SAMVĀD: PARTNERS

June 22, 2017

NBFCs – TIME TO SPRUCE UP IT FRAMEWORK

In its effort to align the information technology framework of non-banking financial companies ("**NBFC**") with evolving best practices, the Reserve Bank of India ("**RBI**") has issued a Master Direction on June 8, 2017 on the 'Information Technology Framework for the NBFC Sector' ("**Directions**').

These Directions focus on - the governance of information technology ("**IT**") framework, audit of information systems, outsourcing of IT services, business continuity planning and the formulation of IT and cyber security policies for non-deposit taking NBFCs. The primary objective of these Directions are to enhance the safety, security and operational efficiency of NBFCs.

- **Applicability**

  The Directions apply to two categories of non-deposit taking NBFCs:

  - NBFCs with asset size above Rupees 500 crores, i.e. systemically important NBFCs ("**NBFC-SI**").

  - NBFCs with asset size below Rupees 500 crores ("**NBFC-Non SI**").

- **Framework for NBFC-SIs**

  - ***IT Governance and IT Strategy Committee***

    The board of directors and the executive management of an NBFC-SI are responsible for effective IT governance.

    NBFC-SI must constitute an 'IT Strategy Committee', comprising – (a) an independent director (as the chairman); (b) a chief information officer ("**CIO**"); and (c) a chief technical officer ("**CTO**"). The IT Strategy Committee must meet at least twice a year. All deliberations / recommendations of the IT Strategy Committee are to be placed before the board of directors of the NBFC-SI. The functions of the IT Strategy Committee are:

- To approve IT strategies and policy documents of the NBFC-SI.
- To ascertain whether the NBFC-SI's management has implemented processes / practices which ensure that IT delivers value to business.
- To ensure that the budgets allocated *vis-à-vis* IT investments in the NBFC-SI are commensurate in nature.
- To monitor the method that the NBFC-SI's management uses to ascertain the IT resources needed to achieve strategic goals.
- To provide high-level directions for sourcing and use of IT resources.

➢ ***IT Policy***

NBFC-SI is recommended to formulate an 'IT Policy', duly approved by the board of directors of the NBFC-SI. Such IT Policy must contain details of the IT organizational structure of the NBFC-SI, commensurate to its size, scale and nature of operations. As a part of its IT Policy, the NBFC-SI should provide periodic technical training to its middle and senior level employees. All NBFCs-SI are required to migrate to the IPv6 platform, as notified by the Government of India under the National Telecom Policy, 2012.

A senior executive such as the CIO or any officer in-charge of the IT operations of the NBFC-SI should be responsible for the implementation of the IT Policy.

➢ ***Information Security Policy***

NBFC-SI must formulate an 'Information Security Policy' ("**IS Policy**"), duly approved by its board of directors. Such IS Policy must contain details pertaining to:

- Inventory of information assets maintained at the NBFC-SI.
- Segregation of duties of personnel / officers dealing exclusively with the security of information systems and functioning of IT divisions.
- Segregation of responsibilities of personnel / officers dealing with system administration, database administration and transaction processing.
- Providing access to information on well-defined user roles.
- Detailed background check of personnel / officers in charge of privileged / confidential information.
- Implementation of a 'maker-checker system', ensuring the participation of at least two individuals for the completion of critical IT tasks.
- Creation of audit trails for IT assets - facilitating audits and legal due diligences, serving as forensic evidence and assisting in dispute resolution.
- Increase in the usage of public key infrastructure (PKI) - to ensure

confidentiality, access control, data integrity, authentication and nonrepudiation of data.

- ***Cyber Security Policy***

NBFC-SI must formulate a 'Cyber Security Policy', duly approved by its board of directors, in order to – (a) combat cyber threats; and (b) eliminate 'cyber vulnerabilities', caused by a defect / configuration flaw in hardware or software components of the NBFC-SI's IT framework.

- ***Cyber Crisis Management Plan***

An NBFC-SI must formulate a 'Cyber Crisis Management Plan', entailing preventive and corrective measures to be undertaken by the NBFC-SI upon the occurrence of a cyber threat / intrusion.

- ***IT Risk Assessment***

An NBFC-SI must undertake a comprehensive risk assessment of its IT systems, on an annual basis. The assessment should analyze the existent / anticipated threats to the IT assets and the existing security controls and processes of the NBFC-SI. The risk assessment should be brought to the notice of the Chief Risk Officer ("**CRO**"), CIO and the board of directors of the NBFC.

- ***IT Operations and Change Management Policy***

An NBFC-SI must realign its IT systems on a regular basis with the changing needs of its customers and business. For this purpose, an NBFC-SI must formulate a 'Change Management Policy' that addresses the following:

- prioritizing 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.

- ***Information System Audit***

NBFC-SI must adopt an 'Information System Audit Framework', duly approved by its board of directors. Information System Audits ("**IS Audits**") conducted as a part of such Information System Audit Framework must – (a) identify risks and methods to mitigate risks arising out of the IT infrastructure of an NBFC-SI; and (b) evaluate the adequacy of processes and internal controls.

An IS Audit should be conducted at least once a year, either internally, or by an external agency, subject to appropriate background investigations. The reports generated pursuant to an IS Audit should be submitted to the board of directors of the NBFC-SI, or any of the committees thereof, as may be stipulated in the Information System Audit Framework.

NBFC-SI must adopt a proper mix of manual techniques and Computer-Assisted Audit Techniques (CAATs) for conducting IS Audits for critical functions having financial / regulatory / legal implications, such as - detection of revenue leakage, treasury functions and assessing impact of control weaknesses.

- ***Business Continuity Planning***

NBFC-SI must formulate a 'Business Continuity Planning Policy' ("**BCP Policy**"), duly approved by its board of directors. The BCP should aim at minimizing the operational, financial, legal, reputational and other material consequences arising from a disaster / data loss. The CIO shall be responsible for periodic review and monitoring of the BCP.

Such BCP Policy shall be based on certain identified factors, including:

- Business Impact Analysis - Critical business verticals, locations and shared resources of an NBFC-SI must identify the impact of any unforeseen natural or man-made disaster on the business of the NBFC-SI (in order of priority).
- Recovery Plan / Contingency Plan - An NBFC-SI must analyze various flaws / vulnerabilities caused due to inter-dependence between various systems, departments and business processes. Based on such analysis, the BCP should identify future failure scenarios, and accordingly suggest cost-effective and practical strategies to minimize losses in case of such disasters / failures.
- Review - An NBFC-SI must review the BCP either annually, or upon the occurrence of a significant IT or business changes. The results of such review should be placed before the CIO, or the board of directors of the NBFC-SI.

- ***IT Services Outsourcing***

NBFC-SI may enter into outsourcing arrangements with service providers *vis-à-vis* its IT related business, subject to the approval of the board of directors of the NBFC-SI. All outsourcing arrangements with service providers will need to be in the form of duly executed legal contracts. Such legal contracts will need to address the following aspects:

- Continuous monitoring and assessment of the service providers.
- Access to books, records and information available with the service provider relevant to the outsourced activity.
- Right to conduct audits on the service provider, either internally or through external consultants, and obtain copies of any such audit or review reports.

➢ ***Other Directions***

- NBFC-SIs must consider using digital signatures to protect the authenticity and integrity of important electronic documents and with respect to high value funds transfer.
- NBFC-SIs must conduct regular user trainings and information security awareness programs.
- With respect to NBFC-SIs using mobile financial services, the Directions suggest that an appropriate mechanism be devised to provide end-to-end encryption of information assets that are used by mobile applications to provide services to customers.
- With respect to NBFC-SIs using social media to market their products, the Directions suggest that an appropriate mechanism be devised to deal with risks such as account takeovers and malware distributions.

- **<u>Framework For NBFC Non-SIs</u>**

NBFC Non-SIs are <u>recommended</u> to formulate an information technology / information system policy, approved by its board of directors. While formulating such information technology / information system policy, NBFC Non-SIs may consider the following:

➢ Implementation of basic security standards - such as physical / logical access controls and a well-defined password policy.
➢ A well-defined user role.
➢ Implementation of the maker-checker concept to reduce the risk of errors and to ensure reliability of information.
➢ Provisions pertaining to information and cyber security.
➢ Safeguards *vis-à-vis* use of mobile financial services and social media, in line with the requirements prescribed for NBFC-SIs in the Directions.
➢ Creation of system generated reports for senior management, containing details *vis-à-vis* financial positions, operating / non-operating revenues and expenses, cost benefit analysis of segments / verticals and cost of funds.
➢ Requirement to file regulatory returns to the RBI.
➢ Business continuity planning (BCP) policy, duly approved by the board of directors of the NBFC Non-SIs and regular review thereof by the board of directors (at least once every year).

- Arrangement for backup of data, with periodic testing thereof.

- **Timelines for Compliance**

  - NBFCs are required to conduct a formal gap analysis between their current framework and the stipulations laid out in the Directions and put in place a time-bound action plan to address the gaps, if any, and comply with the Directions.
  - NBFCs have been recommended to place these Directions, as well as the results of its gap-analysis, before its respective board of directors by September 30, 2017.
  - NBFC-SIs are required to comply with the Directions by June 30, 2018, and NBFC-Non SIs are required to comply with the Directions by September 30, 2018.

Key takeaways: While the Directions impose mandatory obligations on NBFC-SIs to constitute committees / formulate policies (as stipulated therein), the Directions have not emphasized on compliance by NBFC-Non SIs. Also, while the Directions for NBFC-SIs state that certain committees / policies will be monitored by officers designated as – 'chief information officers' and 'chief risk officers', it fails to clarify who is eligible to be so appointed / other conditions in relation thereto. It is to be seen whether such officers are to be appointed externally or internally, as well as the qualifications to be considered for such appointment.

The details pertaining to the Directions are available at:

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

****This is an update for general information purposes only and does not constitute legal advice. Please contact us if you require further clarifications on this subject.***

BENGALURU	CHENNAI	HYDERABAD	MUMBAI	NEW DELHI
+91 80 4268 6000	+91 44 4306 3208	+91 40 6721 6500	+91 22 6104 4000	+91 11 4172 6200

www.samvadpartners.com