

## **Broad Scope of Work**

The Bank intends to select CERT-IN empanelled Information Systems (IS) Audit Firms/Organizations to conduct IS Audit and VA-PT at Bank's DC and DR at mentioned 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 which should be whitelisted and in CertIN site and get it approved by the Bank for its utilization. The tool should be capable to work in VM environment also. The bidder has to ensure that they remain CERT-IN Empanelled IS Audit firm/Organisation throughout the contract period.

During the execution of Audit work, the bidder must station auditor onsite until completion of Audit work and for checking compliance without additional charges to Bank. Remote access will not be given to the vendor. The Bank will only arrange space plan to the auditors.

The bidders selected by the RFP should possess deep understanding of both IT Systems and Banking procedures, allowing them to assess interconnectedness between Bank's Technology and its Financial operations.

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.

The bidder should adhere to the guidelines of RBI, Govt. of India, NPCI, UIDAI, SWIFT, NCIIPC etc. and Bank's internal guidelines during conducting the IS Audit covering the various key areas:

- Preparation of IS Audit Plan in Consultation with concerned Bank officials.
- Defining Checklist for different applications/area of audit in Consultation with the Bank.
- Planning execution of the Audit.
- Conducting the IS Audit.
- Documenting the audit process.
- Report submission to the Bank.
- Conducting the compliance audit.
- Imparting training to Bank's internal audit team on audit areas

## **Offices/Units covered:**

- Data Centers at Bengaluru (Primary site for CBS and non-CBS applications) NOC, SOC at Kolkata.
- Disaster Recovery Sites for CBS applications and non-CBS applications at Kolkata, NDR-Bengaluru.

- Treasury Division, SWIFT Center at Bengaluru/Kolkata/Mumbai.
- Digital Banking Facilities at Bengaluru/Kolkata.
- Bank's CTS Centers at Delhi, Chennai & Mumbai.
- Bank's Contact Centers/ Call Centres at Kolkata/New Delhi/Bengaluru.
- Premises/activities of any third party/service providers (outsourced activities) to review compliance of services/T&C under service level agreements at Bengaluru/Mumbai/Kolkata /Chennai or any other Bank's office/ Vendors location.
- Other HO divisions/ Service Providers at Bengaluru / Mumbai/ Kolkata/ Chennai or any other Bank's office at any place, where critical application/ IT infrastructure is installed or may be installed in future.
- Locations of Service Providers to whom specific services are outsourced.

## **Broad Areas of Audit**

### **I. Regular IS Audits:**

1. **VULNERABILITY ASSESSMENT (VA)** - Vulnerability Assessment (VA) shall be carried out of all IT assets deployed in Data Centre (DC), Cloud and Disaster Recovery Centre (DR), like Network Intrusion Prevention System (NIPS), Intrusion Detection System (IDS), Routers, Switches, Web Servers, Operating Systems, Data Base Systems, IOSs, Clouds, etc.
2. **PENETRATION TESTING (PT) (EXTERNAL/INTERNAL)** - Penetration Testing shall be for IT assets (Applications, Systems, Hardware, Network Infrastructure, Cloud Applications, etc.)
3. **APPLICATION AUDIT-** Application audit shall be conducted for all applications within the bank.
4. **PROCESS AUDIT** - Process audit must be conducted for Data Centre (DC), Disaster Recovery (DR) Centre and any critical location where our critical IT infrastructure is hosted and Critical IT applications and any new applications before go-live or on major changes.
5. **NETWORK ARCHITECTURE REVIEW** - Network design of critical network architecture and infrastructure performance controls shall be reviewed.
6. **FIREWALL RULE BASED REVIEW** - All the configuration output of the firewall rules shall be captured and studied, policy/rule-wise, manually or using the tools so that any mis-configuration residing may be mitigated.
7. **SOURCE CODE AUDIT/REVIEW** - Source Code Audit or Secure Code Review, as applicable, of inhouse- developed packages or outsourced applications.

## **8. DATABASE AUDIT**

## **9. KRIs and KPIs Prepared by CISO OFFICE**

**10. VA/PT OF INTERNET CONNECTED PCs** - VA/PT (Vulnerability Assessment and Penetration Testing) of Internet connected Desktops/ PCs of Corporate Departments.

## **11. SECURITY AUDIT OF CLOUD SERVICES**

**12. PERFORMANCE TESTING** - Load Testing, Stress Testing, Capacity Testing and Spike Testing of Mobile Banking Applications.

**13. AUDIT OF CHANGE LOGS** - Audit of Change Logs refers to the process of reviewing and examining the records that documents changes made to a system, software application, database, or any other type of information system.

**14. VENDOR AUDIT & SITE AUDIT** - Vendor Audit is a process of evaluating and assessing the IT-related practices and controls of a third-party vendor or supplier.

**15. SECURE CONFIGURATION REVIEW/AUDIT** - Secure Configuration Review of Operating System (OS) and Database (DB). Configuration Audit of Servers, Network and Security Devices covering critical Applications, like CBS (domestic and overseas), Mobile Banking, Internet Banking, UPI, GBM, RTGS, NEFT, SWIFT, etc.

**16. GOVERNANCE AUDIT-** A governance audit is an independent review of governance framework, policies, and processes of various departments / verticals across the Bank.

**17. AUDIT OF STORAGE OF PAYMENT SYSTEM DATA** - Bank shall conduct audit to ensure that the entire data relating to payment systems operated by them are stored in a system only in India.

## **18. SYSTEM AUDIT REPORT (SAR) NSDL**

## **19. IS AUDIT OF AADHAAR USER AUTHENTICATION (AUA)**

**20. AUDIT OF DIGITAL LENDING** - Periodic validation tests of the algorithm/model used in Business Rule Engine (BRE) – once in six months during the first two years and suggest any remedial measures basis operational audit observations.

**21. CYBER SECURITY FRAMEWORK REVIEW** - As part of IS Audit Program, the adequacy and adherence to the controls of RBI's Cyber Security Framework and other applicable regulatory guidelines.

22. **SWIFT Customer Security Program (CSP) Assessment** - SWIFT Customer Security Controls Framework (CSCF) (latest version – Current version is CSCF - V2025).
23. **AUDIT OF VIRTUAL MACHINES (VMs)**
24. **Comprehensive Cyber Security Audit of Applications, Platforms, and Databases related to CBS**
25. **Audit/Review of Software Bills of Material (SBOM) and Cryptography Bill of Materials (CBOM)**
26. **Information Security Management System (ISMS) for ISO 27001:2022 Certification**
27. **Cyber Security Audit/Assessment/Risk Assessment as per C-RAF framework of HKMA for Hongkong**
28. **MAS Cyber Audit/Risk Assessment as per TRM framework of MAS for Singapore**
29. **Migration Audit**
30. **Forensic Audit/ Forensic Analysis/Investigations:**
31. **Security cum functional audit of new applications**

## **II. Security cum Functional Audit:**

Security cum Functional Audit will be done before GO-Live for New developed application/ After Major Changes in existing applications (both in-house and developed by external vendors).

### **Deliverables**

#### **Time Lines**

- a) Selected IS Auditor will provide schedule of audit like Annual/Quarterly/Special Audit, at least 7 working days prior to start of audit along with full credentials of Audit team (with qualification & experience as defined in RFP) who will be conducting the audit.
- b) Completion of quarterly Process Review Audit, Device Level Audit, VA & PT audit as mentioned above within 18 working days.
- c) Minutes of daily meeting will be prepared by next day where observations are based on discussion and will be signed by all participants.
- d) Giving draft report for discussions with owners within 3 working days after completion of audit.

- e) Discussion of the issues with Divisional Head/owner after 2 working days from date of submission of draft report.
- f) The Security Cum Functional Audits have to be initiated within three days of allotment of audit and completed within 21 working days.

## **Training**

Training to be provided to Bank's officials on half yearly basis.

