Draft Master Direction on IT Governance, Risk, Controls and Assurance Practices

An analysis of its impact on NBFCs

– Team Finserv, Vinod Kothari Consultants | finserv@vinodkothari.com

Table of Contents

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 30 years, and is currently operating out of offices in Kolkata, Mumbai and Delhi, 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.

Copyright and Disclaimer

No part of this article is intended to be professional advice, or solicitation of professional assignment.

Introduction

On October 20, 2022, the RBI published the ***Draft Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices*** ('Draft IT Directions')[1]. These Draft IT Directions follow the publication of the ***Draft Master Direction on Outsourcing of IT Services*** ('Draft IT Outsourcing Directions') on June 23, 2022. Both of these proposed directions had found a mention in the RBI's ***Statement on Developmental and Regulatory Policies (February 2022)[2].***

While NBFCs are currently subject to Information technology regulations that are specific to them, the draft directions look at providing an unified regulatory framework for Banks, AIFIs, CICs and NBFCs (other than base layer NBFCs). This is largely in line with what we are observing for the rest of the scale-based regulations with top, upper and middle level NBFCs being subjected to similar regulatory rigour as commercial banks. While these regulations will have an appreciable impact on the specified NBFCs, they will be particularly of interest for NBFCs offering/ intending to offer digital lending[3] products and those mandated to implement a core financial services solution (CFSS)[4].

In this article we compare the Draft IT Directions with the information technology guidelines[5] that currently exist for NBFCs and construct a 'to-do' list that arise from it.

Overview of the Changes

These draft directions cover the overall IT function of the specified NBFCs 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, these directions put the responsibility on the CEO to institute effective oversight on the planning and execution of IT Strategy. The CEO is also mandated to put 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 proposed 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 Operations. The draft directions, however, call for designating a sufficiently senior level executive of the NBFC as the Chief Information Security officer (CISO) who will be responsible for driving information/ cyber security, ensuring compliance to related regulatory guidelines, enforcing policies of the NBFC used to protect information

[1] https://rbidocs.rbi.org.in/rdocs/Content/PDFs/DRAFTITGPRACTICESE5785D2C27CC41FAB3F5E426F4DB3FBD.PDF

[2] https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=53248

[3] Read our FAQs on the RBI Digital lending Guidelines for NBFCs here - https://vinodkothari.com/2022/08/faqs-on-digital-lending-regulations

[4] Read our Article on the Core Financial Services Solution for NBFC here - https://vinodkothari.com/2022/06/exploring-core-financial-services-solution-for-nbfcs/

[5] https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD53E0706201769D6B56245D7457395560CFE72517E0C.PDF

assets and managing and coordinating information/ cyber security related issues/ implementation within the NBFC as well as with relevant external agencies.

From a high level perspective, the Draft IT Directions appear to delve into greater granularity and detail whereas the existing guidelines were more broad-based and referred to tenets and principles. The Draft IT Guidelines prescribe adoption of a number of procedures, process and methodologies (some recommendatory) like IT Strategic Planning, IT Standard Operating Procedures (SOP), Service Level Management (SLM), formal product approval and quality assurance process (for new IT based business products), Change Management procedure, SOP to identify "critical information infrastructure", scorecard/ metrics and methodology to measure IT performance and maturity level, DR architecture and procedures, standardised checklist of IS Audit, etc.

The RBI has anticipated that we are at an inflection point of technology adoption and innovation in the financial services space and the draft guidelines direct specific focus on project and change management, IT capacity planning and technology refresh plans. The proposed directions go on to recommend adoption of standard enterprise architecture planning methodology/ framework (for adoption of new technology) and security standards/ IT control frameworks (like the ISO 27001) for critical functions. 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/ IT Strategy Committee in strategic IT planning, monitoring IT performance, and aligning IT activities with business needs.

