaging applications.

15. Audit of User Access and Authentication

- User Access Management: User Access Management: Assess the processes for granting, modifying, and revoking user access at application/Database/Operating system levels.
- Authentication Mechanisms: Review the effectiveness of authentication mechanisms (e.g., passwords, multi-factor authentication).
- Adequacy of User Access controls at OS / DB / Application for IT systems
- Policy for usernames / passwords, shared documents.
- Guest users, adding new staff, removing old staff access.
- User access to outsourced staff and other outside consultants appointed by the Bank.
- Review of documentation for formal naming standards, design process of job roles, activity, groups, profiles, assignment, approval & periodic review of users,
  assignment & use of Super user access.

16. Reconciliation: Reconciliation mechanism of all payment channels.

17. Risk Based Transaction Monitoring: Review the effectiveness of the Bank's EFRM (Enterprise Fraud Risk Management) solution in addressing significant increases in digital transactions and ATM cash withdrawals during specific periods, such as observed during extended weekends and holidays.

18. Redundancy Configuration:

a) Check whether redundancy is configured for all critical applications/ assets including all components of data center set up and work in times of contingency. Comment on the bank's capability of conducting DR testing by completely shifting from the primary site to alternate site for all its applications running on the primary site(s).
b) Review the resiliency by evaluating the bank's preparedness to shift to alternate
site at a very short notice for its critical applications from a given primary site for one/more critical application(s).
c) Comment upon quality and robustness of data migration from Finacle 7 to
Finacle 10.
d) Review back-end correction process in the new system and also on the control mechanism in place in the bank to carry out such requests emanating from business units.

19. System Integration, Architecture Review: -

a) STP between CBS and other IT system with accounting software, data warehouse solutions and MIS system.
b) Logical consistency with various field in the various tables of database and its logical control, if any. Evaluation of controls available in case the data in the data warehouse are modified/deleted and corresponding changes in the base systems, if any.

20. Exception Management: Complete Flow, Exception related to any change in the application or configuration to be covered. Reporting and monitoring of the exceptions. Check how the exceptions are granted and monitored by information security committee/ CISO and handled from IT/ information security angle – including the framework, competent authority, and adequacy of compensating controls in such exceptions.

21. Emerging Technologies/ implementation of new Product and Process: To evaluate the bank's strategy for adopting emerging technologies (e.g., AI, Blockchain, IoT), New Products and Processes and the associated risk management practices (If applicable).

22. Review the bank's crisis management plan, strategy, execution, and its response mechanism while handing complaints received especially through social media related to service disruption.

23. Microservices Architecture: Evaluate the adoption and security of microservices architecture (If applicable).

24. Review of Endpoint Security: - Review of all endpoint security postures and its effectiveness as below

a) Active Directory
b) Network Access Control (NAC)
c) Anti-Virus
d) End point DLP
e) Web DLP
f) E-mail DLP
g) Application Whitelisting
h) Patch Management

25. Management and monitoring of Logs: - Review of management and monitoring of logs like trace logs, CDCI Logs, Fatal Logs, Archive Logs, SU Logs, Syslogs, Alert Logs, Last Logs, application Logs, Security Logs, System Logs, File retention Logs, File Replication service log, DNS Log, IDS Log, AIPS Logs, Event Logs, Access Log, ISS logs, AV Logs.

Note: No deletion or omission or modification in the scope will be entertained either during the bidding period or after selection of auditor.