1. Training is to be given to internal IS Audit team on uses of Tools used for Audit purpose, understanding scripts to be run on server, conducting VAPT, preparation of the Reports based on the identified vulnerabilities (i.e. identifying Risk Impact and Recommendation to mitigate the identified risks).
2. The IS Auditor should explain, to the bank's team all the processes, procedures involved in arriving at audit findings including interpretation of outputs generated by various audit tools.

## **Reports:**

Report should be provided with snap shot / evidence/ documents details from which observation made wherever is easily understood by Bank.

Reporting formats should at the minimum include

- Compliance status of previous quarter report will include observations with status as following- Found complied/ found partially complied/ Found Non-complied/ Exception taken as a separate report.
- Audit report of current quarter with status Repeat/ Exception / New.
- The IS Auditor shall provide different types of reports which would address all issues/observations regarding compliances.
- If repeated – (i) Since when on same server. (ii) Since when on Similar asset.
- If exception– expiry date & authorized by whom.
- Vulnerability ID (Unique identification number (alpha numeric) for each vulnerability and the Identifier should be such that it is Unique for any previous Vulnerability process also.
- Vulnerability Identified (specific to equipment / resources - indicating name and IP address of equipment, Application name where Vulnerability exists and office / department name and should not be generalized).
- Broad domain categorization of activity (Port/SQL Injection/ Services/Physical Access Control/ Logical Access Control/ Environment etc.).
- Risk category & Exploitable status as against –Critical, High, Medium, Low level observations.
- Servers/ Resources affected with IP address.
- Department (in office) to whom the Vulnerability relates.
- Risk / Implication.
- Recommendation for risk mitigation/ removal – step wise. If not resolved, alternate solutions will be provided over phone/ email or personal visits to department if required. Response over phone/ email should come within 4 hours of receipt of request.

- Provision for updating owner's compliance comments.
- Reports should be department wise with brief about Identification of auditee (Address & contact information), Date, location &, time span of audit.
- Explicit reference to key policy and procedure documents of the Bank/RBI against identified risk/observation.
- The reports shall be customized as per the requirements of the Bank.
- Additional mandatory or voluntary standards or regulations applicable to the banking industry as best practices should be reported under "Improvement /suggestions".
- Standards followed
- Summary of audit findings including identification tests, tools used and results of tests performed (like vulnerability assessment, application security assessment) a. Tools used b. List of vulnerabilities identified. c. Description of vulnerability d. Test cases used for assessing the vulnerabilities. e. Analysis of vulnerabilities and issues of concern.
- Personnel involved in the audit, including identification of any trainees.
- The various audit reports/ templates should be got integrated with the Bank's ITGRC Application.
- All the reports should contain the URL, IP Address, Application and Server Name, Host Name etc. in respect of the assets which are subjected to Audit.

The auditor may further provide any other required information as per the approach adopted by them and which they feel is relevant to the audit process.

### **MIS:**

Successful bidders will use some tools preferably Web Based (cost if any, should be included in audit fee), which shall be capable of providing audit report, and which should support dashboard format (Major gaps with subsequent details through links). It should be capable of presenting reports sorted on following major domains and presentable in pie chart/ graphs/excel sheet. Bank will have the right to use that tool.

Should be able to view/ print report sorted on following:

- Compliance status of previous quarter report –Found Complied/ Found partially complied/ Found Non complied/ Exception taken wise
- Audit report of current quarter with status Repeat/ Exception or New Vulnerability wise.
- Repeated.
- Exceptions.
- Broad domain activity wise.
- Risk category & Exploitable status as against – Critical, High, Medium, Low level observations
- Servers/ Resources affected wise.
- Each server/ resources vulnerability history (activity wise) should be maintained so that trend analysis can be done at any point of time.
- Department wise Vulnerability reports.

- Report showing the major vulnerabilities for a given period of 3, 6 or 12 months for broad domain, server, resources, office, department wise etc.
- Report will be given in editable (Excel) and non-editable softcopy so that editable can be used in updating compliances by User Department
- Report will be given in signed hard copy also.
- Presentation on findings of audit will be given to Management by the Auditor within a week's time of final report submission and should be accompanied by senior consultant for each quarterly audit.
- Any other ADHOC report as per requirement by the Bank.
- Dashboards should be available in respect of the movement of posture of audits during given period based on various parameters.

### **RISK MOVEMENT:**

- Overall risk of each Office – Critical, High, Medium, Low
- Overall risk for Domain and department wise
- Risk movement as compared to previous audits – broad category wise.
- Will maintain history of all previous audit risks scores conducted by successful bidder.

Successful bidder and Auditee will decide Major domains, departments, activities before start of 1st audit based on which report will be prepared. The same can be reviewed whenever there is a change.

### **Audit Units/Areas:**

The Applications/Infrastructure and Site Audit under the IT Universe of the Bank shall include but not limited to the following Audit Units.

#### **1. Governance Audit**

A governance audit is an independent review of governance framework, policies, and processes of various departments / verticals across the Bank. It assesses whether the concerned departments / verticals systems are effective in Supporting the organization's mission, mitigating risks, promoting transparency and defining accountability, adhering to laws, regulations, and internal policies (IT Policy, Digital Policy, Cyber Security Policy etc) of the Bank, meeting the regulatory guidelines etc.

#### **2. Process Audit**

##### **2.1.1 Process Audit shall cover but not limited to the following units: -**

- i. Anti-Money Laundering (AML) – Domestic
- ii. Anti-Money Laundering (AML) - Overseas
- iii. Lending Automation Processing System (LAPS)/Lead Originating (Processing) System (LPS) including STP
- iv. E-KYC/C-KYC authentication infrastructure.
- v. RTGS/NEFT Infrastructure
- vi. Core Banking System (CBS) including Connect 24 Interface and Central Stand in Application Server (CSIS) - Domestic Application

- vii. Core Banking System (CBS) including Connect 24 Interface and Central Stand in Application Server (CSIS)- Overseas Application
- viii. Government Business Module (GBM) (DC & DR)
- ix. Integrated Treasury Management System (ITMS)
- x. LPS/EDPMS/IDPMS/TRACCS
- xi. Alternate Delivery Channels includes
  - **Internet Banking/E Banking (FEBA):-** Shall cover but not limited to the following aspects
    - A. Detailed review of the Internet Banking security architecture vis-à-vis the RBI guidelines.
    - B. Bank's internet Banking product line, transaction flow, Operational activities.
    - C. Review on internal controls & security are in place to minimize errors & frauds.
    - D. Interface with other organizations for utility bill payments/share Trading etc.
    - E. Interface with CBS & other applications.
    - F. Process of creation/Activation/Resetting/delivery of Internet Banking User IDs/ passwords.
    - G. Password/PIN management.
    - H. Authentication controls.
    - I. Two Factor Authentication Solutions for E-Banking.
    - J. Information Security Framework.
    - K. Web Server
    - L. Logs of activity
    - M. De-militarized zone & Firewall.
    - N. Security reviews of all servers used for Internet Banking.
    - O. Database and System administration
  - **Mobile Banking /UCO mBanking plus/Corporate mBanking Audit:**  
 Mobile Banking Audit shall cover but not limited to the following aspects
    - A. Detailed review of the Mobile Banking Security architecture vis-à-vis the RBI guidelines.
    - B. Bank's Mobile Banking product line, transaction flow.
    - C. Review on internal controls in place to minimize errors & frauds.
    - D. Interface with other organizations for utility bill payments & other purposes etc.
    - E. Interface with CBS, Financial Transaction Switch & other applications.
    - F. Parameterization & customization of Mobile Banking.
    - G. Process of creation/Activation/Resetting/delivery of M- PINS.
    - H. Authentication controls.
  - BHIM UCO UPI
  - UCO Secure (Digisafe)
  - mPassbook (Domestic)
  - mPassbook (Singapore)
  - mPassbook (Hongkong)