List of Committees

Committee	Constitution	Meeting Frequency (minimum)
IT Strategy Committee (ITSC)	Board Level	Quarterly
IT Steering Committee	Not specified	Not specified
Information Security Committee (ISC)	Under the oversight of the RMC	Not specified

Under the Draft IT Directions, the Risk Management Committee (RMC) and Audit Committee (ACB) also play a significant role in NBFCs 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	Board	Annual
Information Systems (IS)	Board	Annual
Business Continuity	Board	Annual
Information Security	Board	Annual
Cyber Security (incl. Incident Response and Recovery Management/ Cyber Crisis Management)	Board	Annual
Enterprise-wide risk management policy/ operational risk management policy needs to incorporate IT-related risks	RMC	Annual
Data Migration	Not specified	Not specified
IS Audit	Audit Committee of Board	Annual

List of Assessments/ Reviews and Testing

Area	Undertaken/ Reviewed by	Frequency (minimum)
IT risk assessment	IT Security Committee (ISC)	Not specified (will depend on policy and standard adopted)
Review of cyber security risks/ arrangements/ preparedness	CISO and reviewed by the Board (or Board level Committee)	Quarterly
IT training requirement/ effectiveness	Head of IT Operations	Not specified
IT vendor risk assessment and controls	Not specified	Not specified
Capacity assessment	Reviewed by Board or ITSC	Annual
Review of security infrastructure	Not specified	Annual

Area	Undertaken/ Reviewed by	Frequency (minimum)
Vulnerability testing (VT)/ Penetration testing (PT)	Should be conducted by appropriately trained and independent information security experts/ auditors	Throughout the lifecycle (pre-implementation, post implementation, after major changes, etc.) of IT Assets (refer to 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 at least on a yearly basis
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 Draft IT Directions is Management Information Systems (MIS). Whereas the existing 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 the Draft IT Guidelines.

Comparison of Draft IT Directions with existing Guidelines

Para no.	Draft Provision	Existing provision	Comments/ Action needed
Chapter I - Preliminary			
3	The Draft IT Directions apply to Scheduled Commercial Banks (excluding RRBs), Small Finance Banks, Payments Banks, all NBFCs (in the Top, Upper and Middle Layers), All India Financial Institutions and Credit Information Companies.	Separate guidelines were prescribed by the RBI for NBFCs and Banks. The existing NBFC specific Guidelines will continue to apply to Base Layer NBFCs once the Draft IT Directions become effective	-
Chapter II - IT Governance			
5	An IT Governance Framework is required to put in place, which shall comprise:	Guidelines on governance were on similar lines although there are more specific prescriptions made for certain areas as indicated below.	

Para no.	Draft Provision	Existing provision	Comments/ Action needed
	● 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.		
6	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.	Existing directions call for adoption the below list of Policies - ● IT Policy, ● Information Security/ Cybersecurity Policy, ● Change Management policy, ● IS Audit Policy, ● BCP Policy, ● IT Services Outsourcing Policy.	List of Board approved policy areas remain on the same lines, however, content of existing Policies will need to be reviewed and updated.
7	REs are required to establish a Board-level IT Strategy Committee (ITSC)	Existing directions also require constituting a 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 Draft IT Guidelines extend the remit of the ITSC as noted below
	Composition - Minimum of two directors as members. At least one member should have substantial expertise in managing/ guiding technology initiatives.	Composition - Should have a chairman who is an independent director (ID); CIO & CTO should be a part of the committee.	Requirement for an ID to preside over the the ITSC is done away with
	The IT Strategy Committee shall meet at least on a quarterly basis.	The IT Strategy Committee should meet at an appropriate frequency but not	Frequency of ITSC meetings increases under the Draft IT Directions

Para no.	Draft Provision	Existing provision	Comments/ Action needed
		more than six months should elapse between two meetings.	
8	The Board/ IT Strategy Committee 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; ● 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	The ToR was on similar but narrower lines. The existing 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 draft directions do not explicitly specify this, budgetary controls are to be exercised by the IT Strategy Committee.	The Draft IT Directions additionally require the IT Strategy Committee to monitor BCP and DR. While the existing guidelines put the ITSC's focus on IT capex activity under the draft IT Directions their remit covers operation aspects as well.
9	CEO shall have the overall responsibility and should institute an effective oversight on the plan and execution of IT Strategy; The CEO 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.	No such responsibilities on the CEO. The said responsibilities were rather on the Board and Senior Management	While the Board remains ultimately responsible, onus has been put on the CEO to ensure operational effectiveness of the NBFC's IT Strategy.

