Title: *IT Governance, Risk, Controls and Assurance Practices Directions, 2023: Focus on governance, risk management, resilience, and responses*

Authors: *Kaushal Shah & Subhojit Shome | Team Finserv | finserv@vinodkothari.com*

Date: November 11, 2023

Vinod Kothari Consultants Pvt Ltd

IT Governance, Risk, Controls and Assurance Practices Directions, 2023:

Focus on governance, risk management, resilience, and responses

Table of Contents

Introduction

On 7th November, 2023, the RBI notified the **Master Directions on Information Technology Governance, Risk, Controls and Assurance Practices** ('Directions' or 'IT Directions') an unified Information Technology framework across regulated entities of the RBI. These Directions were preceded by the ***Draft Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices*** ('Draft IT Directions') which were put in public domain on October 20, 2022. The new IT Directions also follow the publication of the unified ***Master Direction on Outsourcing of Information Technology Services*** ('IT Outsourcing Directions') on April 10, 2023. Both these directions had found a mention in the RBI's ***Statement on Developmental and Regulatory Policies (February 2022)***.

For financial sector entities, a robust IT and related risk management framework is crucial - for reasons which are multiple and obvious. First, financial sector entities are key players in payment and settlement systems, and any disruption there may have a major ripple effect on the entire system. Second, financial entities house data relating to the masses, and this data is sensitive personal financial data. Any security breach there may lead to severe implications. What aggravates the issue is that there are several instances of such cyber-attacks. There are several other similar reasons.

The Basel Committee has also issued principles of operational resilience, which imbibe information systems, cyber-security, and related issues.

In this article we have attempted to provide a summarised view of the changes, the enhanced governance structure and information/ cyber-security mandates for the regulated entities as well a comparative between the new Directions and the erstwhile Information Technology framework applicable to NBFCs.

Applicability

These Directions shall come into effect from April 1, 2024 and will apply to the following Regulated Entities ('RE');

- Commercial banks, including Banking Companies, Corresponding New Banks, and the State Bank of India.
- NBFCs falling under the 'Top Layer,' 'Upper Layer,' and 'Middle Layer' categories as per the Scale Based Regulation (SBR) framework.
- Credit Information Companies (CICs).
- All India Financial Institutions (AIFIs) such as EXIM Bank, NABARD, NaBFID, NHB, and SIDBI.

However, the following REs are exempted from the ambit of these Master Directions

- Local Area Banks;
- NBFC- Core Investment Companies

In case of Foreign Banks, operating in India through branch mode shall be subject to a 'comply or explain' approach for applicability of these Master Directions.

Applicability on NBFCs

These regulations shall apply on all NBFCs (except NBFC-CICs) which fall under following three layers as per the SBR framework ('Specified NBFCs'):

- Top Layer;
- Upper Layer; and
- Middle Layer.

Further, it is pertinent to note that these directions are not applicable on Base Layer NBFCs. Thus, Base Layer NBFCs shall continue to follow Section-B of the 2017 ***Master Direction - Information Technology Framework for the NBFC.***

Overview of the Changes

These Directions cover the overall Information Technology Function ('IT Function') of the specified NBFCs and the other REs and also provide guidance for related functions like information security management and information system audit (IS Audit).

While the approval of strategies and policies related to the IT function lies in the hands of the Board of Directors ('Board'), these Directions put the responsibility on shoulders of the IT Strategy Committee (ITSC), the IT Steering Committee and the Information Security Committee (ISC) as well as on the Head of the IT Function (CIO/ CTO) to institute effective oversight on the planning and execution of IT Strategy and information system. The Senior Management is also mandated to for putting in place appropriate mechanisms to ensure IT/ IS and their support infrastructure are functioning effectively and efficiently; cyber security posture of the NBFC is robust; and overall, IT contributes to productivity, effectiveness and efficiency in business operations.

The new Directions no longer call for the creation of separate roles of the CIO and CTO and put extended operational responsibilities on the shoulders of the Head of IT Function. The new Directions, however, call for designating a sufficiently senior level executive of the entity as the Chief Information Security officer (CISO) who will be responsible for driving information/ cyber security, ensuring compliance to related regulatory guidelines, enforcing the policies of the RE used to protect information assets and managing and coordinating information/ cyber security related issues/ implementation within the entity as well as with relevant external agencies.

From a high-level perspective, these new Directions delve into greater granularity and detail (although certain micro-level provisions from the Draft have been omitted) compared to the previously applicable guidelines which were more broad-based and referred to tenets and principles. The concept of a risk-based approach to information system management and the identification of "critical information systems" have also been introduced with more rigorous prescriptions for such systems.

A graphical summary of the changes/ action items mandated by the new Directions has been presented in the following section.

