Scope of work for Information Systems Audit, Cyber Security and EDP Audit

The Audit to cover

1) RBI Circular No. UBD.BPD.Cir.No. 71/12.09.000/2013-14 dated June 11, 2014 on Introduction of Information System(IS) Audit for Urban Cooperative Banks
2) RBI Circular DCBR.CO.BPD. (PCB).MC.No.3/12.05.001/2015-16 dated July 1, 2015 on Master Circular on Inspection & Audit Systems in Primary (Urban) Co-operative Banks.
3) RBI Circular DCBS.CO.PCB.Cir.No.1/ 18.01.000/2018-19 dated October 19, 2018 on Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs).
4) DoS.CO/CSITE/BC.4083/31.01.052/2019-20 dated December 31, 2019 on Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach.
5) IS Security Policy and Cyber Security Policy of the Bank.
6) RBI/2023-24/102,DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 dated 10.04.2023, Master Direction on Outsourcing of Information Technology Services
7) RBI/2024-25/99 CO.DPSS.RPPD.No.S987/04.03.001/2024-25 dated 30.12.2024 Introduction of beneficiary bank account name look-up facility for Real Time Gross Settlement (RTGS) and National Electronic Funds Transfer (NEFT) Systems
8) RBI/2024-25/31 DOR.ORG.REC.21/14.10.001/2024-25 dated 30.4.2024 Guidance Note on Operational Risk Management and Operational Resilience.
9) RBI/2024-25/83 CO.DPSS.POLC.No.S-708/02-12-004/2024-25 dated 11.10.2024 Facilitating accessibility to digital payment systems for Persons with Disabilities – Guidelines.
10) RBI/2023-24/132 DOR.RAUG.AUT.REC.No.81/24.01.041/2023-24 dated 7.3.2024 Amendment to the Master Direction - Credit Card and Debit Card – Issuance and Conduct Directions, 2022.
11) DoS.CO.CSITE.SEC.No.1852/31.01.015/2020-21 dated February 18, 2021 – Master Direction on Digital Payment Security Controls, as amended from time to time.
12) Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds- Implementation of recommendations. (As specified in para (ii) of the Annex to Master Direction on Information Technology, Governance, Risks, Controls and Assurance Practices dated November 07, 2023, as amended from time to time)
13) UBD.No.Admn.46b/17:36:00/97-98 dated March 30, 1998 – Risks and Control in Computer and Telecommunication Systems, as amended from time to time.
14) DOS.CO.FMG.SEC.No.6/23.04.001/2024-25 dated July 15, 2024 – Master Direction on Fraud Risk Management in Urban Cooperative Banks (UCBs) /State Cooperative Banks (StCBs) / Central Cooperative Banks (CCBs), as amended from time to time.
15) RBI/2025-26/28 CO.DIT.DCD.No.S81/01-71-110/2025-26 dated 22.04.2025 Circular - Migration to '.bank.in' domain.
16) RBI/2025-26/33 DCM.RMMT.No.S312/20-02-001/2025-2026 dated April 28, 2025, Dispensation of ₹100 and ₹200 denomination banknotes through ATMs.
17) RBI/2025-26/31 DCM (NPD) No.S287/18.00.014/2025-26 April 24, 2025 Note Sorting Machines: Standards issued by the Bureau of Indian Standards - Revised Timeline for Implementation.

18) RBI/2024-25/105 CEPD.CO.OBD.No.S1270/50-01-001/2024-25 dated 17.01.2025 Prevention of financial frauds perpetrated using voice calls and SMS – Regulatory prescriptions and Institutional Safeguards.

19) RBI/DOR/2025-26/293 DOR.ORG.REC.No.212/21-04-158/2025-26 Reserve Bank of India (Urban Co-operative Banks – Managing Risks in Outsourcing) Directions, 2025.

20) RBI/2025-26/79 CO.DPSS.POLC.No. S 668/02-14-015/2025-2026 September 25, 2025 Reserve Bank of India (Authentication mechanisms for digital payment transactions) Directions, 2025.

21) RBI/DOR/2025-26/278 DOR.AUT.REC.No.197/24-01-041/2025-26 November 28, 2025 Reserve Bank of India (Urban Co-operative Banks – Credit Cards and Debit Cards: Issuance and Conduct) Directions, 2025.

22) RBI/DOR/2025-26/385 DOR.RAUG.AUT.REC.308/24.01.041/2025-26 Reserve Bank of India (Urban Co-operative Banks – Digital Banking Channels Authorisation) Directions, 2025.

23) RBI/2025-26/77 CO.DPSS.ODD.No.S604/06-08-024/2025-2026 September 05, 2025 Returns – Department of Payment and Settlement Systems – Submission in CIMS.

24) RBI/2010-11/494 DBS.CO.ITC.BC.No. 6 /31.02.008/2010-11 April 29, 2011-Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds-Implementation of recommendations.

25) C-Site Advisory UCB-2/2025 dated 19.8.2025

26) Reserve Bank of India (Urban Co-operative Banks – Digital Banking Channels Authorisation) Directions, 2025, RBI/DOR/2025-26/385DOR.RAUG.AUT. REC.308/24.01.041/2025-26 dated November 28, 2025

27) Reserve Bank of India (Urban Co-operative Banks – Managing Risks in Outsourcing) Directions, 2025, RBI/DOR/2025-26/293 DOR.ORG.REC. No.212/21-04-158/2025-26 dated November 28, 2025.

1. The Auditor to conduct and test vulnerabilities (VA) once in 6 months and (PT) at least once a year for all critical IT assets and those on DMZ including and applicable to Internet Banking application & Mobile Banking application and also to comment on the same in terms of the Bank's circular no. 2018-19/39 on Policy Document on Cyber Security.
2. The auditor to conduct the VA/PT from Bank Internal as well as external environment using red team exercises. The auditor needs to access their own Application-account- during the red box testing.
3. The Auditor to conduct Cyber security audit for all critical IT assets and comment on the same in terms of various circular issued by RBI on Cyber Security.
4. Certificate to be issued by CERT-IN empanelled Auditor as per directives from RBI (Ref: Data Localization Guidelines on April 6, 2018 under the Payment and Settlement Systems Act, 2007) stating the following:-

"All system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction".

5. Compliance report of the RTGS & NEFT related systems by a CERT-In empanelled IS auditor as per RTGS procedural guidelines dated 21.10.2024 & NEFT procedural guidelines dated 15.2.2024 & 25.10.2024.

6. To set out timelines to remediate the Vulnerabilities observed during the Penetration Testing.

7. The type of Penetration Testing/ scan which will be performed (Eg; Network/Application layer), to be clearly mentioned in the report.

8. Details such as the clear roles & responsibilities for managing this VAPT exercise to be mentioned as per Information Security Management System Policy mentioned under Exceptions.

9. Configuration Benchmarks/approach followed while performing VAPT (Eg. OWASP Top 10, NIST guidelines etc.) to be clearly mentioned in the Audit report

10. The Penetration Testing at Application layer must cover the following techniques to identify known Vulnerabilities on the Bank's Public facing applications such as Mobile banking, PFMS & Internet Banking (citizencreditbank.com).
    - a.1.i. Parameter Tampering/ Cookie Poisoning/Session hijacking.
    - a.1.ii. User privilege escalation/ Credential manipulation/ Forceful Browsing
    - a.1.iii. Backdoors & Debug Options/ Input validation bypass.
    - a.1.iv. SQL injection/Cross-site scripting.

Additionally, Auditor to conduct the Network Penetration Testing on public facing Servers hosting Critical Applications such as Mobile banking, PFMS and Internet Banking (citizencreditbank.com & citizencredit.bank.in).

1. Branch Routers & Switches to be included for VAPT Assessment.

2. In Application Security Life cycle, the types of security testing to be conducted (Static/ Dynamic), methodology used, approach followed while testing (OWASP Top10 or any other standard), Clear roles and responsibilities for managing this application security as per the Bank's Risk Exception Policy in case of any deviation, has to be included in the report. Follow a 'secure by design' approach in the development of critical applications. Further, ensure that applications are inherently more secure by embedding security within their development lifecycle.

The following guidelines mentioned below with regards to IS audit to be incorporated:-
1. The specialized nature of the Information Systems (IS) auditing and the skills necessary to perform such audits require standards that apply specifically to IS auditing. Such standards will require to be internationally accepted standards only. This will ensure that the IS auditor performs auditing, conforming to the minimum level of acceptable performance and meeting the required professional responsibilities.

2. The IS auditing Standards define the mandatory requirements for IS auditing and reporting. The IS auditing Guidelines provide the guidance for the application of the IS auditing standards. The IS auditor should take care of how to achieve the implementation of the Standards, the use of professional judgment in the application of the Standards and should also be prepared to justify any departure/deviation there from in the IS auditing work.

3. The IS auditor shall prepare the procedure including the information on how to meet the Standards while performing the IS auditing work. However, the procedure shall not set the requirements for IS auditing.

4. IS auditing should be performed by personnel with the required expertise and skills such as Certified Information Systems Auditor, Certified Information Systems, Security Professionals etc.

5. The profitability and the future viability of the organizations in the banking and financial sector increasingly depends on the continued, secured and uninterrupted operations of the Information Systems. Therefore, it is essential for the IS auditors to be conversant with various aspects of Information Technology and the developments taking place in this area. The role of the IS auditors is to see that the organization's assets are protected and suitable internal controls are in place to protect its information and information resources.

IS audit is responsible for providing an organization with independent and objective views on the level of security that should be applied to the Information Systems. Computer Security on the other hand is responsible for implementing security in the computerized environment. The IS auditor will learn to co-exist with the Computer Security function and work together for the benefit of the whole organization ensuring that professional standards are maintained at all times.