Para no.	Draft Provision	Existing provision	Comments/ Action needed
10	REs shall establish an IT Steering Committee	Existing directions also call for constituting a steering committee for operating at an executive level and focusing on priority setting, resource allocation and project tracking.	
	The IT Steering Committee should have representation at Senior Management level from IT, business functions for assisting the Board/ IT Strategy Committee in the implementation of the IT Policy and IT Strategy.	The existing directions require 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 Board/ ITSC in strategic IT planning, oversight of IT performance, and aligning IT activities with business needs; ● Update Board/ IT Strategy Committee and CEO periodically on its activities; ● Oversee the BCP process including determining how it will manage and control identified risks as well as prioritise critical business functions; ● Put in place a framework/ mechanism for effective DRM; ● Define IT project success measures and follow up progress on IT projects; ● Ensure compliance with technology standards and guidelines; and ● Ensure implementation of a robust IT architecture meeting statutory and regulatory compliance	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 project, including deliverables to be realised at each phase of the project and milestones to be reached according to the project timetable.	The Committee's role has been extended from merely being project specific to setting general standards for IT projects, ensuring compliance with technology standards, ensuring effective implementation of the IT infrastructure, advising the Board/ ITSC 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.
	Appoint/ designate a sufficiently senior level, technically competent and experienced in IT related aspects as Head of IT Operations (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 draft directions do not call for the additional CTO role.
	Responsibilities of Head of IT Operations -	Chief Information Officer (CIO)/ in-	Responsibilities of the Head

Para no.	Draft Provision	Existing provision	Comments/ Action needed
	● Ensure implementation of IT Policy, IT Strategy and Vision of the RE; ● Put in place documented IT Standard Operating Procedures; ● Ensure that the execution of IT projects/ initiatives is aligned with the RE's IT Policy and IT Strategy; ● Implement and manage suitable IT architecture that efficiently supports existing as well as future IT capabilities needed by the business; ● 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. ● Ensuring adherence to extant instructions on Outsourcing of IT activities	Charge of IT operations responsibilities were on similar lines. In the existing 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.	of IT Operations are extended in the Draft IT Directions. Responsibilities of the Head of IT Operations are extended in the Draft IT Directions.
13	The Head of IT Operations shall also have additional responsibility - assessment of training requirements of human resources. There should be a documented and tracked training plan/ programme for periodic training/ awareness workshops for the ● Board, ● Senior Management, ● CxOs, ● Members of the IT Function and ● Other employees	Requirements on the same lines NBFCs need to maintain an updated status on user training and awareness relating to information security Not explicitly placed responsibility on the in-Charge of IT Operations	
Chapter III - IT Infrastructure and Service Management			
14	Establish a robust IT Service Management Framework	The existing IT Directions do not contain specific guidelines in this area. However, tenets and principles applicable to the IT Policy/ Governance	

Para no.	Draft Provision	Existing provision	Comments/ Action needed
		Framework will apply to IT Service Management as well.	
15	Put in place a Service Level Management (SLM) process - manage the IT operations and ensure segregation of duties	The existing directions also call 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 Draft IT Directions.
16	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 are 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 toDraft Technology Refresh Plan. The intention of the RBI here is to make REs anticipate and be proactive in making technology/ capacity upgrades.
17	Ensure clock/ time synchronisation between all its IT systems using appropriate protocols.	No such specific provision.	This should already be ensured as part of good IT practice, the RBI's explicit inclusion of this provision highlights in the current digital era a single transaction takes place across multiple integrated systems which need to be coordinated in time.
18	For Third-party arrangement in the Information Technology/ Cyber Security ecosystem that are not considered "outsourcing of IT Services, or, not considered "material" outsourcing of IT Services, the draft 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	Existing IT Directions do 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 incorporate such a framework if not already covered.