- UCO Pay plus
- Corporate mBanking
- NPA tracker
- UCO Cluster
- UCO Sandeh Nivaran
- Digilocker
- Value Added Services (3<sup>rd</sup> Party) – Trade Market Place, E-Com Market Place, Wealth Management
- UCO ARBD mobile app
- IMPS
- UPI
- Chatbot (UMA)
- BHIM Aadhaar Pay
- UCO Smart Pay
- Online Fee Collection (In-house & Outsourced) Module.
- Process Audit OTC (One Time Combination) vault opening in Bank's ATM and Cash Recycler.
- Smartpay Fee Collection System.
- Debit Card
- Prepaid Card (Retail)
- Prepaid Card (Corporate)
- Merchant Application for onboarding & Digital payment acceptance hosted at Cloud/ QR Kit/ Sound Box
- Whatsapp Banking hosted at Cloud
- UPI123 hosted at Cloud
- E-Commerce marketplace hosted Cloud
- POS Terminal, Portal/App, Switch, Reconciliation
- MSME Suite
- Micro ATM
- Any Other
- **Automated Teller Machine (ATM)/Cash Recycler & Digital Banking Unit:** Installed at different locations in Metros, Urban and Rural areas (5 ATM/ Cash Recycler in each location). ATM Centre/Switch Audit shall cover but not limited to the following aspects: --
  - A.** ATM center management: PIN Management, Card Management, Time Management in delivering ATM Card/PIN to Customers and Hot listing of cards.
  - B.** ATM helpdesk and monitoring.
  - C.** Branch procedures.
  - D.** Reconciliation: -Visa, Rupay, POS, NFS, Us-on-Us Chargeback procedures etc. (at ATM Transaction Banking Division, Mumbai/Kolkata).
  - E.** Card Printing/Dispatch, Green PIN Generation through various channels.
  - F.** Instant Debit Card Printer
  - G.** ATM/Prepaid Card Switch setup, configuration, Security, control & Risk Management.
  - H.** ATM Switch operational controls, Consortium issues & Reconciliation/ Functional Managerial activities.

- I. Monitoring procedure of ATM's / Cash Recycler Status (Uptime/downtime).
- J. Processing of requests received through Debit Card Request (DCR) module in Finacle.
- K. Review of EWDIT Software of Euronet.
- L. Interface systems (Connect 24, Verified by Visa, Rupay etc.).
- M. Offsite Security Services.
- N. Status of required certifications as per International as well as regulatory stipulations.
- Bharat Bill Payment System (BBPS) / Bill Desk
- On-Line account opening System
- PFMS (Public Financial Management System)
- Digital Customer Onboarding
- CRM (Customer Relationship Management)
- Micro ATM
- MSME Suite
- Central Bank Digital Currency (CBDC), wallet
- Omni Channel Application
- Any other existing and upcoming applications related to Alternate Delivery Channel

**xii. Privacy and Data Protection:** Privacy and Data Protection Audit shall cover but not limited to the following aspects:

- A. Controls established for data conversion process.
- B. Information classification based on criticality and sensitivity to business Operations.
- C. Fraud prevention and Security standards.
- D. Isolation and confidentiality in maintaining of Bank's customer Information, documents, records and procedure by banks.
- E. Procedures for identification of owners.
- F. Procedures of erasing, shredding of documents and
- G. Media containing sensitive information after the period of usage.
- H. Media control within the premises.
- I. Compliance with Regulatory/Statutory Data Privacy/Protection/Localization guidelines.

**xiii. IT Architecture:** IT Architecture shall cover but not limited to the following aspects: -

- **Acquisition and Implementation of Packaged software**
  - Requirement Identification and Analysis
  - Product and Vendor selection criteria
  - Vendor selection process
  - Contracts
  - Implementation
  - Post Implementation Issues
- **Development of software- In-house and Out-sourced**
  - Audit framework for software developed in house, if any
  - Software Audit process
    - Audit at Program level

- Audit at Application level
- Audit at Organizational level
- Audit framework for software outsourcing
- **Operating Systems Controls**
  - Adherence to licensing requirements
  - Version maintenance and application of patches
  - Network Security
  - User Account Management
- **Access Controls**
  - System Administration
  - Maintenance of sensitive user accounts
- **Application Systems and Controls**
  - Logical Access Controls
  - Input Controls
  - Processing Controls
  - Output Controls
  - Interface Controls
  - Authorization Controls
  - Data Integrity/ File Continuity controls
  - Review of logs and audit trails
- **Database Controls**
  - Physical access and protection
  - Referential Integrity and accuracy
  - Administration and Housekeeping
- **Network Management audit**
  - Process
  - Risk acceptance (deviation)
  - Authentication
  - Passwords
  - Personal Identification Numbers ('PINS')
  - Dynamic password
  - Public key Infrastructure ('PKI')
  - Biometrics Authentication
  - Access Control
  - Cryptography
  - Network Information Security
  - E-mail and Voicemail rules and requirements
  - Information Security Administration
  - Microcomputer/ PC security
  - Audit trails
  - Violation logging management
  - Information storage and retrieval
  - Penetration Testing

**xiv. Security System for Online Card Transaction (SSOCT):**

The SSOCT shall cover but not limited to the following aspects

- A. Detailed review of the SSOCT security architecture vis-à-vis the RBI, Card scheme (VISA/MASTER/Rupay card etc.) guidelines.
- B. Bank's SSOCT product line, transaction flow.
- C. Review on internal controls in place to minimize errors & frauds.
- D. Interface with ATM Switch & other applications.
- E. Process of creation/Activation/Resetting/delivery of PIN.
- F. Authentication controls.
- G. Compliance with industry standards of security such as, Payment Card Industry Data Security Standard (PCIDSS) etc.

**XV. Review of IT Processes and IT Management Tools:** The review of IT Processes and Management tools shall cover but not limited to the following aspects:

- A. IT Asset Management
- B. Enterprise Management System
- C. Help Desk
- D. SDLC & Change Management
- E. Incident Management
- F. Network Management
- G. Backup & Media Management
- H. Anti-Virus Management
- I. IT Governance
- J. Implementation of Active Directory & Desktop management.
- K. Vendor & SLA Management
- L. ESCROW Management System
- M. Cyber Security Management Plan.

**xvi. IT/Digital/Cyber Security Policies review:** An assessment/review of all the important Policies/ Procedure Documents of the Bank such as

- A. Information Technology (IT) Policy
- B. Information Security Policy
- C. Cyber Security Policy
- D. Application Security Policy
- E. Active Directory Policy
- F. ATM Policy
- G. Internet Banking Policy
- H. Vendor and Outsourcing Policy
- I. Cyber Crisis Management Plan Policy
- J. Policy on Document Management System (DMS) Digitization of Critical Records AND Documents
- K. Fintech Policy
- L. Data Privacy and Security Policy
- M. IT Purchase Policy
- N. Hardware Acquisition Maintenance Upgradation Policy
- O. IT Skillset Development Policy
- P. Debit Card Policy
- Q. IT Asset Disposal Policy
- R. Mobile Banking Policy
- S. Network Policy

- T. Prepaid Card Policy
- U. Merchant On-boarding Policy
- V. Digital Banking Outlet Policy
- W. Social Media Policy
- X. Any other policies related to IT/Digital Banking/Cyber Security of the bank which are not listed above.

**xvii. Asset Management:** Asset Management shall cover but not limited to the following aspects:

- A. Records of assets mapped to owners
- B. For Payment Card Industry (PCI) covered data, the following should be implemented:
  - B.1 Proper usage policies for use of critical employee facing technologies
  - B.2 Maintenance of Inventory logs for media
  - B.3 Restriction of access to assets through acceptable usage policies, explicit management approval, authorized use of technology, access control list covering list of employees and devices, labeling of devices, list of approved company products, automatic session disconnection of remote devices after prolong inactivity.
  - B.4 Review of duties of employees having access to asset on regular basis.