6. Major areas, which will require to be IS audited, are broadly as under:
a) Safeguarding of Assets
b) Data Integrity
c) System Effectiveness
d) System Efficiency
e) Organization and Administration
f) Business Continuity Operations
g) Data privacy protection

7. Few pointers for IS auditing of the above areas at the micro level are as under:

a) Safeguarding of Assets:
The IS auditors will require to concentrate on the following areas to ensure that the Information Systems Assets of the organization are safeguarded:
a) Environmental Security
b) Data
c) Uninterrupted Power Supply
d) Electrical Lines
e) Data Cables & Networking Products
f) Fire Protection
g) Insurance of Assets
h) Annual Maintenance Contract
i) Logical Security & Access Control - Operating System Level
j) Logical Security & Access Control – Application System Level

The IS auditor shall be required to verify/inspect the following points in respect of the areas mentioned above.

A. Environmental Security :
Checking: (SFMS / CCIL/ CTS)
The IS auditors should verify whether:

a. There is separate room for the server.
b. Server room has adequate space for operational requirements.

c. Server room is away from the basement, water/drainage systems.
d. Server room can be locked and the key being under the custody of the authorized persons (System Administrator) only. Any failed attempts or system tampering as also unscheduled movement in restricted areas, glass breakage or the opening of doors will require to be logged and immediately reported to the Control Staff at the site.
e. Server is not in close proximity to the UPS room.
f. Access to server room is restricted to authorized persons and activities in the server room are monitored.
g. Air-conditioning system provides adequate cooling.
h. Storage devices to keep stationary and other such items are not kept inside the server room.
i. Smoking, eating and drinking are prohibited in the server room to prevent spillage of food or liquid into sensitive computer equipment.
j. Briefcases, handbags and other packages are restricted from the server room, tape library and other sensitive computer area to prevent unauthorized removal of data held on removable media as also to prevent entry of unacceptable material into the area.
k. Server room is neat and clean to ensure dust free environment.

A. Uninterrupted Power Supply :
Checking: (SFMS / CCIL/ CTS / (server room))/Branch/Department Level

a) Maintenance agency provides battery service regularly.
b) There is a regular contract for maintenance of the UPS and the preventive maintenance is carried as per the contract.
c) The record of the tests undertaken is maintained to verify the satisfactory functioning of the UPS.
d) UPS cabin has adequate ventilation to take care of acid fumes emitted by the Lead Acid batteries.
e) Capacity of the UPS system is sufficient to take care of the electricity load required for computers installed.
f) UPS is free of the electricity load relating to the tube-lights, fans, water coolers etc.
g) UPS functions properly when electricity fails.

A. Electrical lines :
Checking: (SFMS / CCIL/ CTS (server room))/Branch/Department Level
The IS auditors should verify whether:

a) Power supply to computer equipment is through UPS system only.
b) The electrical wiring looks concealed and is not hanging from ceiling or nodes.
c) The circuit breaker switches exist in locked condition only.

A. Data Cables :
Checking: Central server level /Branch/Department Level
The IS auditors should verify whether:

a) A map of the cable layout is kept in a secure place with proper authority. This is helpful in timely and fast repairs of LAN cable faults.
b) Electrical cable and data cable do not cross each other to avoid possible disturbance during data transfer within the network.

A. Insurance :
Checking: Central Server Level
The IS auditors should verify whether:

a) All the computer equipment are covered under the appropriate electronic equipment insurance policy with a reputed insurance firm.

b) A record of the original policy is maintained with the detailed list of the equipment covered under the policy.
c) Information regarding shifting of computer equipment to or from or within the department/office is conveyed to the insurance firm.
d) Adequacy of the insurance cover should be verified as per the policy of the organization.

A. Annual Maintenance Contract :
Checking: Central Server Level and Branch/Department Level
The IS auditors should verify whether:

a) Stamped agreements for maintenance contract are executed and available.
b) Activities carried out during maintenance have been reported in the registers and duly authenticated.
c) Contract renewal rates are maintained in the register.
d) Access for maintenance purpose is granted only on verifying the identity of the service person.
e) The maintenance staff support is available in time.
f) Right to audit clause is incorporated

A. Logical Security & Access Control – Operating System
Checking: Central Server Level, Dept. of Information Technology Level and Branch/Department Level
The IS auditors should verify whether:

a) Access to the systems is only through password protected user IDs.
b) Operating System (OS) allots unique user identity (ID) for all users.
c) OS provides for different levels of access rights to volumes, directories and files.
d) OS prompts for change of the user password after the lapse of specified periods.
e) OS ensures secrecy and security of the user passwords and the access rights granted to a user.
f) Unrestricted access to the systems is provided only to the System Administrator.
g) Administration level access is restricted to authorized and limited persons.
h) All the security features available in the OS are enabled/taken advantage of as far as possible for ensuring better security.
i) Administration access should not be available to the officials who are under notice period, retiring shortly, under disciplinary action etc.
j) OS provides for loading of virus prevention software and is implemented.
k) Record is maintained and authenticated regarding the installation of the Operating System, its up-gradation, re-installation and maintenance.
l) A register is maintained in respect of all the OS level users, giving the details such as the date of creation, suspension, cancellation, access rights granted, purpose of creation etc.
m) Users created for audit/maintenance purpose are disabled immediately after the work is over.
n) The department reviews the number of the OS level users periodically.
o) Multi / Two factor authentication

A. Logical Security & Access Control – Application System
Checking: Dept. of Information Technology Level and Branch/Department Level

The IS auditors should verify whether:

a) System provides for different levels of access.
b) System prompts for change of user password after lapse of specified period.
c) System ensures secrecy and security of the user passwords and the access rights granted to users.
d) Unrestricted access to the entire application system menus is provided only to a Super User.

e) Super User access in application level is not given to staff who is under notice period, retiring shortly, under disciplinary action etc.
f) The application system user list is periodically reviewed.
g) The access privileges granted in the system are in accordance with the designation/duties performed.
h) None of the staff members has multiple level or duplicate access ID in the system.
i) Allocation of the suspended, disabled user ID to new users is avoided.
j) Active user IDs of the transferred, retired, suspended or dismissed employees are not present in the system.
k) There is no dummy user ID created in the system.
l) The user ID of staff on long leave, training etc. is suspended.
m) System logs out automatically if the user is inactive for a specified time (or user consciously logs out when he/she leaves a terminal).
n) System does not allow concurrent login to a single user ID from different nodes.
o) Users, created for maintenance purpose, are cancelled on completion of the job.
p) The system does not allow user to cancel his/her own user ID.
q) Authority periodically reviews the user login status report.
r) Users do not share their passwords.
s) Passwords of alphanumeric characters are used.
t) Users do not write their passwords on wall, desk diary etc. and are aware of the need for the secrecy of their passwords.
u) System automatically locks the user ID after unsuccessful login attempts.
v) User log indicating date, time, node, user ID, transactions performed etc. are generated by the system and evaluated by the System Administrator.

b) Data Integrity:

Checking: Central Server Level and Dept. of Information Technology Level
The IS auditor will require to address, among others, the following areas under IS auditing:

a) Data Input Controls
b) Data Processing Controls
c) Patch Programs
d) Purging of Data Files
e) Backup of data
f) Restoration of Data
g) Business Continuity Planning
h) Output Reports
i) Version Control
j) Virus Protection

A. Data Input Controls:
The organizations in the banking and financial sector undertake diverse activities relating to the receipt of deposits, advancement of credit, investment of funds etc. Further, the areas of operation and the level of economic activities could also be different. All these activities, the transactions resulting there from, the data inputs required therefore including the data input controls to be in place in the organization will require to be judiciously addressed.
However, illustratively, such data input controls may relate to the following areas of activity and the IS auditors will require to verify the same.

a) The entire stock of cheque books is fed to the system.

b) The cheque books issued are entered and confirmed in the system on day-to-day basis.
c) The data fed in to various accounts including the customer accounts is accurate and correct.
d) Clear administrative guidelines exist regarding the access to live data.
e) Data Owner (DA) and Database Administrator (DBA) are independent of both the systems development and operational activities.

f) The roles of DA and DBA are clearly defined in respect of , among others,
(i) definition, creation & retirement of data, (ii) database availability to Users, (iii) information and services to Users, (iv) maintenance of database integrity and (v) monitoring and performance.

B. Data Processing Controls:

The IS auditor should verify whether:

a) The designated/authorized officials do start-of-day process.
b) The operating staff pay attention to the error messages displayed on the screen and initiates corrective action.
c) Entries are cancelled only by the appropriate authority.
d) Cash entries are not deleted from the system.
e) Prescribed reports are generated at the end-of-day process.
f) Printouts are scrutinized and preserved.
g) Proper record is maintained in respect of the corrections made in database under authentication.
h) Master data printouts are preserved carefully
i) Use of the scanner is monitored and controlled.

C. Patch Programs:

The IS auditors should verify whether:

a) The application programs are exactly identical with the standard list of approved programs in respect of file name, file size, date and time of compilation.
b) Only approved programs have been loaded in the system.
c) There are programs other than the approved ones.
d) There is a record of the patch programs used and the reason thereof under authentication.

D. Back up of Data:

The IS auditors should verify whether:

a) All the external drive/tapes, purchased, pertaining to the OS software, application software and utility programs, drivers etc. are recorded in a register and properly stored.
b) Hardware, software, operating system, printer manuals are properly labelled and maintained.
c) Latest user manuals of the application software and other end-user packages running on the system are available for guidance.
d) Daily/weekly/monthly and quarterly back-up of data is taken without fail and is available (as per requirement).
e) Backup drives/tapes are properly labeled and numbered.
f) Proper storage procedures and facilities are in place for backup copies.
g) There is offsite storage of one set of the backup data.
h) Backup devices are verified/tested periodically by restoring the data and record maintained.
i) Back up media is verified periodically for readability.
j) Record is available in respect of such verification.
k) Backup media are phased out of use after a specified period.
l) Backup register is maintained wherein all the events pertaining to the backup including the procedure of backup are recorded.

m) Physical and fire protection is provided to backup media.

E. Restoration of Data:

The IS auditors should verify whether:

a) The instructions for restoration of the back-up data have been compiled.
b) The data integrity is verified after the restoration work is over.
c) Activities carried out during the restoration work are recorded indicating date, time, reason for restoration and size of the data restored.

F. Output Reports:

The IS auditors should verify whether:

a) The audit trail report generates the user ID of the operator and the official for any addition / modification / deletion of the transaction data effected in the database.
b) List of the cancelled entries is scrutinized and reasons for cancellation are recorded.

G. Virus Protection:

The IS auditors should verify whether:

a) Anti virus software is loaded in the system.
b) Anti virus software is regularly updated to cover software updates against the latest viruses.
c) All extraneous devices are checked for virus including the devices carried by the IS auditors.

a) System Effectiveness:

Checking: Branch/Department Level

The IS auditors should verify whether:

a) Computerized operations provide better customer service in terms of time and quality.
b) Staff serves a larger number of customers during the day than prior to the introduction of online operations.
c) Customer information is provided timely and accurately.
d) The system reflects any improvement in the overall quality of products and services offered.
e) System has improved the tasks accomplishment capacity of its users by enabling them to be more productive.
f) Users are satisfied with the performance of the system.
g) System is user friendly and takes less effort.
h) The users are putting the software to frequent use, which requires less effort and is easier to use and the users are satisfied with the performance of the software.

a) System Efficiency:

Checking: Dept. of Information Technology Level, Central Server Level, Branch/Department Level & Central Office Level

The IS auditors should verify whether:

a) Department/Office ensures the use of every computer asset.
b) Department/Office utilizes every computer asset to its optimum capacity.
c) Periodical maintenance of the hardware asset ensures its uninterrupted service.

d) The online operations help complete day's workload on the same day consuming less time than the time taken for the respective manual operations.
e) The online operations provide accurate, complete and consistent data at each stage of processing.
f) Department/Office takes consistency check of balances daily to aid in the detection of errors or fraud.
g) Department/Office uses the hardware peripherals such as printers, nodes etc. efficiently.

a) Organization and Administration:

Checking: Dept. of Information Technology Level and Branch/Department Level & Central Office Level

The IS auditors should verify whether:

a) There is an Information Systems Security Programme for the entire organization, approved by the Board of Directors.
b) There is a Corporate Information Systems Security Policy, well defined and documented and implemented including Information Systems Awareness Programme.
c) There is an established hierarchy in the organization with a Senior Executive in charge of the implementation of the Corporate Security Policy with Information Systems Security Officials at various levels in an Office.
d) Identified System Administrator for each computerized Office / Department, as required.
e) Job description for each level is prepared and implemented (including System Administrator).
f) Training is imparted to all staff members in turn for better results and output. Emphasis on training pertaining to Cyber Security
g) Dual control aspect is implemented for the important operations.
h) The functions of initiating, authorizing, inputting, processing and checking of the data are separated to ensure that no person has complete control over a particular function.
Therefore, abuse of that function is not possible without collusion between two or more individuals.
i) Rotation of duties is carried out at regular intervals.
j) System Administrator is supervised and controlled with respect to the creation of user ids at the OS level and Application Software level.
k) There are at least 2 persons for key functions of operations to take care of absenteeism.
l) Computers are covered to keep them free from dust, rain water etc.
m) Clear communication from the Management of the organization to the effect that each member of the staff is responsible for maintaining security in the organization, as per the Security Policy.
n) DR - Drill plan and execution

a) Business Continuity Operations

1. Business Continuity Plan (BCP) Documentation

- **Existence and Completeness**: Verify if the Business Continuity Plan is documented and covers all key aspects of business continuity, such as disaster recovery, incident management, and emergency response.
- **Review of Objectives and Scope**: Ensure the plan defines the scope of operations, critical business functions, recovery objectives (RTOs, RPOs), and key roles and responsibilities.

- **Version Control**: Check that the BCP is up-to-date, regularly reviewed, and properly version-controlled.

2. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)

- **Defined RTO/RPO**: Ensure that Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) are clearly defined for all critical business processes.
- **Alignment with Business Needs**: Validate that these objectives are aligned with business requirements and stakeholders' expectations.

3. Roles and Responsibilities

- **Key Personnel Identification**: Ensure that the business continuity team is clearly identified, and their roles and responsibilities are documented.
- **Training and Awareness**: Verify that the team receives regular training and that there is awareness of their roles in the event of an emergency.

4. Backup and Data Recovery

- **Data Backup Strategy**: Review the organization's data backup strategy, including the frequency of backups and the location of backup data (on-site, off-site, or cloud).
- **Testing Data Restoration**: Check if data restoration exercises are regularly conducted to ensure that backups are valid and recoverable.
- **Critical Systems and Data Identification**: Verify that all critical systems and data are appropriately backed up and accessible within the recovery timeframe.

5. Communication Plan

- **Internal Communication**: Review if the BCP includes a communication strategy for internal stakeholders (employees, departments, management) during a disruption.
- **External Communication**: Ensure that there is a clear plan for communicating with external stakeholders (customers, vendors, regulatory authorities) during an incident.

6. Testing and Drills

- **Regular Testing**: Confirm that regular testing of the BCP is done to evaluate the effectiveness of the plan.
- **Test Documentation**: Verify that test results are documented, and action plans are updated based on lessons learned from each test.

7. Third-Party Dependencies

- **Third-Party Risk Assessment**: Ensure that the organization has assessed the business continuity plans of key third parties (vendors, service providers) critical to business operations.
- **Service Level Agreements (SLAs)**: Review SLAs with third parties to confirm they align with the organization's BCP requirements, including acceptable downtime and recovery timelines.

8. Incident Management and Escalation

- **Incident Response Procedures**: Verify that clear procedures are in place for responding to various types of incidents, including escalation protocols and decision-making processes.
- **Incident Logging and Reporting**: Ensure there is a system for logging incidents, tracking progress, and reporting to senior management.

9. Technology and Infrastructure Resilience

- **IT Disaster Recovery**: Review IT disaster recovery plans, including the recovery of hardware, software, and networks.
- **Redundancy and Failover Mechanisms**: Check if critical IT infrastructure has redundancy (e.g., power supply, servers, data centers) and failover mechanisms to minimize service disruption.

a) Data privacy protection

1. Data Privacy Governance

- **Privacy Policies**: Ensure that the organization has a clear and comprehensive **data privacy policy** that is regularly reviewed and updated to reflect changes in regulations and practices.

2. Data Classification and Inventory

- Sensitive Data Classification**:** Verify that sensitive personal data is properly classified**,** and that additional protections are in place.
- Data Minimization: Ensure that data collection is limited to what is necessary for the specific purpose and that unnecessary data is not collected or stored.

3. Data Collection, Consent, and Transparency

- Verify that explicit consent is obtained from individuals before collecting their personal data, where required by law
- Ensure that **privacy notices** or statements are clear, easily accessible, and include information about:
    - Data collection purposes
    - Data sharing practices
    - Retention periods
    - Rights of individuals (e.g., right to access, rectify, or erase data)

4. Data Access and Security

- Ensure that role-based access controls **(**RBAC) are in place to restrict access to personal data based on the needs of the employee's role.
- Verify that personal data **is** encrypted both at rest and in transit, especially sensitive data such as payment information, health records, etc.
- Check that strong authentication (e.g., multi-factor authentication) is enforced for accessing systems containing personal data.

5. Data Retention and Disposal

- Review the organization's data retention policy to ensure that personal data is only kept for as long as necessary and is securely disposed of once no longer needed.
- Verify that mechanisms for secure data deletion (e.g., using data-wiping software, ensuring all copies are destroyed) are in place to prevent unauthorized access to deleted data.

6. Third-Party and Vendor Management

- Ensure that third-party vendors who process personal data on behalf of the organization (e.g., cloud services, payment processors) are subject to appropriate data protection agreements**.**
- Verify that vendor contracts include provisions that require third-party vendors to comply with data privacy laws and implement appropriate security measures.

- Ensure that third-party vendors are audited regularly or subject to independent assessments to verify compliance with data privacy requirements.

7. Data Breach Response and Notification

- **Incident Response Plan**: Ensure the organization has a **data breach response plan** in place, with clear procedures for detecting, reporting, and managing data breaches.
- **Breach Notification**: Verify that the organization has a process for notifying affected individuals and relevant authorities (e.g., regulatory bodies) within the required timelines if a data breach occurs (e.g., within 72 hours under GDPR).
- **Breach Investigation and Remediation**: Check that the organization investigates breaches thoroughly, implements corrective actions, and documents the incident.

8. Employee Training and Awareness

- **Employee Training**: Ensure that employees handling personal data are regularly trained on data privacy best practices, internal policies, and relevant regulations.

Structural Financial Messaging System (SFMS Audit)

The scope of SFMS Audit is as follows:

1. Verification of internal controls on SFMS process at branch level as well as centralized level.
2. Verification of Software and Hardware, if they are according to the norms decided by IDRBT.
3. Verification of Security aspects of Hardware, Software, passwords and digital signatures.
4. Verification of the user rights at the different levels of SFMS system.
5. Verification of messaging system followed for different type of Fund Transfers i.e. RTGS, NEFT, ECS etc.
6. Verification of messaging system followed for Bank Guarantees
7. Verification of records and logs maintained for the past transactions i.e. verification of transactions of at least last 3 months.
8. Verification of Compatibility of CBS Software (Turing from BSG) with SFMS interface.
9. Verification of DRP/BCP arrangements, to confirm the uninterrupted and continuous services.
10. IS Security in terms of Physical Infrastructure, accessibility, OS Application, Connectivity, VAPT, Personnel, Communication System, Database Backup, Monitoring, Archiving, Monitoring, Controls, Logs, Vendor Monitoring, Password Controls. All other features which are necessary for maintenance of security, availability, accessibility and serviceability.

Basic Cyber Security Controls for Primary (Urban) Cooperative Banks (UCBs)

Scope of Audit

1) Inventory Management of Business IT Assets

1.1 UCBs should maintain an up-to-date business IT Asset Inventory Register containing the following fields, as a minimum:

a. Details of the IT Asset (viz., hardware/software/network devices, key personnel, services, etc.) based on 'Configuration of IT assets control' as stated in the Bank IS Policy so that it will take care of facilitating the security measures at all times.

b. Details of systems where customer data are stored

c. Associated business applications, if any

d. Criticality of the IT asset (For example, High/Medium/Low)
e. Minimum, Basic cyber security control framework shall be evaluated yearly to integrate risks that arise due to newer threats, product or processes.
f. Not to use outdated and unsupported hardware or software and monitor software's end-of-support (EOS) date and Annual Maintenance Contract (AMC) dates of IT hardware on an ongoing basis

1.2 Classify data/information based on sensitivity criteria of the information

1.3 Appropriately manage and provide protection within and outside UCB/network, keeping in mind how the data/information is stored, transmitted, processed, accessed and put to use within/outside the UCB's network, and level of risk they are exposed to depending on the sensitivity of the data/information

2) Preventing access of unauthorized software

2.1 Maintain an up-to-date and preferably centralized inventory of authorized software(s)/approved applications/software/libraries, etc.

2.2 Put in place a mechanism to control installation of software/applications on end-user PCs, laptops, workstations, servers, mobile devices, etc. Also, put in place a mechanism to block/prevent and identify installation and running of unauthorized software/applications on such devices/systems.

2.3 The web browser settings should be set to auto update and consider disabling scripts like JavaScript, Java and ActiveX controls when they are not in use.

2.4 Internet usage, if any, should be restricted to identified standalone computer(s) in the branch of a UCB which are strictly separate from the systems identified for running day to day business. If allowed in any of such end points, the same should be adequately secured through proxy servers on an ongoing basis. Internet usage is strictly prohibited in SFMS/NEFT/RTGS infrastructure including the zone where these infrastructures are hosted.

3) Environmental Controls

3.1 Put in place appropriate controls for securing physical location of critical assets (as identified by the UCB under its inventory of IT assets), providing protection from natural and man-made threats.

3.2 Put in place mechanisms for monitoring of breaches/ compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access logs, etc. Appropriate physical security measures shall be taken to protect the critical assets of the UCB.

4) Network Management and Security

4.1 Ensure that all the network devices are configured appropriately and periodically assessed to ensure that such configurations are securely maintained.

4.2 The default passwords of all the network devices/systems should be changed after installation.

4.3 Put in appropriate controls to secure wireless local area networks, wireless access points, wireless client access systems.

4.4 Critical infrastructure of UCB (viz., NEFT, RTGS, CBS, ATM infrastructure) should be designed with adequate network separation controls.

4.5 Conduct yearly security audit for all critical PCs/terminals which are used for
- Accessing corporate Internet Banking applications of Scheduled Commercial Banks (SCBs),
- CBS servers
- Network perimeters

4.6. Network boundary defenses should be multi-layered with properly configured firewalls, proxies, De-Militarized Zone (DMZ) perimeter networks and network-based Intrusion Prevention System (IPS)/ Intrusion Detection System (IDS). Mechanism to filter both inbound and outbound traffic shall be put in place.

4.7 Critical applications which are installed on a shared infrastructure of an Application Service Provider (ASP) shall get application including the infrastructure hosting it subjected to VA/PT through the ASP.

4.8 Security testing should be conducted after any major change in the web/ mobile application before going live. The detected vulnerabilities to be remedied promptly in terms of the risk management/treatment framework, so as to avoid exploitation of such vulnerabilities.

4.9 VAPT to be carried out by professionally qualified teams. Findings of VA/PT and the follow up actions necessitated are to be monitored closely by the Information Security/Information Technology Audit team as well as Top Management.
4.10 Use of firewalls to protect the network perimeter
4.11 Perimeter security implementation and blocking of all unnecessary ports.
4.12 Network segmentation implementation to restrict lateral movement of attacker.

5) Secure Configuration
5.1 The firewall configurations should be set to the highest security level and evaluation of critical device (such as firewall, network switches, security devices, etc.) configurations should be done periodically.

5.2 Systems such as Network, application, database and servers should be used dedicatedly for the purpose for which they have been set up.

5.3 Document and apply baseline security requirements/configurations for all critical devices (end-points/workstations, operating systems, databases, network devices, security devices, etc.) and yearly reviews to be carry out.

5.4 Provide Access to Internet websites/system after white listing on security perimeter device.

6) Anti-virus and Patch Management
6.1 Put in place systems and processes to identify, track, manage and monitor the status of patches to servers, operating system and application software running at the systems used by the UCB officials (end-users).

6.2 Implement and update antivirus protection for all servers and applicable end points preferably through a centralized system.

7) User Access Control / Management

7.1 Disallow administrative rights on end-user workstations/PCs/laptops and provide access rights on a 'need to know' and 'need to do' basis.

7.2 Passwords should be set as complex and lengthy and users should not use same passwords for all the applications/systems/devices.

7.3 Remote Desktop Protocol (RDP) which allows others to access the computer remotely over a network or over the internet should be always disabled and should be enabled only with the approval of the authorized officer of the UCB and shall be accessible securely using VPN (encryption) technology. Logs for such remote access shall be enabled and monitored for suspicious activities. Such access should be immediately stopped, if logging and effective monitoring mechanisms are not implemented. Restricted access in case of exceptions, may be provided only on need basis through Multi Factor Authentication and with appropriate monitoring.

7.4 Implement appropriate (e.g. centralized) systems and controls to allow, manage, log and monitor privileged/super user/administrative access to critical systems (servers/databases, applications, network devices etc.) The solution should enforce strong password policy, separation of duties, multi faction of authentication, and access as per business requirement.

7.5 Enable restricted access to authorized users only from authorized client and severs of ATM/SWIFT application environments.

7.6 Endpoint security policies to white list/blacklist/restrict removable media use should be enforced through central policy system.

7.7 Implement multi-factor authentication (MFA) for all critical applications, especially for privileged accounts.

8) Secure mail and messaging systems

8.1 Implement secure mail and messaging systems, including those used by UCB's partners & vendors, that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.

8.2 Document and implement email server specific controls. All users shall use only Bank registered email-ID/Domains (i.e. for citizencreditbank.com) for sending or receiving of all email messages.

8.3 Bank Email domain shall be enabled for anti-phishing and anti-malware, DMARC controls.

9) Removable Media

9.1 As a default rule, use of removable devices and media should not be permitted in the banking environment unless specifically authorized for defined use and duration of use.

9.2 Secure the usage of removable media on workstations/PCs/Laptops, etc. and ensure erasure/ deletion of data on such media after use

9.3 Get the removable media scanned for malware/ anti-virus prior to providing read/write access

10) User/ Employee/ Management Awareness

10.1 Communicate to users/employees, vendors, partners & all levels of stakeholder including Board and Top Management, security policies covering secure and acceptable use of UCB's network/assets including customer information/data, educating them about cyber security risks and protection measures at their level. The awareness/familiarization will include but not limited to.

- Reasons for Increased Cyber incidents
- Major types of Cyber security threats
- Misconception regarding Cyber attacks
- Consequences/Impact of Cyber Attacks
- Regulatory guidelines on Cyber Security
- Recent Cyber Incident occurred
- Do's and Don'ts on Cyber security (as per Annex I)

10.2 Conduct awareness/training for staff on basic information security controls (Do's/Don'ts), incident reporting, etc.

10.3 Board members may be kept updated on basic tenets/principles of IT risk/cyber security risk at least once a year.

10.4 The end-users should be made aware to never click or open or download an email attachment from unknown sources.

11) Customer Education and Awareness

11.1 Improve and maintain customer awareness and education with regard to cyber security risks

11.2 Educate the customers on keeping their card, PIN etc. secure and not to share with any third party

12) Backup and Restoration

Take periodic back up of the important data and store this data 'off line' (i.e., transferring important files to a storage device that can be detached from a computer/system after copying all the files). Maintain regular and secure backup of critical data and systems, with tested recovery procedures in place.

13) Cryptographic controls

The key length, algorithms, cipher suites and applicable protocols used in transmission channels, processing of data and authentication purpose shall be strong. Internationally accepted and published standards, that are not deprecated/ demonstrated to be insecure/ vulnerable, should be adopted, and the configurations involved in implementing such controls shall be compliant with extant laws and regulatory instructions.

Members to follow the latest IDRBT CA guidelines related to cryptographic devices and digital certificates. Entities should maintain and operationalize required policy in order to ensure that renewal of Digital Security Certificates (DSCs) are undertaken before expiry of ongoing certificates.

14) Vendor/Outsourcing Risk Management

Vendor contracts must have:-

14.1 All the outsourcing service level agreements (SLAs) signed with the vendors must clearly mention the responsibility of the UCB and vendor in case of any failure of services. Exit clause with safeguards like non-disruption, handover support to new Vendor.

14.2 Penalty Clause

14.3. Right to audit clause. Credentials of vendor/third-party personnel accessing and managing the UCB's critical assets Background checks. Non-disclosure and security policy compliance agreements.

14.4 Regulatory changes/upgrades to be provided at no additional cost.

14.5 Undertaking from Vendor to comply with all regulatory requirements on an ongoing basis and submission of annual certificate of compliance.

14.6 The agreements must clearly mention the grievance redressal mechanism to resolve customer complaints

14.7 Vendors' service level agreements shall be periodically reviewed for performance in security controls.

14.8 A formal Risk Assessment for third party vendors/service providers and partners shall be carried out before entering into any key/critical/high value contract by Procurement team.

14.9 Procurement department will yearly conduct effective due diligence, oversight and management of Third party vendors/service providers and partners.

14.10 Regulatory and Supervisory requirements
A) Bank shall take steps to ensure that the service provider employs the same high standard of care in performing the services as would have been employed by the Bank, if the same activity was not outsourced.
B) Bank shall ensure that the outsourcing does not impede the RBI in carrying out its supervisory functions and objectives.
C) Bank shall ensure that the service provider, if not a group company, shall not be owned or controlled by any director, or key managerial personnel, or approver of the outsourcing arrangement of the Bank, or their relatives. However, an exception to this requirement may be made with the approval of Board/ Board level Committee, followed by appropriate disclosure, oversight and monitoring of such arrangements.
D) Usage of Cloud Computing Services

Bank shall adopt the following requirements for storage, computing and movement of data in cloud environments:
1. Cloud adoption ranges from moving only non-business critical workloads to the cloud to moving critical business applications such as SaaS adoption and the several combinations in-between, which should be based on a business technology risk assessment.

2. In engaging cloud services, Bank shall ensure, *inter alia,* that the Outsourcing of IT Services policy addresses the entire lifecycle of data, i.e., covering the entire span of time from generation of the data, its entry into the cloud, till the data is permanently erased/ deleted. The Bank shall ensure that the procedures specified are consistent with business needs and legal and regulatory requirements.

3. In adoption of cloud services, Bank shall take into account the cloud service specific factors, viz., multi-tenancy, multi-location storing/ processing of data, etc., and attendant risks, while establishing appropriate risk management framework. Cloud security is a shared responsibility between the Bank and the Cloud Service Provider.

4. Cloud Governance, Bank shall adopt and demonstrate a well-established and documented cloud adoption policy.

5. Cloud Service Providers (CSP):- Bank shall ensure that the selection of the CSP is based on a comprehensive risk assessment of the CSP. Bank shall enter into a contract only with CSPs subject to jurisdictions that uphold enforceability of agreements and the rights available thereunder to Banks, including those relating to aspects such as data storage, data protection and confidentiality.

6. Cloud Services Management and Security Considerations
a) Service and Technology Architecture: Bank shall ensure that the service and technology architecture supporting cloud-based applications is built in adherence to globally recognised architecture principles and standards. Bank shall prefer a technology architecture that provides for secure container-based data management, where encryption keys and Hardware Security Modules are under the control of the Bank. The architecture should provide for a standard set of tools and processes to manage containers, images and releases. Multi-tenancy environments should be protected against data integrity and confidentiality risks, and against co-mingling of data. The architecture should be resilient and enable smooth recovery in case of failure of any one or combination of components across the cloud architecture with minimal impact on data/ information security.

b) Privileged Access Management (PAM): PAM shall be agreed upon with the CSP and ensured for providing role-based access to the cloud hosted applications, in respect of user-access and privileged-access. Access provisioning should be governed by principles of 'need to know' and 'least privileges'. In addition, multi-factor authentication should be implemented for access to cloud applications.

c) Security Controls: Bank shall ensure that the implementation of security controls in the cloud-based application achieves similar or higher degree of control objectives than those achieved in/ by an on-premise application. This includes ensuring - secure connection through appropriate deployment of network security resources and their configurations; appropriate and secure configurations, monitoring of the cloud assets utilised by the Bank; necessary procedures to authorise changes to cloud applications and related resources.

d) Robust Monitoring and Surveillance:
Bank shall accurately define minimum monitoring requirements in the cloud environment. Bank should ensure to assess the information/ cyber security capability of the cloud service provider (CSP), such that, the
i) CSP maintains an information security policy framework commensurate with its exposures to vulnerabilities and threats;
ii) CSP is able to maintain its information/ cyber security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets or its business environment;
iii) nature and frequency of testing of controls by the CSP in respect of the outsourced services is commensurate with the materiality of the services being outsourced by the Bank and the threat environment; and
iv) CSP has mechanisms in place to assess the sub-contractors with regards to confidentiality, integrity and availability of the data being shared with the sub-contractors, where applicable.

V) Implement mechanism to detect and remedy any unusual activities in critical systems, servers, databases, network devices and endpoints

e) Appropriate integration of logs, events from the CSP into the Bank's SOC, wherever applicable and/ or retention of relevant logs in cloud shall be ensured for incident reporting and handling of incidents relating to services deployed on the cloud.
f) The Bank's own efforts in securing its application shall be complemented by the CSP's cyber resilience controls. The CSP / Bank shall ensure continuous and regular updates of security-related software including upgrades, fixes, patches and service packs for protecting the application from advanced threats/ malware.

g) Vulnerability Management: Bank shall ensure that CSPs have a well-governed and structured approach to manage threats and vulnerabilities supported by requisite industry-specific threat intelligence capabilities.

7. Disaster Recovery & Cyber Resilience

a) The Bank's business continuity framework shall ensure that, in the event of a disaster affecting its cloud services or failure of the CSP, the Bank can continue its critical operations with minimal disruption of services while ensuring integrity and security.

b) Bank shall ensure that the CSP puts in place demonstrative capabilities for preparedness and readiness for cyber resilience as regards cloud services in use by them. This should be systematically ensured, *inter alia*, through robust incident response and recovery practices including conduct of Disaster Recovery (DR) drills at various levels of cloud services including necessary stakeholders.

c) Outsourcing of Security Operations Centre
Outsourcing of Security Operations Centre (SOC) operations has the risk of data being stored and processed at an external location and managed by a third party (Managed Security Service Provider (MSSP)) to which Bank have lesser visibility. To mitigate the risks, in addition to the controls prescribed in these Directions, Bank shall adopt the following requirements in the case of outsourcing of SOC operations:
i) Unambiguously identify the owner of assets used in providing the services (systems, software, source code, processes, concepts, etc.);

ii) Ensure that the Bank has adequate oversight and ownership over the rule definition, customisation and related data/ logs, meta-data and analytics (specific to the Bank);

iii) Assess SOC functioning, including all physical facilities involved in service delivery, such as the SOC and areas where client data is stored / processed periodically;

iv) Integrate the outsourced SOC reporting and escalation process with the Bank's incident response process; and

v) Review the process of handling of the alerts / events.

vi) Disaster recovery drills for critical systems should be conducted at least once in a half-year, preferably once a quarter.

14.11. Grievance Redressal Mechanism

Outsourcing arrangements shall not affect the rights of a customer against the bank, including the ability of the customer to obtain redressal as applicable under relevant laws.

14.12 Inventory of Outsourced Services

Bank shall create an inventory of services provided by the service providers (including key entities involved in their supply chains). Further, Bank shall map their dependency on third parties and periodically evaluate the information received from the service providers.

14.13 IT Outsourcing Policy

The policy shall incorporate, *inter alia*, the roles and responsibilities of the Board, Committees of the Board (if any) and Senior Management, IT function, business function as well as oversight and assurance functions in respect of outsourcing of IT services. It shall further cover the criteria for selection of such activities as well as service providers, parameters for defining material outsourcing based on the broad criteria, delegation of authority depending on risk and materiality, disaster recovery and business continuity plans, systems to monitor and review the operations of these activities and termination processes and exit strategies, including business continuity in the event of a third-party service provider exiting the outsourcing arrangement.

14.14 Role of Senior Management

a) Formulating IT outsourcing policies and procedures.
b) Prior evaluation of prospective IT outsourcing arrangements.
c) Identifying IT outsourcing risks as they arise, monitoring, mitigating, managing and reporting of such risks to the Board/ Board Committee in a timely manner.
d) Ensuring that suitable business continuity plans based on realistic and probable disruptive scenarios, including exit of any third-party service provider, are in place and tested periodically.
e) Ensuring (i) effective oversight over third party for data confidentiality and (ii) appropriate redressal of customer grievances in a timely manner.
f) Ensuring an independent review and audit on a periodic basis for compliance with the legislations, regulations, Board-approved policy and performance standards and reporting the same to Board/ Board Committee.
g) Creating essential capacity with required skill sets within the organisation for proper oversight of outsourced activities.

14.15 Role of IT Function

The responsibilities of the IT Function of the Bank shall, inter alia, include:
a) Assisting the Senior Management in identifying, measuring, monitoring, mitigating and managing the level of IT outsourcing risk in the organization.
b) Ensuring that a central database of all IT outsourcing arrangements is maintained and is accessible for review by Board, Senior Management, Auditors and Supervisors.
c) Effectively monitor and supervise the outsourced activity to ensure that the service providers meet the laid down performance standards and provide uninterrupted services, report to the Senior Management; co-ordinate periodic due diligence and highlight concerns, if any; and
d) Putting in place necessary documentation required for contractual agreements including service level management, monitoring of vendor operations, key risk indicators and classifying the vendors as per the determined risk.

14.16 Outsourcing Agreement

a) Agreement shall be legally binding agreement. Bank shall ensure that their rights and obligations and those of each of their service providers are clearly defined and set out in a legally binding written agreement.
b) In principle, the provisions of the agreement should appropriately reckon the criticality of the outsourced task to the business of the Bank, the associated risks and the strategies for mitigating or managing them.
c) The terms and conditions governing the contract shall be carefully defined and vetted by the Bank's legal counsel for their legal effect and enforceability. The agreement shall be sufficiently flexible to allow the Bank to retain adequate control over the outsourced activity and the right to intervene with appropriate measures to meet legal and regulatory obligations.
d) The agreement shall also bring out the nature of legal relationship between the parties.

The agreement at a minimum should include (as applicable to the scope of Outsourcing of IT Services) the following aspects:

Details of the activity being outsourced, including appropriate service and performance standards including for the sub-contractors, if any.

Effective access by the Bank to all data, books, records, information, logs, alerts and business premises relevant to the outsourced activity, available with the service provider.

Regular monitoring and assessment of the service provider by the Bank for continuous management of the risks holistically, so that any necessary corrective measure can be taken immediately.

Type of material adverse events (e.g., data breaches, denial of service, service unavailability, etc.) and the incidents required to be reported to the Bank to enable the Bank to take prompt risk mitigation measures and ensure compliance with statutory and regulatory guidelines.

Compliance with the provisions of Information Technology Act, 2000, other applicable legal requirements and standards to protect the customer data;

The deliverables, including Service-Level Agreements (SLAs) formalising performance criteria to measure the quality and quantity of service levels;

Storage of data (as applicable to the concerned Bank) only in India as per extant regulatory requirements;

Clauses requiring the service provider to provide details of data (related to Bank and its customers) captured, processed and stored;

Controls for maintaining confidentiality of data of Bank's and its customers', and incorporating service provider's liability to Bank in the event of security breach and leakage of such information.

Types of data/ information that the service provider (vendor) is permitted to share with Bank's customer and / or any other party.

Specifying the resolution process, events of default, indemnities, remedies, and recourse available to the respective parties;

Contingency plan(s) to ensure business continuity and testing requirements. Right to conduct audit of the service provider (including its sub-contractors) by the Bank, whether by its internal or external auditors, or by agents appointed to act on its behalf, and to obtain copies of any audit or review reports and findings made about the service provider in conjunction with the services performed for the Bank.

Right to seek information from the service provider about the third parties (in the supply chain) engaged by the former.

Recognising the authority of regulators to perform inspection of the service provider and any of its sub-contractors. Adding clauses to allow RBI or person(s) authorised by it to access the Bank's IT infrastructure, applications, data, documents, and other necessary information given to, stored or processed by the service provider and/ or its sub-contractors in relation and as applicable to the scope of the outsourcing arrangement.

Including clauses making the service provider contractually liable for the performance and risk management practices of its sub-contractors.

Obligation of the service provider to comply with directions issued by the RBI in relation to the activities outsourced to the service provider, through specific contractual terms and conditions specified by the Bank.

Clauses requiring prior approval/ consent of the Bank for use of sub-contractors by the service provider for all or part of an outsourced activity.

Termination rights of the Bank, including the ability to orderly transfer the proposed IT-outsourcing arrangement to another service provider, if necessary or desirable.

Obligation of the service provider to co-operate with the relevant authorities in case of insolvency/ resolution of the Bank.

Provision to consider skilled resources of service provider who provide core services as "essential personnel" so that a limited number of staff with back-up arrangements necessary to operate critical functions can work on-site during exigencies (including pandemic situations);

Clause requiring suitable back-to-back arrangements between service providers and the OEMs; and clause requiring non-disclosure agreement with respect to information retained by the service provider.

14.17 Risk Management Framework

Bank has put in place a Risk Management framework for Outsourcing of IT Services that shall comprehensively deal with the processes and responsibilities for identification, measurement, mitigation, management, and reporting of risks associated with Outsourcing of IT Services arrangements. Risk assessments are documented with necessary approvals in line with the roles and responsibilities for the Board of Directors, Senior Management and IT Function. Such risk assessments shall be subject to internal and external quality assurance on a periodic basis as determined by the Board-approved policy.

The Bank shall ensure that cyber incidents are reported to the Bank by the service provider without undue delay, so that the incident is reported by the Bank to the RBI within 6 hours of detection by the Third party service provider.

The Bank shall review and monitor the control processes and security practices of the service provider to disclose security breaches. The Bank shall immediately notify RBI in the event of breach of security and leakage of confidential customer related information. In these eventualities, Bank shall adhere to the extant instructions issued by RBI from time to time on Incident Response and Recovery Management.

Bank shall effectively assess the impact of concentration risk posed by multiple outsourcings to the same service provider and/or the concentration risk posed by outsourcing critical or material functions to a limited number of service providers.

14.18. Business Continuity Plan and Disaster Recovery Plan

a) Bank shall require their service providers to develop and establish a robust framework for documenting, maintaining and testing Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) commensurate with the nature and scope of the outsourced activity as per extant instructions issued by RBI from time to time on BCP/ DR requirements.
b) In establishing a viable contingency plan, Bank shall consider the availability of alternative service providers or the possibility of bringing the outsourced activity back in-house in an emergency, and the costs, time and resources that would be involved.

14.19 Monitoring and Control of Outsourced Activities

Bank shall have in place a management structure to monitor and control its Outsourced IT activities.

Bank shall conduct regular audits (as applicable to the scope of Outsourcing of IT Services) of service providers (including sub-contractors).The audits shall assess the performance of the service provider, adequacy of the risk management practices adopted by the service provider, compliance with laws and regulations, etc.
Bank, depending upon the risk assessment, may also rely upon globally recognised third-party certifications made available by the service provider in lieu of conducting independent audits.

The Bank shall periodically review the financial and operational condition of the service provider to assess its ability to continue to meet its Outsourcing of IT Services obligations.

In the event of termination of the outsourcing agreement for any reason in cases where the service provider deals with the customers of the Bank, the same shall be given due publicity by the Bank so as to ensure that the customers stop dealing with the concerned service provider.

Bank shall ensure that the service provider grants unrestricted and effective access to a) data related to the outsourced activities; b) the relevant business premises of the service provider; subject to appropriate security protocols, for the purpose of effective oversight use by the Bank, their auditors, regulators and other relevant Competent Authorities, as authorised under law.

14.20 Exit Strategy

a) The Outsourcing of IT Services policy shall contain a clear exit strategy with regard to outsourced IT activities/ IT enabled services, while ensuring business continuity during and after exit. The strategy should include exit strategy for different scenarios of exit or termination of services with stipulation of minimum period to execute such plans, as necessary. In documenting an exit strategy, the Bank shall, *inter alia*, identify alternative arrangements, which may include performing the activity by a different service provider or Bank itself.
b) Bank shall ensure that the agreement has necessary clauses on safe removal/ destruction of data, hardware and all records (digital and physical), as applicable. However, service provider shall be legally obliged to cooperate fully with both the Bank and new service provider(s) to ensure there is a smooth transition. Further, agreement shall ensure that the service provider is prohibited from erasing, purging, revoking, altering or changing any data during the transition period, unless specifically advised by the regulator/ concerned Bank.

15) Application General Control

15.1 Multi factor of authentication to be checked of critical systems like CBS, digital banking applications etc.

15.2 Appropriate and adequate checks and balance to be included in digital banking applications to ensure that customer is using genuine/authorized applications. Customer shall be authenticated centrally and securely.

15.3 Anti-phishing/anti-rogue services to be checked

15.4 Procedure shall be developed to safeguard sensitive business and customer data/information using data loss/leakages prevention strategy for in-house as well as outsourced services.

15.5 For critical applications obtain assurance certificate from the application provider periodically, containing that the application is free from embedded malicious/fraudulent code.

15.6 Ensure following security requirement in the critical application at initial and on-going stages
- System access control,
- Authentication,
- Transaction authorization,
- Data integrity,
- System activity logging,
- Audit trail,
- Session management,
- Security event tracking and exception handling
- Layered security

15.7 Risk based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system across all -delivery channels.

16) Change Management
Each change to business applications, supporting technology, service components and facilities should documented, studied for feasibility, approved and tracked till movement into production.

Effective plan addresses the entire crisis management lifecycle with phases of Detection, Response, Recovery and Containment. Each phase of this lifecycle presents opportunities to protect the Bank from risks, costs, and damage originating from an incident—and to strengthen the Bank defenses going forward:-

(i) Detection/ Technology Readiness:

1. IS Department to design a Security solution which can conduct deep packet inspection on the fly for Bank network.
2. The solution will enable for identification/detection of the location for sensors and administrative user action to collect the logs that are required to carry out the analysis and investigation.
3. Bank need to implement proactive monitoring capabilities aligned with the banking technology risk profile and business and regulatory requirement.
4. A well-prepared, multi-functional team to Monitor/vigil (24/7) and should poised to deal with all aspect of an incident or crisis. The team should have following capabilities to carry out some of these actions
5. At monitoring stage, to determine the severity of the incident
6. Engage in on-going threat monitoring of the criminal underground to assess the extent to which criminal plans to continue attacks on the Banks systems.
7. Identify sensitive data environments, instances of data leakages.
8. At a remediation phase, to ensure security vulnerabilities are properly repaired against future attacks.
9. At respond phase, may need to breach notification services to contact groups within the bank/external agencies.
10. Enabling of security policy/rules to protect from emerging threats and which can be further used to process the logs immediately and respond with possible recommendations with options for further deep drive investigations.

(ii) Response

1. In event of cyber crisis, on duty cyber incident management official will contain the problem to minimize the impact or escalate an incident; a quick response to the incidents limit lost time, money, and customers, as well as damage to reputation and the costs of recovery.
2. If required, Information Security (IS) department will engage third party support to perform forensic analysis and to understand full impact of the incident. For major impact, management must be prepared to communicate, as needed, across all media, including social media, in ways that assure stakeholders that the Bank response is equal to the situation.
3. If require, Bank will contact law enforcement immediately after forensic investigation commenced.

(iii) Recovery

1. The IS and IT teams to develop and implement mechanisms for detecting, monitoring, responding to, and recovering from a cyber-incident or crisis.
2. IS department to create the needed architecture and IT works to maintain systems that are resistant to attacks.
3. Post-event steps shall include assessments of the causes and of the management of the incident. The crisis will be reported to MD and Board for guidance and oversight.
4. Technical forensic and investigative capabilities are vital to preserving evidence and analysing control failures, security lapses, and other conditions related to the incident.
5. Customer notification can be made as soon as the forensic investigation commenced.

(iv) Containment / Remediation plan

1. Remediation begins after critical business operations resume, with short- and long-term efforts to close gaps.
2. The Bank must verify that attack vectors are destroyed and take steps to prevent similar attacks in the future.
3. Remediation must eliminate or minimize root causes of incidents and return businesses, functions, IT, and stakeholders to a secure operating environment.

17) Organizational Arrangements

SOC (Security Operations Centre) to be setup to ensure continuous surveillance on Cyber-attacks/threats. IS Department to develop procedure for continuous monitoring, surveillance and managing cyber risk at real time. The SOC to keep itself regularly updated on the latest nature of emerging cyber threats. Key Responsibilities of SOC should include:

i) Monitor, analyze and escalate security incidents

ii) Develop Response - protect, detect, respond, recover

iii) Conduct Incident Management and Forensic Analysis

iv) Co-ordination with contact groups (CERT-IN, IDRBT, etc)

18) Supervisory reporting framework

Cyber security Incident to be reported to Director's Executive Committee (DEC) for guidance and oversight. Incident to be brought to the notice of concern department and MD immediately and an update with action taken to the DEC. In case of fraud, the same to be reported to RBI is as per Bank "Fraud" policy.

All unusual cyber security incidents (whether they were successful or mere attempts) should report immediately to RBI, CERT-In and IB-CART by email, giving full details of the incident.

19) Log management

Put in place comprehensive log management procedures addressing aspects of identification of log sources, log generation, log transmission and storage, log normalisation & parsing, log analysis, log disposal, log security and periodic review of log readiness.

20) Transaction Monitoring

Implement mechanism for identifying suspicious transactional behaviour in respect of rules, preventive, detective types of controls, mechanism to alert the customers in case of failed authentication, time frame for the same, etc.

Adherence to rules & guidelines of INFINET, INFINET framework and SFMS, as updated from time to time.

As per circular No. RBI/2024-25/99 CO.DPSS.RPPD.No.S987/04.03.001/2024-25 dated 30.12.2024 circular on beneficiary bank account name look-up facility for Real Time Gross Settlement (RTGS) and National Electronic Funds Transfer (NEFT) Systems to be introduced.

ATM & Electronic Channel Department

The scope of ATM Department Audit is as follows:

1. Verification if the requisite regulatory requirements are adhered to by the bank in case of new ATMs installed and operations of ATM.

2. Verify whether periodic visits are made by the Bank official other than Branch staff.

3. Verify whether monitoring of uptime is done on a real time basis by the department.

4. Verify whether online system for enabling immediate notification to vendor about breakdown is available.

5. Verify whether system of periodic preventive maintenance is done by the Bank.

6. Verify whether corrective actions are taken on the basis of root cause analysis.

7. Verify whether network penetration testing for ATMs is conducted to check that they are on network or not.

8. Verify discrepancies in cash dispensation:

i) Whether complaints related to cash dispensation are resolved within 7 days.
ii) Whether online monitoring of ATMs having higher dispenser problem is done.

9. Check whether regular monitoring and forecasting of cash requirements is made.

10. Verify whether cash levels are set and monitored at intervals? Whether the branch is informed to replenish cash immediately when cash in the machine falls below a pre-determined level?

11. Verify whether the message regarding non-availability of cash in ATMs is displayed before transaction is initiated by the customer.

12. Verify access to grievance redressal mechanism:

i) Whether systems are in place to provide smooth access to grievance redressal mechanism for ATM related complaints.
ii) Whether the requisite circulars and grievance redressal procedure is displayed in the

ATM premises.
iii) Procedure of customer complaints redressal and whether time limits for redressals is adhered to by the department.

13. Verify Security measures:
i) Is the security measures adequate at the ATM centres and ATM machines? What are the internal checks and controls in place?
ii) Analysis of complaints to identify complaint prone ATMs and monitoring transactions at the said ATMs.
iii) Customer awareness and education measure.

14. Are there backup power arrangements for the ATMs? If yes, for how long can ATM operations be supported by it.

15. Is the communication link being used for connecting the ATM and branch host server with the ATM controller adequate?

16. Verify whether new ATM cards and PINs are mailed to customers at different time Intervals? Verify the procedures in place for customer due diligence and its implementation.

17. Are the records of ATM cardholders, fee status, renewal of cards, hot/warm cards being properly documented?

18. Sanction from appropriate authority and requisite documentation is in place for issue of duplicate, renewed cards and re issue of PIN mailers.

19. Is there a procedure in place for destruction of ATM cards and PIN mailers lying in the branch uncollected beyond a certain period.

20. Verification of immediate blocking of ATM cards in case of loss of ATM card or closure of account by the ATM card holder.

21. Verification of documentation and recording maintained by the department for the following:
i) Stock Records for ATM applications sent to the vendor form embossment of cards, receipt of the embossed cards from the vendor, dispatch of the embossed cards to the branches.
ii) Stock Valuation and reconciliation of ATM/Debit Card Stock lying with the vendor

22. Verify if the ATMs of the Bank are adequately insured.

23. Verify the POS/ ECOM, ATM and IMPS set up of the Bank with respect to adherence to regulatory requirements and bank's policy.

24. Verify if the reconciliation of the following is done by the branch on a regular basis:
i) ATM payable and receivable
ii) POS/ECOM payable and receivable
iii) IMPS payable and receivable.

All regulatory circulars and guidelines are adhered by the department.

Kindly note the above scope is indicative and not exhaustive.

ADVISORIES / ALERTS from regulatory bodies action based

Audit for Electronic Data Processing System:

1 Primary (urban) co-operative banks which have partially / fully computerized their operations should introduce EDP audit system on perpetual basis. The EDP audit cell should be constituted as part of their

Inspection and Audit Department in banks having an independent Inspection and Audit Department and other primary (urban) co-operative banks, which do not have an independent Inspection & Audit Department, should create a dedicated group of persons, who can perform functions of an EDP Auditor. Entire domain of EDP activities (from policy to implementation) should be brought under scrutiny of Inspection and Audit Department. The overall control and supervision of these EDP Audit Cells should be vested in the Audit Committees. Financial outlay as well as activities to be performed by EDP department should be reviewed by senior management at periodical intervals.

Primary (Urban) Co-operative Banks may comply with following guidelines while carrying out EDP Audit.

2 A team of competent and motivated EDP personnel may be developed in order to take care of a possible exodus of key personnel. EDP auditors' technical knowledge should be augmented on a continuing basis through deputation to seminars/conferences, supply of technical periodicals and books etc.

3 Duties of system programmer/designer should not be assigned to persons operating the system. System person would only make modifications /improvements to programs and the operating persons would only use such programs without having the right to make any modifications. In order to bring about uniformity of software used by various branches/offices there should be a formal method of incorporating change in standard software and it should be approved by senior management. Inspection and Audit Department should verify such changes from the view-point of control and for its implementation in other branches in order to maintain uniformity.

4 Major factors which lead to security violations in computers include inadequate or incomplete system

design, programming errors, weak or inadequate logical access controls, absent or poorly designed procedural controls, ineffective employee supervision and management controls. These may be plugged by:

- Strengthening physical, logical and procedural access to system;
- Introducing standards for quality assurance and periodically testing and checking them; and
- Screening employees prior to induction into EDP application areas and keeping a watch on their behavioral pattern.
- Putting in place appropriate control measures to protect the computer system from attacks of unscrupulous elements.

5 Replacement of manual procedures by computer applications should be done after a parallel run of the system and ensuring that all aspects of security, reliability and accessibility of data.

6 In order to ensure that the EDP applications have resulted in a consistent and reliable system for inputting of data, processing and generation of output, various tests to identify erroneous processing, to assess the quality of data, to identify inconsistent data and to compare data with physical forms should be introduced.

7 The bank should make a formal declaration of system development methodology, programming and documentation standards to be followed, compliance should be verified by EDP Auditors.

8 Contingency plans/procedures in case of failure of system should be introduced/ tested at periodic intervals. EDP auditor should put such contingency plan under test during the audit for evaluating the effectiveness of such plans.

9 While engaging outside computer agencies, banks should ensure to incorporate the "clause of visitorial rights" in the contract, so as to have the right to inspect the process of application and also ensure the security of the data/inputs given to such outside agencies.

Debit card Controls:-

As per circular No.RBI/2023-24/132 DOR.RAUG.AUT.REC.No.81/24.01.041/2023-24 dated 7.03.2024 Amendment to the Master Direction - Credit Card and Debit Card – Issuance and Conduct Directions, 2022.

No bank shall issue debit cards to cash credit/loan accounts. However, it will not preclude the banks from linking the overdraft facility provided along with Pradhan Mantri Jan Dhan Yojana accounts or Kisan Credit Card accounts with a debit card.

No card-issuer shall dispatch a card to a customer unsolicited. In case of renewal of an existing card, the cardholder shall be provided an option to decline the same if he/she wants to do so before dispatching the renewed card. Further, in case a card is blocked at the request of the cardholder, replacement card in lieu of the blocked card shall be issued with the explicit consent of the cardholder.

Card-issuers shall not reveal any information relating to customers obtained at the time of opening the account or issuing the card to any other person or organization without obtaining their explicit consent, with regard to the purpose/s for which the information will be used and the organizations with whom the information will be shared

Card-issuers shall ensure adherence to the Master Direction DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 dated April 10, 2023 on ‘Outsourcing of Information Technology Services’ and guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services’, as amended from time to time. Further, the card-issuers shall not share card data (including transaction data) of the cardholders with the outsourcing partners unless sharing of such data is essential to discharge the functions assigned to the latter. In case of sharing of any data as stated above, explicit consent from the cardholder shall be obtained. It shall also be ensured that the storage and the ownership of card data remains with the card-issuer.

In case card-issuers, at their discretion, decide to block/deactivate/suspend a debit card, it shall be ensured that a standard operating procedure is followed as approved by their Board. Further, it shall also be ensured that blocking/deactivating/suspending a card or withdrawal of benefits available on any card is immediately intimated to the cardholder along with reasons thereof through electronic means (SMS, email, etc.) and other available modes.

The banks shall undertake review of their operations/issue of debit cards on half-yearly basis. The review shall include, inter-alia, card usage analysis including cards not used for long durations and the inherent risks therein.

Persons with Disabilities:-

As per circular No. RBI/2024-25/83 CO.DPSS.POLC.No.S-708/02-12-004/2024-25 dated 11.10.2024 accessibility to digital payment systems for Persons with Disabilities to be provided.

To promote effective access, payment system participants (PSPs, that is, banks and authorised non-bank payment system providers) are advised to review their payment systems / devices in terms of accessibility to Persons with Disabilities. Based on the review they may carry out the necessary modifications, such that all their payment systems and devices, such as Point-of-Sale machines, can be accessed and used by Persons with Disabilities with ease.

C-Site Advisory UCB-2/2025 dated 19.8.2025

1. Whether CBS is accessible using end of life/ support versions of web browsers.
2. Is debit card data stored in the CBS database encrypted?
3. Is there a process to maintain and review a list of exceptional transactions (large value, new beneficiaries, etc.) during weekends and public holidays?
4. Whether alert monitoring mechanism relating to any unauthorised backend changes in CBS database is in place?
5. Whether CBS facilitate enabling time based administrative access to CBS application?
6. Whether controls to allow, manage, log and monitor privileged/super user/administrative access to critical systems in place (PIM/PAM, Log monitoring, SOC etc)?
7. Whether CBS application as well as Mobile banking/Internet banking applications have provision for time-based and value/volume-based controls for enforcing appropriate controls on transactions after business hours based on their risk appetite.
8. Is a real-time performance monitoring tool available for the CBS application (memory and CPU).
9. Whether alert mechanism is in place to monitor any change in the log settings?
10. Bank to carry out a gap assessment with respect to the prescribed controls in the CBS Handbook and develop time bound action plan to comply with gaps observed, if any, from the assessment. Progress in this regard shall also be monitored periodically by the Board and Senior Management of the UCB.

Controls from Comprehensive Cyber Security Framework for Primary UCBs, A Graded Approach, issued on December 31, 2019.

1. Two factor authentication for accessing their CBS and applications connecting to the CBS, with the 2nd factor being dynamic in nature is in place.
2. The development/test and production environments need to be properly segregated. The data used for development and testing should be appropriately masked.
3. Software/Application development approach should incorporate secure coding principles, security testing (based on global standards) and secure rollout.

4. The bank must ensure to get the VAPT done of the IT infrastructure wherever they have taken shared infrastructure hosting their CBS application and get the relevant reports from the vendor.
5. The audit logs must capture at minimum the information to uniquely identify the log for example by including a date, timestamp, source addresses, destination addresses. Such arrangements should facilitate forensic auditing, if need be.
6. An alert mechanism should be set to monitor any change in the log settings.
7. In respect of CBS, vendor may provide assurance that the application is free from embedded malicious / fraudulent code. Ensure that software/application development practices adopt principle of defence in-depth to provide layered security mechanism.
8. Data should be appropriately secured at rest as well as in transit (by using methodologies for example encryption/hashing etc.)
9. UCBs should have a robust change management process in place to record/ monitor all the changes that are moved/ pushed into production environment. Changes to business applications, supporting technology, service components and facilities should be managed using robust configuration management processes that ensure integrity of any changes thereto.
10. UCBs are responsible for meeting the requirements prescribed for incident management and BCP/DR even if their IT infrastructure, systems, applications, etc., are managed by third party vendors/service providers.

11. Additional security measures specific to CBS application:-

    a) CBS should facilitate Role Based Access Controls (RBAC).

    b) Active Directory authentication must be enabled in the CBS.

    c) All the passwords should be securely stored (for example – hashing, salting etc.).

    d) The password complexity should be enforced as per password policy of the bank. Further, pass

    word should be mandatorily changed after first login by the user. Also, the password should be

    mandatorily changed at defined intervals.

    e) CBS should allow only one active session for the user.

    f) CBS should facilitate enabling time based administrative access to CBS application.

    g) UCBs (level IV, III and level II having digital payment services) may consider implementing suitable tools/mechanism for ensuring time-based access to CBS database for non-application users.

    h) A method to assure the integrity of critical fields of the data (such as account balance) in the CBS database should be maintained (for example, implementing checksum).

    i) Data in the critical fields should be appropriately masked for front-end display through CBS application. (Display of the critical fields should only be to the extent required)

    j) CBS should have the facility to generate a list of all internal accounts (active and inactive) at any point of time.

k) CBS should facilitate maintenance of user wise transaction limits, user working time and holiday calendar.

l) All entries in CBS, irrespective of having any financial impact, should include maker-checker controls.

m) Controls such as client IP validation, allowing connection to secured API only should be con figured for establishing trusted connections.

n) CBS should not be accessible using end of life/ support versions of web browsers.

o) Comprehensive application security testing shall be done periodically and also after any major change, for CBS application deployed at the bank

Other security measures in CBS ecosystem:-

a) Direct access to critical 'CBS' database should be restricted and wherever allowed, should be closely monitored.

b) All API access should also be appropriately secured and logged.

c) Grant/revoke of user access to be managed by a centralized team.

d) Generic user ids shall be avoided and if any in use shall be identifiable with the concerned officials.

e) Approved user role matrix for the CBS shall be defined.

f) Mechanism for real time monitoring of user account activities such as biometric disabling, user account creation, modification, allocation of profiles, privilege escalation, etc. shall be in place.

g) List of authorised users of CBS along with user privileges should be readily available and the usage of the privileged accounts shall be monitored closely. Review of the authorised users may be done periodically. The user privileges shall be decided on "need to know/ need to do" basis.

h) Access to CBS to be restricted to Bank’s intranet only. (Refer to para 2.1.1.4 for exceptions)

i) Only secured services (for e.g., HTTPS and SFTP) should be allowed for CBS operations.

j) Risk assessment should be performed before using any open-source technology element for developing the CBS application.

k) KYC document images should be made visible in CBS on need-to-know basis.

l) Debit card data should not be stored in CBS database. In case it needs to be saved, it should be encrypted/securely stored.

m) Real time performance monitoring tool for CBS application (memory and CPU) shall be available with the bank for performance monitoring.

n) Audit logs of critical activities such as bypassing of biometric login/MFA, user account profile change, allocation of highest privilege to users etc. shall be enabled in CBS.

o) Secure configuration – the bank shall maintain hardening documents approved at appropriate levels and accordingly the configurations shall also be reviewed periodically.

p) Reconciliation of payment (RTGS/NEFT/IMPS etc.) messages shall be undertaken frequently (preferably daily) by comparing the outward payment with CBS confirmations (in case of doubt, confirmation from respective branch etc. shall be taken).

q) Banks shall introduce an additional layer of approval for all payments (RTGS/NEFT/IMPS etc.) exceeding a particular threshold, which can be decided internally on the basis of business volumes and trends. Such approval shall be preferably centralised.

r) Secure code and functional testing may be carried out after any major change in CBS application.

s) There shall be a process to maintain and review list of exceptional transactions (large value transactions, new beneficiaries etc.) carried out during weekends and public holidays.

t) The bank shall have a detailed SLA with IT vendors with clear demarcation of the roles and responsibilities.

u) Security and functional issues of interface between CBS and other critical applications (treasury, RTGS, ATM Switch, SWIFT, Trade Finance/Remittances) shall be reviewed and addressed holistically.

v) Total number of unsecured communication channel/APIs/interfaces (those that do not preserve the confidentiality and integrity of data/information in transit within the bank) shall be reviewed and closed after conducting proper risk assessment.

w) The bank shall implement mechanism to suitably monitor and review the CBS database access. In this regard, Level III and Level IV UCBs must implement tool-based review mechanism for the monitoring of database logs. The Level II UCBs offering digital payment services (like IMPS, UPI, internet banking, mobile banking etc.) may also implement tool-based review mechanism for the monitoring of database logs.

x) Manual Interventions in transaction processing may be avoided, modification of Master Data (if done) shall be with proper documentation with availability of Audit Trail. Any instances of deviations/exceptions shall be recorded and reviewed.

y) The CBS application shall have a logout function (auto logout mechanism) after a stipulated time of inactivity.

z) User IDs shall be unique for all users across entities.

aa)The configuration files shall be secured and only accessible on need-toknow basis.

bb) CBS application as well as Mobile banking/Internet banking applications should have provision for time-based and value/volume-based controls for enforcing appropriate controls on transactions after business hours based on their risk appetite etc., if required.

cc) UCBs to design and implement/modify the existing architecture to ensure that applications like mobile banking, internet banking, etc. communicate with CBS database through common interface of CBS application.