Para no.	Draft Provision	Existing provision	Comments/ Action needed
	● Comply with applicable legal, regulatory requirements and standards to protect customer data ● Provide high availability ● Manage supply chain risks effectively ● REs may consider applying the instructions provided in “Master Direction on Outsourcing of IT Services” to their non-material IT outsourcing also, if felt necessary, depending upon the risk perceived.		
19, 20	Capacity Management - Annual assessment of capacity compared to past trends (peak usage), current as well as planned business activities along with sufficient safety Assessment to be reviewed by Board/ IT Strategy Committee	Existing Directions call 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 Board/ ITSC.
21	IT Capacity Planning - across all components, services, system resources, supporting infrastructure shall be consistent with the current business requirements and projected future needs as per the IT strategy of the RE. IT systems and infrastructure are able to support business functions and ensure availability of all service delivery channels.	Existing Direction do not prescribe specifically for such a process	IT Capacity planning of which capacity assessment process is a part needs to be put into place.
22	Project Management - Adopt standard enterprise architecture planning methodology/ framework - for adopting new technology. Emerging technology adoption should be commensurate with the risk appetite and align with overall business/ IT strategy.	The existing directions contain guidelines with regard to 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.
	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 existing 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).

Para no.	Draft Provision	Existing provision	Comments/ Action needed
23	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.	Monitoring of project progress is currently placed on the shoulders of the IT Steering Committee. Specific prescription to formally define a project management approach not in existing Directions.	Develop/ adopt a formally defined project management approach.
24	IT projects to undergo appropriate strategic and cost/ reward analysis on a periodic basis. Projects having significant impact on the RE's risk profile and strategy shall be reported to the IT Strategy Committee	As mentioned above, the IT Steering Committee was tasked with providing oversight and monitoring of the progress of the project, including deliverables to be realised at each phase of the project and milestones to be reached according to the project timetable.	ITSC also becomes a part of the project tracking process for projects having significant impact on the RE's risk profile and strategy.
25	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 updates and programme fixes are also included in the escrow agreement.	No such specific prescription	Specified NBFCs will not put such an arrangement in place.
	If the code is not owned by the RE, then, the RE shall obtain a certificate from the application developer stating that the application is free of known vulnerabilities, malwares and any covert channels in the code.	No such specific prescription	Specified NBFCs will not put such an arrangement in place.
26	New IT application proposed to be introduced as a business product should undergo - ● Formal product approval ● Quality assurance process ● Assessment of functionality, security, performance related aspects and compliance to relevant legal and regulatory prescriptions. ● Assurance of high availability and fault tolerance requirements	Similar guidelines were provided as part of the Change Management Policy of the NBFC developed with approval of the Board Additionally, the existing 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.
27, 28	Change Management procedure -	As mentioned above, under the current directions, NBFCs are expected to develop, with the approval of their	Mandates the requirement to have a test environment to evaluate patches before

Para no.	Draft Provision	Existing provision	Comments/ Action needed
	● 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.	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.	being applied to the live environment.
29	Data Migration Controls - 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 sign-offs from business users/ application owners at each stage of migration, audit trails etc.	No such specific provision	Documented data migration policy will need to be put into place. This provision becomes especially significant for specified NBFCs required to implement CFSS.
30	Outsourcing of IT Services continue to be guided by Master Direction on Outsourcing of IT Services	Existing Directions included provisions related to IT Services Outsourcing	Specified NBFC will need to comply with Draft IT Outsourcing Master Directions once they come into effect.
31	Audit Trail should be maintained for every application which can affect critical/ sensitive data, capturing - ● Transaction id ● Timestamp (date, time) ● Originator id ● Authoriser id ● Action taken ● Other details - IP address of client machine, terminal identity/ location, wherever applicable	As per the current directions IT Policy of 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 Draft IT Directions. Specified NBFCs will need to ensure that their current systems capture such data.