**xviii. IT Financial Control Audit:** IT Financial Control shall cover but not limited to the following aspects

- A. Comprehensive outsourcing policy
- B. Coverage of confidentiality clause and clear assignment of liability for loss resulting from Information Security lapse in the vendor contract
- C. Periodic review of financial and operational condition of Service Provider with emphasis to performance standards, confidentiality and Security, business continuity preparedness
- D. Contract clauses for vendor to allow RBI or personnel authorized by RBI
- E. Access relevant information/ records within reasonable frame of time.

**xix. IT Operations Audit:** IT Operations shall cover but not limited to the following aspects:

- A. Application Security covering access control
- B. Business Relationship Management
- C. Customer Education and awareness for adaptation of security measures.
- D. Mechanism for informing Banks for deceptive domains, suspicious emails
- E. Trade-marking and monitoring of domain names to help prevent entity for registering in deceptively similar names
- F. Use of Secure Socket Layer (SSL) and updated certification in website
- G. Informing client of various attacks like phishing

- H. Capacity Management
- I. Service Continuity and availability management
- J. Consistency in handling and storing of information in accordance to its classification
- K. Securing of confidential data with proper storage
- L. Media disposal
- M. Infrastructure for backup and recovery
- N. Regular backups for essential business information and software
- O. Continuation of voice mail and telephone services as Part of business contingency and disaster recovery Plans
- P. Adequate insurance maintained to cover the cost of Replacement of IT resources in event of disaster
- Q. Avoidance of single point failure through contingency Planning
- R. Service Level Management.

**xx. Project Management:** Project Management shall cover but not limited to the following aspects:

- A. Information System Acquisition, Development and Maintenance
- B. Sponsorship of senior management for development projects
- C. New system or changes to current systems should be adequately specified, programmed, tested, documented prior to transfer in the live environment
- D. Scrambling of sensitive data prior to use for testing purpose
- E. Release Management
- F. Access to computer environment and data based on job roles and responsibilities
- G. Proper segregation of duties to be maintained while granting access in the following environment – Live, Test, Development
- H. Segregation of development, test and operating environments for software.

**xxi. Record Management:** Record processes and controls shall cover but not limited to the following aspects:

- A. Policies for media handling, disposal and transit
- B. Periodic review of Authorization levels and distribution lists
- C. Procedures of handling, storage and disposal of information and media
- D. Storage of media backups
- E. Protection of records from loss, destruction and falsification in accordance to statutory, regulatory, contractual and business requirement.

**xxii. Technology Licensing:** Technology Licensing shall cover but not limited to the following aspects:

- A. Periodic review of software licenses
- B. Legal and regulatory requirement of Importing or

exporting of software.

**xxiii. IT outsourcing related controls:** The following correlates significant third party risks to the assessments utilized by organizations to evaluate the effectiveness of third party controls in place to mitigate risks.

- A. Compliance:** Assess the third-party's ability/control framework in place to comply with laws/regulations.
- B. Information Security & Privacy:** Assess third party controls over the Availability, confidentiality, and integrity of third party data.
- C. Physical Security:** Assess facility access and security measures implemented by the third party.
- D. Country Risk:** Assess political, geographic, regulatory, legal, and economic risks of sourcing to a country or region.
- E. Business Continuity & Resiliency:** Assess the third parties ability to perform in the event of a process failure or catastrophic event.
- F. Financial:** Assess financial stability for the third party to continue provide the product/service.
- G. Technology:** Assess the adequacy and appropriateness of the third parties systems and applications to provide the product/service
- H. Subcontractor:** Assess the risk management processes surrounding the use of subcontractors by third parties.
- I. Operational Competency:** Assesses the ability of the third party to deliver the contracted products/services.

**xxiv. Business Continuity Management & Cyber Crisis Management:**

Business Continuity Management Audit shall cover but not limited to the following aspects:

- A.** Top Management guidance and support on BCP& DRP
- B.** Addressing of HR issues and training aspects
- C.** Providing for the safety and wellbeing of people at branch or location at the time of disaster
- D.** Assurance from Service providers of critical operations for having BCP & DRP in place with testing performed on periodic basis.
- E.** Independent Audit and review of the BCP/DRP and test result
- F.** Participation in drills conducted by RBI for Banks using RTGS/NDS/CFMS Services
- G.** Maintaining of robust framework for documenting, maintaining and Testing business continuity and recovery plans by Banks and Service Providers.
- H.** The BCP methodology covering the following:
  - B.1 Identification of critical business
  - B.2 Owned and shared resources with supporting function
  - B.3 Risk assessment on the basis of Business Impact Analysis ('BIA')

- B.4 Formulation of Recovery Time Objective ('RTO') and Identification of Recovery Point Objective ('RPO')
- B.5 Minimizing immediate damage and losses
- B.6 Restoring of critical business functions, including customer-facing systems and payment settlement systems
- B.7 Establishing management succession and emergency powers.

**xxv. Call Centre Audit:** Call Centre Audit shall cover but not limited to the following aspects

- A. Review of the call center architecture.
- B. Vulnerability/ Threat Assessment.
- C. Review on internal controls in place to minimize errors & frauds.
- D. Manageability of the solution implemented by means of administrative control such as administrative password.
- E. Adequacy of security features of the application implemented.
- F. Solution should not breach the security of any other installations of Bank in any way.
- G. Review of interfaces if any
- H. Authentication controls.

**xxvi. Operating System Audit:** The Operating System audit shall cover but not limited to the following aspects for Servers, Databases, Network equipments, Security Systems, Storage Area Networks.

- A. Set up and maintenance of system parameters.
- B. Configuration Management
- C. Patch Management
- D. Change Management Procedures
- E. Logical Access Controls
- F. User Management & Security
- G. OS Hardening
- H. Performance, Scalability and Availability

**xxvii. Email/Mail Messaging System Audit:** The Mail Messaging audit shall cover but not limited to the following aspects:

- A. Overall Mail Messaging System management.
- B. Architecture & design review of Mail Messaging System.
- C. Performance of Mail Messaging Servers.
- D. Archival & Backup process.
- E. Configuration Audit/Hardening review for all servers, network devices (Routers, Firewall, Switches) used in Mail Messaging System.
- F. Impact Analysis of Mail Servers.

**xxviii. Risk Based Internal Audit (RBIA) Audit:** Risk Based Internal Audit shall cover but not limited to the following aspects:

- A. Review of System Architecture of RBIA.
- B. Vulnerability Assessment of the Servers and associated peripherals.



- C. Review of risk based Internal Audit & Off-site Surveillance implemented in the System including work flow.
- D. Manageability of the solution implemented by means of administrative control such as administrative password.
- E. Adequacy of security features of the application implemented.
- F. Solution should not breach the security of any other installations of Bank in any way.
- G. Review of interfaces, particularly with Finacle & others, if any.
- H. Authentication controls.

**xxix. Maintenance Audit:** The IS Asset maintenance shall cover but not limited to the following aspects: -

- Change Request Management
- Software developed in-house
- Version Control
- Software procured from outside vendors
- DC Operations (KDC & BDC) both Internal and External
- Software trouble-shooting
- Helpdesk
- File/ Data reorganization
- Backup and recovery
- Software Data
- Purging of data
- Hardware maintenance
- Training

**xxx. MIS & Automated Data Flow (ADF) Audit:**

Audit of Automated Data Flow (MIS-ADF) to RBI shall cover but not limited to the following aspects:

- A. Vulnerability/ Threat Assessment of the Servers and associated Peripherals.
- B. Review of MIS ADF Architecture.
- C. Review of DC-DR Replication.
- D. IS Audit with respect to Data Integrity & Consistency.
- E. Manageability of the solution implemented by means of administrative control such as administrative password.
- F. Adequacy of security features of the application implemented. (Testing for known vulnerabilities and configuration issues on Web Server & Web Application, Denial of Service Attack, Testing for SQL Injection Vulnerability etc.).
- G. Review of interfaces, particularly with Finacle & others, if any. Authentication controls (OS, Database, Storage and Application Security & Authentication).
- H. Controls for managing change, patch, Source Code and Sensitive DB password.

- I. Controls for performing/changing parameter setup of functionality across applications (also controls for impact analysis of changes made).

**xxxii. Cheque Truncation System (CTS) Audit:**

CTS at Chennai, Mumbai & Delhi audit shall cover but not limited to the following aspects (Southern, Western & Northern Grids)-

- A. Detailed review of the CTS architecture vis-à-vis the RBI guidelines.
- B. Review on internal controls in place to minimize errors & frauds.
- C. Interface with CBS & other applications.
- D. Authentication controls.
- E. Review of the Work Flow.
- F. Vulnerability / Threat Assessment.

**xxxiii. Security Operating Centre (SOC) – (includes modules viz. WAF, PIMS, DAM, APT, NBA, SIEM, DECOY, ITGRC, NAC, DLP, NPM, VAS, Patch Management Solution, etc.) with ARC Sight as a single Window incident management, ticketing and reporting System. **The audit should include Review of rules of SOC Devices/Tools including Arc Sight, DAM etc.****

**xxxiii. SWIFT Infrastructure, XMM Middleware.**

SWIFT Centre Review cover the following aspects

- A. Data Center controls related to SWIFT systems (DC and DR).
- B. Access controls, Authentication framework.
- C. Application Registration Controls
- D. IT Architecture Audit - related to SWIFT Transaction processing
- E. Incident and Change Management
- F. Audit for OS Security baselines and Application Security Controls
- G. Review of Firewall rules and Network security/ Management controls of all other interfacing systems including CBS
- H. Network Security controls of SWIFT infrastructure
- I. Disaster Recovery and Business Continuity Process
- J. Compliance in line with Bank's RTO and RPO
- K. Version Control and Change Management Process
- L. Scalability and Availability
- M. IT Operations for SWIFT related Applications
- N. Log monitoring process pertaining to SWIFT Infrastructure, assurance on log manipulation, Ensure logs cannot be manipulated /deleted by third party including administrator of the system.
- O. Application Security Review of SWIFT Infrastructure
- P. Arrangements for source code review

- Q. Review of Risk Assessment and suggest mitigation measures for the identified service
- R. VAPT of OS, Database and Network devices
- S. Review of SWIFT architecture including VPNs hosting SWIFT Alliance access, Payment validation (AML and suspicious transactions) engine.
- T. Perform malware analysis of memory of important systems
- U. Control assessment at the key entry points for malware
- V. Review of malware Incident Management and Response
- W. Active scanning of the target hosts to identify any malware infections
- X. SWIFT certificate / SSL review
- Y. Encryption of data in static / transmit mode
- Z. Review of outsourcing arrangement (SLA) vis-a-vis industry standards
- AA. Review of Firewall internal/ external rules w.r.t. SWIFT
- BB. Antivirus scanning on servers and user PCs
- CC. Review of security controls / Management controls of all other interfacing systems including CBS
- DD. Arrangements for Anti-phishing/ takedown of rogue applications
- EE. Review of Standard Operating Procedures
- FF. Review of Middleware between systems
- GG. Review of Fraud Risk Management System related to SWIFT activities/ functions
- HH. IT General controls review
- II. Creation, approval of SWIFT transaction process in Core Banking
- JJ. Control at pre-transmission stage (i.e. before sending payment messages to Bank with which Nostro Account is maintained)
- KK. Controls post transmission of payment messages
- LL. Review of Nostro Reconciliation Process
- MM. Review of operations carried out by Trade Finance Team
- NN. Review of various SWIFT related activities/ functions carried out by domestic branches
- OO. To comply with SWIFT Customer Security Program - Guidance given by SWIFT covering 16 mandatory and 11 advisory controls of SWIFT customer security controls framework
- PP. Compliance audit post ATR submitted by the Bank on remediation of the identified gaps.
- QQ. Functionality review of SWIFT systems
- RR. Validation of financial parameters, etc.
- SS. Assessment of gaps in implementation of policies
- TT. Compliance to the legal/regulatory guidelines.

Controls and implementation of advisory/circular issued by RBI/SWIFT system to strengthen the SWIFT infrastructure.

- xxxiv. Registration Authority (RA) Office Audit:** RA office set-up under IDRBT Set-up audit shall cover but not limited to the following aspects:
- A.** Audit of all RA functions
  - B.** Compliance to the requirements of IT acts 2000 & 2008, Rules and Regulations.
  - C.** Compliance of RA functions as per IDRBT checklist.
  - D.** Reconciliation of digital signatures issued/revoked by RA with IDRBT.
  - E.** Digital Certificates details/record maintenance as per IDRBT requirements.
- xxxv.** MPLS Network Architecture, Management & Audit
- xxxvi.** Document Management System (DMS)
- xxxvii.** Active Directory
- xxxviii.** Proxy Application Server
- xxxix.** **Payment Gateway Audit:** -Review of interface with approx. 10 Payment Gateways used by the Bank viz. ATM, Cash Recycler Mobile Banking, Internet Banking, Bill Desk, Citrus etc. Verification of controls for RTGS, NEFT, SFMS, SWIFT, NFS etc. at Payment Gateway as per the regulator's policies and guidelines.
- xl.** Biometric Infrastructure for Finacle Login, Attendance System, e-KYC.
  - xli.** Centralized Anti-Virus Solution
  - xlII.** UCO Bank Rewardz Program
  - xlIII.** Audit for IT Act Compliance
  - xliv.** Audit of Disaster Recovery Plans
  - xlV.** Audit of privileged users (Database, OS)
  - xlvi.** Capacity Planning of IT Infrastructure of Critical Applications
  - xlVII.** Audit of Service Level Management
  - xlVIII.** Audit of License Management
  - xlIX.** Cyber Security Framework Audit
  - I.** Application Audit-ADC applications (Mobile Banking, E-Banking, UPI etc.)  
on various platforms
  - II.** **ANTI VIRUS:**
    - Proactive virus prevention and detection procedures are in place and implemented. Virus definitions are updated regularly.
    - Monitoring of antivirus servers located at different locations and other locations for having updated latest versions and definitions (t+1) basis.
    - Monitoring procedures effectiveness for branch level client's updations.
    - Antivirus rules/policy review as per Global standard practices /RBI Guidelines.

- Assurance on release of patches by various osd vis-à-vis implementation status on desktops/pcs/servers/systems and submit a gap analysis report.
- Ensuring Organization units are created as per the business requirement and users are authenticated through active directory system.
- BCP on ad (Active Directory) system, back up and its resilience.

**lii. Others:**

- A.** Privileges available to Systems Integrator and Outsourced Vendors.
- B.** Evaluate role, responsibility and accountability of IT Process owners.
- C.** Review of DR Drills undertaken for CBS/ADC & other delivery channels at Treasury branch and reports thereof Comments on sufficiency and periodicity etc. of DR Drills undertaken and planned.
- D.** Audit of Anti Virus protection at host and at desktop levels, procedure of antivirus updates at DC, Servers and Desktops, Gateway level AV protection etc
- E.** Alignment of IT strategy with Business strategy.
- F.** IT Governance related processes.
- G.** Long Term IT strategy and Short Term IT plans.
- H.** Information security governance, effectiveness of implementation of Security policies and processes.
- I.** Review of RBI, IT examination report (GAP assessment of Cyber Security Control).

**Note:-**

1. For the above, the Infrastructure at both DC & DR is to be covered under the Scope
2. For all Critical Processes where there is no Straight Through Processes (STP) are to be reviewed

**3. Source Code Audit**

The in-house developed Applications/ Outsourced application approx. 250(+/- 20%) application/API / Customization and any outsourced applications if required.

Source Code Audit or Secure Code Review, as applicable, of inhouse-developed applications or outsourced applications (In case of respective vendors are unable to provide the Third-party Independent IS Audit Certificate). Version control aspect of in-house software must be covered under Source Code Audit.

