भारतीय रिज़र्व बैंक
Reserve Bank of India

RBI/DoS/2026-27/437
DoS.CO.CSITEG.31/31.01.015/2026-27 July 31, 2026

Reserve Bank of India (Urban Co-operative Banks – Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026

Table of Contents

पर्यवेक्षण विभाग, भारतीय रिज़र्व बैंक, केंद्रीय कार्यालय, मेकर टावर-ई, 20वीं मंजिल, कफ परेड, कोलाबा, मुंबई-400 005
दूरभाष: 022-2216 1816 ई-मेल: csite@rbi.org.in

Department of Supervision, Reserve Bank of India, Central Office, Maker Tower-E, 20th floor, Cuffe Parade, Colaba, Mumbai- 400 005
Tel: 022- 2216 1816 Email: csite@rbi.org.in

In exercise of the powers conferred by Section 27 and Section 35-A read with Section 56 of the Banking Regulation Act, 1949, and all other provisions / laws enabling the Reserve Bank of India ('RBI') in this regard, RBI being satisfied that it is necessary and expedient in the public interest so to do, hereby issues Directions hereinafter specified.

Chapter I - Preliminary

A. Short Title and Commencement

1. These Directions shall be called the Reserve Bank of India (Urban Co-operative Banks – Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026.

2. These Directions shall come into force with immediate effect.

B. Applicability

3. These Directions shall be applicable to Urban Co-operative Banks, hereinafter collectively referred to as 'UCBs' and individually as 'UCB'.

   For the purpose of these Directions, 'urban co-operative banks' means Primary Co-operative Banks as defined under Section 5(ccv) read with Section 56 of Banking Regulation Act, 1949.

4. For the purpose of these Directions, a UCB is categorised into one of the four levels based on its digital depth and interconnectedness to the payment systems landscape. Depending on the UCB category, the applicability of Chapter II to Chapter VI of these Directions is as given below:

Level	Criteria	Applicable Chapters
Level I	Applicable to the UCB irrespective of digital services / products offered by it.	Chapter II and Chapter III
Level II	The UCB which is a sub-member of Centralised Payment Systems (CPS) and satisfies at least one of the criteria given below**:**	Chapter II, Chapter III and Chapter IV

	(1) offers internet banking facility to its customers (either view or transaction based) (2) provides Mobile Banking facility through an application (Smartphone usage) (3) is a direct member of Cheque Truncation System (CTS) / Immediate Payment Service (IMPS) / Unified Payments Interface (UPI) As per Master Directions on Access Criteria for Payment Systems, 2017, the CPS will include Real Time Gross Settlement (RTGS) System and National Electronic Fund Transfer (NEFT) system and any other system as may be decided by RBI from time to time.	
Level III	The UCB which satisfies at least one of the criteria given below: (1) direct member of CPS; (2) has its own Automated Teller Machine (ATM) Switch; (3) has Society for Worldwide Interbank Financial Telecommunication (SWIFT) interface.	Chapter II, Chapter III, Chapter IV, and Chapter V
Level IV	The UCB which is a direct member / sub-member of CPS and satisfies at least one of the criteria given below: (1) has its own ATM Switch and SWIFT interface; (2) hosts data centre or provides software support to other banks on its own or through its wholly owned subsidiaries.	Chapter II, Chapter III, Chapter IV, Chapter V, and Chapter VI

C. Definitions

5. The following definitions are sourced from FSB Cyber Lexicon unless explicitly mentioned otherwise. In these Directions, unless the context states otherwise, the terms herein shall bear the meanings assigned to them below:

(1) '*Audit Trail'* - A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to result.

(*Source*: NIST SP 800-53r5 on Security and Privacy Controls for Information Systems and Organizations)

(2) '*Availability*' - Property of being accessible and usable on demand by an authorised entity.

(3) '*Confidentiality*' - Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes, or systems.

(4) '*Cyber*' - Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.

(5) '*Cyber Event*' - Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring.

(6) '*Cyber Incident*' - A cyber event that adversely affects the cybersecurity of an information asset whether resulting from malicious activity or not.

(*Source*: Cyber incident definition is adapted from FSB Cyber Lexicon. By the definition, it includes cybersecurity incidents as well as IT incidents)

(7) '*Cyber Resilience*' - The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.

(8) '*Cybersecurity*' - Preservation of confidentiality, integrity, and availability of information and / or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

(9) 'Cyber Threat' - A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cybersecurity.

(10) '*Cyber-attack*' - Malicious attempt(s) to exploit vulnerabilities through the cyber medium to damage, disrupt or gain unauthorised access to assets.

(11) '*De-militarised Zone or DMZ*' - A perimeter network segment that is logically between internal and external networks.

(*Source*: NIST SP 800-82 Rev. 2)

(12) '*Digital Forensics*' - The process used to acquire, preserve, analyse, and report on evidence using scientific methods that are demonstrably reliable, accurate, and repeatable.

(*Source*: adapted from NIST Cloud Computing Forensic Science Challenges)

(13) '*Distributed Denial of Service (DDoS)*' - A denial of service that is carried out using numerous sources simultaneously.

(14) '*Framework*' - A structured set of strategies, policies, processes, methods, and best practices that guides organisational activities, enables governance and control, and supports the achievement of defined objectives.

(*Source*: adapted from ISACA glossary and ISO 22340:2024)

(15) '*Information Asset*' - Any piece of data, device or other component of the environment that supports information-related activities. Information Assets include information system, data, hardware, and software.

(Source: Information Asset definition is adapted from “Guidance on cyber resilience for financial market infrastructures” publication of Bank for International Settlements and International Organization of Securities Commissions of June 2016)

(16) ‘*Information Systems (IS)*’ - Set of applications, services, information technology assets or other information-handling components, which includes the operating environment and networks.

(17) ‘*Integrity*’ - Property of accuracy and completeness.

(18) ‘Information Technology (*IT) Governance*’ - The responsibility of executives and the board of directors; consists of the leadership, organisational structures and processes that ensure that the enterprise’s IT sustains and extends the enterprise's strategies and objectives.

(*Source*: ISACA glossary and COBIT)

(19) ‘*IT Risk*’ - The business risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an enterprise.

(*Source*: ISACA glossary)

(20) ‘*Malware*’ - Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems.

(21) ‘*Penetration Testing*’ - A test methodology in which assessors typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.

(22) ‘*Phishing*’ - A digital form of social engineering that attempts to acquire private or confidential information by pretending to be a trustworthy entity in an electronic communication.

(23) ‘*Ransomware*’ - Malware that is used to commit extortion by impairing the use of an information system or its information until a ransom demand is satisfied.

(24) '*Recovery Time Objective*' - The overall length of time an information system's components can be in the recovery phase before negatively impacting the organisation's mission or mission / business processes.

(*Source*: NIST glossary)

(25) '*Social Engineering*' - A general term for trying to deceive people into revealing information or performing certain actions.

(26) '*Vulnerability*' - A weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats.

(27) '*Vulnerability Assessment (VA)*' - Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.

6. All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Reserve Bank of India Act, 1934, the Banking Regulation Act, 1949, the Information Technology Act, 2000, the Companies Act, 2013 or any statutory modification or re-enactment thereto or other regulations issued by RBI or the Glossary of Terms published by RBI or as used in commercial parlance, as the case may be.

Chapter II - Role of the Board

A. Board Approved Policies

7. The Board of Directors (Board) shall approve the strategies and policies related to Technology and Cybersecurity frameworks.

B. Committees of the Board

8. The Level IV UCB may consider setting up Information Technology Strategy Committee (ITSC) of the Board with a minimum of two directors as members, one of whom shall be a professional director. The roles and responsibilities of ITSC are provided in paragraph 173 of these Directions.

9. In respect of Level IV UCB, the Audit Committee of the Board (ACB) shall review highlighted critical Information Systems (IS) audit issues, provide appropriate guidance to the UCB's management, and monitor compliance arising from information security reviews and Vulnerability Assessment and Penetration Testing (VA-PT) audits as detailed in paragraph 179 of these Directions.

Chapter III - Level I Baseline Cybersecurity and Resilience Requirements

A. Self-Assessment

10. The UCB shall undertake a self-assessment of the level in which it fits into, based on the above-mentioned criteria, and ensure compliance with the applicable controls. However, the UCB may adopt higher level of security measures as decided by the Board based on its own assessment of risk and capabilities. Further, if the UCB, irrespective of its asset size already has a dedicated Chief Information Security Officer (CISO) and / or governance framework as discussed in Chapter VI of these Directions, then as a matter of best practice, the UCB may continue with the existing governance structure.

B. Cybersecurity Policy

11. The UCB shall put in place a Cybersecurity Policy duly approved by its Board / Administrator, containing a suitable approach to check cyber threats depending on the level of complexity of business and acceptable levels of risk. It shall be ensured that the cybersecurity policy covers the broad aspects given in paragraphs 12 to 15 of these Directions, keeping in view the level of technology adoption and digital products offered to the customers.

12. The cybersecurity policy shall be distinct from the UCB's IT / Information Security policy so that it highlights the risks from cyber threats and the measures to address / reduce these risks. While identifying and assessing the inherent risks, the UCB shall keep in view the security technologies adopted such as Security Information and Event Management (SIEM), Privileged Identity Management (PIM), and database activity monitoring; digital delivery channels, such as ATMs, Point of Sale (PoS) terminals, internet banking and mobile banking; digital payment products and services, such as IMPS, UPI, and e-Wallet; internal threats, including compromise of critical and sensitive data, password theft, and source code exposure; and external threats such as Distributed Denial of Services (DDoS) attacks and ransomware. The UCB shall rate each identified risk as low, medium, high, or very high.

C. Information Technology Architecture

13. The Board level ITSC (or the Board, wherever ITSC is not constituted) shall review the IT architecture of the UCB periodically. The IT architecture, encompassing network, server, database, application, and end-user systems, shall ensure that appropriate security measures are implemented and always maintained. For this purpose, the UCB shall carry out the following steps:

    (1) identify weak / vulnerable areas in IT systems and processes;

    (2) allow restricted access to networks, databases, and applications wherever permitted, through well-defined processes and approvals including rationale for permitting such access;

    (3) assess the cost of impact in case of breaches / failures in these areas;

    (4) put in place suitable cybersecurity controls to address them; and

    (5) specify and document clearly the responsibility for each of above steps.

14. The UCB shall ensure to maintain proper record of the entire process mentioned in paragraph 13 of these Directions to enable supervisory assessment.

D. Cyber Crisis Management Plan

15. The UCB may refer to Indian Computer Emergency Response Team (CERT-In) / National Critical Information Infrastructure Protection Centre (NCIIPC) guidelines as reference material for guidance on preparation of Cyber Crisis Management Plan (CCMP).

16. The UCB shall promptly detect any cyber intrusions (unauthorised entries) so as to respond / recover / contain impact of cyber-attacks. Among other things, the UCBs, especially those offering services such as internet banking, mobile banking, mobile wallet, RTGS / NEFT / IMPS, SWIFT, debit cards, and credit cards, shall take necessary detective and corrective measures / steps to address various types of cyber threats, such as Denial of Service (DoS), DDoS, ransomware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser

gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, and password related frauds.

E. Role of the Board of Directors and Senior Management

17. The Board shall be ultimately responsible for the information / cybersecurity of the UCB and shall play a proactive role in ensuring an effective IT and Information Security governance. The major role of the Senior Management involves implementing the Board approved cybersecurity policy, establishing necessary organisational processes for cybersecurity, and providing necessary resources for ensuring adequate cybersecurity.

18. The UCB shall review the organisational arrangements so that the security concerns are brought to the notice of suitable / concerned officials to enable quick action.

F. Inventory Management of Information Assets

19. The UCB shall classify data / information based on sensitivity criteria of the information.

20. The UCB shall appropriately manage and protect data and information within and outside its network, considering the way it is stored, transmitted, processed, accessed, and used, as well as the risks arising from its sensitivity and ownership.

21. The UCB shall maintain an up-to-date information asset inventory register containing the following fields, as a minimum:

    (1) details of the information asset (such as hardware / software / network devices, key personnel, services);

    (2) details of systems where customer data are stored;

    (3) associated business applications, if any; and

    (4) criticality of the systems (for example, high / medium / low).

G. Protection of Customer / Payment Information

22. The UCB, as owner of customer data, shall take appropriate steps in preserving the confidentiality, integrity, and availability of the same, irrespective of whether the data is stored / processed / accessed / in transit within or outside the UCB's network including third-party vendors; the confidentiality of such custodial information shall not be compromised in any situation. To achieve this, suitable systems and processes across the data / information lifecycle shall be put in place by the UCB. As regards customers, the UCB shall educate and create awareness among them about cybersecurity risks.

23. The UCB shall ensure that the standard encryption and integrity checks are put in place where sensitive data is transmitted over the network.

24. The UCB shall also ensure that the encryption keys are securely stored and accessed.

H. Cryptographic Controls

25. The UCB shall adopt internationally accepted encryption algorithms that are not deprecated / demonstrated to be insecure / vulnerable, and the configurations involved in implementing such controls shall be compliant with extant laws and regulatory instructions.

I. Preventing Access of Unauthorised Software

26. The UCB shall put in place a mechanism to control installation of software / applications on its information systems including end-user Personal Computers (PCs), laptops, workstations, servers, and mobile devices. The UCB shall also, put in place a mechanism to block / prevent and identify installation and running of unauthorised software / applications on such devices / systems.

27. The UCB shall maintain an up-to-date and preferably centralised inventory of authorised / approved applications / software / libraries, and other relevant software components.

28. The UCB shall set the web browser settings to auto update and disable scripts like JavaScript, Java, and ActiveX controls when they are not in use.

29. The UCB shall restrict the Internet usage, if any, to identified standalone computer(s) in its branch(es) which are strictly separate from the systems identified for running day to day business.

J. Environmental Controls

30. The UCB shall put in place appropriate controls for securing physical location of its critical assets providing protection from natural and man-made threats.

31. The UCB shall put in place mechanisms for monitoring of breaches / compromises of environmental controls including temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), and access logs.

32. The UCB shall take appropriate physical security measures to protect its critical assets.

K. Network Management and Security

33. The UCB shall ensure that all the network devices are configured appropriately, periodically assessed, and such configurations are securely maintained.

34. The UCB shall ensure that the default passwords of all the network devices / systems are changed after installation.

35. The UCB shall put in place appropriate controls to secure wireless local area networks, wireless access points, and wireless client access systems.