Para no.	Draft Provision	Existing provision	Comments/ Action needed
32	IT Policy should articulate preservation period of such audit trails/ logs considering regulatory and legal requirements	Existing directions do not make a mention of preservation period	The IT Policy will need to specifically provide for a preservation period for audit trail/ logs.
33	Audit trail should serve to facilitate conduct of audit, serve as forensic evidence, dispute resolution, including for non-repudiation purposes	Existing directions are on similar lines	
	REs need to put in place effective log management and retention framework - tools to manage, collect and store system and application logs that would facilitate incident investigation and analysis	Existing directions do not explicitly specify such a framework requirement	Specified NBFCs will need to put in place a log management and retention framework.
Chapter IV - IT Risk and Information Security			
34	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	The Board or Senior Management 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 explicitly tasked with overseeing the IT risk management and integrating it with the RE's risk management policy.
	Guidelines with regard to Outsourcing of IT function are provided separately under Draft IT Outsourcing Directions.	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.	
35	Establish a robust risk management framework involving - ● Identification of the RE's IT assets and their security classification based on their criticality to the RE's operations; ● Periodic Risk Assessment; ● Implementation of a comprehensive information security function; ● Periodic review of internal controls and processes; ● Define roles and responsibilities of stakeholders (including third-party personnel) involved in risk	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.	Under the Draft IT Directions, Risk Assessment should be reviewed by the ISC. Identification of "crown jewels" and "critical information infrastructure" required. Under the existing guidelines, such identification would have been required in the context of of BCP/ DRM

Para no.	Draft Provision	Existing provision	Comments/ Action needed
	management. Areas of conflict and accountability gaps must be specifically identified; - Identify "Crown Jewels" - information systems that are most critical to the accomplishment of an organisation's objectives - and fortification the security environment of such systems; - Identify "Critical Information Infrastructure" - and evolve standard operating procedures in identifying and protecting such systems/ group of systems.	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	(critical business processes, critical business verticals, locations and shared resources, critical business systems and data centres).
36	Define metrics for each IT system/ service/ application in terms of system performance, recovery and business resumption - recovery point of objective (RPO) and recovery time objective (RTO)	No such specific provision	Specified NBFCs need to put in place such metrics.
37	Implement appropriate scorecard/ metrics/ methodology to measure IT performance and IT maturity level.	No such specific provision	Specified NBFCs need to formulate such a methodology.
38	Board to establish necessary organisational processes/ functions for information security. Information Security Policy should include - - Alignment with business objectives - Objective, scope, ownership and responsibility for the Policy - Information security organisation structure - Information security roles and responsibilities - Exceptions - Knowledge and skill sets required - Periodic training and continuous professional education - Compliance review - Penal measures for non-compliance with Policy	Current Directions provide information security tenets - confidentiality, integrity, availability and authenticity - that should guide NBFCs. 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 actually 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.	Specified NBFCs need to review whether their current IT/ IS policies.

Para no.	Draft Provision	Existing provision	Comments/ Action needed
	REs shall also put in place a Cyber Security Policy.	Board approved cybersecurity policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk Vulnerability management strategy should be part of Cyber Security Policy	
	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.	Existing guidelines also contain requirements for putting in place such a Plan.	
39	Information Security Committee (ISC) should be created under the oversight of the RMC 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 RMC) • Representative from IT Function (decided by the RMC)	No such requirement	
	Responsibilities of the ISC shall include - • Approving / monitoring security projects • Approving / monitoring security plans/ budgets • Establishing priorities • Approving standards and procedures • Supporting development/ Implementation of information security management programme • Reviewing information/ cyber security incidents	No such requirement	

Para no.	Draft Provision	Existing provision	Comments/ Action needed
	● Reviewing security assessments, monitoring and mitigation activities ● Reviewing security awareness programs ● Assessing new developments/ issues related to information/ cyber security ● Reporting to Board/ Board level Committee on information security activities		
40	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	No such requirement	Specified NBFCs will need to appoint CISO.
41	CISO responsibilities should be clearly defined and documented, and should include - ● Driving and ensuring compliance to regulatory requirements; ● Enforcing RE policy within the NBFC as well as relevant external agencies; ● Preparedness to threats; ● Attend ITSC meeting and IT Steering Committee meetings; ● Manage and monitor Security Operations Centre (SOC) and drive security related projects; ● Coordinate activities wrt cybersecurity, incident Response Team (CSIRT) within the RE; ● Prepare cyber security KRIs and KPIs; ● Maintain working relationship with CRO to Enable holistic risk management approach.	No such requirement	