Summary of the Action Items

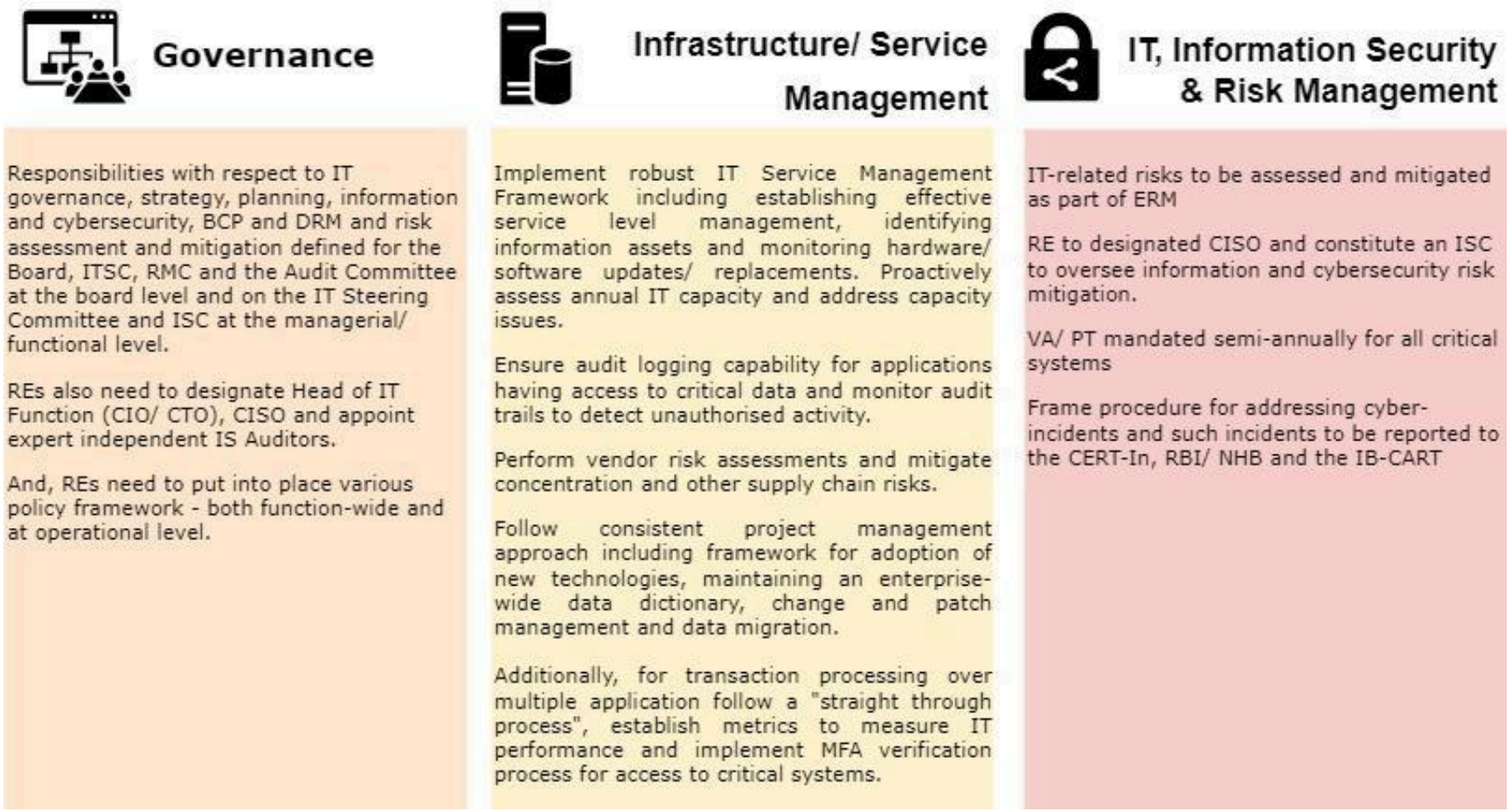

Figure 1: Action Items w.r.t. Governance, Infra & Service Management & IT Risks

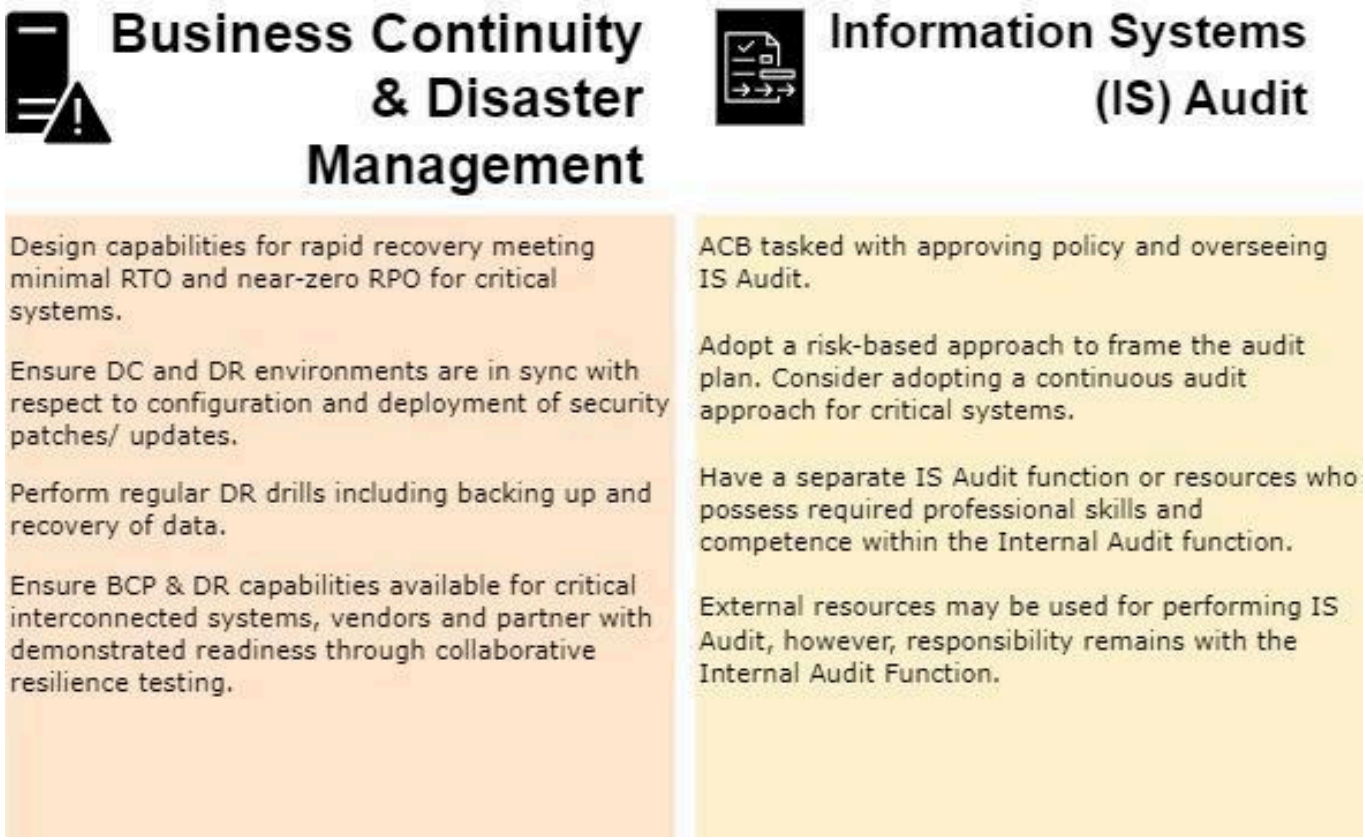

Figure 2: Action Items w.r.t. Business Continuity & Disaster Management and Information (IS) Audit

In the following sections we examine the governance framework that needs to be implemented by the RE to fulfil these regulatory prescriptions of the RBI.