**4. Vulnerability Assessment**

The Vulnerability Assessment (**VA**): VA of IT assets (applications, systems and

infrastructure) deployed in Data Centre (DC), Cloud and Disaster Recovery Centre (DR), like Network Intrusion Prevention System (NIPS), Intrusion Detection System (IDS), Routers, Switches, Web Servers, Operating Systems, Data Base Systems, IOSs, Clouds, etc. through their life cycle (pre-implementation, post implementation, major changes etc.) shall cover a minimum of 1200-1500 (+/-10%) **devices on half-yearly basis** and VA of IT infrastructure related to PCI DSS compliance will be done on **Quarterly basis**. A list of Servers/devices in different locations will be given to the selected vendor.

Threat Vulnerability and Risk Assessment (TVRA) for Data Centre as per scope of Monetary Authority of Singapore (MAS) and Hong Kong Monetary Authority (HKMA) shall also be covered. Credential based Vulnerability Assessment (VA) shall be conducted.

Scope of Vulnerability / Threat Assessment shall include, but not be limited to:

- Vulnerability assessment of all servers along with their operating system, Switch, network equipment, security equipment installed, ATM etc.
- Placement/ Deployment of security equipments, network equipments for securing database, application, web servers of various applications.
- Configurations and Monitoring of logs of Intrusion Detection/Prevention Systems, firewalls and response capabilities. Exercise will be carried out from the place where servers are placed. Appropriate updated tools should be used for each phase of test.

## **5. Penetration Testing**

Penetration Testing shall be for IT assets (Applications, Systems, Hardware, Network Infrastructure, Cloud Applications, etc.) throughout their lifecycle (pre-implementation, post-implementation and/or after major changes). Penetration Testing (External) shall be conducted mandatorily on all public facing applications/URLs/Website/APIs/Cloud Applications exposed to the internet.

The final list of IT assets (Applications, Systems, Hardware, Network Infrastructure, Cloud Applications, etc.) for Penetration Testing will be provided to the selected bidders. The Approximate Number of public facing websites/URLs/applications/APIs for Penetration Testing is about 250 (+-20%).

**In addition, the same shall be conducted as and when any new IT Infrastructure or Application is introduced or when any major change is performed on Application or Infrastructure.**

Black Box Penetration Testing (BB PT) will be done of IT infrastructure. However, for PCI DSS compliance related IT Infrastructure, Grey Box Testing (GBT)/ White Box Testing (WBT) shall be done.

Scope of External Penetration Testing should be designed to simulate a real-world attack keeping in view prevailing RBI guidelines, IT acts 2000 & 2008 and other applicable regulations in India and shall at the minimum cover the following: --

- Port Scanning
- System Fingerprinting

- Services Fingerprinting
- Vulnerability Scanning
- Firewall & Access Control List Mapping
- Attempt to guess passwords using password-cracking tools.
- Session Hijacking
- Buffer Overflow
- SQL Injection
- Command Injection
- Cross Site Scripting
- Malicious Input Checks
- Checking Vulnerabilities for defacement and unauthorized modification of corporate websites.
- Search for back door traps in the programs.
- Attempt to overload the system using DDoS (Distributed Denial of Service) e.g. Botnet and DoS (Denial of Service) attacks.
- Check if commonly known bugs in the software, especially the browser and the email software exist.

## 6. **Vendor & Site Audit:**

### 6.1.1 Vendor Audit

Vendor Audit is a process of evaluating and assessing the IT-related practices and controls of a third-party vendor or supplier. **Vendor Audit** shall cover specific aspects of the vendor's operations, such as data security, compliance with contractual agreements, service level agreements (SLAs) and adherence to industry standards, regulations. This shall be done as per scope given in RBI Master Direction on Outsourcing of Information Technology Services 2023, other regulatory guidelines and Bank's outsourcing policy. In the case of infrastructure hosted at Vendor site, Auditor will conduct On-Site visits to the vendor's facilities to access physical security measures and observe their operational practices. The Audit typically begins with a risk assessment to identify potential vulnerabilities or weaknesses in vendor's systems or processes that could pose a risk to the organization.

### 6.1.2 Site Audit for Various IT Infrastructure/Facilities like Data Centre, Treasury, CTS Centers, ATM vendor site etc.

As part of the audit the following are to be covered

- Bangalore Datacenter,
- Kolkata Datacenter/DR,
- Treasury Mumbai,
- CTS-(New Delhi, Chennai, Mumbai or any other new location)
- Near DR Site-Bangalore,
- ATM Switch Audit at Mumbai
- Prepaid Card Facility Chennai
- POS Infrastructure Facility

- SMS system,
- Card printing facility (Chennai & Pune),
- SWIFT centers
- Vendor's Sites wherever applicable

Site Audit shall cover but not limited to the following aspects

- Changes in System/process related to RBI and other Statutory Bodies Circular /Guidelines
- Review of PCI DSS Report Compliance (ROC) and Attestation of Compliance (AOC) during site Audit.
- Data Security steps taken by Vendor
- Review of VA and PT report of Vendor during Site Audit
- Financial Strength of the Vendor

The Data Centre facilities Audit at the above-mentioned sites shall cover but not limited to the following aspects:

- Building Management Systems
- Power Supply, UPS & DG
- Logical Access Control
- Physical Access Controls
- Environment Control
- Datacenter infrastructure - network cabling, raceways, server/ Communication racks, Rack Power Distribution Units (PDU), KVM
- Fire & Smoke, Water leak Detection and suppression Systems
- Air-conditioning: -Temperature & Humidity Control Systems
- Assets safeguarding, Handling of movement of Man /Material/Media/ Backup / Software/ Hardware / Information.
- Surveillance systems.
- Pest prevention (rodent prevention) systems.
- Lightning Protection
- Training, Documentation, Monitoring, Duty List, Storage Management
- Asset Register, asset tracking, asset management
- High availability

**Note: Any new addition/up-gradation in sites, hardware, software, new deliverables and change in architecture or due to regulatory requirement during the contract period will also be covered in the scope of this audit without any additional cost to the bank.**

## **7. Application Audit**

Application audit shall be conducted for all applications within the bank based on the checklist approved from the Vertical Head of Audit and Inspection Department. Entire checklist based on the applicability shall be covered for each audit.

Some critical applications are CBS (Domestic & Overseas), Internet Banking (Domestic & Overseas), ADC channels, GBM, LAPS, MMS, NEFT,



RTGS, SWIFT, UPI, BBPS, IMPS, DMS, Mobile Banking, CTS, Biometric Authentication System (BAS), AEPS etc.

The Application audit shall cover but not limited to the following aspects:-

- Controls for performing/changing parameter setup of functionality across applications.
- Segregation of duties.
- Application parameterization process.
- Availability of necessary audit logs and its accuracy and effectiveness.
- Adherence of reporting to legal and statutory requirements.
- Automated batch processing, scheduled tasks, critical calculations etc.
- End of Day, Start of Day, period closure operations including End of Month, End of Quarter and End of Year operations.
- Integration with Delivery Channels including data and transaction integrity for the same
- Release of software governed by formal procedures-ensuring sign-off through testing, handover etc.
- Formal procedure for change management being adopted.
- Impact analysis of changes made.
- Associated documents and procedures being/to be updated accordingly.
- Maintenance personnel have specific assignments and that their work is properly monitored. Their system access rights are controlled to avoid risks of unauthorized access to automated systems.
- Regular updation of job cards , SOPs with new version releases.
- If outsourced, escrow arrangement with application vendors.
- Interfacing between Finacle/ADC & other ancillary Applications.
- Controls for opening/modifications of Office Accounts /GL heads.