36. The UCB shall design its critical infrastructure with adequate network segregation controls.

37. Remote Desktop Protocol (RDP) shall be disabled and enabled only with the approval of the authorised officer of the UCB. Logs for such remote access shall be enabled and monitored for suspicious activities.

L. Secure Configuration

38. The UCB shall ensure that the firewall configurations are set to the highest security level and conduct evaluation of configurations of critical devices (such as firewall, network switches, and security devices) periodically.

39. The UCB shall ensure that the systems such as network, application, database, and servers are used dedicatedly for the purpose for which they have been set up.

M. Anti-virus

40. The UCB shall implement and update antivirus protection for servers and end points. The UCB may ensure anti-virus updation through a centralised system.

N. Change and Patch Management

41. The UCB shall put in place systems and processes to identify, track, manage, and monitor the status of patches to servers, operating system, and application software running on the systems used by the end-users.

42. The UCB shall test all the changes sufficiently to ensure that they function as intended and changes are implemented in a controlled manner.

O. User Access Control / Management

43. The UCB shall disallow administrative rights on end-user workstations / PCs / laptops and provide access rights on a ‘need to know’ and ‘need to do’ basis.

44. The UCB shall put in place a robust password management policy, with specific emphasis for sensitive activities like accessing critical systems, putting through financial transactions. The UCB shall avoid usage of trivial passwords. (An illustrative but not exhaustive list of practices that should be strictly avoided are: For example, XYZ bank having password as xyz@123; network / server / security solution devices with passwords as device / solution_name123 / device_name / solution@123; hard coding of passwords in plain text in thick clients or storage of passwords in plain text in the databases)

45. The UCB shall set complex and lengthy passwords and ensure that users shall not use same passwords for all the applications / systems / devices.

46. The UCB shall implement appropriate (e.g., centralised) systems and controls to allow, manage, log, and monitor privileged / super user / administrative access to critical systems (such as servers, operating systems, databases, applications, middleware, and network devices).

47. The UCB shall put in place two factor authentication for accessing its Core Banking Solution (CBS) and applications connecting to the CBS, with the 2nd factor being dynamic in nature. For example, the 2nd factor shall not be a static password and must not be associated with the PC / terminal used for putting through payment transactions.

48. The UCB shall ensure that sensitive or high value transactions are put through maker checker controls.

49. The UCB shall ensure that access to sensitive IT facilities is restricted to authorised personnel, and that users and IT staff in such roles are subject to close monitoring.

50. The UCB shall define roles and responsibilities of staff / third party personnel operating in its premises in accordance with the principle of segregation of duties, particularly for those performing system administration and other privileged IT functions.

51. The UCB shall ensure that the duties of system programmer / designer / administrator shall not be assigned to persons operating the system / application. System programmer / designer shall only make modifications / improvements to programs, and the operating persons shall only use such programs without having the right to make any modifications.

P. Secure Mail and Messaging Systems

52. The UCB shall implement secure mail and messaging systems, including those used by the UCB's partners and vendors, that include measures to prevent email spoofing, identical mail domains, protection of attachments, and malicious links.

53. The UCB shall document and implement email server specific controls.

54. The UCB shall implement its bank name specific email domains (For example, XYZ bank with mail domain xyz.bank.in) with anti-phishing and anti-malware, Domain-based Message Authentication, Reporting, and Conformance (DMARC) controls enforced at the email solution.

Q. Removable Media

55. The UCB, as a default rule, shall not permit the use of removable devices and media in the banking environment unless specifically authorised for defined use and duration of use.

56. The UCB shall secure the usage of removable media on various types / categories of devices including but not limited to workstations, PCs, and laptops, and secure erasure / deletion of data on such media after use.

57. The UCB shall get the removable media scanned for malware / anti-virus prior to providing read / write access.

58. The UCB shall put in place procedures to prevent unauthorised removal or accidental movement of storage media containing sensitive data out of the UCB. The UCB shall also ensure that the storage media containing sensitive data is completely erased or physically destroyed before disposal.

R. User / Employee / Management / Board Awareness

59. The UCB may update its Board members on basic tenets / principles of IT risk / cybersecurity risk at least once a year.

60. The UCB shall ensure to create a high level of awareness / familiarisation among staff at all levels including Board and Senior Management to create a cyber-safe environment.

61. The UCB shall actively promote among its employees, vendors, service providers, and other concerned parties an understanding of its cybersecurity objectives and potential impact of cyber-attacks.

62. The UCB shall communicate to users / employees, vendors and partners security policies covering secure and acceptable use of the UCB's information assets including customer information / data and educating them about cybersecurity risks and protection measures at their level.

63. The UCB shall conduct awareness and training programmes for its staff on basic information security controls, including applicable Do's and Don'ts and incident reporting procedures. The UCB shall educate employees to strictly avoid clicking any links received via email (to prevent phishing / spear-phishing attacks).

    (*Note*: For the purpose of these Directions, the term 'incident' implies cyber incident)

64. The end-users shall be made aware to never open or download an email attachment from unknown sources.

65. The UCB shall ensure to provide necessary training and manuals to the staff managing its information systems and to the end-users when new applications are implemented.

S. Customer Education and Awareness

66. The UCB shall improve and maintain customer awareness and education regarding cybersecurity risks.

67. The UCB shall educate the customers on securing their account and card details, credentials, and other sensitive authentication information, and on not sharing such information with any third party.

68. The UCB shall promote awareness of its cyber resilience objectives among its customers.

T. Backup and Restoration

69. The UCB shall take periodic back up of the important data and securely store this data 'offline' (i.e., transferring important files to a storage device that can be detached from a computer / system after copying all the files).

70. The UCB shall define and implement necessary procedures covering online storage, application-wise backup arrangements, and data retention period as per business, regulatory, and legal requirements.

U. Vendor / Outsourcing Risk Management

71. The UCB shall be accountable for ensuring appropriate management and assurance on security risks in outsourced vendor arrangements. The UCB shall carefully evaluate the need for outsourcing critical processes and selection of vendor / partner based on comprehensive risk assessment. The UCB shall regularly conduct effective due diligence, oversight and management of third-party vendors / service providers and partners.

72. In considering or renewing the outsourcing of IT Services arrangement, the UCB shall perform appropriate due diligence to assess the capability of the service provider to comply with obligations in the outsourcing agreement on an ongoing basis. The due diligence shall involve evaluation of all available information, as applicable, about the service provider (including another bank), including but not limited to the following:

    (1) The UCB shall assess the service provider's security governance for adequacy, maturity, and meeting the UCB's security requirements. The UCB shall put in place appropriate processes and controls for effective governance, risk management, and compliance.

    (2) The UCB shall assess the legal issues while dealing with a service provider including functional and service-related legal implications, applicable jurisdictions and regulatory oversight, contractual terms and conditions, delineation of provider and consumer roles, preservation of data including logs, data storage locations, contingency planning for unexpected contract termination, orderly return or secure disposal of assets, and retention of ownership of data in its original form.

    (3) The UCB shall put in place appropriate vendor risk assessment process, and controls to mitigate concentration risk. The UCB shall ensure

appropriate exit clauses in the agreement to avoid lock-in to a single vendor.

(4) The UCB shall assess the compliance and audit functions of the service provider. In this regard, the UCB shall analyse compliance scope, assess regulatory impact on data security, forensic (the term 'forensic' implies 'digital forensic' in these Directions) evidence requirements and compliance to appropriate certifications, as per applicability.

(5) The UCB shall ensure that the information lifecycle management process is put in place by the service provider incorporating data location and security aspects. The service provider shall also ensure that all copies and backups are stored only at locations allowed as per Service Level Agreement (SLA) and extant regulations.

(6) The UCB shall analyse portability and interoperability considering factors such as switching between service providers, prices, bankruptcy of service provider, service shutdown, decrease in service quality, and business dispute.

(7) The UCB shall assess the security, business continuity, and disaster recovery capabilities of the service provider.

(8) The UCB shall assess the virtualisation framework of the service provider including the type of virtualisation, virtual operating system (virtual OS) controls, protection of admin interfaces, and security technologies.

73. The UCB shall ensure that the agreement with the service provider incorporates the aspects mentioned in paragraph 72 of these Directions. The agreement shall, inter alia, provide for right to audit by the UCB. The outsourcing agreements shall include clauses to recognise the right of RBI to cause an inspection to be made of a service provider of the UCB and allow RBI or persons authorised by it to access the UCB's documents, records of transactions, logs and other necessary information given to, stored or processed by the service provider within a reasonable time.

74. The UCB shall thoroughly satisfy itself about the credentials of vendor / third-party personnel accessing and managing the UCB's critical assets. Background checks, non-disclosure and security policy compliance agreements shall be mandated for all third-party service providers.

75. The UCB shall ensure that all outsourcing Service Level Agreements (SLAs) signed with the vendors clearly mention the responsibility of the UCB and the vendor in case of any failure of services. Also, the agreements shall clearly mention the grievance redressal mechanism to resolve customer complaints.

76. The UCB shall ensure that the vendors' SLAs are periodically reviewed and updated for adherence to necessary security controls.

77. The UCB shall have clear escalation procedures in the agreement including levels of authority and time scales for monitoring disputes and problems.

78. The UCB shall evaluate the criticality of the services availed from the service provider and analyse the potential impact of adverse scenarios such as accidental public disclosure of sensitive data, unauthorised access by employees of service-provider, external manipulation, failure to deliver expected outcomes, unauthorised data modification, and temporary or prolonged unavailability of the service.

79. The UCB shall map the end-to-end data flow between the UCB, service providers, customers, and other interconnected nodes to clearly identify the data movement in / out of shared third-party infrastructure for each of the available models. The UCB shall select a suitable model as per its risk tolerance.

80. The UCB shall ensure appropriate application security at the service provider's end by defining appropriate trust boundaries for different shared resources, ensuring robust application security controls, and securing inter-host communication channels.

81. The UCB shall ensure that the service provider devises effective encryption and key management procedures for data in transit, at rest, and on backup media, secure storage and protection of encryption keys, use of industry standards,

restricted access to key stores, key backup and recoverability, and periodic testing of these procedures.

82. The UCB shall assess the user access management process of service provider including provisioning, de-provisioning, authentication, federation, authorisation, and user profile management.

83. The UCB shall ensure that following cybersecurity controls are implemented and maintained by third-party ATM Switch Application Service Providers (ASPs) where the UCB manages its ATM Switch ecosystem through their shared services:

(1) Preventing Access of Unauthorised Software: Paragraph 26 of these Directions.

(2) Environmental Controls: Paragraphs 30, 31 of these Directions.

(3) Network Management and Security: Paragraphs 33, 34, 36, 105, 106, 134, 135 of these Directions.

(4) Secure Configuration: Paragraphs 109, 136, 137 of these Directions.

(5) Application Security Life Cycle (ASLC): Paragraph 110 of these Directions.

(6) Patch / Vulnerability and Change Management: Paragraph 114 of these Directions.

(7) User Access Control / Management: Paragraphs 120, 145 of these Directions.

(8) Audit Logs: Paragraphs 126, 127, 150, 151 of these Directions.

(9) Incident Response and Management: Paragraph 152 of these Directions.

(10) Advanced Real-time Threat Defence and Management: Paragraph 147 of these Directions.

(11) Vulnerability Assessment and Penetration Test: Paragraph 118 of these Directions.

(12) Forensics: Paragraph 170 of these Directions.

84. Controls at paragraph 83 of these Directions shall be suitably factored in the contract agreement signed with the third-party ATM Switch ASPs. These controls shall be applicable to the ASPs limited to the IT ecosystem (such as physical infrastructure, hardware, software, reconciliation system, network interfaces, security solutions, hardware security module, middleware, associated people, processes, systems, data, and information) providing ATM switch services as well as any other type of payment system related services to the UCB.

85. The UCB shall ensure to mandate the following baseline cybersecurity controls in their contractual agreements with these ASPs:

(1) The ASP shall continuously monitor the release of patches by various vendors / Original Equipment Manufacturers (OEMs), advisories issued by CERT-In and other similar agencies and expeditiously apply the security patches as per the patch management policy of the ASP. If a patch / series of patches is / are released by the OEM / manufacturer / vendor for protection against well-known / well publicised / reported attacks exploiting the vulnerability patched, the ASPs must have a mechanism to apply them expeditiously following an emergency patch management process.

(2) The ASP shall put in place a clearly defined framework including requirements justifying the exception(s), duration of exception(s), process of granting exceptions, and authority for approving, authority for review of exceptions granted on a periodic basis by officer(s) preferably at senior levels who are well equipped to understand the business and technical context of the exception(s).

(3) The ASP shall prepare and maintain an up-to-date network architecture diagram at the organisation level including wired / wireless networks.

(4) The ASP may consider implementing solutions to automate network discovery and management.

(5) The ASP shall put in place mechanisms to identify authorised hardware / mobile devices such as laptops, mobile phones, and tablets, and ensure that they are provided connectivity only when they meet the security requirements prescribed by the ASP.

(6) The ASP shall put in place a mechanism to automatically identify unauthorised device connections to the ASP's network and block such connections.

(7) The ASP shall establish Standard Operating Procedures (SOP) for all major IT activities including for connecting devices to the network.

(8) The ASP shall periodically evaluate the configuration of all such devices including firewall, network switches, and security devices, and patch levels for all systems in the ASP's IT ecosystem.

(9) The ASP shall ensure the software integrity of the ATM Switch related applications.

(10) The ASP shall ensure information security across all stages of application life cycle.

(11) The ASP shall implement secure coding practices for internally / collaboratively developed applications.

(12) The ASP shall ensure that the Software / Application development approach is based on threat modelling, incorporate secure coding principles, security testing (based on global standards), and secure rollout.

(13) The ASP shall ensure that adoption of new technologies is adequately evaluated for existing / evolving security threats and that the IT / security team of the ASP achieve reasonable level of comfort and maturity with such technologies before introducing in the IT ecosystem.

(14) The ASP shall certify any new products, updates, and upgrades as having been developed following secure coding practices. The application architecture shall be tested to safeguard the confidentiality and integrity of

data being stored, processed, and transmitted. An assurance to this effect shall be shared with the UCB / RBI as and when requested.

(15) In respect of critical business applications, the ASP shall conduct source code audits by professionally competent personnel / service providers. They shall provide assurance to the UCB that the application is free from embedded malicious / fraudulent code.

(16) The ASP shall ensure that their software / application development practices address common vulnerabilities highlighted in baselines such as Open Web Application Security Project (OWASP) proactively and adopt the principle of defence-in-depth to provide layered security mechanism.

(17) The ASP shall follow a documented risk-based strategy for inventorying IT components that need to be patched, identification of patches and applying patches to minimise the number of vulnerable systems and the time window of vulnerability / exposure.

(18) The ASP shall periodically conduct Application security testing of web / mobile applications throughout their lifecycle (pre-implementation, post implementation, after changes) in an environment closely resembling or a replica of the production environment.

(19) As a threat mitigation strategy, the ASP shall identify the root cause of incident and apply necessary patches to plug the vulnerabilities.

(20) The ASP shall periodically evaluate the access device configurations and patch levels to ensure that all access points, nodes between (i) different Virtual Local Area Networks (VLANs) in the Data Centre, (ii) Local Area Network (LAN) / Wide Area Network (WAN) interfaces, (iii) ASP's network to external network and interconnections with partner, vendor, and service provider networks are securely configured.

(21) The ASP shall put in place a robust change management process in place to record / monitor all the changes that are moved / pushed into the production environment. Such a change management process must clearly

mention the test cases, chain of approving authority for the particular change, deployment plan, and rollback plan.

(22) The ASP shall carefully protect access credentials such as logon user-id, authentication information and tokens, access profiles, against leakage / attacks.

(23) The ASP shall implement controls to monitor and minimise invalid logon counts and deactivate dormant accounts.

(24) The ASP shall ensure that access to critical servers, network and security devices / systems is provided through Privileged User Management Systems / Identity and Access Management (IAM) systems.

(25) The ASP shall monitor any abnormal change in pattern of logon.

(26) The ASP shall put in place a mechanism to monitor the database security events, backend access to the databases to ensure access to the database is restricted and the activities carried out through the backend are logged and reviewed.

(27) The ASP shall ensure that trivial and / or default passwords are not used.

(28) The ASP shall develop a comprehensive data loss / leakage prevention strategy to safeguard sensitive (including confidential) business and customer data / information. This shall include protecting data processed in end point devices, data in transmission, as well as data stored in servers and other digital stores, whether online or offline.

(29) The ASP shall ensure to generate and capture logs from devices / applications / databases.

(30) The ASP shall ensure that logs / audit trails of device / system software and application software capture relevant elements, as per the applicability of each packet, event, and / or transaction.

(31) The ASP shall put in place a mechanism / resources to take appropriate action in case of any cyber incident. The ASP shall have written incident

response procedures including the roles of staff / outsourced staff handling such incidents. The response strategies shall consider readiness to meet various incident scenarios based on situational awareness, potential / post impact, and consistent communication and co-ordination with stakeholders, specifically with the UCB, during response.

(32) The ASP shall be responsible for meeting the requirements prescribed for incident management and Business Continuity Plan (BCP) / Disaster Recovery (DR) even if their information assets including IT infrastructure, systems, and applications are managed by third party vendors / service providers. The ASP shall have necessary arrangements, including a documented procedure for such purpose. This shall, inter alia, include informing the UCB about any cyber incident occurring in respect of the UCB on a timely basis to mitigate the risk at the earliest as well as to meet extant regulatory requirements.

(33) The ASP shall implement anti-malware, antivirus protection including behavioural detection capabilities across all relevant devices and environments, such as endpoints, servers (including operating systems, databases, and applications), Web / Internet gateways, email-gateways and wireless networks. The ASP shall also implement tools and processes for centralised management and monitoring of such protection.

(34) The ASP shall periodically conduct Vulnerability Assessment / Penetration Testing (VA / PT) of applications, servers, and network components.

(35) The ASP shall ensure to share the VA / PT report(s) and compliance to its findings with the UCB / RBI as and when requested.

(36) The ASP shall ensure constant and continuous monitoring of the environment using appropriate and cost-effective technology tools, clearly defined policies and procedures based on best practices and monitored by technically competent and capable manpower. The ASP shall setup a Cyber Security Operations Centre (CSOC). It is also essential that the CSOC, inter alia, ensures seamless collection of the logs relevant to the IT ecosystem, storing, processing and correlation of the logs through

appropriate SIEM solution for continuous surveillance and keeps itself regularly updated on the latest nature of emerging cyber threats.

(37) The ASP shall comply with the relevant standards including Payment Card Industry Data Security Standard (PCI-DSS) and Payment Card Industry - Software Security Framework (PCI-SSF), as applicable to the IT ecosystem.

86. The UCB shall share regulatory instructions (including circulars / advisories / alerts) issued from time to time, as applicable to the ATM switch ecosystem with the ASPs for necessary compliance.

V. Cyber Incident Response and Recovery Management

87. The UCB shall put in place an effective mechanism to report the cyber incidents in a timely manner and take appropriate action to mitigate the incident. The UCB shall also proactively notify CERT-In regarding cyber incidents.

88. The UCB shall report cyber incidents within six hours of detection on DAKSH platform (Reserve Bank's Advanced Supervisory Monitoring System - https://daksh.rbi.org.in).

89. The UCB may share the threat intelligence arising from the cyber incidents with the Indian Banks-Centre for Analysis of Risks and Threats (IB-CART) set up by Institute for Development and Research in Banking Technology (IDRBT).

90. The UCB may hold adequate insurance to cover against cyber incidents.

W. Deployment of New Application / System

91. The UCB shall ensure that all new system developments are tested, reviewed by IS auditor prior to implementation to confirm that adequate control procedures, including exception reporting, are built into the systems.

92. The UCB shall ensure that the sensitive data used for application development and testing, whether by the UCB or by third-party shall be appropriately masked.

93. The UCB shall ensure that appropriate reconciliation and validation procedures are carried out during any data conversion process when new systems are introduced.

X. Information Systems Audit

94. The UCB shall constitute an IS Audit Cell as part of its Inspection and Audit Department. If an independent Inspection and Audit Department is not constituted, the UCB shall create a dedicated group of persons, who, when required, can perform functions of an IS Auditor.

95. The UCB shall develop a team of competent personnel for IS Audit. The UCB shall ensure to augment the technical skill set of IS auditors on a continuous basis.

96. The UCB shall conduct security review of PCs / terminals used for accessing corporate Internet Banking applications of Scheduled Commercial Banks (SCBs), CBS servers and network perimeter through a qualified IS auditor.

97. The UCB shall adopt an IS audit policy, appropriate to its level of operations, complexity of business and level of computerisation and review the same at regular intervals in tune with guidelines issued by RBI from time to time.

98. The UCB may also adopt appropriate systems and practices for conducting IS audit on annual basis covering critically important branches (in terms of nature and volume of business).

99. Such audits may be undertaken prior to the statutory audit so that IS audit reports are available to the statutory auditors well in time for examination and for incorporating comments, if any, in the audit reports.

100. IS audit reports shall be placed before the Audit Committee of the Board (ACB) and compliance shall be ensured within the time frame as outlined in the IS audit policy.

101. IS Audit team of the UCB shall verify changes to the software to ensure uniform implementation of software changes across its branches.

102. The UCB shall put in place a manual of instructions for the IS auditors which shall be updated periodically to keep in tune with the latest developments in its area of operations and in its policies and procedures.

Chapter IV – Level II Baseline Cybersecurity and Resilience Requirements

A. Information Technology Resource Planning

103. The UCB shall prepare and formally adopt IT operational plans and budgets with clearly identified IT components, put in place mechanisms to monitor IT performance, review IT architecture against business needs, ensure user requirements for system changes are identified and prioritised, implement appropriate project management and quality assurance practices, and maintain effective capacity planning processes.

B. Chief Information Security Officer or Equivalent Official

104. The UCB shall identify an official (not necessarily designated as CISO), responsible for articulating and enforcing the policies used by the UCB to protect its information assets, apart from coordinating the cybersecurity related issues / implementation within the UCB as well as relevant external agencies. The official shall be primarily responsible for ensuring compliance to various instructions issued on information security / cybersecurity by RBI.

C. Network Management and Security

105. The UCB shall maintain an up-to-date / centralised inventory of authorised devices connected to its network (within / outside the UCB's premises) and related network devices in the UCB's network.

106. The UCB shall ensure that the boundary defences are multi-layered with properly configured firewalls, proxies, De-Militarised Zone (DMZ) perimeter networks, and network-based Intrusion Prevention System (IPS) and Intrusion Detection System (IDS). Mechanism to filter both inbound and outbound traffic shall be put in place.

107. The UCB shall ensure that the LAN segments for in-house / onsite ATM and CBS / branch network are different.

108. The UCB shall enable its public facing IT infrastructure to handle Internet Protocol version 6 (IPv6) traffic.

D. Secure Configuration

109. The UCB shall document and apply baseline security requirements / configurations to all categories of devices including end-points / workstations, mobile devices, operating systems, databases, applications, middleware, network devices, and security solutions, throughout the lifecycle (from conception to deployment) and carry out reviews periodically.

E. Application Security Life Cycle

(*These controls shall be applicable to the UCB developing the application software (e.g., core banking solution) itself or through its subsidiaries. Otherwise, the UCB, apart from securing its production environment, may enforce these requirements with its respective third-party vendors developing application software)*

110. The UCB shall ensure that the development / test and production environments are properly segregated.

111. The UCB shall ensure that the software / application development approach incorporates secure coding principles, security testing, and secure rollout.

112. The UCB shall put in place system development methodology, programming, and documentation standards to ensure quality of system maintenance / improvement. IS auditors shall verify compliance in this regard.

F. Change and Patch Management

113. The UCB shall have a robust change management process in place to record / monitor all the changes that are moved / pushed into production environment.

114. The UCB shall ensure that the changes to business applications, supporting technology, service components, and facilities are managed using robust configuration management processes that ensure integrity of any changes thereto.

G. Periodic Testing

115. The UCB shall ensure that the application security testing of web / mobile applications is conducted before going live and after every major change in the applications.

116. The UCB shall periodically conduct VA / PT of internet facing web / mobile applications, servers, and network components throughout their lifecycle (pre-implementation, post implementation, and after changes). VA of critical applications and those on DMZ shall be conducted at least once in every six months. PT shall be conducted at least once in a year.

117. The UCB having its CBS on a shared infrastructure of an Application Service Provider (CBS-ASP) shall get its CBS application including the infrastructure hosting it subjected to VA / PT through the CBS-ASP.

118. The UCB shall ensure that the vulnerabilities detected are remediated promptly in terms of the UCB's risk management / treatment framework so as to avoid exploitation of such vulnerabilities.

119. The UCB shall ensure that the penetration testing of public facing systems as well as other critical applications are carried out by professionally qualified teams. Findings of VA / PT and the follow up actions necessitated shall be monitored closely by the Information Security / IS Audit team as well as Senior Management.

H. User Access Control / Management

120. The UCB shall provide secure access to its assets / services from within / outside its network by protecting data / information at rest (e.g., using encryption, if supported by the device) and in-transit (e.g., using technologies such as Virtual Private Network (VPN) or other standard secure protocols).

I. Authentication Framework for Customers

121. The UCB shall have adequate checks and balances to ensure (including security of customer access credentials held with them) that transactions are put only through the genuine / authorised applications and that authentication methodology is robust, secure, and centralised.

122. The UCB shall implement an authentication framework to securely verify and identify the applications of UCB to customers.

J. Anti-Phishing

123. The UCB shall subscribe to anti-phishing / anti-rogue application services from external service providers for identifying and taking down phishing websites / rogue applications.

K. Data Leak Prevention Strategy

124. The UCB shall develop and implement a comprehensive data loss / leakage prevention strategy to safeguard sensitive (including confidential) business and customer data / information. Similar arrangements need to be ensured at vendor managed facilities as well.

L. Database Integrity

125. The UCB shall implement database integrity checks to prevent the corruption or unauthorised modifications of databases.

M. Audit Logs

126. The UCB shall capture the audit logs pertaining to user actions in a system. Such arrangements shall facilitate forensic auditing, if need be.

127. The UCB shall set an alert mechanism to monitor any change in the log settings.

128. The retention of audit logs / trails shall be in line with business, regulatory, and legal requirements.

N. Incident Response and Management

129. The UCB shall put in place an effective Incident Response plan. The UCB shall have a mechanism / resource to take appropriate action in case of any cyber incident. The UCB shall have written incident response procedures including the roles of staff / outsourced staff handling such incidents.

130. The UCB shall be responsible for meeting the requirements prescribed for incident management and BCP / DR even if its information assets including IT infrastructure, systems, and applications are managed by third party vendors / service providers.

131. The UCB shall ensure that the single points of failure are avoided by ensuring availability of contingent resources.

132. The UCB shall ensure monitoring of system availability / down time, operational failures, and IT service levels by its Senior Management.

133. The UCB shall test its BCP / DR plans at periodic intervals. IS auditor shall assess the effectiveness of such BCP / DR plans.

Chapter V - Level III Baseline Cybersecurity and Resilience Requirements

A. Network Management and Security

134. The UCB shall put in place a mechanism to detect and remedy any unusual activities in systems, servers, network devices, and endpoints.

135. The UCB shall define firewall rules to block unidentified outbound connections, reverse Transmission Control Protocol (TCP) shells and other potential backdoor connections.

B. Secure Configuration

136. The UCB shall disable remote connections from outside machines to the network hosting critical payment infrastructure (e.g., RTGS, NEFT, ATM Switch, SWIFT Interface) and disable RDP on all critical systems.

137. The UCB shall enable Internet Protocol (IP) table to restrict access to the clients and servers in SWIFT and ATM Switch environment only to authorised systems.

138. The UCB shall ensure the software integrity of the ATM Switch / SWIFT related applications.

139. The UCB shall disable PowerShell in servers where not required and disable PowerShell in Desktop systems.

140. The UCB shall restrict default shares including IPC$ share (Inter-Process Communication share).

C. Application Security Life Cycle

141. In respect of critical business applications, the UCB may conduct source code audits by professionally competent personnel / service providers or have assurance from application providers / OEMs that the application is free from embedded malicious / fraudulent code.

142. The UCB shall ensure that besides business functionalities, security requirements relating to system access control, authentication, transaction authorisation, data integrity, system activity logging, audit trail, session

management, security event tracking, and exception handling are clearly specified at the initial and ongoing stages of system development / acquisition / implementation.

143. The UCB shall ensure that software / application development practices adopt the principle of defence-in-depth to provide a layered security mechanism.

144. The UCB shall ensure that adoption of new technologies is adequately evaluated for existing / evolving security threats and that the IT / security team of the UCB achieves a reasonable level of comfort and maturity with such technologies before introducing them for critical systems of the UCB.

D. User Access Control

145. The UCB shall implement a centralised authentication and authorisation system through an IAM solution for accessing and administering critical applications, operating systems, databases, network, and security devices / systems, point of connectivity (local / remote) including enforcement of strong password policy, two-factor / multi-factor authentication, securing privileged accesses following the principle of least privileges and separation of duties. This shall be implemented either with the in-house team managing the infrastructure or through the service provider if its infrastructure is hosted at a shared location at the service provider’s end.

146. The UCB shall implement centralised policies through Active Directory or Endpoint management systems to whitelist / blacklist / restrict removable media use.

E. Advanced Real-time Threat Defence and Management

147. The UCB shall build a robust defence against the installation, spread, and execution of malicious code at multiple points in its environment.

148. The UCB shall implement whitelisting of internet websites / systems.

F. Maintenance, Monitoring, and Analysis of Audit Logs

149. The UCB shall consult all the stakeholders before finalising the scope, frequency, and storage of log collection.

150. The UCB shall manage and analyse audit logs in a systematic manner so as to detect, respond, understand, or recover from an attack.

151. The UCB shall implement and periodically validate settings for capturing appropriate logs / audit trails of each device, system software, and application software, ensuring that such logs include the minimum information required to uniquely identify each log, such as date, timestamp, source addresses, and destination addresses.

G. Incident Response and Management

152. The UCB's BCP / DR capabilities shall adequately and effectively support its cyber resilience objectives and shall be so designed to enable the UCB to recover rapidly from cyber-attacks / other incidents and safely resume critical operations aligned with recovery time objectives while ensuring security of processes and protection of data.

153. The UCB shall have necessary arrangements, including a documented procedure, with third-party vendors / service providers for such purpose. This shall, inter alia, include being informed about any cyber incident occurring in respect of the UCB on a timely basis to mitigate the risk early as well as to meet extant regulatory requirements.

154. The UCB shall have a mechanism to dynamically incorporate lessons learnt to continually improve the response strategies. Response strategies shall consider readiness to meet various incident scenarios based on situational awareness, potential / post impact, and consistent communication, and co-ordination with stakeholders during response.

H. User / Employee / Management Awareness

155. The UCB shall encourage the reporting of suspicious behaviour incidents to the incident management team.

156. The UCB shall conduct mandatory cybersecurity awareness programs for new recruits and web-based quiz and training for lower, middle, and upper management every year.

157. The UCB shall sensitise its Board members on various technological developments and cybersecurity related developments periodically.

I. Risk - based Transaction Monitoring System

(This control shall be applicable to the UCB which is a direct member of CPS as well as *having its own ATM Switch interface or SWIFT interface*)

158. The UCB, which is a direct member of CPS as well as having its own ATM Switch interface or SWIFT interface, shall implement risk-based transaction monitoring or surveillance process as part of fraud risk management system across all delivery channels.

Chapter VI - Level IV Baseline Cybersecurity and Resilience Requirements

A. Cyber Security Operations Centre

159. The UCB shall put in place a CSOC. It is also essential that CSOC ensures continuous surveillance and keeps itself regularly updated on the latest nature of emerging cyber threats.

A.1 Expectations from CSOC

160. The UCB shall ensure that the CSOC delivers the following:

(1) ability to protect critical business and customer data / information, demonstrate compliance with relevant internal guidelines, country regulations and laws;

(2) ability to provide real-time / near-real time information on and insight into the security posture of the UCB;

(3) ability to effectively and efficiently manage security operations by preparing for and responding to cyber risks / threats, facilitate continuity and recovery;

(4) ability to know who did what, when, how and preservation of evidence;

(5) integration of various log types and logging options into a SIEM system, ticketing / workflow / case management, unstructured data / big data, reporting / dashboard, and use cases / rule design (customised based on risk and compliance requirements / drivers); and

(6) monitor the logs of various network activities and the capability to escalate any abnormal / undesirable activities.

161. The UCB shall ensure that CSOC is responsible for the following:

(1) monitoring, analysing and escalating security incidents;

(2) developing and executing response measures across the protect, detect, respond, and recover phases;

(3) conducting incident management and forensic analysis; and

(4) coordinating with relevant contact groups within the UCB as well as with external agencies, as required.

A.2 Technological Aspects

162. The UCB shall arrive at a suitable and cost-effective technology framework designed and implemented to ensure proactive monitoring capabilities aligned with the technology risk profile, business, and regulatory requirements. The UCB shall have clear understanding of the service delivery architecture deployed to enable identification of the location for the sensors, to collect the logs that are required to carry out the analysis, and investigation.

163. The CSOC shall have security analytics engine which can process the logs within a reasonable time frame and come out with possible recommendations with options for further deep dive investigations including deep packet inspections.

164. The CSOC shall have tools and technologies for malware detection and analysis as well as imaging solutions for data to address the forensics requirements.

165. The UCB shall ensure that the solution architecture deployed addresses performance and scalability requirements in addition to high availability requirements. Some of the aspects to be considered are:

(1) staffing of CSOC for continuous monitoring on 24x7 basis;

(2) finding staff with required skills / managing security service provider with required skill set;

(3) metrics to measure performance of CSOC; and

(4) ensuring scalability and continuity of staff through appropriate capacity planning initiatives.

B. Participation in Cyber Drills

166. The UCB shall participate in cyber drills conducted under the aegis of institutions / agencies such as CERT-IN and IDRBT.

C. Incident Response and Management

167. The UCB shall ensure incident response capabilities in all interconnected systems and networks including those of vendors and partners and readiness demonstrated through collaborative and co-ordinated resilience testing that meets the UCB's recovery time objectives.

168. The UCB shall implement a framework for aligning CSOC, Incident Response and Digital forensics to reduce the business downtime / to bounce back to normalcy.

D. Metrics

169. The UCB shall develop a comprehensive set of metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators. Some illustrative metrics include coverage of anti-malware software and their updation percentage, patch latency, extent of user awareness training, vulnerability related metrics, number of open vulnerabilities, and IS / security audit observations.

E. Forensics

170. The UCB shall have support / arrangement for network forensics / forensic investigation / DDoS mitigation services on standby.

F. Information Technology Strategy and Policy

171. The UCB shall have a Board approved IT-related strategy and policy covering the following:

    (1) Existing and proposed hardware and networking architecture for the UCB and its rationale.

    (2) Standards for hardware or software prescribed by the proposed architecture.

    (3) Strategy for outsourcing, in-sourcing, procuring off-the-shelf software, and inhouse development.

(4) IT Department’s organisational structure.

(5) Desired number and level of IT expertise or competencies in UCB's human resources, plan to bridge the gap (if any) and requirements relating to training and development.

(6) Strategy for keeping abreast with technology developments and to upgrade systems as and when required.

(7) Strategy for independent assessment, evaluation and monitoring of IT risks, findings of IT / IS / cybersecurity related audits.

G. Information Technology and Information Systems Governance Framework

G.1 Cybersecurity Function / Group

172. The UCB shall form a separate cybersecurity function / group to focus exclusively on cybersecurity management. The organisation of the cybersecurity function shall be commensurate with the nature and size of activities of the UCB including factors such as technologies adopted, delivery channels, digital products being offered, internal and external threats. The cybersecurity function shall be adequately resourced in terms of the number of staff, level of skills and tools or techniques such as risk assessment, security architecture, vulnerability assessment, and forensic assessment.

G.2 Information Technology Strategy Committee

173. The UCB may consider setting up a Board level IT Strategy Committee (ITSC) with a minimum of two directors as members, one of whom shall be a professional director. At least two members of the ITSC shall be technically competent, while at least one member shall have substantial expertise in managing / guiding technology initiatives. Technically competent herein shall mean the ability to understand and evaluate technology systems. A member shall be considered to have ‘substantial expertise’ if they have a minimum of five years of experience in managing IT systems and / or in leading / guiding technology initiatives / projects. Such a member shall also have an understanding of banking processes at a broader level and of the impact of IT on such processes. If not,

then the member shall be trained on these aspects. A member with substantial expertise is deemed to be considered as technically competent. Roles and responsibilities of the ITSC / Board shall, inter alia, include the following:

(1) approving IT strategy and policy documents;

(2) ensuring that the management has put an effective strategic planning process in place;

(3) ensuring that the IT organisational structure complements the business model and its direction;

(4) ensuring IT investments represent a balance of risks and benefits and that budgets are acceptable; and

(5) reviewing IT performance measurement and contribution of IT to businesses.

G.3 Information Technology Steering Committee

174. The UCB shall form an IT Steering Committee with representatives from the IT, HR, legal, and business verticals. Its role is to assist the Senior Management in implementing Board-approved IT strategy, including prioritisation of IT-enabled investment, reviewing the status of projects (including, resource conflict), monitoring service levels and improvements, and IT service delivery. The IT Steering Committee shall report to the ITSC / Board periodically. Its functions, inter-alia, include:

(1) defining project priorities and assessing strategic fit for IT proposals;

(2) reviewing, approving, and funding initiatives, after assessing value addition to business process;

(3) ensuring that all critical projects have a component for ‘project risk management’;

(4) assisting in governance, risk and control framework, and monitoring key IT governance processes;

(5) defining project success measures and following up progress on IT projects;

(6) providing direction relating to IT architecture design, technology standards and practices;

(7) ensuring that vulnerability assessments of new technology are performed;

(8) verifying compliance with technology standards and guidelines; and

(9) ensuring compliance to legal, regulatory, and statutory requirements.

G.4 Chief Information Security Officer

175. The UCB shall designate a sufficiently senior level official as Chief Information Security Officer (CISO) who will be responsible for articulating and enforcing the policies that the UCB uses to protect its information assets apart from coordinating the cybersecurity related issues / implementation within the UCB as well as relevant external agencies. The CISO shall be primarily responsible for ensuring compliance to various instructions issued on information security / cybersecurity by RBI. The UCB shall ensure the following in this regard:

(1) The CISO shall report directly to the top executive overseeing the risk management function or in their absence to the Managing Director and Chief Executive Officer (MD and CEO).

(2) The CISO shall have the requisite technical background and expertise.

(3) The CISO shall have a reasonable minimum term.

(4) The CISO shall place a separate review of cybersecurity arrangements / preparedness of the UCB before the ITSC / Board on a quarterly basis.

(5) The CISO shall be responsible for bringing to the notice of the Board about the vulnerabilities and cybersecurity risks that the UCB is exposed to.

(6) The CISO, by virtue of its role as member secretary of information security and / or related committee(s), if any, shall, inter alia, ensure discussion of

current / emerging cyber threats to banking (including payment systems) sector and the UCB's preparedness in these aspects in such committee(s).

(7) The CISO's office shall manage and monitor the CSOC and drive cybersecurity related projects.

(8) The CISO shall not have any direct reporting relationship with the Chief Information Officer (CIO) / Chief Technology Officer (CTO) and shall not be given any business targets.

(9) The CISO shall be an invitee to the ITSC and IT Steering Committee. The CISO may also be a member of (or invited to) committees on operational risk where IT / Information Security risk is also discussed.

(10) The CISO's office shall be adequately staffed with technically competent people, if necessary, through recruitment of specialist officers, commensurate with the business volume, extent of technology adoption, and complexity.

(11) The budget for IT security / CISO's office shall be determined keeping in view the current / emerging cyber threat landscape.

176. The Board shall objectively assess the effectiveness of the CISO's office.

G.5 Information Security Committee

177. The UCB shall form an Information Security Committee (ISC) as a Committee of executives, with formal terms of reference, to consider IT and cybersecurity from a UCB-wide perspective. The CISO shall be the member secretary of the Committee. The ISC shall, inter alia, include, the MD and CEO or designee and two Senior Management officials well versed in the subject. ISC shall meet at least on a quarterly basis. Major responsibilities of the ISC, inter-alia, include:

(1) developing and facilitating the implementation of information security / cybersecurity policies, standards, and procedures to ensure that all identified risks are managed within the UCB's risk appetite;

(2) approving and monitoring major cybersecurity projects and the status of cybersecurity plans and budgets, establishing priorities, approving standards and procedures;

(3) supporting the development and implementation of a UCB-wide information security management programme;

(4) reviewing the position of cyber incidents and various information security assessments and monitoring activities across the UCB;

(5) reviewing the status of security awareness programmes; and

(6) assessing new developments or issues relating to information security / cybersecurity.

178. The UCB shall ensure that minutes of the ISC meetings are maintained and that decisions, activities, and reviews relating to cybersecurity are escalated to the Board / ITSC on a quarterly basis.

G.6 Audit Committee of the Board

179. The Audit Committee of the Board (ACB) shall be responsible for the following:

(1) devoting sufficient time to identified IS Audit findings, review of critical issues highlighted and providing appropriate guidance to the UCB's management; and

(2) monitoring the compliance in respect of the information security reviews / VA-PT audits under various scopes conducted by internal as well as external auditors / consultants to ensure that open issues are closed on a timely basis and sustenance of the compliance is adhered to.

Chapter VII - Repeal and Other Provisions

A. Repeal and Saving

180. With the issue of these Directions, the existing directions, instructions, and guidelines relating to Cybersecurity Framework for UCBs stand repealed, as communicated vide circular no. DoS.CO.PPG.66/11.01.005/2026-27 dated July 31, 2026. The directions, instructions and guidelines repealed prior to the issuance of these Directions shall continue to remain repealed.

181. Notwithstanding such repeal, any action taken or purported to have been taken, or initiated under the repealed directions, instructions, or guidelines shall continue to be governed by the provisions thereof. All approvals or acknowledgments granted under these repealed lists shall be deemed as governed by these Directions. Further, the repeal of these directions, instructions, or guidelines shall not in any way prejudicially affect:

(1) any right, obligation or liability acquired, accrued, or incurred thereunder;

(2) any penalty, forfeiture, or punishment incurred in respect of any contravention committed thereunder;

(3) any investigation, legal proceeding, or remedy in respect of any such right, privilege, obligation, liability, penalty, forfeiture, or punishment as aforesaid; and any such investigation, legal proceedings or remedy may be instituted, continued, or enforced and any such penalty, forfeiture or punishment may be imposed as if those directions, instructions, or guidelines had not been repealed.

B. Application of Other Laws Not barred

182. The provisions of these Directions shall be in addition to, and not in derogation of the provisions of any other laws, rules, regulations, or directions, for the time being in force.

C. Interpretations

183. For the purposes of giving effect to the provisions of these Directions or for removing any difficulties in their application or interpretation, RBI may, if it deems necessary, issue such clarifications as it considers appropriate in respect of any matter covered herein. The interpretation of any provision of these Directions by RBI shall be final and binding on all concerned entities.

(N. Suganandh)
Chief General Manager