Para no.	Draft Provision	Existing provision	Comments/ Action needed
	The CISO may be invited to Information Security Committee (where IT/ Information risk discussed) Separately review cyber security risks/ arrangements/ preparedness and place before Board/ Board level Committee at a quarterly basis		
42 to 49	Information Security Management - ● REs should consider implementing security standards/ IT control frameworks (such as ISO 27001) for their critical functions; ● Privacy related safeguards as mandated under different laws should be built into the information systems; ● 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; ● Encryption standards - Data transfers from one process to another/ application to another, particularly with respect to critical or financial application, - 'straight through processing' without any possibility of intervention.	Existing directions call for creating a 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 existing directions.	
50, 51	Implement physical/ environmental controls across DC and DR sites DC and DR should be geographically well separated so that both site are not affected by similar threats DC and DR monitored through CCTV	Existing Direction contains requirements on similar lines. Requirement to install CCTV not present.	NBFCs may be required to install additional security hardware/ systems.

Para no.	Draft Provision	Existing provision	Comments/ Action needed
52, 53	Access Control ● Documented standards/ procedure approved by the appropriate authority and kept up to date, for administering need based access ● Personnel with elevated system access entitlements - closely supervised, all system activities logged and periodically reviewed ● Privileged users should adopt multi-factor authentication	Existing directions require the IT Policy of NBFCs to put in role based access controls and effective segregation of functions between the IT security and operations divisions. Requirement of multi-factor authentication (MFA) not present in existing directions.	Greater formal rigour prescribed.
54	Controls on teleworking - ● Secure (encrypted) connection should be assured from Alternate Work Location (AWL) to environment hosting RE's information assets ● Multi-factor authentication (MFA) for enterprise access to critical systems ● Mechanism to identify all remote access devices attached/ connected to RE's systems ● Where remote access is not provided, teleworking should also be secured appropriately depending on sensitivity of data/ information shared/ handled.	Specific prescriptions for teleworking not present in the existing directions. Will follow general IT/ cyber security guidelines and the NBFC IT/ security policies	With 'remote work' becoming more prevalent in the post pandemic era, formalising an adequate IT framework for such teleworking is now called for.
55	Vulnerability Testing (VA)/ Penetration Testing (PT) by appropriately trained and independent information security experts/ auditors prescribed.	Current directions provide requirements to assess vulnerability and take remedial measures. Master Direction - Know Your Customer (KYC) Direction, 2016 ("KYC Master Directions")[6] contains requirements to perform vulnerability assessment and penetration testing to 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 Draft IT Guidelines.

[6] *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

Para no.	Draft Provision	Existing provision	Comments/ Action needed
	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 all other IT assets or any new IT infrastructure/ application or when an existing application has undergone major change - based on criticality and inherent risk as defined by the RE.	No such specific provision	
56 to 59	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; ● REs may also run automated scanning tools on all systems on the network that are critical, public-facing or store sensitive customer data on a continuous/ more frequent basis; ● All vulnerability scanning in authenticated mode.	No such specific provision	
60, 61	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	

Para no.	Draft Provision	Existing provision	Comments/ Action needed
62	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.
63	Definition of incident - *… any event or the threat of such an event adversely impacting the confidentiality, integrity and/ or availability of* ● *information assets of the RE and/ or* ● *the physical infrastructure and/ or* ● *environment hosting the information assets of the RE.*	Left to Information Security Policy to define.	
64 to 69	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 reg. Cyber security incidents as per regulatory requirements; ● 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, ● Conduct of tests and drills BCP/ DR capabilities should be designed to effectively support its resilience objectives, enable it to recovers and securely resume its critical operations	Current guidelines require sharing of information on cybersecurity incidents with RBI. The list of relevant cyber security incidents are specified in the CSIR Form of Annex I .[7]	