Governance Structure

The governance structure conceived by the new IT Directions may be visualised as follows –

Figure 3: Governance Framework

We discuss the elements of this framework in detail in the following sections.

Authorities & their Responsibilities

Authorities	Responsibilities/ tasks
Board of Directors ('Board')	Setting up and approving strategies and policies related to IT, Information Assets, Business Continuity, Information Security, Cyber Security (including Incident Response and Recovery Management/ Cyber Crisis Management). Review of policies and strategies to be undertaken annually.
IT Strategy Committee (ITSC)	● Ensure effective IT strategic planning process. ● Guide in the preparation of IT Strategy aligned with overall RE strategy. ● Validate IT Governance and Information Security Governance structure. ● Oversee IT and cybersecurity risk assessment and management processes. ● Review budgetary allocations for IT function and cybersecurity.

Authorities	Responsibilities/ tasks
	● Conduct annual review of Business Continuity Planning and Disaster Recovery Management.
IT Steering Committee	● Assists ITSC in strategic IT planning, oversight of IT performance, and aligning IT activities with business needs. ● Oversees processes for business continuity and disaster recovery. ● Ensures implementation of a robust IT architecture meeting statutory and regulatory compliance. ● Updates ITSC and CEO periodically on its activities.
Information Security Committee (ISC)	● Shall manage cyber/ information security. ● Develop and implement cybersecurity policies for risk management. ● Approve and monitor security projects and awareness initiatives. ● Review and address cyber incidents, audit observations, and mitigation activities. ● Periodically update ITSC and CEO on its activities.
Head of IT Function (CTO/ CIO)	● Ensure alignment of IT projects/ initiatives with RE's IT Policy and Strategy. ● Establishes an effective organizational structure to support IT functions. ● Implements disaster recovery setup and business continuity strategy/plan. ● First line of defence for assessing, evaluating, and managing IT controls and risks. ● Secure RE's information assets and ensures compliance with internal policies and regulatory requirements.
Senior and other management	● Ensure execution of Board-approved IT Strategy. ● Ensure effective functioning of IT/IS and their support infrastructure. ● Implement necessary IT risk management processes. ● Maintain a robust cyber security posture. ● Ensure overall IT contribution to productivity and efficiency in business operations.
Chief Information Security Officer (CISO)	● Drive cybersecurity strategy and ensure compliance with regulatory instructions. ● Enforce policies for protecting information assets and manage external coordination. ● Serve as a permanent invitee to ITSC and IT Steering Committee. ● Manage Security Operations Centre (SOC) and lead

Authorities	Responsibilities/ tasks
	cybersecurity projects. ● Ensure effective functioning of deployed security solutions and report to the Executive Director quarterly on cyber risks and preparedness.
Information System Auditor(s)	● Plan and perform IS Audits adopting a risk-based approach and consider continuous auditing for critical systems.
Audit Committee	● Responsible for IS Audit oversight. ● Approve IS Audit Policy. ● Review critical IT, information security, and cyber security issues.
Risk Management Committee	● Periodically review IT-related risks. ● Review and update the risk management policy with IT related risks. ● Collaborate with IT Steering Committee on risk matters. ● Ensure effective IT risk management processes.

Committees - Composition, Meetings and ToR

Committee	Constitution	Composition	Meeting Frequency (minimum)
IT Strategy Committee (ITSC)	Board level	● Three directors ● Independent Chairperson ● Technically competent members	Quarterly
IT Steering Committee	Management level	● Management level committee, senior management representation from IT and business functions	Quarterly
Information Security Committee (ISC)	Management level Under the oversight of the ITSC	● CISO & other representatives from Business & ITSC on recommendation of ITSC	Not specified

Under these new IT Directions, the Risk Management Committee (RMC) and Audit Committee (ACB) also play a significant role in IT Function with the RMC exercising oversight over the ISC and determining its constitution; while, the ACB is responsible for drafting and updating the IS Audit Policy as well as reviewing critical issues highlighted during such audit.

List of Policies

Policy Area	Approving Authority	Review Frequency (minimum)
Information Technology/ Information System	Board	Annual
Business Continuity (BCP) and Disaster Recovery (DRM)	Board	Annual (also, should be updated based on major developments/ risk assessment)
Information Security	Board	Annual
Information and Cyber Security (incl. Incident Response and Recovery Management/ Cyber Crisis Management and Cyber Security Policy and Cyber Crisis Management Plan (CCMP))	ISC (reviewed by the Board)	Annual
Enterprise-wide risk management policy/ operational risk management policy needs to incorporate IT-related risks	Risk Management Committee (RMC) in consultation with the ITSC	Periodic
Change and Patch Management	Not specified	Not specified
Data Migration	Not specified	Not specified
IS Audit	Audit Committee of Board (ACB)	Annual

List of Assessments, Reviews and Testing

Area	Undertaken/ Reviewed by	Frequency (minimum)
IT risk assessment	Not specified (logically fits into the role of the	Not specified (will depend on policy and

	ISC/ CISO)	standard adopted)
Review of cyber security risks/ arrangements/ preparedness	CISO and reviewed by the Board/ RMC/ ITSC	Quarterly
IT vendor risk assessment and controls	Not specified	Not specified
Capacity assessment	Review by ITSC	Annual
Review of security infrastructure	Not specified (logically fits into the role of the ISC/ CISO)	Annual
Vulnerability testing (VT)/ Penetration testing (PT)	Should be conducted by appropriately trained and independent information security experts/ auditors	Throughout the lifecycle based on critically and risk assessment (ref. Chapter IV for details)
DR drills	Not specified. Will depend on the Policy and standard adopted	For critical systems shall be at least on a half-yearly basis and for all other systems based on risk assessment
IS Audit	ACB and Senior Management	Not specified (will be based on the NBFC's IS Audit Policy)

Management Information System (MIS)

One area that is conspicuous by its absence in the Directions (as we had spotted in the Draft IT Directions) is Management Information Systems (MIS). Whereas the previously applicable IT guidelines for NBFC lay down quite detailed directions in this area including building a dashboard for Top Management to view and track financial performance of the NBFC against targets, its use in pricing financial products , identification of Special Mention Accounts (SMA) and NPAs, fraud and suspicious transaction analysis, tracking regulatory compliances, capacity and performance analysis of IT security systems, Incident reporting and integration with the RBI's COSMOS for reporting and supervision purposes; MIS does not find even a mention in these new guidelines.

In the next section we take a more detailed look at the new and the erstwhile information technology framework that was applicable to NBFCs.

Focus on NBFCs - Comparison of new IT Directions with the Earlier Guidelines

Para no.	New Provision	Erstwhile Provision	Comments/ Action Needed
Chapter I - Preliminary			
3	The IT Directions apply to all Banking Companies, excluding Local Area Banks but including Small Finance Banks, Payments Banks, and Foreign Banks, all NBFCs (in the Top, Upper and Middle Layers) except NBFC-CIC, All India Financial Institutions and Credit Information Companies.	Separate guidelines were prescribed by the RBI for NBFCs and Banks. The erstwhile NBFC specific guidelines will continue to apply to Base Layer NBFCs.	-
Chapter II - IT Governance			
4	An **IT Governance Framework** is required to put in place, which shall comprise: ● Governance structure and processes necessary to meet the RE's business/ strategic objectives; ● Roles and responsibilities of the Board/ Board level Committees and Senior Management; ● Adequate oversight mechanisms to ensure accountability and mitigation of business risks; ● The key focus areas of IT Governance shall include strategic alignment, value delivery, risk management, resource management, performance management and Business Continuity/ Disaster Recovery Management.	Guidelines on governance were on similar lines although there are more specific prescriptions made for certain areas as indicated below.	
4, 5	Strategies, policies related to IT, Information Systems (IS), Business Continuity, Information Security, Cyber Security shall be approved by the Board and reviewed at least annually. Enterprise-wide risk management policy or operational risk management policy needs to incorporate IT-related risks also.	The erstwhile directions called for adoption the below list of Policies - ● IT Policy, ● Information Security/ Cybersecurity Policy, ● Change Management policy, ● IS Audit Policy, ● BCP Policy,	List of Board approved policy areas remain on the same lines; however, content of existing Policies will need to be reviewed and updated.

		● IT Services Outsourcing Policy.	
6	REs are required to establish a **Board-level IT Strategy Committee (ITSC)**	Erstwhile directions also required constituting an ITSC that shall carry out review and amend the IT strategies in line with the corporate strategies, Board Policy reviews, cyber security arrangements and any other matter related to IT Governance. Its deliberations may be placed before the Board.	The IT Directions extend the remit of the ITSC as noted below
	Composition - ● Minimum of three directors as members. ● Chairperson shall be an independent director having min. Seven years of experience in managing IT systems or leading IT projects. ● All members should have the ability to understand/ evaluate information systems and associated IT/ cyber risks.	Composition - Should have a chairman who is an independent director (ID); CIO & CTO should be a part of the committee.	ITSC becomes a Board-level committee. Qualification/ experience of chairperson prescribed.
	The IT Strategy Committee shall meet at least on a quarterly basis.	The IT Strategy Committee should meet at an appropriate frequency but not more than six months should elapse between two meetings.	Frequency of ITSC meetings increased.
	The ITSC shall, inter alia: ● Ensure that the RE has put an effective IT strategic planning process in place; ● Guide in preparation of IT Strategy ● Ensure that the IT Strategy aligns with the overall strategy of the RE ● Satisfy that the IT Governance and Information Security Governance structure fosters accountability, is effective and efficient, has well defined objectives and unambiguous responsibilities for each level in the organisation;	The ToR was on similar but narrower lines. The erstwhile Directions also specifically provide that the IT Strategy Committee monitor the method that management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sourcing and use of IT resources. Although the erstwhile guidelines do not explicitly specify this, budgetary controls are to be exercised by the IT Strategy Committee.	The new IT Directions additionally require the ITSC Strategy Committee to monitor BCP and DR. While the erstwhile guidelines put the ITSC's focus on IT capex activity under the new Directions their remit covers operation aspects as well.

	● Put in place processes for assessing and managing IT risks, including cyber security risks; ● Ensure that the budgetary allocations for the IT function (including for IT security) are commensurate with the RE's IT maturity, digital depth, threat environment and industry standards and are ● Ensure Budget is utilised in a manner intended for meeting the stated objectives; ● Exercise oversight over the BCP and DRM of the RE		
7	**Senior Management** shall have the overall responsibility and should institute an effective oversight on the plan and execution of IT Strategy; Senior Management is tasked to put in place appropriate mechanism to - ● Ensure IT/ IS and their support infrastructure are functioning effectively and efficiently; ● Cyber security posture of the RE is robust; and ● IT contributes to productivity, effectiveness and efficiency in business operations.	The said responsibilities were on the Board and Senior Management	While the Board remains ultimately responsible, onus has been put on the Senior Management to ensure operational effectiveness of the NBFC's IT Strategy.
	REs shall establish an **IT Steering Committee**	Erstwhile directions also called for constituting a steering committee for operating at an executive level and focusing on priority setting, resource allocation and project tracking.	IT Steering Committee mandated.
	The IT Steering Committee should have representation at Senior Management level from IT, business functions for assisting the IT Strategy Committee in the implementation of the IT Policy and IT Strategy.	The erstwhile directions required the steering committee to consist of business owners, the development team and other stakeholders involved in specific projects.	
	The responsibilities of IT Steering Committee, inter alia, shall be to - ● Assist the ITSC in strategic IT planning, oversight of IT performance, and	The Steering Committee should be involved in priority setting, resource allocation and project tracking. It should provide oversight and monitoring of the progress of the	The Committee's role has been extended from merely being project specific to setting general standards for IT projects, ensuring

	aligning IT activities with business needs; ● Update IT Strategy Committee and CEO periodically on its activities; ● Oversee the BCP and DRM process; ● Ensure implementation of a robust IT architecture meeting statutory and regulatory compliance	project, including deliverables to be realised at each phase of the project and milestones to be reached according to the project timetable.	compliance with technology standards, ensuring effective implementation of the IT infrastructure, advising the ITSC/ CEO w.r.t. IT Strategy, overseeing the BCP, etc.
	The IT Steering Committee shall meet at least on a quarterly basis.	No such specific provision.	Mandatory meetings prescribed.
8	Head of IT Function: Appoint/ designate a sufficiently senior level, technically competent and experienced in IT related aspects as Head of IT Function (by whatever name called - Chief Technology Officer/ Chief Information Officer).	Appoint/ designate a Chief Information Officer (CIO)/ in-Charge of IT operations. IT Governance Stakeholders also included Chief Technology Officer(s) (CTO)	The new Directions do not call for the additional CTO role.
	Responsibilities of Head of IT Function- ● Ensure that the execution of IT projects/ initiatives is aligned with the RE's IT Policy and IT Strategy; ● Ensure effective organisation structure that supports the IT functions of the RE; ● Put in place an effective disaster recovery setup and business continuity strategy/ plan. ● Act as a first line of defence, ensuring effective assessment, evaluation and management of IT risk including the implementation of robust internal controls to ○ secure the RE's information/ IT assets ○ comply with extant internal policies, regulatory and legal requirements on IT related aspects.	Chief Information Officer (CIO)/ in-Charge of IT operations responsibilities were on similar lines. In the erstwhile IT Directions overall responsibilities towards IT outsourcing fell on the Board/ IT Strategy Committee who were required to put into place an appropriate governance mechanism and did not specifically make a mention of the CIO/ in-Charge of IT Operations in this regard.	Responsibilities of the Head of IT Function are extended in the Draft IT Directions.
	[omitted]	Requirement on NBFCs to maintain an updated status on user training and awareness relating to information security prescribed in the erstwhile guidelines.	No such requirement in the new Directions.

Chapter III - IT Infrastructure and Service Management			
9	Establish 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)	The erstwhile guidelines do not contain specific guidelines in this area. However, tenets and principles applicable to the IT Policy/ Governance Framework will apply to IT Service Management as well.	
	Put in place a **Service Level Management (SLM) process** - manage the IT operations and ensure segregation of duties	The erstwhile directions also called for a segregation of functions between the security and operational functions in the IT division as part of the IT Policy of the specified NBFC	Specified NBFCs will need to put in place an SLM process in line with new IT Directions.
	Develop **technology refresh plan** - 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 ongoing basis	NBFCs were required to realign their IT systems on a regular basis in line with the changing needs of its customers and business.	Specified NBFCs will need to draft Technology Refresh Plan. The intention of the RBI here is to make REs anticipate and be proactive in making technology/ capacity upgrades.
10	For t**hird-party arrangement** in the Information Technology/ Cyber Security ecosystem that are within the applicability of the Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023[1]s, the Directions mandate - ● Appropriate vendor risk assessment and controls proportionate to the risk and materiality assessed; ● Mitigate concentration risk including aspects pertaining to conflict of interest; ● Mitigate risks associated with single point of failure; ● Comply with applicable legal, regulatory requirements and standards to protect customer data; ● Provide high availability; ● Manage supply chain risks effectively.	Erstwhile guidelines did not contain such specific prescription for software/ hardware vendor management. However, REs would be expected to have such a framework in place as part of their overall IT governance and risk management frameworks.	Specified NBFCs will need to introduce such a framework if not already covered.

[1] Read our article on IT Services Outsourcing here - https://vinodkothari.com/2023/04/rbi-regulates-outsourcing-of-it-services-by-financial-entities/

11	**Capacity Management** - Annual assessment of capacity compared to past trends (peak usage), current as well as planned business activities. Assessment including requirements and measures taken to address issues to be reviewed by the ITSC.	Erstwhile guidelines called for capacity assessment of IT Security Systems, however, capacity management processes for maintaining service level against transaction volumes are not explicitly specified under the existing directions	Specific NBFCs need to put in place a capacity assessment process. Such capacity assessment should be reviewed by the ITSC.
	IT systems and infrastructure are able to support business functions and ensure availability of all service delivery channels.		Should be part of IT Capacity planning/ assessment process.
12	**Project Management** Apply consistent and formally defined project management approach to IT projects that should enable appropriate stakeholder participation for effective monitoring and management of project risks and progress.	The erstwhile directions contained guidelines regarding Change Management and put the responsibility of the monitoring IT related projects on the IT Steering Committee.	Specified NBFCs need to adopt standard enterprise architecture planning methodology/ framework for adoption (acquisition/ development) of new technology.
	Adopt standard enterprise architecture planning methodology/ framework - for adopting new/ emerging technology. Emerging technology adoption should be commensurate with the risk appetite and align with overall business/ IT strategy.		
	Maintain enterprise data dictionary to enable sharing of data among applications and systems and promote a common understanding of data among IT and business users.	No such specific prescription in the erstwhile directions	The enterprise data dictionary becomes essential. This artefact is also significant for NBFC that need to migrate data from one system to another (say during implementation of CFSS).
	Formal agreement for maintenance and support to be entered into for applications provided by vendors		
	Source codes for all critical applications are received from the vendors or a software escrow agreement is in place with the vendors for ensuring continuity of services in case the vendor defaults or is unable to provide services. REs shall also ensure that product	No such specific prescription	Specified NBFCs will not put such an arrangement in place.

	updates and programme fixes are also included in the escrow agreement.		
	RE shall obtain a certificate from the application developer/ developer stating that the application is free of known vulnerabilities, malware and any covert channels in the code. Such certificate should also be obtained when there is a material change in code including upgrades.	No such specific prescription	Specified NBFCs will not put such an arrangement in place.
	New IT application proposed to be introduced as a business product should undergo - ● Formal product approval ● Quality assurance process.	Similar guidelines were provided as part of the Change Management Policy of the NBFC developed with approval of the Board Additionally, the erstwhile directions also provided principles to apply when providing Mobile Financial Services - confidentiality, integrity, authenticity and must provide for end-to end encryption	IT based business product launch will become subject to more formal rigour under the Draft IT Directions.
13	**Change and Patch Management** procedure - ● Have documented policies and procedures in place for change/ patch management ● IT systems are implemented and reviewed in a controlled manner and in a controlled environment ● Effectiveness of integration and interoperability of complex IT processes shall be put in place Patches as per their criticality shall be evaluated in a test environment before being pushed into live environment.	As mentioned above, under the current directions, NBFCs are expected to develop, with the approval of their Board, a Change Management Policy. Such a Policy should cover - ● Prioritising and responding to change proposals from business, ● Cost benefit analysis of the changes proposed, ● Assessing risks associated with the changes proposed, ● Change implementation, monitoring and reporting. It was the responsibility of the senior management to ensure that the Change Management Policy is being followed on an ongoing basis.	Mandates the requirement to have a test environment to evaluate patches before being applied to the live environment.
14	**Data Migration Controls** - Documented data migration policy specifying a systematic process for data migration, ensuring data integrity, completeness and	No such specific provision	Documented data migration policy will need to be put into place.

	consistency. The policy shall, inter-alia, contain provisions pertaining to sign-offs from business users/ application owners at each stage of migration, audit trails etc.		This provision becomes especially significant for specified NBFCs required to implement CFSS.
[Ref. IT Outsourcing Directions]	[omitted]	Erstwhile Directions included provisions related to IT Services Outsourcing	Subsumed in the IT Services Outsourcing Directions.
15	**Audit Trail** should be maintained for every application which can affect critical/ sensitive information and should have necessary audit and system logging capability	As per the erstwhile directions, IT Policy of 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.	Minimum set of fields/ data that should be captured for the purposes of an audit trail explicitly provided in the Directions. Specified NBFCs will need to ensure that their current systems capture such data.
	Audit trail should serve to facilitate conduct of audit, serve as forensic evidence, dispute resolution, including for non-repudiation purposes	Erstwhile directions were on similar lines	
	REs need to put in place system for regularly monitoring the audit trails and system logs to detect any unauthorised activity.	Existing directions do not explicitly specify such a framework requirement	Specified NBFCs will need to put in place a log management and retention framework.
16	**Cryptographic Controls** - 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.	Encryption and PKI requirements were part of the erstwhile guidelines.	Encryption continues to be mandated.
17	**Straight Through Processing (STP)** - There should not be any 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. Data transfer mechanism between processes or applications must be properly tested, securely automated with necessary checks and balances, and properly integrated through	Erstwhile directions did not contain such a provision.	Specified NBFC to ensure such technical architecture is in place.

	STP methodology with appropriate authentication mechanism and audit trails		
18	**Physical/ Environmental Control -** Implement suitable physical/ environmental controls across DC and DR sites DC and DR should be geographically well separated DC and DR should be subjected to necessary e-surveillance mechanisms	Requirement for physical security was included in the erstwhile guidelines.	Requirements for e-surveillance mechanism and a geographically well separated DR site need to be implemented.
19	**Access Controls -** Access based on valid business needs; Documented and updated SOPs approved by the IT Strategy Committee for need-based access; Close supervision of personnel with elevated access with all their systems activities logged and periodically reviewed; Multi-factor authentication (MFA) for privileged users of critical information/ activities based on risk assessment.	Role-based access control measures present in erstwhile guidelines.	Concept of "Privileged User" and mandate for MFA introduced.
20	Teleworking - ● Systems used and access from alternative work location are secure; ● MFA to be applied for access to critical systems; ● Mechanism in place to identify devices accessing the REs systems; Data/ information shared over the network is secured appropriately.	Prescription regarding tele/ remote working were not in the erstwhile guidelines.	Remote working facilities should adhere to the new Directions.
21	Metrics - ● 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; ● For non-critical information systems, REs shall adopt a risk-based approach to define suitable metrics; Implement suitable scorecard/ metrics/ methodology to measure IT performance and IT maturity level	No such specific provision.	Specified NBFCs need to put in place such metrics/ methodology

Chapter IV - IT Risk and Information Security			
22	IT Risk Management Policy - The RMC to review and update the IT Risk Management Policy at least on a yearly basis as part of the risk management policy of the RE in consultation with the IT Strategy Committee	The Board or Senior Management were responsible for taking into consideration risks associated with existing and planned IT Operations and the risk tolerance and then establish and monitor policies for risk management.	RMC is now explicitly tasked with overseeing the IT risk management and integrating it with the RE's risk management policy.
	[omitted]	IT Strategy Committee responsible for developing sound and responsive outsourcing risk management policies and procedures commensurate with the nature, scope, and complexity of outsourcing arrangements.	Subsumed in the IT Services Outsourcing Directions.
23	Establish a robust **Risk Management Framework** involving - ● Implementation of a comprehensive information security management function; ● Periodic review of internal controls and processes; ● Define roles and responsibilities of stakeholders (including third-party personnel) involved in risk management. Areas of conflict and accountability gaps must be specifically identified; ● Identify "Critical Information system" - and evolve standard operating procedures in identifying and protecting such systems/ group of systems. ● Define and implement necessary systems, procedures and controls to ensure secure storage/ transmission/ processing of data/ information	Specified NBFCs undertake comprehensive risk assessment at least on a yearly basis. The risk assessment should be brought to the notice of the Chief Risk Officer (CRO), CIO and the Board of the NBFC and should serve as an input for Information Security auditors. No mention of specific Information Security Function. Contains requirements for physical security for "critical data." In the context of BCP/ DR - critical business processes, critical business verticals, locations and shared resources, critical business systems and data centres	Under the new IT Directions, risk assessment should be reviewed by the ISC. Identification "critical information system" required. Under the erstwhile guidelines, such identification would have been required in the context of BCP/ DRM (critical business processes, critical business verticals, locations and shared resources, critical business systems and data centres).
24	**Information and Cyber Security Policy** - Adopted Information Security Policy should, inter alia, include - ● Objective, scope, ownership and responsibility for the Policy	Erstwhile guidelines provided information security tenets - confidentiality, integrity, availability, and authenticity - that should guide NBFCs.	Specified NBFCs need to review their current IT/ IS policies.

	• Information security organisation structure • Information security roles and responsibilities • Exceptions • Compliance review • Penal measures for non-compliance with Policy	The Information Security Policy should provide for a framework containing - • Identification/ classification of information assets; • Segregation of functions - Security Officer/ Group vis-à-vis Information Technology division which implements the computer systems; • Role based access control - well-defined user roles (system administrator, user manager, application owner etc.); • Personnel security; • Physical security; • Trails • Use of PKI.	
	[Does not explicitly call for putting in place a cyber resilience framework. However, such a framework should get covered under the cyber security management provisions.]	Cyber resilience framework - cyber security preparedness indicators should be used for comprehensive testing through independent compliance checks and audits carried out by qualified and competent professionals.	
	Cyber Crisis Management Plan (CCMP) addressing - Detection, Response, Recovery and Containment - should be put into place.	Erstwhile guidelines also contain requirements for putting in place such a Plan.	CCMP continues to be mandated.
	Information Security Committee (ISC) should be created under the oversight of the IT Strategy Committee for managing information security.	Calls for creation of an adequately resourced Information Security Function. However, it does not contain a specific requirement to constitute such a Committee.	Specified NBFCs will need to constitute ISC.
	Constitution of ISC should be as follows - • Chief Information Security Officer (CISO) • Representative from business (decided by the IT Strategy Committee) Representative from IT Function (decided by the IT Strategy Committee)	No such requirement.	

	The head of the ISC shall be from the risk management vertical.	No such requirement.	
	Responsibilities of the ISC shall include - ● 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 ● Approving / monitoring security projects and awareness initiatives ● Reviewing information/ cyber security incidents, IS audit observations, monitoring and mitigating activities ● Reporting to ITSC and CEO on information security activities	No such requirement.	
	Chief Information Security Officer (CISO) should be appointed. CISO should **not** have a direct reporting line to IT Ops head, should not have business targets. Reasonable minimum term, CISO office adequately staffed, information/ cyber security/ CISO office budget determined in view of threat landscape. CISO, preferably, should have the rank of GM or equivalent. The CISO shall directly report to the Executive Director or equivalent executive overseeing the risk management function.	No such requirement.	Specified NBFCs will need to constitute ISC and appoint CISO
	CISO responsibilities should be clearly defined and documented, and should include - ● driving cyber security strategy and ensuring compliance to regulatory requirements; ● Enforcing information asset and security policies; ● Preparedness to threats; ● Coordinate activities w.r.t. cybersecurity, incident Response Team (CSIRT) within the RE;	No such requirement	

	• Attend ITSC and IT Steering Committee meetings as permanent invitee; • Manage and monitor Security Operations Centre (SOC) and drive security related projects; • ensure effective functioning of the security solutions deployed; • Review cyber security risks/ arrangements/ preparedness and place before Board/ RMC/ ITSC at least on a quarterly basis		
25	**Information Security Management** - • Risk assessment for each information asset guided by appropriate security standards/ IT control frameworks - business, compliance and/ or contractual perspective; • Staff members and service providers should comply with extant information security and/ or acceptable-use policies as applicable to them; • Review security infrastructure and security policies at least annually;	Erstwhile directions call for creating an Information Security Framework as contained in the IS Policy. Existing directions do not specify/ recommend adoption of specific standards or framework. Requirement to specifically review security infrastructure and policy annually also not provided under the erstwhile directions.	
26	**Vulnerability Testing (VA)/ Penetration Testing (PT)** by appropriately trained and independent information security experts/ auditors prescribed.	Erstwhile directions provide requirements to assess vulnerability and take remedial measures. Master Direction - Know Your Customer (KYC) Direction, 2016 ("KYC Master Directions")[2] contains requirements to perform vulnerability assessment and penetration testing to	VA/ PT becomes essential for all IT assets and not just V-CIP infrastructure. Significant norms with respect to how VA/ PT should be performed are specified in the Draft IT Guidelines.

[2] *The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by suitably accredited agencies as prescribed by RBI. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines* - https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11566

		the NBFC's V-CIP infrastructure.	VA/ PT becomes essential for all IT assets and not just V-CIP infrastructure. Significant norms with respect to how VA/ PT should be performed are specified in the new IT Directions. Specified NBFCs will need to review their existing Information Security Policy and modify their current reporting and mitigation processes.
	Critical IT assets and those in the DMZ (Demilitarised Zone) - VA should be performed every 6 months and PT at least every 12 months ● For non-critical IT systems based on risk-based approach adopted by the organisation.	No such specific provision	
	VA/ PT Environment - ● VA/ PT should be performed in the production environment; ● Under unavoidable circumstances if VA/ PT is conducted in a test environment then the test environment should have a version and config that resembles prod. Any deviation should be documented and approved by ISC; ● Ensure to fix the identified vulnerabilities and associated risks in a timebound manner; ● Avoid recurrence of known vulnerabilities such as those available in Common Vulnerabilities and Exposures (CVE) database.	No such specific provision	

	Documented approach to conduct VA/ PT - scope, coverage, vulnerability scoring mechanism (e.g., Common Vulnerability Scoring System - CVSS). This also applies to RE's infrastructure/ application hosted in a cloud environment. PT should be performed in a controlled manner within the scoped IT system components/ applications for any known as well as unknown vulnerability which may exist before the PT exploits	No such specific provision	
27	**Cyber Incident Response and Recovery Management** - Policy should provide for classification and assessment of incidents, contain exposures and achieve timely recovery.	The Information Security Policy should define what constitutes an incident. NBFCs shall develop and implement processes for preventing, detecting, analysing and responding to information security incidents.	Specified NBFCs will need to review their existing Information Security Policy and modify their current reporting and mitigation processes.
3(iv)	Definition of Cyber Incident - ● …shall mean a cyber event that adversely affects the cyber security of an information asset whether resulting from malicious activity or not.	Left to the Information Security Policy to define.	
	Written incident response and recovery procedures to be documented. Incident management measures - ● Take measure to mitigate the adverse impact of such incidents; ● Clear communication plans for escalating and reporting incidents to Board and Senior Management as well as customers are required; ● Proactively inform Cert-In and the RBI (NHB in case of HFCs) reg. Cyber security incidents as per regulatory requirements;	Erstwhile guidelines required sharing of information on cybersecurity incidents with RBI. The list of relevant cyber security incidents are specified in the CSIR Form of Annex I.[3]	

[3] https://rbidocs.rbi.org.in/rdocs/content/pdfs/MD52E07062017_AN1.pdf

	• Recommended to report incidents to Indian Banks - Centre for Analysis of Risks and Threats (IB-CART), IDRBT; • Establish processes to improve incident response and recovery activities and capabilities through lesson learnt from past incidents/ tests/ drills; • Conduct of tests and drills with stakeholders (including service providers) to ensure effectiveness of crisis communication plan/ process.		
Chapter V - Business Continuity and DRM			
28	**BCP and DRM policy** shall adopt best practices based on international standards (e.g., ISO 22301). Policy shall be updated on major developments/ risk assessments. 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.	NBFCs were required to adopt a Board approved BCP Policy. The functioning of BCP is monitored by the Board by way of periodic reports. NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centres.	Need to adopt best practices based on international standards now a mandate.
	Regularly test BCP - all possible types of contingencies to ensure that it is up-to-date and effective.	As per erstwhile guidelines - NBFCs needed to test the BCP either annually or when significant IT or business changes take place to determine if the entity could be recovered to an acceptable level of business within the timeframe stated in the contingency plan. The test should be based on 'worst case scenarios. The results along with the gap analysis may be placed before the CIO and the Board. The GAP Analysis along with Board's insight should form the basis for construction of the updated BCP.	
29	**Disaster Recovery Management** Backup data and periodically restore such backed-up data to check its usability. The	No specific requirement to perform DR drills	DR drills to be performed.

	integrity of such backup data shall be preserved along with securing it from unauthorised access; DR drills critical systems - at least on a half-yearly basis ● Others - as per risk assessments		Specified NBFCs need to meet RTO and RPO metrics and will need to review their existing DR testing process. The new IT Directions call for greater alignment of the DR environment with DC.
	DR testing should involve - ● Switching over to DR site and using it as the primary site for period where usual business operations of at least a full working day (including BoD and EoD operations) are covered; Securely backup data and periodically restore backed-up-data to check usability.	Did not specify steps at such a granularity	
	Ensure DR architecture and procedures are robust meeting the defined RTO and RPO criteria (as approved by the ITSC) - near zero in case of critical information systems.	Requirement to specify RTO and RPO not provided under existing directions	
	Configuration and security patches at DC and DR are identical	No such specific requirement	
	BCP and DR capabilities in critical interconnected systems and networks including those of vendors and partners. Ensure demonstrated readiness through collaborative and co-ordinated resilience testing that meets the REs' RTO	Provisions on IT Outsourcing in the erstwhile directions required NBFCs to ensure that their business continuity preparedness is not adversely compromised on account of outsourcing. However, it does not go to the extent of requiring co-ordinated testing	Co-ordinated testing with relevant vendors and partners called for in the new IT Directions.
Chapter VI - Information System (IS) Audit			
30	Audit Committee (ACB) responsible for exercising oversight	IS Audit framework required to be duly approved by Board.	NBFC should already have a Board approved IS Audit Framework. Such Framework should be reviewed as per the new IT Directions. Such reviewed Framework/ Policy may be approved and adopted by the Company's
	IS Audit Policy should cover mandate, purpose, authority, audit universe, periodicity. Policy needs to be approved by Audit Committee/ LMC and reviewed annually	IS Audit framework required to be duly approved by Board. IS Audit covered effectiveness of policy and oversight of IT systems, evaluating adequacy of processes and internal	

		controls and recommend corrective action to address deficiencies and follow-up. IS Audit should also evaluate the effectiveness of business continuity planning, disaster recovery set up and ensure that BCP is effectively implemented in the organisation. During the process of IS Audit, due importance should be given to compliance of all the applicable legal and statutory requirements.	Audit Committee. The internal audit framework should specifically provide for IS Audit. Use of external agency to conduct IS Audit continues to be available as an option for the Company.
	ACB should review critical issues related to IT/ Information Security/ cybersecurity and provide appropriate direction and guidance to management.		
	Separate IS Audit function within internal audit.	Integral part of internal audit.	
	May use external resources for IS Audit but overall ownership and responsibility remain with internal audit function - audit planning, risk assessment and follow up of compliances.	In case of inadequate internal skills, NBFCs may appoint an outside agency having enough expertise in the area of IT/ IS audit for such purpose.	
	IS Auditors shall act independently of RE's management.	IS Auditors should act independently of NBFCs' Management both in attitude and appearance. In case of engagement of external professional service providers, independence and accountability issues may be properly addressed.	
	IS Audit planning should use risk-based approach	NBFCs shall adopt a proper mix of manual techniques and CAATs for conducting IS Audit.	The new IT Directions focus on the Audit approach (risk-based) rather than the technique used. Adoption of continuous audit for critical systems recommended in the new IT Directions.

	May consider, wherever possible, continuous audit approach - control and risk assessment on a more frequent basis - for critical systems.	Periodicity of IS audit should ideally be based on the size and operations of the NBFC but may be conducted at least once in a year	Adoption of continuous audit for critical systems recommended in the new IT Directions.

Conclusion

As we had stated in our assessment of the draft guidelines, the new IT Directions have been introduced at an inflection point of technology adoption and innovation in the financial services space and these guidelines direct specific focus on project and change management, IT capacity planning and technology refresh plans. Adoption of information technology best practices based on international standards now becomes a mandate. The CISO becomes an important officer tasked with ensuring information security alongside the ISC. Operationally, the IT Steering Committee gains prominence beyond providing IT project oversight and monitoring and its responsibilities are extended to overseeing and implementing a framework for BCP/ DRM, information technology related compliances and assisting the Board/ ITSC in strategic IT planning, monitoring IT performance, and aligning IT activities with business needs.

About Vinod Kothari Consultants

Vinod Kothari Consultants Private Limited (VKCPL) is a company focused on providing consulting services, in diverse financial fields including non-banking-financial-services, housing finance, housing microfinance, mortgage lending, securitisation, green financing, asset backed financing, corporate finance etc. VKCPL has been in existence for more than 35 years, and is currently operating out of offices in Kolkata, Mumbai, Delhi and Bengaluru, with a specialised team consisting of CMAs, CAs and company secretaries. In the specialised fields of financial services such as securitization, housing finance, asset-backed financing, etc. VKCPL has had some of India's top companies and banks/ NBFCs as its clients. It has also been associated with multilateral organisations like World Bank, International Finance Corporation and Asian Development Bank.

Apart from consulting, we have also been quite active in the field of financial training; we have been imparting specialised training workshops all over the world. Among the unique strengths of VKCPL, is the ability to put together a multi-faceted team of corporate professionals, to handle an assignment from a range of relevant and diverse perspectives - taxation, accounting, legal and financial. We value and put emphasis on research. We regularly write for top journals and put together industry reports and reviews. Moreover, we also publish books, some of which have gone on to become canonical works in their subject areas.

To Get in Touch with Us on Social Media