**8. Database Audit (CBS, ADC, LAPS, RTGS, NEFT, ITMS, RBIA, GBM, MISADF, M-Banking, E-Banking, UPI, IMPS, PFMS, SWIFT, Smart Fee Collection System, GST, BBPS etc. (approximately 80 databases)).**

The Database audit shall cover but not limited to the following aspects:--

- Role of DBA
- Authorization, authentication and access control review.
- Audit of data integrity controls.
- Database Backup Management.
- Review of Database privileges assigned to DBAs/Users.
- Security of Oracle systems files.
- Review of Users having access to the Database Server
- Synchronization between DC & DR Databases for CBS/Alternate Delivery Channels (ADC), between Treasury Primary Database at Mumbai & Treasury DR Database at Kolkata and between MISADF Database at Kolkata & Treasury DR Database at Mumbai etc.
- Patch Management.

- Review of control procedures for changes to parameter files.
- Review of Control procedures for sensitive DB passwords.
- Review of Control procedures for purging of Data Files.
- Review of Procedures for data backup, restoration, recovery and readability of backed up data.
- Maintenance/Monitoring/Review of Audit log and Archiving

**9. Performance Testing – Load Testing, Stress Testing, Capacity testing and Spike Testing of following applications:**

- UCO mBanking plus
- BHIM UCO UPI
- UCO Secure (Digisafe)
- mPassbook (Domestic)
- mPassbook (Singapore)
- mPassbook (Hongkong)
- UCO Pay+
- Corporate mBanking
- NPA tracker
- UCO Cluster
- UCO Sandeh Nivaran (Cloud environment)
- UCO ARBD mobile app
- UCO Merchant etc.

**10. Network Audit**

The Network audit shall cover but not limited to the following aspects:--

- Overall Network architecture
- Overall Network management
- Review of detailed Network architecture
- Network traffic analysis and base lining
- Virtual LANS (VLANs) & Routing.
- Evaluate procedures adopted for:
  - i. Secured transmission of data through leased line/VPN/VSATs/ MPLS, Wireless etc.
  - ii. Bandwidth management
  - iii. Uptime of network – its monitoring as per SLA.
  - iv. Fault management
  - v. Capacity Planning
  - vi. Performance Management.
  - vii. Monitoring of logs.
- Verification of Network Devices for any security threats
- Configuration Checking vis-à-vis load and Access control audit for all the Networking Devices viz. Routers, Switches, IDS/IPS, Firewalls, Servers etc.
- Access list in networking devices for securing data transmission.
- Structured LAN cabling in DC and DR.
- Carry out “war driving” (or equivalent exercise) to identify rogue access points and mis-configured access points.
- Integration of various extranet with Bank's network.

## **11. Firewall Rule Based Review**

All the configuration output of the firewall rules shall be captured and studied, policy/rule-wise, manually or using the tools so that any mis-configuration residing may be mitigated.

## **12. Assessment of KPI & KRI**

As per RBI Circular Ref.No.DBS(CO).CSITE/9094/31.01.015/2016-17 dated 23.05.2017, "CISO shall develop Cyber Security KRIs and KPIs and get an independent assessment of the same including its coverage at least on a quarterly basis". Assessment of KRIs and KPIs prepared by CISO.

## **13. Audit for Sustenance of ISO-27001 Certification for DC-DR Operations:**

Auditor for Internal Audit shall provide onsite handholding support to Bank prior to the Surveillance Audit(s) and liaise with the External Auditor, each year, for sustenance of ISO-27001 Certification. During the course of Certification, broadly following documents have been provided / created and shall be made available for the on boarded Auditor:

1. ISMS Scope, Framework and Policy.
2. Risk Treatment Plan / Risk Management Register.
3. Statement of Applicability
4. Measurement of Effectiveness.
5. Internal Audit Report.
6. Corrective and Preventive Actions (CAPA) Report.

Department envisages the following scope for the Auditor to be on boarded for Internal Audit in regard to the sustenance of ISO-27001 Certification:

1. Guidance for compliance of non-Complied items mentioned in Risk Management Register.
2. Ensure sustenance of the complied items mentioned in the Risk Management Register.
3. Conducting Internal Audit before commencement of Final Audit each year for ascertaining the readiness of Bank for the Final Audit and recommending for the same.
4. Liaising with External Auditor for smooth conduct of ISO-27001 Compliance Audit (the details of the Audit Firm shall be shared with the selected bidder for liaising).  
Any other items relevant to ISO-27001 Certification as per standard may be part of the scope.

#### **14. AUDIT OF CHANGE LOGS**

Audit of Change Logs refers to the process of reviewing and examining the records that documents changes made to a system, software application, database, or any other type of information system. Change logs are typically used to track and record modifications, updates, or alterations made to these systems over time.

#### **15. SECURITY AUDIT OF CLOUD SERVICES**

IS Audit of Cloud Services shall be conducted for assurance on deployment of cloud security on systems hosted in clouds.

It shall also be conducted as and when any new IT Infrastructure or application is introduced or migrated to cloud.

#### **16. SECURE CONFIGURATION REVIEW/AUDIT**

Secure Configuration Review of Operating System (OS) and Database (DB) shall be done on yearly basis. Configuration Audit of Servers, Network and Security Devices covering critical Applications, like CBS (domestic and overseas), Mobile Banking, Internet Banking, UPI, GBM, RTGS, NEFT, SWIFT, etc.

The configuration review shall be done based on the Secure Configuration Documents.

#### **17. AUDIT OF STORAGE OF PAYMENT SYSTEM DATA**

Audit to ensure that the entire data relating to payment systems operated by them are stored in a system only in India as per RBI and other regulatory guidelines. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required.

#### **18. SYSTEM AUDIT REPORT (SAR) NSDL**

The audit will be conducted as per the checklist provided by NSDL and all the points of the checklist are required to be addressed.

#### **19. IS AUDIT OF AADHAAR USER AUTHENTICATION (AUA)**

As per Regulation 14(1)(h) of Aadhaar (Authentication and Offline Verification) Regulations, 2021, operations and systems are audited by information systems auditor certified by a recognized body on an annual basis to ensure compliance with the Authority's standards and specifications and the audit report should be shared with the Authority upon request;

"Compliance checklist for certifying compliance with controls that the AUA/KYC User Agency (KUA) is required to have in place."

Compliance checklist for certifying compliance with controls that the AUA/KUA is required to have in place Version 1.0 [issued in March 2024] and latest version also.

## 20. AUDIT OF DIGITAL LENDING

Periodic validation tests of the algorithm/model used in Business Rule Engine (BRE) – once in six months during the first two years and suggest any remedial measures basis operational audit observations.

IS Audit of digital lending IT Infrastructure and Process Audit of new product before moving into live

Regular audit of Digital Lending Process and compliance thereon (at least annually).

## 21. CYBER SECURITY FRAMEWORK REVIEW

As part of IS Audit Program, the adequacy and adherence to the controls of RBI's Cyber Security Framework and other applicable regulatory guidelines will be reviewed and measured, to assess the level of risk /preparedness arising due to newer threats in products or processes.

## 22. SWIFT Customer Security Program (CSP) Assessment

SWIFT Customer Security Controls Framework (CSCF) (latest version – Current version is CSCF - V2025)

The SWIFT Customer Security Controls Framework (CSCF) consists of mandatory and advisory security controls for SWIFT users. The controls evolve over time to combat new and arising threats and to implement new developments in Cybersecurity.

## 23. AUDIT OF VIRTUAL MACHINES (VMs)

An audit of Virtual Machines (VMs) includes:

- (a) **Access Controls** – Review user access, authentication, and privilege management.
- (b) **Configuration Management** – Check VM settings, hardening, and compliance with security baselines.
- (c) **Patch Management** – Verify OS and application updates.
- (d) **Logging & Monitoring** – Ensure logging is enabled and logs are reviewed.
- (e) **Backup & Recovery** – Assess backup frequency, integrity, and restoration process.
- (f) **Network Security** – Review firewall rules, segmentation, and traffic monitoring.
- (g) **Resource Utilization** – Analyze CPU, memory, and storage usage.
- (h) **Incident Response** – Check for security event handling procedures.
- (i) **Encryption & Data Protection** – Validate encryption for data at rest and in transit.

**Compliance & Policy Adherence** – Ensure alignment with regulatory and internal policies.

## **24. Comprehensive Cyber Security Audit of Applications, Platforms, and Databases related to CBS**

Comprehensive audit should cover the entire application, including the following:

- (a) web application (both thick client and thin client);
- (b) mobile apps;
- (c) APIs (Including API whitelisting);
- (d) databases;
- (e) hosting Infrastructure and obsolescence;
- (f) cloud hosting platform and network infrastructure; and
- (g) Aadhaar security compliance as mandated under the Aadhaar Act, 2016, the regulations made thereunder and Aadhaar Authentication Application Security Standard available on UIDAI's website (irrespective of whether or not the application owner/administrator is a requesting entity under the Act, the cybersecurity compliance for Aadhaar use should be benchmarked against the said standards as the relevant Information security best practice, including, in particular, use of Aadhaar Data Vault for storage of Aadhaar number and Hardware Security Module for management of encryption keys).

Limited audit shall be performed six months after the comprehensive audit, and should be carried out even earlier if there is—

- (a) modification in application functionality; or
- (b) addition/modification of APIs; or
- (c) migration to new infrastructure platform or cloud service; or
- (d) change in configuration of application hosting, servers, network components and security devices; or
- (e) change in access control policy.

## **25. Audit/Review of Software Bills of Material (SBOM) and Cryptography Bill of Materials (CBOM)**

Regular audits and assessments of SBOM and CBOM processes should be conducted to ensure accuracy and completeness. An SBOM is a list of all the components, libraries and modules that make up software providing transparency into its composition.

## **26. Cyber Security Audit/Assessment/Risk Assessment as per C-RAF framework of HKMA for Hongkong**

Cyber Security Audit/Assessment/Risk Assessment of Hongkong centre of Bank having one branch as per Cyber Resilient Assessment Framework of Hong Kong Monetary Authority (HKMA).

## **27. MAS Cyber Audit/Risk Assessment as per TRM framework of MAS for Singapore**

Cyber Security Audit/IT Risk Assessment of Singapore centre of Bank having one branch as per Technology.

## **28. MIGRATION AUDIT**

Data Migration Audit will verify the migration of the legacy system to the new system with minimal disruption or downtime, with data integrity and no loss of data.

## **29. VA/PT OF INTERNET CONNECTED PCs**

VA/PT (Vulnerability Assessment and Penetration Testing) of Internet connected Desktops/ PCs of Corporate Departments shall be done.

## **30. SECURITY CUM FUNCTIONAL AUDIT OF NEW APPLICATIONS:**

Security cum Functional Audit of approximately 100 applications per year will be done before GO-Live for New in-house developed application/ After Major Changes in existing applications (both in-house and developed by external vendors). Scope of Security cum Functional Audit include:-

- Functionality implemented vis-à-vis the Bank's requirements.
- Input, processing and output controls across various schemes across the bank.
- Coverage and adequacy of UAT test cases.
- IS Audits i.e. Vulnerability Assessment, Penetration Testing, External Assessment, Configuration Audit, Data Migration Audit, Application security Audit etc.
- Controls for performing/changing parameter setup of functionality across applications.
- Through-put validation.
- Automated batch processing, scheduled tasks, critical calculations etc.
- IT General Control Review.
- In case of web based application, the validation against top 10 OWASP, CWE/SANS Top 25 vulnerabilities, etc.
- Regular updation of job cards with new version releases.
- Checks against network attacks.
- Code Review, wherever possible.
- Code obfuscation.
- Application Security & Controls Review.
- Database Security & Integrity Review.
- Review of Interface Controls with other applications (both Internal and External).

- Review of Network & Communication Controls with relation to the application package.
- Test of robustness of the system by running a specific number of transactions on it.
- Evaluation of Efficiency & Effectiveness of the package vis-à-vis business processes and requirements. Whether the objectives of the application are likely to be fulfilled by implementation.
- Assessment of the risk component in the package.
- Compliance testing of the changes in software made for mitigation of the discrepancies pointed out in the audit report.

### **31. Forensic Audit/ Forensic Analysis/Investigations:**

- Bank may assign Forensic Analysis/Investigations as per the requirement, same to be conducted as by adhering following minimum guidelines:
- The bidder should have well established procedure for conducting Forensic Analysis/Investigation and the same shall be provided to Bank.
- The original evidence should be acquired in a manner that protects and preserves the integrity of the evidence and examination of the evidences should be done in the copy of the original evidences.
- Persons conducting an examination of digital evidence should have been suitably trained and should have sufficient experiences.
- Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review.
- The process or lifecycle of doing forensics should be followed as per the Industry best practice and regulatory guidelines.
- The bidder shall provide their findings with recommendations in report format as per the incidence investigation process.
- Bidder should arrange to deployment of forensic team within 1 hour of reported incidences.

### **TYPES OF AUDIT & FREQUENCY OF AUDIT**

The IS Auditor shall broadly cover but not limited to the following Audit Types at defined frequency per Audit Round.

<b>Sl. No.</b>	<b>Type of IS Audit</b>	<b>Frequency</b>
1.	PENETRATION TESTING (PT) (EXTERNAL/INTERNAL)	Half Yearly
2.	VULNERABILITY ASSESSMENT (VA)	Half Yearly/Quarterly, as applicable



3.	APPLICATION AUDIT	Yearly
4.	MIGRATION AUDIT	As and when required.
5.	PROCESS AUDIT	Yearly
6.	NETWORK ARCHITECTURE REVIEW	Yearly
7.	FIREWALL RULE BASED REVIEW	Half Yearly
8.	SOURCE CODE AUDIT/REVIEW	Yearly
9.	DATABASE AUDIT	Yearly
10.	KRIs and KPIs Prepared by CISO OFFICE	Quarterly
11.	VA/PT OF INTERNET CONNECTED PCs	Half Yearly
12.	SECURITY AUDIT OF CLOUD SERVICES	Yearly
13.	PERFORMANCE TESTING	Yearly
14.	AUDIT OF CHANGE LOGS	Quarterly
15.	VENDOR & SITE AUDIT	Yearly
16.	SECURE CONFIGURATION REVIEW/ CONFIGURATION AUDIT	Yearly
17.	GOVERNANCE AUDIT	Yearly
18.	AUDIT OF STORAGE OF PAYMENT SYSTEM DATA	Yearly
19.	SYSTEM AUDIT REPORT (SAR) NSDL	Yearly
20.	IS AUDIT OF AADHAAR USER AUTHENTICATION (AUA)	Yearly
21.	PRE-IMPLEMENTATION AUDIT OF NEW APPLICATION (SECURITY & FUNCTIONAL)	As and when required.
22.	AUDIT OF DIGITAL LENDING	Yearly
23.	RBI CYBER SECURITY FRAMEWORK REVIEW	Yearly
24.	SWIFT CSP Assessment	Yearly
25.	AUDIT OF VIRTUAL MACHINES (VMs)	Yearly
26.	Comprehensive Cyber Security Audit of Applications, Platforms, and Databases related to CBS	Yearly (One Time)
	Limited audit shall be performed six months after the comprehensive audit	Half Yearly
27.	Audit/ Review of Software Bills of Material (SBOM) and Cryptography Bill of Materials (CBOM)	Yearly or as and when required.
28.	Information Security Management System (ISMS) for ISO 27001:2022 Certification Sustenance	Yearly
29.	Forensic Audit/ Forensic Analysis/Investigations:	As and when required
30.	Cyber Security Audit/Assessment/Risk Assessment as per C-RAF framework of HKMA for Hongkong	Yearly
31.	MAS Cyber Audit/Risk Assessment as per TRM framework of MAS for Singapore	Yearly

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