आज़ादी का अमृत महोत्सव

Azadi Ka Amrit Mahotsav

भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA

RBI/2023-24/107
DoS.CO.CSITEG/SEC.7/31.01.015/2023-24 November 7, 2023

The Chairman/Managing Director/Chief Executive Officer
Scheduled Commercial Banks (excluding Regional Rural Banks);
Small Finance Banks; Payments Banks;
Non-Banking Financial Companies;
Credit Information Companies; and
All India Financial Institutions (EXIM Bank, NABARD, NaBFID, NHB and SIDBI)

Madam/Dear Sir,

Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices

Please refer to paragraph IV (8) of the Statement on Developmental and Regulatory Policies released with the Bi-monthly Monetary Policy Statement 2021-22 on February 10, 2022, wherein it was announced that draft guidelines, updating and consolidating the instructions relating to Information Technology (IT) Governance and Controls, Business Continuity Management and Information Systems Audit, will be issued by the Reserve Bank of India.

2. Accordingly, a draft Master Direction on the subject was published in October 2022 seeking public comments. Based on feedback received, the final Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023 are enclosed herewith.

Yours faithfully,

(T.K.Rajan)
Chief General Manager
Encl: Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023

Contents

भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA

RBI/2023-24/xx
DoS.CO.CSITEG/SEC.7/31.01.015/2023-24 November 7, 2023

Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023

In exercise of the powers conferred by Section 35A of the Banking Regulation Act, 1949; Section 45L of the Reserve Bank of India Act, 1934 and Section 11 of the Credit Information Companies (Regulation) Act, 2005, and all other provisions/ laws enabling the Reserve Bank of India in this regard, the Reserve Bank being satisfied that it is necessary and expedient in the public interest to do so, hereby issues the Directions hereinafter specified.

Chapter I - Preliminary

1. Short Title and Commencement

(a) These Directions shall be called the Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023.

(b) These Directions incorporate, consolidate and update the guidelines, instructions and circulars on IT Governance, Risk, Controls, Assurance Practices and Business Continuity/ Disaster Recovery Management. The list of circulars repealed is given in Chapter VII of this Master Direction.

(c) These Directions shall come into effect from April 1, 2024.

2. Applicability

(a) These Directions shall be applicable to the following entities (collectively referred to as 'regulated entities' or 'REs' in these directions):

(i) all Banking Companies[1], Corresponding New Banks and State Bank of India as defined under subsections (c), (da) and (nc) of section 5 of the

[1] Includes banks incorporated outside India licensed to operate in India ('Foreign Banks'), Small Finance Banks (SFBs), Payments Banks (PBs)

Banking Regulation Act, 1949 (collectively referred to as 'commercial banks' hereinafter).

(ii) Non-Banking Financial Companies (hereinafter referred to as 'NBFCs') as defined under clause (f) of section 45I of the Reserve Bank of India Act, 1934 and included in the 'Top Layer', 'Upper Layer' and 'Middle Layer' defined in paragraphs 1.5, 1.4 and 1.3 respectively of the Annex to RBI circular DOR.CRE.REC.No.60/03.10.001/2021-22 dated October 22, 2021 on 'Scale Based Regulation (SBR): A Revised Regulatory Framework for NBFCs'.

(iii) Credit Information Companies as defined under clause (e) of section 2 of the Credit Information Companies (Regulation) Act, 2005 (hereinafter referred to as 'Credit Information Companies' or 'CICs').

(iv) EXIM Bank, National Bank for Agriculture and Rural Development ('NABARD'), National Bank for Financing Infrastructure and Development ('NaBFID'), National Housing Bank ('NHB') and Small Industries Development Bank of India ('SIDBI') as established by the Export-Import Bank of India Act, 1981; the National Bank for Agriculture and Rural Development Act, 1981; the National Bank For Financing Infrastructure and Development Act, 2021; National Housing Bank Act, 1987 and the Small Industries Development Bank of India Act, 1989 respectively (hereinafter referred to as 'All India Financial Institutions' or 'AIFIs').

(b) These Directions shall not be applicable to:

(i) Local Area Banks

(ii) NBFC-Core Investment Companies

(c) In the case of foreign banks operating in India through branch mode, reference to the board or board of directors in these Directions should be read as reference to the controlling office/ head office which has the oversight over the branch operations in India. Further, such foreign banks shall be subject to a 'comply or explain' approach in terms of the applicability of these Directions. The 'comply or explain' approach shall allow such foreign banks to deviate

from any specific part of these Directions subject to examination and acceptance by Reserve Bank of a reasonably justifiable explanation for the same, as part of the supervisory process.

3. Definitions[2]

(a) In these Directions, unless the context states otherwise, the terms herein shall bear the meanings assigned to them below:

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

(ii) 'Cyber event' – Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring.

(iii) 'Cyber security' - 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.

(iv) 'Cyber incident[3]' shall mean a cyber event that adversely affects the cyber security of an information asset whether resulting from malicious activity or not.

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

(vi) 'De-militarized Zone[4]' or 'DMZ' is a perimeter network segment that is logically between internal and external networks.

(vii) 'Information Asset[5]' - 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.

---

[2] Source – FSB Cyber Lexicon (updated in April 2023) unless explicitly mentioned otherwise.

[3] Cyber incident definition is adapted from FSB Cyber Lexicon (updated in April 2023). By the definition, it includes cyber security as well as IT incident.

[4] Source- NIST SP 800-82 Rev. 2

[5] Information Asset definition is adapted from "Guidance on cyber resilience for financial market infrastructures" June 2016 publication of Bank for International Settlements and International Organization of Securities Commissions

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

(ix) 'IT Risk[6]' - The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.

(x) 'Privileged user[7]' refers to 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.

(b) All expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949 or the Reserve Bank of India Act, 1934 or Credit Information Companies (Regulation) Act, 2005 or Information Technology Act, 2000 or Companies Act, 2013 and Rules made thereunder or any statutory modification or re-enactment thereto or as used in RBI Directions / Circulars, as the case may be.

Chapter II - IT Governance

4. IT Governance Framework

(a) The key focus areas of IT Governance shall include strategic alignment, risk management, resource management, performance management and Business Continuity/ Disaster Recovery Management.

(b) REs shall put in place a robust IT Governance Framework based on the aforementioned focus areas that *inter alia*:

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

[6]Source- ISACA glossary

[7]Source - adapted from ISO/IEC 24775-2:2021

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

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

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

5. Role of the Board of Directors

(a) The strategies and policies related to IT, Information Assets, Business Continuity, Information Security, Cyber Security (including Incident Response and Recovery Management/ Cyber Crisis Management) shall be approved by the Board of Directors.

(b) Such strategies and policies shall be reviewed at least annually by the Board.

6. IT Strategy Committee of the Board

(a) REs shall establish a Board-level IT Strategy Committee (ITSC)[8].

(b) While constituting the ITSC, REs shall ensure:

(i) Minimum of three directors as members;

(ii) The Chairperson of the ITSC shall be an independent director and have substantial IT expertise[9] in managing/ guiding information technology initiatives; and

(iii) Members are technically competent[10].

(c) The ITSC shall meet at least on a quarterly basis.

(d) The ITSC shall:

[8] Foreign banks operating in India through branch mode need not constitute any Committees (Board or Executive level) referred in this Master Direction at the branch level. They may leverage upon controlling office/ head office/ regional/ zonal Committees for compliance with this Master Direction as long as governance obligations / responsibilities outlined for the prescribed committees are met.

[9] "Substantial IT expertise" means the person has a minimum of seven years of experience in managing information systems and/or leading/ guiding technology/ cybersecurity initiatives/ projects. Such a member should also understand the business processes at a broader level and the impact of IT on such processes.

[10] Technically competent herein will mean the ability to understand and evaluate information systems and associated IT/ cyber risks.

(i) Ensure that the RE has put an effective IT strategic planning process in place;

(ii) Guide in preparation of IT Strategy and ensure that the IT Strategy aligns with the overall strategy of the RE towards accomplishment of its business objectives;

(iii) 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;

(iv) Ensure that the RE has put in place processes for assessing and managing IT and cybersecurity risks;

(v) Ensure that the budgetary allocations for the IT function (including for IT security), cyber security are commensurate with the RE's IT maturity, digital depth, threat environment and industry standards and are utilised in a manner intended for meeting the stated objectives; and

(vi) Review, at least on annual basis, the adequacy and effectiveness of the Business Continuity Planning and Disaster Recovery Management[11] of the RE.

7. Senior Management and IT Steering Committee

(a) The Senior Management of the RE shall, *inter alia,* ensure:

(i) Execution of the IT Strategy approved by the Board;

(ii) IT/ IS and their support infrastructure are functioning effectively and efficiently;

(iii) Necessary IT risk management processes are in place and create a culture of IT risk awareness and cyber hygiene practices in the RE;

(iv) Cyber security posture of the RE is robust; and

(v) Overall, IT contributes to productivity, effectiveness and efficiency in business operations.

[11] The reference to Business Continuity/ Disaster Recovery Management in this Master Direction is limited to operational resilience focussing on People, Processes and Systems associated with the IT, IS, information/ cyber security controls and operations.

(b) REs shall establish an IT Steering Committee with representation at Senior Management level from IT and business functions.

(c) The responsibilities of IT Steering Committee, *inter alia,* shall be to:

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

(ii) Oversee the processes put in place for business continuity and disaster recovery;

(iii) Ensure implementation of a robust IT architecture meeting statutory and regulatory compliance; and

(iv) Update ITSC and CEO periodically on the activities of IT Steering Committee.

(d) The IT Steering Committee shall meet at least on a quarterly basis.

8. Head of IT Function

(a) REs shall appoint a sufficiently senior level, technically competent and experienced official in IT related aspects as Head of IT Function[12].

(b) The Head of IT Function shall, *inter alia*, be responsible for the following:

(i) Ensuring that the execution of IT projects/ initiatives is aligned with the RE's IT Policy and IT Strategy;

(ii) Ensuring that there is an effective organisational structure to support IT functions in the RE; and

(iii) Putting in place an effective disaster recovery setup and business continuity strategy/ plan.

(c) 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 (i) secure the RE's information assets (ii) comply with extant internal policies, regulatory and legal requirements on IT related aspects.

[12] By whatever name called viz. Chief Technology Officer or Chief Information Officer, etc.

Chapter III - IT Infrastructure & Services Management

9. IT Services Management

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

(b) A Service Level Management (SLM) process shall be put in place to manage the IT operations while ensuring effective segregation of duties.

(c) REs 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 REs' operations.

(d) For seamless continuity of business operations, REs shall avoid using outdated and unsupported hardware or software and shall monitor software's end-of-support (EOS) date and Annual Maintenance Contract (AMC) dates of IT hardware on an ongoing basis.

(e) REs shall develop a technology refresh plan for the replacement of hardware and software in a timely manner before they reach EOS.

10. Third-Party Arrangements

Where third-party arrangements in the Information Technology/ Cyber Security ecosystem are not within the applicability of the Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023, REs shall, put in place appropriate vendor risk assessment process and controls proportionate to the assessed risk and materiality to, *inter alia*:

(a) mitigate concentration risk;

(b) eliminate or address any conflict of interests;

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

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

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

(f) manage supply chain risks effectively.

11. Capacity Management

(a) REs shall ensure that information systems and infrastructure are able to support business functions and ensure availability of all service delivery channels.

(b) On an annual or more frequent basis, REs shall proactively assess capacity requirement of IT resources. REs 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 RE.

(c) The assessment of IT capacity requirements and measures taken to address the issues shall be reviewed by the ITSC.

12. Project Management

(a) REs shall follow a consistent and formally defined project management approach for IT projects undertaken by them. The project management approach shall, *inter alia*, enable appropriate stakeholder participation for effective monitoring and management of project risks and progress.

(b) While adopting new or emerging technologies, tools, or revamping their existing ones in the technology stack, REs shall follow a standard enterprise architecture planning methodology or framework.

(c) Adoption of new or emerging technologies shall be commensurate with the risk appetite and align with overall Business/ IT strategy of the RE. It should facilitate optimal creation, use, or sharing of information by a business in a secure and resilient way.

(d) REs shall maintain enterprise data dictionary to enable the sharing of data among applications and information systems and promote a common understanding of data.

(e) REs shall ensure that maintenance and necessary support of software applications is provided by the software vendors and the same is enforced through formal agreement.

(f) REs shall obtain the source codes for all critical applications from their vendors. Where obtaining of the source code is not possible, REs shall put in place a

source code escrow arrangement or other arrangements to adequately mitigate the risk of default by the vendor. REs shall ensure that all product updates and programme fixes are included in the source code escrow arrangement.

(g) REs 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. Such a certificate or a written confirmation shall also be obtained whenever material changes to the code, including upgrades, occur.

(h) Any new IT application proposed to be introduced as a business product[13] shall be subjected to product approval and quality assurance process.

13. Change and Patch Management

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

(a) the business impact of implementing patches/ changes (or not implementing a particular patch/ change request) are assessed;

(b) the patches/ changes are applied/ implemented and reviewed in a secure and timely manner with necessary approvals;

(c) 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; and

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

14. Data Migration Controls

REs shall have a documented data migration policy specifying a systematic process for data migration, ensuring data integrity, completeness and consistency. The policy shall, *inter alia*, contain provisions pertaining to signoffs from business users and application owners at each stage of migration, maintenance of audit trails, etc.

[13] IT Applications that enable functioning of a business process whether offered as a product to the customers (including potential customers), third parties (or) internal employees could be broadly referred as business product.

15. Audit Trails

(a) Every IT application which can access or affect critical or sensitive information, shall have necessary audit and system logging capability and should provide audit trails.

(b) The audit trails shall satisfy a RE's business requirements apart from regulatory and legal requirements. The audit trails must be detailed enough to facilitate the conduct of audit, serve as forensic evidence when required and assist in dispute resolution, including for non-repudiation purposes.

(c) REs shall put in place a system for regularly monitoring the audit trails and system logs to detect any unauthorised activity.

16. Cryptographic controls

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

17. Straight Through Processing

(a) In order to prevent unauthorised modification of data, REs 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.

(b) 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.

18. Physical and Environmental Controls

(a) REs shall implement suitable physical and environmental controls in Data Centre and Disaster Recovery[14] sites used by them.

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

(c) REs shall ensure that their DC and DR sites are subjected to necessary e-surveillance mechanism.

19. Access Controls

(a) Access to information assets shall be allowed only where a valid business need exists. REs shall have documented standards and procedures, which are approved by the ITSC and kept up to date for administering need-based access to an information system.

(b) Personnel with elevated system access entitlements shall be closely supervised with all their systems activities logged and periodically reviewed.

(c) REs shall adopt multi-factor authentication for privileged users of i) critical information systems and ii) for critical activities, basis the RE's risk assessment.

20. Controls on Teleworking

In the teleworking environment, REs, *inter alia*, shall:

(a) Ensure that the systems used and the remote access from alternate work location to the environment hosting RE's information assets are secure;

(b) Implement multi-factor authentication for enterprise access (logical) to critical systems;

(c) Put in place a mechanism to identify all remote-access devices attached/ connected to the RE's systems; and

(d) Ensure that data/ information shared/ presented in teleworking is secured appropriately.

[14] DC refers to primary data centre for a given application/ system and DR its Disaster Recovery site/ alternate site.

21. Metrics

(a) REs shall define suitable metrics for system performance, recovery and business resumption, including Recovery Point Objective (RPO) and Recovery Time Objective (RTO), for all critical information systems.

(b) For non-critical information systems, REs shall adopt a risk-based approach to define suitable metrics.

(c) REs shall implement suitable scorecard/ metrics/ methodology to measure IT performance and IT maturity level.

Chapter IV - IT and Information Security Risk Management

22. Periodic review of IT related risks

The risk management policy of the RE shall include IT related risks, including the Cyber Security related risks, and the Risk Management Committee of the Board (RMCB) in consultation with the ITSC shall periodically review and update the same at least on a yearly basis.

23. IT and Information Security Risk Management Framework

REs shall establish a robust IT and Information Security Risk Management Framework[15] covering, *inter alia,* the following aspects:

(a) 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;

(b) Definition of 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;

(c) Identification of critical information systems of the organisation and fortification of the security environment of such systems; and

[15] REs may have flexibility to define Information / Cyber security risk management framework distinct from IT risk management framework.

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

24. Information Security Policy and Cyber Security Policy

(a) The Information Security Policy shall take 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. REs shall also put in place a Cyber Security Policy and Cyber Crisis Management Plan (CCMP).

(b) 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 and IT functions, etc., 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:

(i) Development of information/ cyber security policies, implementation of policies, standards and procedures to ensure that all identified risks are managed within the RE's risk appetite;

(ii) Approving and monitoring information security projects and security awareness initiatives;

(iii) Reviewing cyber incidents, information systems audit observations, monitoring and mitigation activities; and

(iv) Updating ITSC and CEO periodically on the activities of ISC.

(c) A senior level executive (preferably in the rank of a General Manager or an equivalent position) shall be designated as the Chief Information Security Officer (CISO). The CISO shall not have any direct reporting relationship with the Head of IT Function and shall not be given any business targets. REs shall ensure the following:

(i) The CISO has the requisite technical background and expertise;

(ii) She/He is appointed for a reasonable minimum term;

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

(iv) The budget for the information/ cyber security is determined keeping in view the current/ emerging threat landscape.

(d) REs shall ensure that the roles and responsibilities of the CISO are clearly defined and documented covering, at a minimum, the following points:

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

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

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

(iv) The CISO's Office shall manage and monitor Security Operations Centre (SOC) and drive cyber security related projects.

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

(vi) The CISO shall directly report to the Executive Director or equivalent executive overseeing the risk management function; and

(vii) CISO shall place a review of cyber security risks/ arrangements/ preparedness of the RE before the Board/ RMCB/ ITSC atleast on a quarterly basis.

25. Risk Assessment

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

(b) REs shall ensure that all staff members and service providers comply with the extant information security and acceptable-use policies as applicable to them.

(c) REs shall review their security infrastructure and security policies at least annually, factoring in their own experiences and emerging threats and risks. REs shall take steps to adequately tackle cyber-attacks including phishing, spoofing attacks and mitigate their adverse effects.

26. Conduct of Vulnerability Assessment (VA) / Penetration Testing (PT)

(a) For critical information systems and/ or those in the De-Militarized Zone (DMZ) having customer interface, VA shall be conducted at least once in every six months and PT at least once in 12 months. Also, REs shall conduct VA/ PT of such information systems throughout their lifecycle (pre-implementation, post implementation, after major changes, etc.).

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

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

(d) In the post implementation (of IT project/ system upgrade, etc.) scenario, the VA/ PT shall be performed on the production environment. Under unavoidable circumstances, if the PT is conducted in test environment, REs 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.

(e) REs 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.

(f) REs 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 may also apply to the RE's information systems hosted in a cloud environment.

27. Cyber Incident Response and Recovery Management[16]

(a) The cyber incident response and recovery management policy shall address the classification and assessment of incidents; include a clear communication strategy and plan to manage such incidents, contain exposures and achieve timely recovery.

[16] The term 'incident' implies 'cyber incident' in this Master Direction

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

(c) REs shall have written incident response and recovery procedures including identification of key roles of staff/ outsourced staff handling such incidents.

(d) REs shall have clear communication plans for escalation and reporting the incidents to the Board and Senior Management as well as to customers, as required. REs shall pro-actively notify CERT-In and RBI[17] regarding incidents, as per regulatory requirements. REs are also encouraged to report the incidents to Indian Banks – Centre for Analysis of Risks and Threats (IB-CART) set up by IDRBT.

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

Chapter V - Business Continuity and Disaster Recovery Management

28. Business Continuity Plan (BCP) and Disaster Recovery (DR) Policy

(a) The BCP and DR policy shall adopt best practices[18] to guide its actions in reducing the likelihood or impact of the disruptive incidents and maintaining business continuity. The policy shall be updated based on major developments/ risk assessment.

(b) RE's BCP/ DR capabilities shall be designed to effectively support its resilience objectives and enable it to rapidly recover and securely resume its critical operations (including security controls) post cyber-attacks/ other incidents.

[17] In respect of Housing Finance Companies, cyber incidents shall continue to be reported to NHB and not RBI.
[18] For example, refer to ISO 22301

29. Disaster Recovery Management

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

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

(c) 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.

(d) REs shall regularly test the BCP / DR under different scenarios for possible types of contingencies, to ensure that it is up-to-date and effective.

(e) REs 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.

(f) REs shall ensure that DR architecture and procedures are robust, meeting the defined RTO and RPO for any recovery operations in case of contingency.

(g) REs should prioritise achieving minimal RTO (as approved by the RE's ITSC) and a near zero RPO for critical information systems.

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

(i) REs shall ensure that the configurations of information systems and deployed security patches at the DC and DR[19] are identical.

(j) REs shall ensure BCP and DR capabilities in critical interconnected systems and networks including those of vendors and partners. REs shall ensure demonstrated readiness through collaborative and co-ordinated resilience testing that meets the REs' RTO.

[19] DC refers to primary data centre for a given application/ system and DR its Disaster Recovery site/ alternate site.

Chapter VI - Information Systems (IS) Audit

30. Information Systems (IS) Audit

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

(b) REs shall put in place an IS Audit Policy. The IS Audit Policy shall contain a clear description of its mandate, purpose, authority, audit universe, periodicity of audit etc. The policy shall be approved by the ACB and reviewed at least annually.

(c) The ACB shall review critical issues highlighted related to IT / information security / cyber security and provide appropriate direction and guidance to the RE's Management.

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

(e) REs shall carry out IS Audit planning by adopting a risk-based audit approach.

(f) REs may consider, wherever possible, a continuous auditing approach for critical systems, performing control and risk assessments on a more frequent basis.

Chapter VII – Repeal and Other Provisions

With the issue of these Directions, the instructions/ guidelines contained in the circulars issued by the Reserve Bank of India listed in Annex shall stand repealed from the dates mentioned in the said Annex. All the instructions/ guidelines given in the circulars referred above shall be deemed as given under these Directions. Any reference in other circulars/ guidelines/ notifications issued by the Reserve Bank containing reference to the said repealed circulars, shall mean the reference to these Directions, namely, the Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023, after the date of repeal. Notwithstanding such repeal, any action taken, purported to have been taken or

initiated under the circulars hereby repealed shall continue to be governed by the provisions of the said circulars/ guidelines/ notifications.

31. Application of other laws not barred

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.

32. Interpretation

For the purpose of giving effect to the provisions of these Directions or in order to remove any difficulties in the application or interpretation of the provisions of these Directions, the Reserve Bank of India may, if it considers necessary, issue necessary clarifications in respect of any matter covered herein and the interpretation of any provision of these Directions given by the Reserve Bank of India shall be final and binding.

****

Annex

The following circulars are **consolidated**[20], while issuing these Directions:

(i) DBS.CO.OSMOS.BC.8/33.01.022/2002-2003 dated December 19, 2002 on Standardised Checklists for Conducting Computer Audit - Report of the Committee on Computer Audit

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

With the coming into effect of these Directions, the instructions/ guidelines contained in the following circulars issued by the Reserve Bank stand **repealed**. These circulars will continue to remain in force till March 31, 2024.

Sr. No.	Circular Reference	Date	Subject	Remarks
1	DBS.CO.ITC.BC.10/31.09.001/97-98	February 4, 1998	Risks and Control in Computer and Telecommunication Systems	
2	DBS.CO.OSMOS.BC/11/33.01.029/2003-04	April 30, 2004	Information System Audit - A Review of Policies and Practices	
3	DBS.CO.IS.Audit.No.19/31.02.03/2004-05	April 15, 2005	Operational Risk Management - Business Continuity Planning	
4	DBS.CO.IS.Audit.No.4/31.02.03/2005-06	February 16, 2006	Business Continuity / Disaster Recovery Planning	
5	DBS.CO.IS.Audit.BC.No.3/31.02.03/2005-06	February 16, 2006	Phishing Attacks	
6	DIT.CO.801/07.71.032/201-11	September 29, 2010	Business Continuity Plan (BCP), Disaster Recovery (DR) drill and Vulnerability Assessment-Penetration Testing (VAPT)	

[20] For compliance purpose, it is sufficient to adhere to this Master Direction by the REs in lieu of the circulars and the reports referred therein.

Sr. No.	Circular Reference	Date	Subject	Remarks
7	DIT.CO(Policy)2036/07.71.032/2011-12	March 2, 2012	Business Continuity Plan (BCP) and Disaster Recovery (DR); Vulnerability Assessment-Penetration Testing(VAPT)	
8	DIT.CO.(Policy).No.674/09.63.025/2013-14	August 30, 2013	Sharing of Information Technology Resources by Banks – Guidelines	
9	DIT.CO(Policy)No.2636/09.63.025/2012-13	June 26, 2013	Business Continuity Planning (BCP), Vulnerability Assessment and Penetration Tests (VAPT) and Information Security	
10	DIT CO No.1857/07.71.099/2013-14	February 26, 2014	Security Incident Tracking Platform - Reporting	
11	DBS (CO).CSITE/9094/31.01.15/2016-17	May 23, 2017	Risk Governance Framework-Role of Chief Information Security Officer (CISO)	
12	DNBS.PPD.No.04/66.15.001/2016-17	June 08, 2017	Master Direction - Information Technology Framework for the NBFC Sector	Repealed only for NBFC-Top, Upper and Middle Layer

Acronyms

ACB	Audit Committee of the Board of Directors
BCP	Business Continuity Plan
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CCTV	Closed-Circuit Television
CERT-In	Indian Computer Emergency Response Team
CRO	Chief Risk Officer
CSIRT	Cyber Security Incident Response Team
CTO	Chief Technology Officer
CVSS	Common Vulnerability Scoring System
DMZ	De-Militarized Zone
DC	Data Centre
DR	Disaster Recovery
EOS	End of Support
IB-CART	Indian Banks – Centre for Analysis of Risks and Threats
IDRBT	Institute for Development and Research in Banking Technology
IP	Internet Protocol
ISC	Information Security Committee
IS	Information Systems
ISO	International Organization for Standardization
IT	Information Technology
ITSC	Board-level IT Strategy Committee
NHB	National Housing Bank
PT	Penetration Testing
RBI	Reserve Bank of India
RE	Regulated Entity
RMCB	Risk Management Committee of the Board
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SOC	Security Operation Center
VA	Vulnerability Assessment