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

Para no.	Draft Provision	Existing provision	Comments/ Action needed
Chapter V - Business Continuity and DRM			
70	BCP/ policy shall adopt best practices based on international standards (e.g. ISO 22301). Policy shall be updated on major developments/ risk assessments. Ensure business continuity even in the event of unforeseen disruptive incidents.	NBFCs 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.	
71	Undertake Business Impact Analysis/ assessment of likelihood of adverse event and assess impact on information assets and business operations	NBFCs shall first identify critical business verticals, locations and shared resources to come up with the detailed Business Impact Analysis. The process will envisage the impact of any unforeseen natural or man-made disasters on the NBFC's business. The entity shall clearly list the business impact areas in order of priority.	
72	Regularly test BCP - all possible types of contingencies and relevant aspects and constituents - people, processes and resources (incl technology)	NBFCs shall 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.	
73	Disaster Recovery Management DR drills critical systems - at least on a half-yearly basis Others - yearly basis	No specific requirement to perform DR drills	DR drills
74	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	Does not specify steps at such a granularity	Specified NBFCs will need to review their existing DR testing process.

Para no.	Draft Provision	Existing provision	Comments/ Action needed
	working day (including BoD and EoD operations) are covered; ● Securely backup data and periodically restore backed-up-data to check usability.		
75, 76	Ensure DR architecture and procedures are robust meeting the defined RTO and RPO criteria In case of non-zero RPO, documented methodology for recon of data	Requirement to specify RTO and RPO not provided under existing directions	
77	Security patches at DC and DR are identical	No such specific requirement	The Draft IT Directions call for greater alignment of the DR environment with DC.
78	BCP and DR capabilities in critical interconnected systems and networks including those of vendors and partners. Collaborative and co-ordinated resilience testing	Provisions on IT Outsourcing in the current directions require NBFCs to ensure that their business continuity preparedness is not adversely compromised on account of outsourcing. However, does not go to the extent of requiring co-ordinated testing	Co-ordinated testing with relevant vendors and partners called for in the Draft IT Directions.
Chapter VI - Information System (IS) Audit			
79	Audit Committee/ Local Management Committee (LMC) (in case of foreign banks) 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 Draft IT Directions. Such reviewed Framework/ Policy may be approved and adopted by the Company's Audit Committee.
80	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 should cover effectiveness of policy and oversight of IT systems, evaluating adequacy of processes and internal controls, 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.	

Para no.	Draft Provision	Existing provision	Comments/ Action needed
		During the process of IS Audit, due importance shall be given to compliance of all the applicable legal and statutory requirements.	
81	Audit Committee/ LMC review critical issues related to IT/ Information Security/ cybersecurity and provide appropriate direction and guidance to management.		
82	Separate IS Audit function within internal audit.	Integral part of internal audit.	The internal audit framework should specifically provide for IS 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.	Use of external agency to conduct IS Audit continues to be available as an option for the Company.
83	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.	
84	Risk-based audit approach in line with extant regulatory instructions on risk-based internal audit.	NBFCs shall adopt a proper mix of manual techniques and CAATs for conducting IS Audit.	The Draft IT Directions focus on the Audit approach rather than the technique used.
85	May consider, wherever possible, continuous audit approach - control and risk assessment on a more frequent basis - for critical systems May have standardised checklist, scoping document as reference material. Checklist should be updated on regular basis to align with IT practices, regulations systems, vulnerability and threat landscape	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 Draft IT Guidelines.

Para no.	Draft Provision	Existing provision	Comments/ Action needed
86	IS Audit report shall be placed before Senior Management, Audit Committee	The framework should clearly prescribe the reporting framework, whether to the Board/ Committee of the Board (Audit Committee of the Board)	Specific reporting line prescribed.
87	Compliance within time frame outlined in the Audit Policy	NBFCs' management is responsible for deciding the appropriate action to be taken in response to reported observations and recommendations during the IS Audit.	The Draft IT Directions have the expectation that the Company's Policy shall provide for the mitigation action including timeframes for gap identified during the IS Audit

Reach us on social media: