भारतीय रिज़र्व बैंक
Reserve Bank of India

RBI/DoS/2026-27/461
DoS.CO.CSITEG. 55 /31.01.015/2026-27 July 31, 2026

Reserve Bank of India (Non-Banking Financial Companies – 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 45-L and 45-M of the Reserve Bank of India Act, 1934, Section 3 read with Section 6 and 31A of the Factoring Regulation Act, 2011, and Sections 30, 30-A, 32 and 33 of the National Housing Bank Act, 1987, 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 (Non-Banking Financial Companies – Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026.

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

B. Applicability

3. The applicability of these Directions is as follows:

   (1) The provisions contained in these Directions shall be applicable to all Non-Banking Financial Companies (hereinafter collectively referred to as 'NBFCs' and individually as 'NBFC') registered with RBI under the provisions of the RBI Act, 1934, Factoring Regulation Act, 2011, National Housing Bank (NHB) Act, 1987, unless specified otherwise.

   (2) The provisions contained in Chapter III shall be applicable only for NBFCs-Base Layer (NBFCs-BL) with asset size below ₹500 crore, and Core Investment Companies (CICs) as defined in Reserve Bank of India (Non-Banking Financial Companies – Registration, Exemptions and Framework for Scale Based Regulation) Directions, 2025.

   (3) The provisions contained in Chapter IV shall be applicable only for NBFCs-BL with asset size ₹500 crore and above.

   (4) The provisions contained in Chapter V shall be applicable only for NBFCs-Top Layer (NBFCs-TL), NBFCs-Upper Layer (NBFCs-UL), and NBFCs-

Middle Layer (NBFCs-ML) as defined in Reserve Bank of India (Non-Banking Financial Companies – Registration, Exemptions and Framework for Scale Based Regulation) Directions, 2025, excluding CICs.

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) *'Framework'* - A framework is a structured set of strategies, policies, procedures, methods, and best practices that guides organisational

activities, enables governance, and supports the achievement of defined objectives.

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

(16) *'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)

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

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

(19) *'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)

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

(*Source*: ISACA glossary)

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

(22) *'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.

(23) *'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.

(24) *'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)

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

(*Source*: NIST glossary)

(26) *'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)

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

(28) *'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, 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

6. The Board of Directors (Board) shall approve the strategies and policies related to Technology and Cybersecurity frameworks which shall be reviewed at least annually by it.

Chapter III - Requirements for NBFCs (Base Layer with asset size below ₹500 crore) and Core Investment Companies

A. Baseline Cybersecurity and Resilience Requirements

7. The NBFC shall prioritise the implementation of basic IT systems to digitise and secure its primary business databases.

8. The NBFC shall put in place a Board approved IT / IS policy. This policy shall be designed considering the undermentioned basic standards. The IT systems shall have:

   (1) basic security aspects such as physical / logical access controls and well-defined password policy;

   (2) well-defined user role;

   (3) maker-checker concept to reduce the risk of error and misuse, and to ensure reliability of data / information;

   (4) robust information security and cybersecurity controls;

   (5) requirements as regards Digital Signature Certificates, Mobile Financial Services, and Social Media (Directions listed under paragraphs 31, 33 and 34 of Chapter IV of these Directions);

   (6) system generated reports for Senior Management summarising financial position including operating and non-operating revenues and expenses, cost benefit analysis of segments / verticals, and cost of funds;

   (7) adequacy to file regulatory returns with RBI;

   (8) Business Continuity Plan (BCP) policy duly approved by the Board ensuring regular oversight of the Board by way of periodic reports (at least once every year); and

   (9) arrangement for backup of data with periodic testing.

9. The NBFC shall progressively scale up its IT systems as the size and complexity of its operations increases.

Chapter IV - Requirements for NBFCs (Base Layer with asset size ₹ 500 crore and above)

A. IT Governance

10. The NBFC shall establish a robust IT Governance framework that is integrated with its overall corporate governance structure. The IT Governance shall be treated as a continuous life-cycle process where IT strategy shall be the primary driver of IT policy and processes. The IT Governance framework shall:

    (1) include leadership support, organisational structures, and processes to ensure that IT effectively sustains and extends the NBFC's business strategies and objectives; and

    (2) be built upon the basic principles of value delivery, IT risk management, IT resource management, and performance management.

11. The NBFC shall adopt relevant aspects of prudential governance standards that are at par with the best practices prevalent in the financial services industry and ensure that necessary resources are allocated and utilised to execute the responsibilities defined under the IT strategy.

12. Effective IT Governance shall be the responsibility of the Board and Senior Management. The NBFC shall establish well-defined roles and responsibilities for the Board and Senior Management in the implementation of IT Governance framework. IT Governance stakeholders include Board of Directors, IT Strategy Committee (ITSC), Chief Executive Officer (CEO), Business Executives, Chief Information Officer (CIO), Chief Technology Officer (CTO), IT Steering Committee (operating at an executive level and focusing on priority setting, resource allocation, and project tracking), Chief Risk Officer, and Risk Committee.

13. The NBFC shall formally document and communicate the well-defined roles, authorities, and responsibilities for all IT Governance stakeholders, to ensure effective project control.

14. The NBFC shall ensure that every stakeholder is aware of the expectations regarding the quality, budget, and timelines of IT deliverables.

A.1 Information Technology Strategy Committee (ITSC)

15. The NBFC shall form an ITSC which shall comply with the following requirements:

    (1) The chairman of the ITSC shall be an independent director.

    (2) The CIO and CTO shall be members of the ITSC.

    (3) The ITSC shall meet at an appropriate frequency but not more than six months should elapse between two meetings.

    (4) The ITSC shall work in partnership with other Board Committees and Senior Management to provide input to them. It shall also review and amend the IT strategy in line with the corporate strategies, Board policy reviews, cybersecurity arrangements, and any other matter related to IT Governance.

    (5) The ITSC's deliberations shall be placed before the Board.

A.2 Roles and Responsibilities

16. The roles and responsibilities of ITSC shall include:

    (1) approving IT strategy and policy documents, and ensuring that the management has put in place an effective strategic planning process;

    (2) ascertaining that the management has implemented processes and practices that ensure that the IT delivers value to the business;

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

    (4) monitoring the method used by the management to determine the IT resources needed to achieve strategic goals, and providing high-level direction for sourcing and use of IT resources; and

(5) ensuring proper balance of IT investments for sustaining NBFC's growth and becoming aware about exposure towards IT risks and controls.

17. The role of ITSC in respect of outsourced operations shall include:

(1) instituting an appropriate governance mechanism for outsourced processes, comprising of risk-based policies and procedures, to effectively identify, measure, monitor, and control risks associated with outsourcing in an end-to-end manner;

(2) defining approval authorities for outsourcing depending on nature of risks and materiality of outsourcing;

(3) developing sound and responsive outsourcing risk management policies and procedures commensurate with the nature, scope, and complexity of outsourcing arrangements;

(4) undertaking a periodic review of outsourcing strategies and all existing material outsourcing arrangements;

(5) evaluating the risks and materiality of all prospective outsourcing based on the framework developed by the Board;

(6) periodically reviewing the effectiveness of policies and procedures;

(7) communicating significant risks in outsourcing to the NBFC's Board on a periodic basis;

(8) ensuring an independent review and audit in accordance with approved policies and procedures; and

(9) ensuring that contingency plans have been developed and tested adequately.

B. IT Policy

18. The NBFC shall formulate a Board approved IT policy, in line with the objectives of its organisation comprising the following:

(1) The NBFC shall put in place IT organisational structure commensurate with the size, scale, and nature of business activities carried out.

(2) The NBFC shall designate a senior executive as the CIO or In-Charge of IT operations whose responsibility is to ensure implementation of IT Policy to the operational level involving IT strategy, value delivery, risk management, and IT resource management.

(3) The NBFC shall periodically assess IT training requirements to ensure the availability of sufficient, competent, and capable human resources, and to ensure technical competence at the senior and middle management levels.

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

C. Information Security and Cybersecurity

19. The NBFC shall put in place a robust Information Security framework to protect the information assets to ensure the achievement of organisational objectives.

C.1 Information Security Policy

20. The NBFC shall have a Board approved Information Security policy which shall incorporate the following basic tenets of information security:

(1) Confidentiality – ensuring access to sensitive data to authorised users only;

(2) Integrity – ensuring accuracy and reliability of information by ensuring that there is no modification without authorisation;

(3) Availability – ensuring that uninterrupted data is available to users when it is needed; and

(4) Authenticity – ensuring that the data, transactions, communications, or documents (electronic or physical) are genuine.

21. The Information Security policy shall cover the following:

(1) **Identification and Classification of information assets**: The NBFC shall maintain detailed inventory of information assets with distinct and clear identification of the assets.

(2) **Segregation of Functions**: The NBFC shall ensure segregation of duties between the IT division / function and Information System security division / function. The Information Security function shall be adequately resourced in terms of the number of staff, level of skill, and tools or techniques such as risk assessment, security architecture, vulnerability assessment, and forensic assessment (the term 'forensics' refers to 'digital forensics' for the purpose of these Directions). The NBFC shall also establish clear segregation of responsibilities relating to system administration, database administration, and transaction processing.

(3) **Role-based Access Control**: Access to information shall be based on well-defined user roles such as system administrator, user manager, and application owner. The NBFC shall avoid dependence on one or few persons for a particular job. There shall be clear delegation of authority for right to upgrade / change user profiles and permissions, and changes to key business parameters (e.g., interest rates), and the same shall also be documented.

(4) **Personnel Security**: The NBFC shall subject its personnel with privileged access to the critical information systems, to rigorous background check and screening.

(5) **Physical Security**: The NBFC shall create a secured environment for physical security of information assets such as secure storage of critical data, restricted access to sensitive areas like Data Centre (DC).

(6) **Maker-Checker:** The NBFC shall implement a maker-checker control for authorisation in its information systems, ensuring that transactions are completed only after independent verification and approval by at least two individuals, thereby enhancing accuracy and reliability of information.

(7) **Incident Management**: The NBFC shall define what constitutes an information security incident and implement processes for preventing, detecting, analysing, and responding to such incidents.

(8) **Audit Trails**: The NBFC shall ensure that audit trails exist for IT assets satisfying its business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required, and assisting in dispute resolution. The NBFC shall ensure to record any unauthorised user activity in the audit trail.

(9) **Public Key Infrastructure (PKI)**: The NBFC shall increase the usage of PKI to ensure confidentiality of data, access control, data integrity, authentication, and non-repudiation.

C.2 Cybersecurity Policy

22. The NBFC shall put in place a Board-approved 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. The NBFC shall 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.

C.3 Vulnerability Management

23. The NBFC shall establish a vulnerability management process to identify, manage, and eliminate the vulnerabilities in the information systems. The vulnerability management aspects shall be covered in the cybersecurity policy.

C.4 Cybersecurity Preparedness Indicators

24. The NBFC shall assess and measure the adequacy of and adherence to cyber resilience framework through development of indicators to assess the level of risk / preparedness. These indicators shall be used for comprehensive testing through independent compliance checks and audits carried out by qualified and competent professionals. The awareness among the stakeholders including employees shall also form a part of this assessment.

C.5 Cyber Crisis Management Plan

25. The NBFC shall put in place a CCMP which shall be a part of the overall Board approved strategy. CCMP shall address the four aspects of crisis resilience lifecycle viz., Detection, Response, Recovery, and Containment.

26. The NBFC shall take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond / recover / contain the fallout. The NBFC shall be well prepared to face emerging cyber-threats such as 'zero-day' attacks, remote access threats, and targeted attacks.

27. The NBFC shall, inter alia, take necessary preventive and corrective measures in addressing various types of cyber threats including, but not limited to, denial of service, distributed denial of services (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.

C.6 Reporting of Cyber Incidents to RBI

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

C.7 Cybersecurity Awareness

29. The NBFC shall ensure that the Board and the Senior Management have a fair degree of awareness of the fine nuances of cyber threats and shall organise appropriate familiarisation programmes.

30. The NBFC shall proactively promote, among its customers, vendors, service providers, and other relevant stakeholders, an understanding of its cyber resilience objectives.

C.8 Digital Signatures

31. The NBFC shall use Digital Signature Certificates (DSCs), to authenticate its identity electronically, and to ensure confidentiality, integrity, authenticity, and non-repudiation of information in online transactions and important electronic documents.

C.9 IT Risk Assessment

32. The NBFC shall undertake a comprehensive risk assessment of its IT systems at least on an annual basis. The assessment shall make an analysis on the threats and vulnerabilities to the IT assets of the NBFC and its existing security controls and processes. The outcome of the exercise shall be to find out the risks present and to determine the appropriate level of controls necessary for appropriate mitigation of risks. The risk assessment shall be brought to the notice of the CRO, CIO, and the Board of the NBFC, and shall serve as an input for Information Security auditors.

C.10 Mobile Financial Services

33. The NBFC, if using or intending to use mobile financial services, shall develop a mechanism for safeguarding information assets that are used by mobile applications to provide services to customers. The technology used for mobile services shall ensure confidentiality, integrity, authenticity, and end-to-end encryption.

C.11 Social Media Risks

34. The NBFC leveraging social media platforms for product marketing shall be well equipped to handle social media risks and threats including unauthorised account takeovers and impersonation fraud.

C.12 Training

35. The NBFC shall establish and implement a robust, ongoing information security training and awareness program for all users. This program shall be periodically

reviewed and updated to remain aligned with evolving IT landscapes, emerging cyber threats, and the NBFC's information security framework.

36. The NBFC shall deploy a formal mechanism to measure and track the effectiveness of such training through periodic assessments or testing. The NBFC shall also maintain an up-to-date repository of the training and awareness status of all users.

D. IT Operations

37. The NBFC shall process and store information in a manner that ensures availability of required information in a timely, reliable, secure, and resilient manner.

38. The NBFC shall identify and assess risks associated with existing and planned IT operations, align such risks with its risk tolerance, and establish, implement, and monitor appropriate risk management policies.

D.1 Acquisition and Development of Information Systems (New Application Software) and Change Management

39. The NBFC shall mitigate risks arising from inadequate system design and execution while implementing IT projects. The NBFC shall identify, document, and remediate system deficiencies and defects during the initial design, development, and testing phases.

40. The NBFC shall establish a steering committee, consisting of business owners, the development team, and other stakeholders, to provide oversight and monitoring of the progress of the project, including deliverables to be realised at each phase of the project, and milestones to be reached according to the project timetable.

41. The NBFC shall realign its IT systems on a regular basis in line with the changing needs of its customers and business. The changes need to be done in such a way that adverse incidents and disruption to services are minimised while maximizing value for the customers. For this purpose, the NBFC shall have a board approved change management policy that encompasses the following:

(1) prioritizing and responding to change proposals from business;

(2) cost benefit analysis of the changes proposed;

(3) assessing risks associated with the changes proposed; and

(4) change implementation, monitoring, and reporting.

(*Note*: The term 'incident' implies cyber incident in these Directions, unless specified otherwise)

42. The Senior Management shall be responsible to ensure that the Change Management policy is being followed on an ongoing basis.

D.2 IT Enabled Management Information System (MIS)

43. The IT function of the NBFC shall support a robust and comprehensive MIS in respect of various business functions as per the needs of the business and for supporting strategic decision-making.

44. The NBFC shall put in place an MIS that assists the Senior Management as well as the business heads in decision making and to maintain an oversight over operations of various business verticals. With robust IT systems in place, the NBFC shall have the following (as per applicability) as part of an effective system-generated MIS (indicative list):

(1) A dashboard for the Senior Management summarising financial position vis-à-vis targets. It shall include information such as trends of return on assets across categories, major growth business segments, and movement of net worth.

(2) A system enabled identification and classification of Special Mention Accounts and Non-Performing Assets (NPAs) as well as generation of MIS reports in this regard.

(3) The MIS shall facilitate pricing of products, especially large ticket loans.

(4) The MIS shall capture regulatory requirements and their compliance.

(5) Financial Reports including operating and non-operating revenues and expenses, cost benefit analysis of segments / verticals, and cost of funds, (also regulatory compliance at transaction level).

(6) Reports relating to treasury operations.

(7) Fraud analysis - Suspicious transaction analysis, embezzlement, theft or suspected money-laundering, misappropriation of assets, and manipulation of financial records. The regulatory requirement of reporting fraud to RBI shall be system driven.

(8) Capacity and performance analysis of IT security systems.

(9) Incident reporting, their impact and steps taken for non-recurrence of such events in the future.

45. The NBFC shall design and maintain its MIS keeping in view the prevailing supervisory reporting structure to facilitate generation of required information / returns for the supervisor.

46. The NBFC shall ensure that all regulatory and supervisory returns are system-driven with seamless integration between the MIS and the supervisory reporting system. The NBFC shall provide ‘read-only’ access to RBI supervisors, to the MIS.

E. Information Systems Audit

47. IS Audit shall identify risks and methods to mitigate risk arising out of IT infrastructure such as server architecture, local and wide area networks, physical and information security, and telecommunications.

48. IS Audit shall form an integral part of Internal Audit system of an NBFC. While designing the IS Audit framework, an NBFC shall refer to guidance issued by Professional bodies such as Information Systems Audit and Control Association (ISACA), Institute of Internal Auditors (IIA), and the Institute of Chartered Accountants (ICAI).

49. The NBFC shall adopt an IS Audit framework duly approved by its Audit Committee of the Board (ACB).

50. The NBFC shall have adequately skilled personnel in ACB who can understand the results of the IS Audit.

51. The IS Audit findings shall be put up to the Board or ACB as per the NBFC's IS Audit framework.

E.1 Coverage

52. IS Audit shall cover effectiveness of policy and oversight of IT systems, evaluate adequacy of processes and internal controls, and recommend corrective action to address deficiencies and follow-up.

53. IS Audit shall evaluate the effectiveness of BCP and Disaster Recovery (DR) set up and ensure that BCP is effectively implemented in the organisation.

54. During the process of IS Audit, due importance shall be given to compliance of all the applicable legal and statutory requirements.

E.2 Personnel

55. IS Audit shall be conducted by an internal team of the NBFC. In case of inadequate internal skills, the NBFC may appoint an outside agency having enough expertise in the area of IT / IS audit for the purpose. There shall be a right mix of skills and understanding of legal and regulatory requirements so as to assess the efficacy of the framework vis-à-vis these standards. IS Auditors shall act independently of NBFCs' Management both in attitude and appearance. In case of engagement of external professional service providers, independence, and accountability issues shall be properly addressed.

E.3 Periodicity

56. The periodicity of IS audit shall ideally be based on the size and operations of the NBFC but may be conducted at least once in a year. IS Audit shall be undertaken preferably 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.

E.4 Compliance

57. The NBFC's management shall be responsible for deciding the appropriate action to be taken in response to reported observations and recommendations during IS Audit. Responsibilities for compliance / sustenance of compliance, reporting lines, timelines for submission of compliance, authority for accepting compliance shall be clearly delineated in the framework. The framework shall provide for an audit-mode access for auditors / inspecting / regulatory authorities.

E.5 Computer-Assisted Audit Techniques (CAATs)

58. The NBFC shall adopt a proper mix of manual techniques and CAATs for conducting IS Audit. CAATs may be used in critical areas (such as detection of revenue leakage, treasury functions, assessing impact of control weaknesses, monitoring customer transactions under AML requirements and generally in areas where a large volume of transactions are reported) particularly for critical functions or processes having financial / regulatory / legal implications.

F. Business Continuity Planning and Disaster Recovery

59. BCP shall be designed to minimise the operational, financial, legal, reputational, and other material consequences arising from a disaster. The NBFC shall have a Board approved BCP policy. The functioning of BCP shall be monitored by the Board by way of periodic reports. The CIO shall be responsible for formulation, review, and monitoring of BCP to ensure continued effectiveness. The BCP shall have the following salient features:

(1) **Business Impact Analysis**- The NBFC shall first identify critical business verticals, locations, and shared resources to come up with the detailed Business Impact Analysis. The process shall envisage the impact of any unforeseen natural or man-made disasters on the NBFC's business. The NBFC shall clearly list the business impact areas in order of priority.

(2) **Recovery strategy / Contingency plan** - The NBFC shall fully understand the vulnerabilities associated with inter-relationships between various systems, departments, and business processes. The NBFC shall assess the probability of various failure scenarios under its BCP, evaluate available recovery options, and select the most cost-effective and practical strategy to minimise losses in the event of a disaster.

(3) The NBFC shall consider the need to put in place necessary backup sites for its critical business systems and data centres.

(4) The NBFC shall test its BCP at least annually and whenever significant IT or business changes occur, to determine whether the entity can be restored to an acceptable level of operations within the timeframe specified in the contingency plan. The NBFC shall conduct the tests using worst-case scenarios and shall place the test results and gap analysis before the CIO and the Board. The NBFC shall use the gap analysis and the Board's observations as the basis for updating the BCP.

(5) The NBFC shall ensure to put in place an appropriate mechanism to support testing of cyber resilience objectives among its vendors, service providers, and other relevant stakeholders.

G. IT Services Outsourcing

G.1 Policy for IT Services Outsourcing

60. Prior to the commencement of any outsourcing arrangement, the NBFC shall undertake a comprehensive assessment of associated risks, threats associated with contractual arrangements, and applicable regulatory compliance obligations to ensure effective risk mitigation and adherence to regulatory requirements.

61. The NBFC shall ensure that the outsourcing of IT Services is aligned with its strategic plan and corporate objectives.

62. The terms and conditions governing the contract between the NBFC and the outsourcing service provider shall be carefully defined in written agreements and

vetted by its legal counsel on their legal effect and enforceability. The contractual agreement shall have the following provisions.

(1) **Monitoring and Oversight**: This shall include:

(i) provisions for continuous monitoring and assessment of the service provider by the NBFC so that any necessary corrective measure can be taken immediately; and

(ii) provisions to ensure that the outsourcing service provider has adequate systems and procedures in place to ensure protection of data / application outsourced.

(2) **Access to Books and Records / Audit and Inspection**: This shall include provisions to:

(i) ensure that the NBFC can access all books, records, and information relevant to the outsourced activity available with the service provider. For technology outsourcing, requisite audit trails and logs for administrative activities shall be retained by the service provider and the same shall be accessible to the NBFC based on approved requests;

(ii) grant the NBFC the right to conduct audits of the service provider either by its internal or external auditors, or by external specialists appointed to act on its behalf as well as the right to obtain copies of any audit or review reports and findings related to the services provided by the service provider to the NBFC; and

(iii) allow RBI / persons authorised by it to access the NBFC's documents, records of transactions, and other necessary information given to / stored / processed by the service provider within a reasonable time. This shall include information maintained in paper and electronic formats.

63. The Board shall be ultimately responsible for outsourcing operations and for managing risks inherent in such outsourcing relationships. The Board or ITSC

shall be responsible for instituting an effective governance mechanism and risk management process for all IT outsourced operations. The Senior Management shall be responsible for effective due diligence, oversight and management of outsourcing, and shall remain accountable for all outsourcing related decisions.

64. The NBFC shall ensure that its business continuity preparedness is not adversely compromised on account of outsourcing. The NBFC shall adopt sound business continuity management practices as issued by RBI and seek proactive assurance that the outsourced service provider maintains readiness and preparedness for business continuity on an ongoing basis.

Chapter V - Requirements for NBFCs (Middle Layer and above excluding CICs)

A. IT Governance

A.1 IT Governance Framework

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

(*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, IS, information security / cybersecurity controls and operations.)

66. The NBFC shall put in place a robust IT Governance Framework based on the focus areas outlined in paragraph 65 above, that inter alia:

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

(2) specifies the roles (including authority) and responsibilities of the 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.

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

A.2 Role of the Board of Directors

68. The Board shall approve the strategies and policies related to IT, information assets, business continuity, information security, cybersecurity (including incident response and recovery management / cyber crisis management).

69. Such strategies and policies shall be placed before the Board for review at least annually.

A.3 IT Strategy Committee (ITSC) of the Board

70. The NBFC shall establish a Board-level IT Strategy Committee (ITSC).

71. While constituting the ITSC, the NBFC 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 will mean the ability to understand and evaluate information systems and associated IT / cyber risks.

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

73. The ITSC shall:

(1) ensure that the NBFC 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 NBFC 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 NBFC 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 NBFC's IT maturity, digital depth, threat environment, and industry standards and are utilised in a manner intended for meeting the stated objectives;

(6) review, at least on an annual basis, the adequacy and effectiveness of the business continuity planning and DR management of the NBFC;

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

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

A.4 Senior Management and IT Steering Committee

74. The Senior Management of the NBFC 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 NBFC;

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

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

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

76. 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.

A.5 Information Security Committee (ISC)

77. 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 the 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 NBFC'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.

A.6 Head of IT Function

78. The NBFC 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 NBFC uses, such as Chief Technology Officer, Chief Information Officer).

79. 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 NBFC's IT policy and IT strategy;

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

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

80. As a 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 NBFC's information assets; and

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

A.7 Chief Information Security Officer

81. 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 NBFC 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 security / cybersecurity is determined keeping in view the current / emerging threat landscape.

82. The NBFC 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 an NBFC uses to protect its information assets apart from coordinating information security / cybersecurity related issues within the NBFC 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 NBFC before the Board / Risk Management Committee of the Board (RMCB) / ITSC at least on a quarterly basis.

A.8 Information Security Policy and Cybersecurity Policy

83. The NBFC 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.

84. The NBFC shall put in place a Cybersecurity Policy and Cyber Crisis Management Plan (CCMP).

A.9 Information Technology (IT) Project Management

85. The NBFC 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.

86. The NBFC shall follow a standard enterprise architecture planning methodology while adopting new or emerging technologies, tools, or while revamping the existing ones in the technology stack.

87. The NBFC 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 NBFC shall also ensure that such adoption facilitates the optimal creation / use / sharing of information in a secure and resilient way.

88. The NBFC 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.)

A.10 IT Services Management

89. The NBFC 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).

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

91. The NBFC 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 NBFC’s operations.

92. For seamless continuity of business operations, an NBFC 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.

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

B. IT and Information Security Risk Management

B.1 Periodic review of IT related risks

94. The risk management policy of the NBFC 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.2 IT and Information Security Risk Management Framework

95. The NBFC shall establish a robust IT and Information Security Risk Management Framework (the NBFC 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.

B.3 Risk Assessment

96. The risk assessment for each information asset within the NBFC's scope shall be guided by appropriate security standards / IT control frameworks.

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

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

C. Baseline Cybersecurity and Resilience Requirements

C.1 Data Migration Controls

99. The NBFC 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.

C.2 Data Dictionary

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

C.3 Physical and Environmental Controls

101. The NBFC shall put in place appropriate physical and environmental controls for securing location of critical assets including DC and 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)

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

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

C.4 Application Security

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

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

106. The NBFC 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 NBFC 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 NBFC 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.

C.5 Capacity Management

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

108. The NBFC shall proactively assess capacity requirement of IT resources on an annual or more frequent basis. The NBFC 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 NBFC.

C.6 Audit Trails

109. The NBFC 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.

110. The NBFC shall ensure that audit trails satisfy its business requirements, in addition to regulatory and legal requirements. The NBFC shall also ensure that audit trails are sufficiently detailed to facilitate the conduct of audits, serve as forensic evidence when required, and assist in dispute resolution, including for non-repudiation purposes.

111. The NBFC 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.

C.7 Change and Patch Management

112. The NBFC 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.

C.8 Access Controls

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

114. The NBFC shall closely supervise personnel with elevated system access entitlements with all their system activities logged and periodically reviewed.

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

C.9 Controls on Teleworking

116. In the teleworking environment, the NBFC shall, inter alia:

(1) ensure that the systems used and the remote access from alternate work location to the environment hosting NBFC'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 NBFC's systems; and

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

C.10 Third-Party Arrangements

(Paragraph 117 is applicable for such third-party arrangements in the information technology / cybersecurity ecosystem, which are not within the applicability of Reserve Bank of India (Non-Banking Financial Companies – Managing Risks in Outsourcing) Directions, 2025)

117. The NBFC 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.

C.11 Cryptographic Controls

118. The key length, algorithms, cipher suites, and applicable protocols used in transmission channels, processing of data, and authentication purposes shall be strong. The NBFC 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.

C.12 Straight Through Processing

119. In order to prevent unauthorised modification of data, the NBFC 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.

120. Data transfer mechanism between processes or applications must 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.

C.13 Vulnerability Assessment (VA) and Penetration (PT) Test

121. The NBFC shall conduct vulnerability assessment (VA) at least once in every six months and penetration testing (PT) at least once in 12 months for critical information systems and / or those in the De-Militarised Zone (DMZ) having customer interface. The NBFC shall also conduct VA / PT of such information systems throughout their lifecycle including pre-implementation, post implementation, and after changes.

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

123. For non-critical information systems, a risk-based approach shall be adopted to decide the requirement and periodicity of conduct of VA / PT.

124. 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 NBFC shall ensure that the version and configuration of the test environment resembles the production environment. Any deviation shall be documented and approved by the ISC.

125. The NBFC 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.

126. The NBFC 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 NBFC's information systems hosted in a cloud environment.

C.14 Business Continuity and Disaster Recovery

127. 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.

128. The NBFC'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 the security of processes and data.

129. 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 NBFC's risk assessment.

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

131. 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.

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

133. The NBFC 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.

134. The NBFC 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.

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

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

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

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

C.15 Cyber Incident Response and Recovery Management

C.15.1 Responding to Cyber-Incidents

139. The NBFC shall put in place cyber incident response and recovery management policy which shall address the following:

    (1) classification and assessment of incidents;

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

    (3) measures to contain exposures and achieve timely recovery.

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

141. The NBFC shall report cyber incidents to RBI within six hours of detection on DAKSH platform (Reserve Bank's Advanced Supervisory Monitoring System -

https://daksh.rbi.org.in). The NBFC shall also pro-actively notify Indian Computer Emergency Response Team (CERT-In) regarding cyber incidents.

(*Note*: In respect of Housing Finance Companies, cyber incidents shall continue to be reported to NHB and not RBI)

142. The NBFC shall have written incident response and recovery procedures including identification of key roles of staff / outsourced staff handling such incidents.

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

144. The NBFC 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 IDRBT.

C.15.2 Recovery from Cyber Incidents

145. The NBFC 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.

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

C.16 Metrics

147. The NBFC 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 NBFC shall adopt a risk-based approach to define suitable metrics.

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

D. Information Systems Audit

149. The ACB shall be responsible for exercising oversight of IS Audit of an NBFC.

150. The NBFC 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.

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

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

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

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

Chapter VI Repeal and Other Provisions

A. Repeal and Saving

155. With the issue of these Directions, the existing directions, instructions, and guidelines relating to Information Technology Framework and IT Governance as applicable to Non-Banking Financial Companies 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.

156. 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

157. 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

158. 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