भारतीय रिज़र्व बैंक
Reserve Bank of India

RBI/DoS/2026-27/419
DoS.CO.CSITEG.13/31.01.015/2026-27 July 31, 2026

Reserve Bank of India (Small Finance Banks - Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026 (Updated as on October 01, 2026)

Table of Contents

Chapter I - Preliminary 4
A. Short Title and Commencement 4
B. Applicability 4
C. Definitions 4
Chapter II - Role of the Board 10
A. Board Approved Policies 10
B. Board Level Committees 10
Chapter III – Information Technology Governance and Oversight 11
A. IT Governance Framework 11
B. Information Security Policy and Cybersecurity Policy 11
C. IT Strategy Committee of the Board 12
D. Senior Management and IT Steering Committee 13
E. Information Security Committee 14
F. Head of IT Function 15
G. Chief Information Security Officer 15
H. Information Technology Project Management 17
I. IT Architecture 17
J. IT Services Management 18
Chapter IV - IT and Information Security Risk Management 19
A. Periodic Review of IT related Risks 19
B. IT and Information Security Risk Management Framework 19
C. Risk Identification, Assessment, and Documentation 19

Chapter V - Baseline Cybersecurity and Resilience Requirements 21
A. Inventory Management of Information Assets 21
B. Data Leak Prevention Strategy 21
C. Data Migration Controls 22
D. Preventing Execution of Unauthorised Software 22
E. Physical and Environmental Controls 23
F. Capacity Management 23
G. Secure Configuration 24
H. Network Management and Security 24
I. Application Security Life Cycle 25
J. Maintenance, Monitoring, and Analysis of Audit Logs 27
K. Patch, Vulnerability and Change Management 28
L. User Access Control / Management 29
M. Controls on Teleworking 30
N. Authentication Framework for Customers 31
O. Secure Mail and Messaging Systems 31
P. Removable Media 31
Q. Third-Party Arrangements 32
R. Cryptographic Controls 38
S. Straight Through Processing 38
T. Continuous Surveillance 38
U. Advanced Real-time Threat Defence and Management 39
V. Anti-Phishing 39
W. Vulnerability Assessment and Penetration Test 39
X. Red Teaming Exercises 41
Y. Business Continuity and Disaster Recovery 41
Z. Cyber Incident Response and Recovery Management 43
AA. Metrics 45
BB. User / Employee / Management Awareness 46
CC. Customer Education and Awareness 47
DD. Risk based Transaction Monitoring 47
EE. Forensics 47

Chapter VI - Cyber Security Operation Centre 48

A. Governance 48

B. Capabilities 48

C. Staff Capabilities 50

Chapter VII - Information Systems Audit 52

Chapter VIII - Repeal and Other Provisions 53

A. Repeal and Saving 53

B. Application of Other Laws Not barred 53

C. Interpretations 54

In exercise of the powers conferred by Section 27 and Section 35-A 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 (Small Finance 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 Small Finance Banks (hereinafter collectively referred to as 'banks' and individually as 'bank').

C. Definitions

4. 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) *'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.

(7) *'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)

(8) *'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.

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

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

(11) *'Data Dictionary'* - A description of data in business terms, including information about the data. It includes elements like data types, structure details, and security restrictions.

(*Source*: ISACA glossary)

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

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

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

(14) *'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)

(15) *'Honeypot'* - A specially configured server, also known as a decoy server, designed to attract and monitor intruders in a manner so that their actions do not affect production systems.

(*Source:* ISACA glossary)

(16) *'Indicators of Compromise (IOCs)'* - Identifying signs that a cyber incident may have occurred or may be currently occurring.

(17) *'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)

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

(19) *'Integrity'* - Property of accuracy and completeness.

(20) *'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)

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

(*Source:* ISACA glossary)

(22) *'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:* ISACA glossary and ISO 22340:2024)

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

(24) *'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.

(25) *'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.

(26) *'Privileged User'* - A user who, by virtue of function, and / or role, has been allocated powers within an information system, which are significantly greater than those available to the majority of users.

(*Source:* adapted from ISO/IEC 24775-2:2021)

(27) *'Recovery Point Objective'* - The point in time to which data must be recovered after an outage.

(*Source:* NIST glossary)

(28) *'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)

(29) *'Red Team'* - A group of people authorised and organised to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.

(*Source:* NIST glossary)

(30) *'Red Teaming Exercise'* - An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt by a red team to compromise organisational missions and / or business processes to provide a comprehensive assessment of the security capability of the information system and organisation.

(*Source:* adapted from NIST glossary)

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

(32) *'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.

5. 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, Payment and Settlement Systems Act, 2007, 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

6. The Board of Directors shall approve the strategies and policies related to Information Technology, Information Assets, Business Continuity, Information Security and Cybersecurity (including Incident Response and Recovery Management / Cyber Crisis Management) frameworks.

7. The Board may delegate the review of such policies and strategies to the Board-level IT Strategy Committee (ITSC). Material amendments thereto shall be approved by the Board. The review shall be undertaken at least annually.[1]

B. Board Level Committees

8. The bank shall put in place a Board-level IT Strategy Committee (ITSC). The composition and functions of the Committee shall be in accordance with paragraphs 15 to 18 of these Directions.

9. The Audit Committee of the Board (ACB) shall be responsible for exercising oversight of IS Audit of the bank.

[1] Substituted w.e.f. October 1, 2026, consequent to Reserve Bank of India (Small Finance Banks - Governance) Amendment Directions, 2026.

Chapter III – Information Technology Governance and Oversight

A. IT Governance Framework

10. The key focus areas of IT Governance shall include strategic alignment, risk management, resource management, performance management, and Business Continuity / DR Management.

11. The bank shall put in place a robust IT Governance Framework based on the focus areas outlined in Paragraph 10 above, that inter alia:

    (1) specifies the governance structure and processes necessary to meet the bank's business / strategic objectives;

    (2) specifies the roles (including authority) and responsibilities of the Board of Directors (Board) / Board level Committee and Senior Management; and

    (3) includes adequate oversight mechanisms to ensure accountability and mitigation of IT and cyber / information security risks.

12. Enterprise-wide risk management policy or operational risk management policy shall also incorporate periodic assessment of IT-related risks (both inherent and potential risk).

B. Information Security Policy and Cybersecurity Policy

13. The bank shall put in place an Information Security Policy that takes into consideration, inter alia, aspects such as the objectives, scope, ownership, and responsibility for the policy; information security organisational structure; exceptions; compliance review and penal measures for non-compliance of policies.

14. The bank shall put in place a Cybersecurity Policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk, duly approved by its Board. The cybersecurity policy shall be distinct and separate from the broader IT policy / Information Security policy so that it can highlight the risks from cyber threats and the measures to address / mitigate these risks.

C. IT Strategy Committee of the Board

15. The bank shall establish a Board-level IT Strategy Committee (ITSC).

16. While constituting the ITSC, the bank shall ensure the following:

    (1) ITSC has minimum of three directors (including the Chairperson of the ITSC) as members.

    (2) The Chairperson of the ITSC is an independent director having substantial IT expertise in managing / guiding information technology initiatives. 'Substantial IT expertise' means having a minimum of seven years' experience in managing Information Systems and / or leading / guiding technology / cybersecurity initiatives / projects. The Chairperson should also understand the business processes at a broader level and the impact of IT on such processes.

    (3) Members are technically competent. 'Technically competent' herein shall mean the ability to understand and evaluate Information Systems and associated IT / cyber risks.

17. The ITSC shall meet at least on a quarterly basis.

18. The ITSC shall:

    (1) ensure that the bank has put an effective IT strategic planning process in place;

    (2) guide in preparation of IT Strategy and ensure that the IT Strategy aligns with the overall strategy of the bank towards accomplishment of its business objectives;

    (3) satisfy itself that the IT Governance and Information Security Governance structure fosters accountability, is effective and efficient, has adequate skilled resources, well - defined objectives, and unambiguous responsibilities for each level in the organisation;

(4) ensure that the bank has put in place processes for assessing and managing IT and cybersecurity risks;

(5) ensure that the budgetary allocations for the IT function, including for IT security / cybersecurity, are commensurate with the bank's IT maturity, digital depth, threat environment, and industry standards and are utilised in a manner intended for meeting the stated objectives;

(6) review the organisational arrangements so that the security concerns are appreciated, receive adequate attention, and get escalated to appropriate levels in the hierarchy to enable quick action; and

(7) review, at least on an annual basis, the adequacy and effectiveness of the Business Continuity Planning and Disaster Recovery (DR) Management of the bank;

(Note: The reference to Business Continuity / Disaster Recovery Management in these Directions is limited to operational resilience focussing on People, Processes, and Systems associated with the IT, Information Systems (IS), information security / cybersecurity controls and operations)

(8) review the assessment of IT capacity requirements and the measures taken to address the issues; and

(9) approve documented standards and procedures for administering need-based access to an information system.

D. Senior Management and IT Steering Committee

19. The Senior Management of the bank shall, inter alia, ensure:

(1) execution of the IT Strategy approved by the Board;

(2) IT / Information Security and their support infrastructure are functioning effectively and efficiently;

(3) necessary IT risk management processes are in place and create a culture of IT risk awareness and cyber hygiene practices in the bank;

(4) cybersecurity posture of the bank is robust; and

(5) overall, IT contributes to productivity, effectiveness, and efficiency in business operations.

20. The bank shall establish an IT Steering Committee with representation at Senior Management level from IT and business functions which shall meet at least on a quarterly basis.

21. The responsibilities of IT Steering Committee, inter alia, shall be to:

(1) assist the ITSC in strategic IT planning, oversight of IT performance, and aligning IT activities with business needs;

(2) oversee the processes put in place for business continuity and DR;

(3) ensure implementation of a robust IT architecture meeting statutory and regulatory compliance; and

(4) update the ITSC and Managing Director (MD) / Chief Executive Officer (CEO) periodically on the activities of IT Steering Committee.

E. Information Security Committee

22. An Information Security Committee (ISC), under the oversight of the ITSC, shall be formed for managing cyber / information security. The constitution of the ISC, with Chief Information Security Officer (CISO) and other representatives from business, IT and other relevant functions, shall be decided by the ITSC. The head of the ISC shall be from risk management vertical. Major responsibilities of the ISC, inter alia, shall include:

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

(2) approving and monitoring information security / cybersecurity projects and security awareness initiatives;

(3) reviewing cyber incidents, IS audit observations, monitoring, and mitigation activities; and

(4) updating the ITSC and MD / CEO periodically on the activities of ISC.

F. Head of IT Function

23. The bank shall appoint a sufficiently senior level, technically competent, and experienced official in IT related aspects as Head of IT Function (or by whatever nomenclature the bank uses, such as Chief Technology Officer, Chief Information Officer).

24. The Head of IT Function shall, inter alia, be responsible for the following:

(1) ensuring that the execution of IT projects / initiatives is aligned with the bank's IT Policy and IT Strategy;

(2) ensuring that there is an effective organisational structure to support IT functions in the bank; and

(3) putting in place an effective DR setup and business continuity strategy / plan.

25. As the first line of defence, the Head of IT Function shall ensure effective assessment, evaluation, and management of IT controls and IT risk, including the implementation of robust internal controls, to

(1) secure the bank's information assets; and

(2) comply with extant internal policies, regulatory and legal requirements on IT related aspects.

G. Chief Information Security Officer

26. A senior level executive (preferably in the rank of a General Manager or an equivalent position) shall be designated as the CISO. The CISO shall not have

any direct reporting relationship with the Head of IT Function and shall not be given any business targets. The bank shall ensure the following:

(1) The CISO has the requisite technical background and expertise.

(2) The CISO is appointed for a reasonable minimum term.

(3) The CISO's office is adequately staffed with people having necessary technical expertise, commensurate with the business volume, extent of technology adoption and complexity.

(4) The budget for the information / cybersecurity is determined keeping in view the current / emerging threat landscape.

27. The bank shall ensure that the roles and responsibilities of the CISO are clearly defined and documented covering, at a minimum, the following points:

(1) The CISO shall be responsible for driving cybersecurity strategy and ensuring compliance to the extant regulatory / statutory instructions on information security / cybersecurity.

(2) The CISO shall be responsible for enforcing the policies that a bank uses to protect its information assets apart from coordinating information security / cybersecurity related issues within the bank as well as with relevant external agencies.

(3) The CISO shall be a permanent invitee to the ITSC and IT Steering Committee.

(4) The CISO's office shall manage and monitor Security Operations Centre (SOC) and drive cybersecurity related projects.

(5) The CISO's office shall ensure effective functioning of the security solutions deployed.

(6) The CISO shall directly report to the Executive Director or equivalent executive overseeing the risk management function.

(7) The CISO shall place a review of cybersecurity risks / arrangements / preparedness of the bank before the Board / Risk Management Committee of the Board (RMCB) / ITSC at least on a quarterly basis.

H. Information Technology Project Management

28. The bank shall follow a consistent and formally defined project management approach for IT projects which shall, inter alia, enable appropriate stakeholder participation for effective monitoring and management of project risks and progress.

29. The bank shall adopt a standard enterprise architecture planning methodology while adopting new or emerging technologies, tools, or while revamping the existing technology stack.

30. The bank shall ensure that the adoption of new or emerging technologies is commensurate with its risk appetite and aligned with the overall business / IT strategy. The bank shall also ensure that such adoption facilitates the optimal creation/ use/ sharing of information in a secure and resilient way.

31. The bank shall ensure that any new IT application proposed for introduction as a business product undergoes the prescribed product approval and quality assurance process.

(*Note:* IT applications that enable functioning of a business process whether offered as a product to the customers (including potential customers) / third parties / internal employees could be broadly referred as business product.)

I. IT Architecture

32. The bank shall design the IT architecture to facilitate security measures being in place at all times. The IT architecture shall be reviewed by the ITSC at least annually and upgraded, as required, based on the bank's risk assessment and in a phased manner. The bank shall document in writing any risk-cost or potential cost trade-off decisions to enable appropriate supervisory assessment.

J. IT Services Management

33. The bank shall put in place a robust IT Service Management Framework for supporting its information systems and infrastructure to ensure the operational resilience of their entire IT environment (including DR sites).

34. The bank shall put in place a Service Level Management (SLM) process to manage the IT operations while ensuring effective segregation of duties.

35. The bank shall ensure identification and mapping of the security classification (in terms of confidentiality, integrity, and availability) of information assets based on their criticality to the bank's operations.

36. For seamless continuity of business operations, the bank shall avoid using outdated and unsupported hardware or software and shall monitor software End-of-Support (EOS) dates and Annual Maintenance Contract (AMC) dates of IT hardware on an ongoing basis.

37. The bank shall develop a technology refresh plan for the replacement of hardware and software in a timely manner before they reach EOS.

Chapter IV - IT and Information Security Risk Management

A. Periodic Review of IT related Risks

38. The risk management policy of the bank shall include IT related risks, including the cybersecurity related risks. The RMCB in consultation with the ITSC shall periodically review and update the same at least on an annual basis.

B. IT and Information Security Risk Management Framework

39. The bank shall establish a robust IT and Information Security Risk Management Framework (the bank may have flexibility to define information security / cybersecurity risk management framework distinct from IT risk management framework) covering, inter alia, the following aspects:

    (1) implementation of comprehensive Information Security management function, internal controls, and processes (including applicable insurance covers) to mitigate / manage identified risks. The implemented controls and processes must be reviewed periodically on their efficacy in a risk environment characterised by change;

    (2) roles and responsibilities of stakeholders (including third-party personnel) involved in IT risk management. Areas of possible role conflicts and accountability gaps must be specifically identified and eliminated or managed;

    (3) identification of critical information systems of the organisation and fortification of the security environment of such systems; and

    (4) definition and implementation of necessary systems, procedures, and controls to ensure secure storage / transmission / processing of data / information.

C. Risk Identification, Assessment, and Documentation

40. The risk assessment for each information asset within the bank’s scope shall be guided by appropriate security standards / IT control frameworks.

41. The bank shall ensure that all staff members and service providers comply with the extant information security and acceptable-use policies as applicable to them.

42. The bank shall review the security infrastructure and security policies at least annually, factoring in its own experiences and emerging threats and risks. The bank shall take steps to adequately tackle cyber-attacks including phishing, spoofing attacks and mitigate their adverse effects.

43. While identifying and assessing the inherent risks, the bank shall reckon the technologies adopted, alignment with business and regulatory requirements, organisational culture, and internal and external threats.

44. Depending on the level of inherent risks, the bank shall identify its riskiness as low, moderate, high, and very high or adopt any other similar categorisation. Riskiness of the business component shall also be factored into while assessing the inherent risks.

45. While evaluating the controls, the bank shall suitably factor in Board oversight, policies, processes, cyber risk management architecture, availability of experienced and qualified resources, training programmes and organisational culture; arrangements for threat intelligence gathering, monitoring, and analysing the threat intelligence received vis-à-vis the situation in banking sector; information sharing arrangements [among peer banks, with Institute for Development and Research in Banking Technology (IDRBT) / RBI / Indian Computer Emergency Response Team (CERT-In)]; preventive, detective and corrective cybersecurity controls; vendor management; and incident management and response.

    (*Note:* The term ‘incident’ implies cyber incident in these Directions)

Chapter V - Baseline Cybersecurity and Resilience Requirements

A. Inventory Management of Information Assets

46. The bank shall maintain an up-to-date inventory of information assets, including business and customer data / information, business applications, supporting IT infrastructure, key personnel and facilities (such as hardware, software, network devices, and services) indicating their business criticality. The bank may have its own criteria for identifying critical assets.

47. The bank shall classify data / information based on its criteria for information classification / sensitivity.

48. The bank shall maintain enterprise data dictionary to enable the sharing of data among applications and information systems and promote a common understanding of data.

49. The bank shall appropriately manage and provide protection within and outside organisation borders / network taking into consideration how the data / information are stored, transmitted, processed, accessed and used within / outside the bank's network, and level of risk it is exposed to depending on the sensitivity of the data / information.

B. Data Leak Prevention Strategy

50. The bank 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.

51. The bank shall ensure similar arrangements at the vendor-managed facilities as well.

52. The bank, as owner of customers' personal and sensitive data, shall take appropriate steps in preserving the confidentiality, integrity, and availability of the same, irrespective of whether the data is stored / in transit within itself or with the

third-party vendors. The bank shall ensure that the confidentiality of such custodial information is not compromised at any situation and to this end, shall put in place suitable systems and processes across the data / information lifecycle.

53. The bank shall implement controls for remote management / wiping / locking of mobile devices including laptops.

C. Data Migration Controls

54. The bank shall put in place a data migration policy specifying a systematic process for data migration, ensuring data integrity, completeness, and consistency. The policy shall, inter alia, contain provisions for maintenance of audit trails of data migration activities and obtaining signoffs from business users and application owners at each stage of the migration.

D. Preventing Execution of Unauthorised Software

55. The bank shall maintain an up-to-date and centralised inventory of authorised / unauthorised software(s). The bank may implement whitelisting of authorised applications / software / libraries and other relevant software components.

56. The bank shall have a mechanism to control installation of software / applications centrally / otherwise on its information systems including end-user Personal Computers (PCs), laptops, workstations, servers, mobile devices, and cloud environments. The bank shall also have a mechanism to block / prevent and identify installation and running of unauthorised software / applications on such devices / systems.

57. The bank 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 bank. Where a patch / series of patches is / are released by the OEM / manufacturer / vendor to mitigate critical vulnerabilities that are actively exploited or widely reported, the bank shall have a mechanism

to deploy such patches expeditiously, in accordance with its emergency patch management process.

58. The bank shall put in place a policy specifying the justification for exceptions, duration of exceptions, process for granting exceptions, approving authority, and periodic review of granted exceptions by officers, at senior levels, who are equipped to understand the business and technical context of such exceptions.

E. Physical and Environmental Controls

59. The bank shall put in place appropriate physical and environmental controls for securing location of critical assets including Data Centre (DC) and Disaster Recovery (DR) sites from natural and man-made threats.

(*Note:* DC refers to primary data centre for a given application / system and DR refers to its Disaster Recovery site/ alternate site.)

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

61. The DC and DR sites shall be geographically well separated so that both the sites are not affected by a similar threat associated to their location.

62. The bank shall ensure that DC and DR sites are subjected to necessary e-surveillance mechanism.

F. Capacity Management

63. The bank shall ensure that information systems and infrastructure are able to support business functions and ensure availability of all service delivery channels.

64. On an annual or more frequent basis, the bank shall proactively assess capacity requirement of IT resources. The bank shall ensure that IT capacity planning across components, services, system resources, supporting infrastructure is consistent with past trends (peak usage), the current business requirements, and projected future needs as per the IT strategy of the bank.

G. Secure Configuration

65. The bank shall document and apply baseline security requirements / configurations to all categories of devices including endpoints / workstations, mobile devices, operating systems, databases, applications, network devices, security devices, and security systems, throughout the lifecycle (from conception to deployment) and carry out reviews periodically.

66. The bank shall put in place a mechanism to periodically evaluate and review critical devices such as firewall, network switches, and security devices, including their configurations and patch levels, across the bank's network including data centres, third-party hosted sites, and shared-infrastructure locations.

H. Network Management and Security

67. The bank shall ensure that only authorised access is permitted to its networks. Wherever the access is permitted, the bank shall ensure that it is provided through well-defined process with strict time limits, which are consistently followed and audited periodically. The bank shall clearly elucidate responsibility over such networks, which shall invariably rest with bank officials.

68. The bank shall prepare and maintain an up-to-date network architecture diagram at the organisation level including wired / wireless networks.

69. The bank shall maintain an up to date / centralised inventory of authorised devices connected to the bank's network (within / outside bank's premises). The bank may consider implementing solutions to automate network discovery and management.

70. The bank shall ensure that all the network devices are configured appropriately. The bank shall periodically assess whether the configurations are appropriate to the desired level of network security.

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

72. The bank shall implement mechanism to identify authorised hardware / mobile devices such as laptops, mobile phones, and tablets, in the network and ensure that they are provided connectivity only when they meet the security requirements prescribed by the bank.

73. The bank shall have mechanism to automatically identify unauthorised device connections to the bank's network and block such connections.

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

75. The bank shall establish Standard Operating Procedures (SOPs) for all major IT activities including for connecting devices to the network.

76. The bank shall ensure that boundary defences are multi-layered with properly configured firewalls, proxies, DMZ perimeter networks, and network-based Intrusion Prevention System (IPS) and Intrusion Detection System (IDS). Additionally, the bank shall establish robust mechanism for real-time filtering of inbound and outbound network traffic.

77. The bank shall enable its public facing IT infrastructure to handle Internet Protocol Version 6 (IPv6) traffic.

I. Application Security Life Cycle

78. The bank shall incorporate / ensure information security across all stages of application life cycle.

79. The bank shall implement secure coding practices for internally / collaboratively developed applications.

80. Besides business functionalities, the bank shall clearly specify 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 during the initial and ongoing stages of system development / acquisition / implementation.

81. The bank shall properly segregate the development, test, and production environments.

82. The bank shall ensure that the software / application development process is guided by threat modelling, adheres to secure coding practices, includes security testing aligned with global standards, and ensures a secure deployment.

83. The bank shall ensure that software / application development practices address the vulnerabilities based on best practices, baselines such as Open Web Application Security Project (OWASP) proactively and adopt principle of defence-in-depth to provide layered security mechanism.

84. The scope of application security assessments shall be comprehensive and shall not be restricted to testing solely against the OWASP top 10 vulnerabilities. The bank shall also refer to other recognised security standards and guidelines, as appropriate.

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

86. The bank shall implement measures such as installing ‘containerised’ apps on mobile / smartphones for exclusive business use that is encrypted and separated from other smartphone data / applications, as applicable. The bank shall implement measures to initiate a remote wipe on the containerised app, rendering the data unreadable, in case of requirement.

87. The bank shall ensure adequate evaluation of adoption of new technologies for existing / evolving security threats. Such technologies shall be introduced for critical systems after IT and security team of the bank reach reasonable level of comfort and maturity.

88. The bank shall ensure that software vendors provide maintenance and necessary support of software applications and shall enforce the same through formal agreements.

89. The bank shall obtain the source codes for all critical applications from its vendors. Where obtaining of the source code is not possible, the bank shall put in place a source code escrow arrangement or other arrangements to adequately mitigate the risk of default by the vendor. The bank shall ensure that all product updates and programme fixes are included in the source code escrow arrangement.

90. In respect of critical business applications, the bank may consider conducting source code audits by professionally competent personnel / service providers.

91. The bank shall obtain a certificate or a written confirmation from the application developer or vendor stating that the application is free of known vulnerabilities, malware, and any covert channels in the code. The bank shall also obtain such a certificate or a written confirmation whenever material changes to the code, including upgrades, occur. The definition of material changes can be mutually agreed upon between the bank and its vendor. 'Material Changes' refer to significant modifications to the software code that could impact the application's functionality, security, or performance. This, however, excludes routine maintenance activities such as minor bug fixes, performance optimisations, and updates that do not alter the application's core functions, security posture, or compliance status. It is essential to conduct a risk assessment when determining whether a change is material.

J. Maintenance, Monitoring, and Analysis of Audit Logs

92. The bank shall ensure that every IT application / system that can access or affect critical or sensitive information has necessary audit logging capabilities and provides audit trails.

93. The bank shall implement and periodically validate settings for capturing appropriate logs and audit trails for 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, destination addresses, and other relevant elements of each packet, event, and / or transaction.

94. The bank shall ensure that audit trails satisfy its business requirements, in addition to regulatory and legal requirements. The bank shall also ensure that audit trails are sufficiently detailed to facilitate the conduct of audits, serve as forensic evidence (the term 'forensics' refers to 'digital forensics' for the purpose of these Directions) when required, and assist in dispute resolution, including for non-repudiation purposes.

95. The bank shall put in place a system for regularly monitoring the audit trails and system logs to detect, understand or recover from any unauthorised activity or attack.

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

K. Patch, Vulnerability and Change Management

97. The bank shall put in place documented policy(ies) and procedures for change and patch management to ensure the following:

    (1) The business impact of implementing patches / changes (or not implementing a particular patch / change request) is assessed.

    (2) The patches / changes are applied / implemented and reviewed in a secure and timely manner with necessary approvals.

    (3) Any changes to an application system or data are justified by genuine business needs and approvals supported by documentation and subjected to a robust change management process.

    (4) A mechanism is established to recover from failed changes / patch deployment or unexpected results.

98. The bank shall adopt a documented, risk-based strategy for maintaining an inventory of IT components that require patching, identifying all applicable patches, and applying them in a timely manner to minimise both the number of vulnerable systems and the duration of exposure.

99. The bank shall put in place systems and processes to identify, track, manage, and monitor the status of patches to operating system and application software running at end-user devices directly connected to the internet and in respect of server operating systems, databases, applications, middleware, and other relevant information systems.

100. The bank shall manage changes to business applications, supporting technology, service components, and facilities through robust configuration management processes and configuration baselines to ensure the integrity of such changes.

101. As part of its threat mitigation strategy, the bank shall determine the root cause of any detected incident and implement necessary patches to address the vulnerabilities.

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

L. User Access Control / Management

103. Access to information assets shall be allowed only where a valid business need exists.

104. Personnel with elevated system access entitlements shall be closely supervised with all their system activities logged and periodically reviewed.

105. The bank 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 secure protocols)

106. The bank shall protect user access credentials such as logon user-id, authentication information and tokens, access profiles, against leakage / attacks.

107. The bank shall disallow administrative rights on end-user workstations / PCs / laptops and provide access rights on a need-to-know basis and for specific duration when it is required following an established process.

108. The bank shall implement centralised authentication and authorisation system for accessing and administering applications, operating systems, databases, network, and security devices / systems, point of connectivity (local / remote) including enforcement of strong password policy, and following the principle of least privileges and separation of duties.

109. The bank, based on the risk assessment, shall implement two-factor or multi-factor authentication, including mandatory multi-factor authentication for privileged users of (i) critical information systems and (ii) critical activities.

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

111. The bank shall implement controls to minimise invalid logon counts and deactivate dormant accounts.

112. The bank shall monitor any abnormal change in pattern of logon.

M. Controls on Teleworking

113. In the teleworking environment, the bank shall inter alia:

(1) ensure that the systems used and the remote access from alternate work location to the environment hosting bank's information assets are secure;

(2) implement multi-factor authentication for enterprise access (logical) to critical systems;

(3) put in place a mechanism to identify all remote-access devices attached / connected to the bank's systems; and

(4) ensure that data / information shared / presented in teleworking is secured appropriately.

N. Authentication Framework for Customers

114. The bank shall implement an authentication framework to ensure positive identity verification for customers accessing its services and to enable customers to verify the authenticity of the bank, across all delivery channels.

115. The bank shall act as the identity provider for identification and authentication of customers for access to partner systems using secure authentication technologies.

O. Secure Mail and Messaging Systems

116. The bank shall implement secure mail and messaging systems with measures to prevent email spoofing, look-alike domain abuse, protect against malicious attachments and links, and email filtering to protect against spam. The bank shall require its partners and vendors to implement similar measures for their mail and messaging systems.

117. The bank shall document and implement email server specific controls.

118. The bank shall implement measures to control permissible attachment types in email systems.

119. The bank shall implement Domain-based Message Authentication, Reporting, and Conformance (DMARC) solution for the email domains. The bank shall impress upon its vendors, partners, and other relevant third parties to implement similar solution securing their mail systems to mitigate email spoofing.

P. Removable Media

120. As a default rule, the bank shall not permit use of removable devices and media in the banking environment unless specifically authorised for defined use and duration of use.

121. The bank shall define and implement policy for restriction and secure use of removable media / Bring Your Own Device (BYOD) on various types / categories of devices including but not limited to workstations, PCs, laptops, mobile devices, servers, and ensure secure erasure of data on such media after use.

122. The bank shall limit media types and information that could be transferred / copied to / from such devices.

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

124. The bank shall consider implementing centralised policies through Active Directory or end-point management systems to whitelist / blacklist / restrict removable media use.

Q. Third-Party Arrangements

(The paragraphs from 125 to 134 are applicable only for such third-party arrangements in the Information Technology / Cybersecurity ecosystem, which are not within the applicability of Reserve Bank of India (Small Finance Banks – Managing Risks in Outsourcing) Directions, 2025)

125. The bank shall, put in place appropriate vendor risk assessment process, and controls proportionate to the assessed risk and materiality to, inter alia:

(1) mitigate concentration risk;

(2) eliminate or address any conflict of interests;

(3) mitigate risks associated with single point of failure;

(4) comply with applicable legal, regulatory requirements and standards to protect customer data;

(5) provide high availability (for uninterrupted customer service); and

(6) manage supply chain risks effectively.

126. The bank shall be accountable for ensuring appropriate management and assurance on security risks in outsourced and partner arrangements.

127. The bank shall carefully evaluate the need for outsourcing critical processes and selection of vendor / partner based on comprehensive risk assessment.

128. The bank shall regularly conduct effective due diligence, oversight, and management of third-party vendors / service providers and partners.

129. The bank shall establish appropriate policies and procedures to evaluate, assess, approve, review, control, and monitor the risks and materiality of all its vendor / outsourcing activities.

130. The bank shall ensure and demonstrate that the service provider adheres to all regulatory and legal requirements of the country.

131. The bank shall necessarily enter into an agreement with the service provider that amongst others provides for right to audit by the bank and right of RBI or person(s) authorised by it to perform inspection.

132. The bank shall ensure that RBI shall have access to all information resources (online / in person) that are consumed by it. Such information shall be made accessible to RBI officials by the bank when sought, though the infrastructure / enabling resources may not be physically located in the premises of bank.

133. The bank shall adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and cross-border movement of data.

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

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

(1) Preventing Access of Unauthorised Software: Paragraphs 56 to 58 of these Directions;

(2) Environmental Controls: Paragraphs 59 and 60 of these Directions;

(3) Network Management and Security: Paragraphs 68 to 70 and Paragraphs 72 to 76 of these Directions;

(4) Secure Configuration: Paragraphs 65 and 66 of these Directions;

(5) Application Security Life Cycle (ASLC): Paragraphs 78, 79, 81, 82, 83 and 87 of these Directions;

(6) Patch / Vulnerability and Change Management: Paragraphs 85, 98, 100 to 102 of these Directions;

(7) User Access Control / Management: Paragraphs 105, 106, 111 and 112 of these Directions;

(8) Data Leak Prevention Strategy: Paragraph 50 of these Directions;

(9) Audit Logs: Paragraphs 93 and 95 of these Directions;

(10) Incident Response and Management: Paragraph 163 of these Directions;

(11) Advanced Real-time Threat Defence and Management: Paragraphs 143 and 144 of these Directions; and

(12) Forensics: Paragraph 210 of these Directions.

136. Controls at paragraph 135 shall be suitably factored in the contract agreement signed with the third-party 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 bank.

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

(1) The default passwords of all the network devices / systems of the ASP shall be changed after installation.

(2) The ASP shall not use trivial and / or default passwords.

(3) The ASP shall implement a centralised authentication and authorisation system through an Identity and Access Management solution for accessing and administering 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 depending on risk assessment, securing privileged accesses following the principle of least privileges and separation of duties.

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

(5) The ASP shall design the infrastructure with adequate network segregation controls.

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

(7) The ASP shall disable remote connections from outside machines to the network hosting the ATM Switch infrastructure.

(8) The ASP shall enable Internet Protocol (IP) table to restrict access to the clients and servers in Society for Worldwide Interbank Financial Telecommunication (SWIFT) and ATM Switch environment only to authorised systems.

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

(10) The ASP shall ensure to appropriately mask the data used for development and testing.

(11) The ASP shall certify any new products and updates, 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 bank / RBI as and when requested.

(12) 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 bank that the application is free from embedded malicious / fraudulent code.

(13) The ASP shall have 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.

(14) 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.

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

(16) The ASP shall ensure to capture audit logs pertaining to user actions in a system. Such arrangements shall facilitate forensic auditing, if need be.

(17) The ASP shall implement an alert mechanism to monitor any change in the log settings.

(18) The ASP is responsible for meeting the requirements prescribed for incident management and Business Continuity Plan (BCP) / DR even if their 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 include, among other things, informing the bank about any cyber incident occurring in respect of the bank on a timely basis to mitigate the risk at the earliest as well as to meet extant regulatory requirements.

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

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

(21) The ASP's risk management / treatment framework shall ensure that the vulnerabilities detected are remediated promptly to avoid exploitation of such vulnerabilities.

(22) The ASP shall have a mechanism and resources to take appropriate action in case of any cyber incident. The ASP shall have a written incident response procedure 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 bank, during response.

(23) The ASP shall set up a Cyber Security Operations Centre (CSOC). The CSOC, among other things, shall ensure to

(i) seamlessly collect the logs relevant to the IT ecosystem;

(ii) store, process, and correlate the logs through appropriate Security Information and Event Management (SIEM) solution for continuous surveillance; and

(iii) regularly update on the latest nature of emerging cyber threats.

(24) 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.

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

R. Cryptographic Controls

139. The key length, algorithms, cipher suites and applicable protocols used in transmission channels, processing of data and authentication purpose shall be strong. The bank shall adopt internationally accepted and published standards 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.

S. Straight Through Processing

140. In order to prevent unauthorised modification of data, the bank shall ensure that there is no manual intervention or manual modification in data while it is being transferred from one process to another or from one application to another, in respect of critical applications.

141. Data transfer mechanism between processes or applications shall be properly tested, securely automated with necessary checks and balances, and properly integrated through ‘Straight Through Processing’ methodology with appropriate authentication mechanism and audit trails.

T. Continuous Surveillance

142. The bank shall set up a CSOC to ensure continuous surveillance and keep itself regularly updated on the latest nature of emerging cyber threats. An indicative, but not exhaustive, minimum baseline guidance on CSOC is given in Chapter VI of these Directions.

U. Advanced Real-time Threat Defence and Management

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

144. The bank shall implement anti-malware, antivirus protection including behavioural detection capabilities across all relevant devices and environments, such as endpoints (including PCs, laptops, and mobile devices), servers (operating systems, databases, and applications), Web / Internet gateways, email-gateways, wireless networks, and Short Message Service (SMS) servers. The bank shall also implement tools and processes for centralised management and monitoring of these measures.

145. The bank shall implement whitelisting of internet websites / systems.

146. The bank shall consider implementing secure web gateways with capability to deep scan network packets including secure Hypertext Transfer Protocol Secure (HTTPS) traffic passing through the web / internet gateway.

V. Anti-Phishing

147. The bank shall subscribe to anti-phishing / anti-rogue app services from external service providers for identifying and taking down phishing websites / rogue applications.

W. Vulnerability Assessment and Penetration Test

148. The bank shall conduct VA and PT exercises periodically for all the critical and internet facing systems.

149. The bank shall periodically conduct VA / PT of critical, internet facing web / mobile applications, servers, and network components throughout their lifecycle including pre-implementation, post-implementation, and after changes.

150. For critical information systems and / or those in the DMZ having customer interface, VA shall be conducted at least once in every six months and PT at least once in 12 months. For non-critical information systems, a risk-based approach shall be adopted to decide the requirement and periodicity of conduct of VA / PT.

151. In the post-implementation (of IT project / system upgrade) scenario, the VA / PT shall be performed on the production environment. Under unavoidable circumstances, if the PT is conducted in test environment, the bank shall ensure that the version and configuration of the test environment resembles the production environment. Any deviation should be documented and approved by the ISC.

152. The bank shall ensure to fix the identified vulnerabilities and associated risks in a time-bound manner by undertaking requisite corrective measures and ensure that the compliance is sustained to avoid recurrence of known vulnerabilities such as those available in Common Vulnerabilities and Exposures (CVE) database.

153. The bank shall put in place a documented approach for conduct of VA / PT covering the scope, coverage, vulnerability scoring mechanism (e.g., Common Vulnerability Scoring System) and all other aspects. This shall also apply to the bank's information systems hosted in a cloud environment.

154. VA / PT shall be conducted by appropriately trained and independent information security experts / auditors.

155. The bank shall have control / check over audit methodology, processes, and competence of auditors so as to ensure that audit objectives are fully met. At the time of selecting, appointing, or engaging or renewing the contract with the VA / PT auditor or consultant, the bank shall consider aspects such as requisite qualification, professional expertise (of the firm or company as well as the audit personnel engaged by the entity), appropriate credentials, and suitable competency.

156. The bank shall review the coverage and scope of the VA / PT and ensure that reasonable assurance for each of the areas therein shall be provided explicitly in the VA / PT audit reports. The same shall be mentioned at the time of empanelling or selecting and awarding the contract with the VA / PT auditor.

157. The bank shall, on an ongoing basis, review the performance of the VA / PT auditor and ensure that appropriate action is taken in case of noting any deficiencies. For instance, systems, applications, or infrastructure that were

subjected to VA / PT, ceteris paribus, if found to have been compromised at a later date, apparently due to vulnerabilities that were not observed or highlighted on timely basis in the VA / PT will qualify as a deficiency in discharge of function by the VA / PT auditor. Such deficiencies shall also be factored in while evaluating the competency when selecting or renewing the contract with the VA / PT auditor.

158. The bank shall continuously interact with the VA / PT auditors during the audit and in case of CERT-In empanelled auditors, the bank shall be guided by CERT-In's Comprehensive Cyber Security Audit Policy Guidelines.

159. Findings of VA / PT and the follow up actions necessitated shall be monitored closely by the Information Security / Information Systems Audit team as well as Senior Management.

160. The status of the closure of the VA / PT observations shall be put to the ITSC and ISC at least on a quarterly basis.

X. Red Teaming Exercises

161. The bank may conduct red teaming exercises to identify the vulnerabilities and the business risk, assess the efficacy of the defences and check the mitigating controls already in place by simulating the objectives and actions of an attacker.

Y. Business Continuity and Disaster Recovery

162. The BCP and DR policy shall adopt best practices (e.g., ISO 22301) to guide its actions in reducing the likelihood or impact of disruptive incidents and maintaining business continuity. The policy shall be updated based on major developments and risk assessments.

163. The bank's BCP and DR capabilities shall be designed to effectively support resilience objectives and enable rapid recovery and secure resumption of critical operations including key cybersecurity controls post cyber-attacks / other incidents aligned with recovery time objectives while ensuring security of processes and data.

164. Periodicity of DR drills for critical information systems shall be at least on a half-yearly basis and for other information systems, as per the bank's risk assessment.

165. Any major issues observed during the DR drill shall be resolved and tested again to ensure successful conduct of drill before the next cycle.

166. The DR testing shall involve switching over to the DR / alternate site and thus using it as the primary site for sufficiently long period where usual business operations of at least a full working day (including Beginning of Day to End of Day operations) are covered.

167. The bank shall regularly test the BCP / DR under different scenarios for possible types of contingencies, to ensure that it is up-to-date and effective.

168. The bank shall backup data and periodically restore such backed-up data to check its usability. The integrity of such backup data shall be preserved along with securing it from unauthorised access.

169. The bank shall ensure that DR architecture and procedures are robust, meeting the defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for any recovery operations in case of contingency.

170. The bank shall prioritise achieving minimal RTO (as approved by the bank's ITSC) and a near zero RPO for critical information systems.

171. In a scenario of non-zero RPO, the bank shall have a documented methodology for reconciliation of data while resuming operations from the alternate location.

172. The bank shall ensure that the configurations of information systems and deployed security patches at the DC and DR are identical.

173. The bank shall ensure BCP and DR capabilities on critical interconnected systems and networks including those of vendors and partners. The bank shall ensure demonstrated readiness through collaborative and co-ordinated resilience testing that meets the bank's RTO.

Z. Cyber Incident Response and Recovery Management

Z.1 Responding to Cyber-Incidents

174. The bank shall put in place cyber incident response and recovery management policy and related procedures which shall address the following:

(1) definition, classification, and assessment of incidents;

(2) allocation of roles and responsibilities of staff as well as outsourced staff manning / handling such incidents;

(3) mechanism for reporting of cyber incidents by employees, vendors, and customers;

(4) clear communication strategy and plan to manage such incidents;

(5) measures to contain exposures and achieve timely recovery;

(6) collection / sharing of threat information;

(7) post incident review; and

(8) periodical testing of incident response plans.

175. The bank shall provide specialised training to the personnel handling cyber incidents.

176. Response plans 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.

177. The bank shall have mechanism to dynamically incorporate lessons learnt to continually improve the response plans.

178. The bank shall document and communicate strategies to respond to advanced attacks such as ransomware / cyber extortion, data destruction, and DDoS.

179. The bank shall contain the level of cyber-attack by implementing shielding controls / quarantining the affected devices / systems.

180. The bank shall analyse cyber incidents (including through forensic analysis, if necessary) for their severity, impact, and root cause. The bank shall take measures, corrective and preventive, to mitigate the adverse impact of incidents on business operations.

181. The bank shall report cyber incidents within six hours of detection on DAKSH platform (Reserve Bank's advanced supervisory monitoring system - https://daksh.rbi.org.in). The bank shall also pro-actively notify CERT-In regarding cyber incidents.

182. The bank shall have clear communication plans for escalation and reporting the incidents to the Board and Senior Management as well as to customers, as required.

183. The bank may actively participate in the activities of CISO's forum coordinated by IDRBT and share the threat intelligence arising from cyber incidents to Indian Banks-Centre for Analysis of Risks and Threats (IB-CART) set up by IDRBT.

184. The bank shall establish appropriate arrangements for external coordination and information sharing, including integration of threat intelligence and security information feeds from relevant internal and external sources, and coordination with industry participants, cyber response agencies, CERT-In, telecom service providers, and other stakeholders, as may be required.

185. The bank shall establish and implement systems to collect and share threat information from local / national / international sources following legally accepted / defined means / process.

Z.2 Recovery from Cyber Incidents

186. The bank shall establish processes to improve incident response and recovery activities and capabilities through lessons learnt from past incidents as well as from the conduct of tests and drills.

187. The bank shall periodically and actively participate in cyber drills and related simulation exercises conducted under the aegis of institutions / agencies such as Cert-IN and IDRBT.

188. The bank shall ensure resilient capabilities in all interconnected systems and networks including those of vendors and partners and readiness demonstrated through collaborative and coordinated resilience testing that meets the bank's recovery time objectives. Adequate capacity shall be planned and maintained, in consideration thereof.

189. The bank, inter alia, shall ensure effectiveness of crisis communication plan / process by conduct of periodic drills / testing with stakeholders (including customers and service providers).

190. The bank shall align Security Operation Centre, Incident Response and Digital forensics to reduce the business downtime and restore normal operations.

Z.3 Cyber Crisis Management Plan

191. The bank shall document a Cyber Crisis Management Plan (CCMP) which shall be part of the overall Board approved framework in cybersecurity.

192. CCMP shall address the following four aspects: (i) Detection, (ii) Containment, (iii) Response, and (iv) Recovery. The bank shall take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to contain / respond / recover from the fallout. The bank shall be well prepared to face emerging cyber-threats such as 'zero-day' attacks, remote access threats, and targeted attacks. Among other things, the bank shall take necessary preventive and corrective measures in addressing various types of cyber threats including, but not limited to, denial of service, DDoS, ransomware / crypto ware, 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.

AA. Metrics

193. The bank 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, and vulnerability related metrics.

194. Additionally, the bank shall define suitable metrics for system performance, recovery, and business resumption, including RPO and RTO, for all critical information systems. For non-critical information systems, the bank shall adopt a risk-based approach to define suitable metrics.

195. The bank shall implement suitable scorecard / metrics / methodology to measure IT performance, and IT maturity level.

196. The adequacy of and adherence to cybersecurity framework shall be assessed and measured through development of indicators to assess the level of risk / preparedness. The awareness among the stakeholders including employees may also form a part of this assessment.

BB. User / Employee / Management Awareness

197. The bank shall proactively promote awareness of its cyber resilience objectives among service providers, partners and other stakeholders, and shall require appropriate actions to ensure aligned implementation and testing.

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

199. The bank shall provide targeted awareness and training for key personnel in executive, operational, and security administration or management roles.

200. The bank shall encourage the reporting of suspicious behaviour incidents to the incident management team.

201. The bank shall evaluate the awareness level of employees periodically.

202. The bank shall establish a mechanism for continuous and adaptive capacity building to strengthen cybersecurity management. Cybersecurity awareness

programmes shall be mandatory for all new recruits, and annual training shall be conducted for lower and middle management.

203. The bank shall ensure that the Board and Senior Management maintain adequate awareness of evolving cyber threats by periodically sensitising them to technological advancements and cybersecurity developments. The bank shall also provide annual training to all Board members and Senior Management on IT and cybersecurity risks and evolving best practices.

CC. Customer Education and Awareness

204. The bank shall improve and maintain customer awareness and education regarding cybersecurity risks.

205. The bank shall encourage customers to report phishing mails / phishing sites and on such reporting, the bank shall take effective remedial action.

206. The bank shall educate the customers about the risks and consequences of sharing their login credentials, passwords, One-Time Passwords (OTPs), Personal Identification Numbers (PINs), and other authentication information.

207. The bank shall proactively promote awareness of its cyber resilience objectives among customers.

DD. Risk based Transaction Monitoring

208. The bank shall implement risk-based transaction monitoring or surveillance process as part of fraud risk management system across all delivery channels.

209. The bank shall notify the customer, through alternate communication channels, of all payment or fund transfer transactions above a specified value determined by the customer.

EE. Forensics

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

Chapter VI - Cyber Security Operation Centre

A. Governance

211. The bank shall put in place a framework for establishment and operation of a Cyber Security Operations Centre (CSOC), commensurate with its technology risk profile, scale and complexity of operations, business requirements and applicable regulatory and legal obligations.

212. The bank shall ensure appropriate governance arrangements while setting up the CSOC, including briefing of the Board / ITSC and Senior Management on threat intelligence; establishment of dashboards for effective oversight; formulation and enforcement of policy with defined measurement and mechanisms such as key metrics and reporting structures specifying what is to be reported; and timely communication with all the stakeholders.

B. Capabilities

213. The CSOC shall ensure proactive monitoring and management capabilities with sophisticated tools for detection, quick response, and sound analytics.

214. The bank shall ensure that the systems implemented for monitoring security operations shall enable collection of logs from deployed systems / products and of various network activities; storage and processing of such logs; correlation of logs through appropriate SIEM tools; continuous monitoring of SIEM dashboards to identify anomalies, if any; and generation of alerts / events / incidents to escalate any abnormal / undesirable activities.

215. The bank shall ensure that the systems as part of CSOC addresses the following:

    (1) identification of the root cause of attacks;

    (2) classification of such attacks into identified categories, and implementation of solutions to contain further attacks of similar nature;

    (3) capabilities for incident investigation and problem management;

(4) dynamic behaviour analysis (including preliminary static and dynamic analysis);

(5) collection of Indicators of Compromise (IOCs);

(6) analytics supported by effective dashboards, including visibility of IP geo-location and counter-response mechanisms; and

(7) honeypot services.

216. The bank 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 bank as well as with external agencies, as required.

217. The CSOC shall have security analytics engine which can process the logs within reasonable time frame and come out with possible recommendations with options for further deep dive investigations and deliver wire speed performance with on-the-fly deep packet inspection.

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

219. The bank shall ensure that the CSOC's solution architecture deployed addresses the performance and scalability requirements in addition to high availability and is capable of

(1) protecting critical business and customer data and information, demonstrating compliance with internal guidelines as well as applicable regulations and laws;

(2) providing real-time or near real-time information and insights into the security posture of the bank;

(3) effectively and efficiently managing security operations by preparing for and responding to cyber risks and threats and facilitating business continuity and recovery;

(4) assessing threat intelligence and proactively identifying and visualising the impact of threats on the bank;

(5) establishing clear attribution of actions including who did what, when and how, along with preservation of evidence; and

(6) integrating various log types and logging options into SIEM and related systems, including ticketing, workflow and case management, unstructured and big data platforms, and development of use cases and rules customised to the bank's risk and compliance requirements and drivers.

C. Staff Capabilities

220. The bank shall put in place an appropriate organisational structure to ensure that the CSOC is managed and monitored on a continuous basis by competent and capable personnel. All personnel engaged in CSOC operations shall possess adequate knowledge of the bank's products, services, and deployed technology environment. The structure shall provide for role-based responsibilities across different levels of operations, including the following:

(1) Round-the-clock Level 1 monitoring by adequately trained personnel with relevant product and vendor certifications;

(2) Level 2 capabilities staffed by personnel with specialised expertise in areas such as network, data, and endpoint security to support root cause analysis and to take suitable corrective actions; and

(3) Level 3 capabilities comprising SOC analysts with advanced security expertise, including deep packet analysis, collection of IOCs, forensic

knowledge for collection of evidence, malware reverse engineering and development of custom scripts, as required.

221. The bank shall adopt a differentiated and structured approach to hiring, managing, and retaining personnel for the CSOC, recognising the specialised nature of the function.

222. The bank shall put in place appropriate mechanisms to determine staffing requirements for continuous monitoring on 24x7 basis. The bank shall adopt suitable sourcing and operating models including in-house staffing or managed service arrangements, ensure adequate training of personnel whether internal or service provider-deployed, establish appropriate compensation and incentive structures to retain skilled staff, define metrics to assess SOC performance, and ensure scalability and continuity of personnel through effective capacity planning initiatives.

Chapter VII - Information Systems Audit

223. The ACB shall be responsible for exercising oversight of IS Audit of the bank.

224. The bank shall put in place an IS Audit Policy. The IS Audit Policy shall clearly describe key aspects, including its mandate, purpose, authority, audit universe, periodicity of audit. The ACB shall approve the policy and review it at least annually.

225. The ACB shall review critical issues highlighted related to IT / information security / cybersecurity and provide appropriate direction and guidance to the bank's Management.

226. The bank shall have a separate IS Audit function or resources who possess required professional skills and competence within the Internal Audit function. Where the bank uses external resources for conducting IS audit in areas where skills are lacking within the bank, the responsibility and accountability for such external IS audits would continue to remain with the competent authority within Internal Audit function.

227. The bank shall carry out IS Audit planning by adopting a risk-based audit approach.

228. The bank may consider, wherever possible, a continuous auditing approach for critical systems, performing control and risk assessments on a more frequent basis.

Chapter VIII - Repeal and Other Provisions

A. Repeal and Saving

229. With the issue of these Directions, the existing directions, instructions, and guidelines relating to Cybersecurity Framework and IT Governance as applicable to Small Finance Banks 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.

230. 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

231. 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

232. 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