RBI/DNBS/2016-17/53

Master Direction DNBS.PPD.No.04/66.15.001/2016-17 June 08, 2017

Master Direction - Information Technology Framework for the NBFC Sector

In exercise of the powers conferred in terms of clause (b) of sub-section (1) of 45-L of the Reserve Bank of India Act, 1934 (Act 2 of 1934), the Reserve Bank of India being satisfied for the purpose of enabling it to regulate the credit system of the country to its advantage it is necessary so to do, hereby issues Master Directions - Information Technology Framework for the NBFC Sector, 2017 hereinafter specified.

Sd/-
(Dr. Sathyan David)
Chief General Manager

Enclosure: Information Technology Framework for NBFC Sector- Directions

INDEX

Introduction:

The NBFC (Non-Banking Finance Company) sector has grown in size and complexity over the years. As the NBFC industry matures and achieves scale, its Information Technology /Information Security (IT/IS) framework, Business continuity planning (BCP), Disaster Recovery (DR) Management, IT audit, etc. must be benchmarked to best practices.

2. Accordingly, directions on IT Framework for the NBFC sector that are expected to enhance safety, security, efficiency in processes leading to benefits for NBFCs and their customers are enclosed. NBFCs may have already implemented or may be implementing some of the requirements indicated in the circular. NBFCs are therefore required to conduct a formal gap analysis between their current status and stipulations as laid out in the circular and put in place a time-bound action plan to address the gap and comply with the guidelines.

3. The focus of the proposed IT framework is on **IT Governance, IT Policy, Information & Cyber Security, IT Operations, IS Audit, Business Continuity Planning and IT Services Outsourcing.** The directions are categorized into two parts, those which are applicable to all NBFCs with asset size above ₹ 500 crore (Considered Systemically Important) are provided in Section-A. Directions for NBFCs with asset size below ₹ 500 crore are provided in Section-B.

4. NBFCs may place these directions before their Board, together with a gap-analysis vis-a-vis the Master Direction and the proposed action by September 30, 2017.

5. NBFCs- Systemically Important shall comply with the Master Directions by June 30, 2018 and other NBFCs (asset size below ₹ 500 crore) shall comply by September 30, 2018.

Section-A

IT GOVERNANCE

1. IT Governance

IT Governance is an integral part of corporate governance. It involves leadership support, organizational structure and processes to ensure that the NBFC's IT sustains and extends business strategies and objectives. Effective IT Governance is the responsibility of the Board of Directors and Executive Management.

Well-defined roles and responsibilities of Board and Senior Management are critical, while implementing IT Governance. Clearly-defined roles enable effective project control. People, when they are aware of others' expectations from them, are able to complete work on time, within budget and to the expected level of quality. IT Governance Stakeholders include: Board of Directors, IT Strategy Committees, CEOs, Business Executives, Chief Information Officers (CIOs), Chief Technology Officers (CTOs), IT Steering Committees (operating at an executive level and focusing on priority setting, resource allocation and project tracking), Chief Risk Officer and Risk Committees.

The basic principles of value delivery, IT Risk Management, IT resource management and performance management must form the basis of governance framework. IT Governance has a continuous life-cycle. It's a process in which IT strategy drives the processes, using resources necessary to execute responsibilities. Given the criticality of the IT, NBFCs may follow relevant aspects of such prudential governance standards that have found acceptability in the finance industry.

1.1 IT Strategy Committee: NBFCs are required to form an IT Strategy Committee. The chairman of the committee shall be an independent director and CIO & CTO should be a part of the committee**.** The IT Strategy Committee should meet at an appropriate frequency but not more than six months should elapse between two meetings. The Committee shall work in partnership with other Board committees and Senior Management to provide input to them. It will also 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.

1.2 Roles and Responsibilities of IT Strategy Committee: Some of the roles and responsibilities include:

- Approving IT strategy and policy documents and ensuring that the management has put an effective strategic planning process in place;
- Ascertaining that management has implemented processes and practices that ensure that the IT delivers value to the business;

- Ensuring IT investments represent a balance of risks and benefits and that budgets are acceptable;
- Monitoring 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;
- Ensuring proper balance of IT investments for sustaining NBFC's growth and becoming aware about exposure towards IT risks and controls.

IT POLICY

2. NBFCs may formulate a Board approved IT policy, in line with the objectives of their organisation comprising the following:

a) An IT organizational structure commensurate with the size, scale and nature of business activities carried out by the NBFC;

b) NBFCs may designate a senior executive as the Chief Information Officer (CIO) or in-Charge of IT operations whose responsibility is to **ensure implementation of IT Policy to the operational level involving IT strategy, value delivery, risk management and IT resource management**.

c) To ensure technical competence at senior/middle level management of NBFC, periodic assessment of the IT training requirements should be formulated to ensure that sufficient, competent and capable human resources are available.

d) The NBFCs which are currently not using IPv6 platform should migrate to the same as per National Telecom Policy issued by the Government of India in 2012. (As per Circular DNBS(Inf.).CC.No 309/24.01.022/2012-13 November 08, 2012)

INFORMATION AND CYBER SECURITY

3. Information Security

Information is an asset to all NBFCs and Information Security (IS) refers to the protection of these assets in order to achieve organizational goals. The purpose of IS is to control access to sensitive information, ensuring use only by legitimate users so that data cannot be read or compromised without proper authorization. NBFCs must have a board approved IS Policy with the following basic tenets:

a) Confidentiality – Ensuring access to sensitive data to authorized users only.

b) Integrity – Ensuring accuracy and reliability of information by ensuring that there is no modification without authorization.

c) Availability – Ensuring that uninterrupted data is available to users when it is needed.

d) Authenticity – For IS it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine.

3.1 The IS Policy must provide for a IS framework with the following basic tenets:

a) **Identification and Classification of Information Assets**. NBFCs shall maintain detailed inventory of Information Asset with distinct and clear identification of the asset.

b) **Segregation of functions**: There should be segregation of the duties of the Security Officer/Group (both physical security as well as cyber security) dealing exclusively with information systems security and the Information Technology division which actually implements the computer systems. The information security function should be adequately resourced in terms of the number of staff, level of skill and tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, etc. Further, there should be a clear segregation of responsibilities relating to system administration, database administration and transaction processing.

c) **Role based Access Control** – Access to information should be based on well-defined user roles (system administrator, user manager, application owner etc.), NBFCs shall avoid dependence on one or few persons for a particular job. There should be clear delegation of authority for right to upgrade/change user profiles and permissions and also key business parameters (eg. interest rates) which should be documented.

d) **Personnel Security** - A few authorized application owners/users may have intimate knowledge of financial institution processes and they pose potential threat to systems and data. NBFC should have a process of appropriate check and balance in this regard. Personnel with privileged access like system administrator, cyber security personnel, etc should be subject to rigorous background check and screening.

e) **Physical Security** - The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. NBFCs need to create a secured environment for physical security of IS Assets such as secure location of critical data, restricted access to sensitive areas like data center etc.

f) **Maker-checker** is one of the important principles of authorization in the information systems of financial entities. For each transaction, there must be at least two individuals necessary for its completion as this will reduce the risk of error and will ensure reliability of information.

g) **Incident Management -** The IS Policy should define what constitutes an incident. NBFCs shall develop and implement processes for preventing, detecting, analysing and responding to information security incidents.

h) **Trails-** NBFCs 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. If an employee, for instance, attempts to access an unauthorized section, this improper activity should be recorded in the audit trail.

i) **Public Key Infrastructure (PKI) -** NBFCs may increase the usage of PKI to ensure confidentiality of data, access control, data integrity, authentication and nonrepudiation.

3.2 Cyber Security

Need for a Board approved Cyber-security Policy

NBFCs should put in place a cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk, duly approved by their Board. NBFCs should review the organisational arrangements so that the security concerns are appreciated, receive adequate attention and get escalated to appropriate levels in the hierarchy to enable quick action.

3.3 Vulnerability Management

A vulnerability can be defined as an inherent configuration flaw in an organization's information technology base, whether hardware or software, which can be exploited by a third party to gather sensitive information regarding the organization. Vulnerability management is an ongoing process to determine the process of eliminating or mitigating vulnerabilities based upon the risk and cost associated with the vulnerabilities. NBFCs may devise a strategy for managing and eliminating vulnerabilities and such strategy may clearly be communicated in the Cyber Security policy.

3.4 Cyber security preparedness indicators

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

3.5 Cyber Crisis Management Plan

A Cyber Crisis Management Plan (CCMP) should be immediately evolved and should be a part of the overall Board approved strategy. CCMP should address the following four aspects: (i) Detection (ii) Response (iii) Recovery and (iv) Containment. NBFCs need to take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond / recover / contain the fall out. NBFCs are expected to be well prepared to face emerging cyber-threats such as 'zero-day' attacks, remote access threats, and targeted attacks. Among other things, NBFCs should take necessary preventive and corrective measures in addressing various types of cyber threats including, but not limited to, denial of service, distributed denial of services (DDoS), ransom-ware / crypto ware, destructive malware, business email

frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, password related frauds, etc.

3.6 Sharing of information on cyber-security incidents with RBI

NBFCs are required to report all types of unusual security incidents as specified in point No. 2 of Annex I which deals with Basic Information including Cyber Security Incidents as specified in CSIR Form of Annex I (both the successful as well as the attempted incidents which did not fructify) to the DNBS Central Office, Mumbai. The other particulars of the reporting have been provided in template as per Annex I.

3.7 Cyber-security awareness among stakeholders / Top Management / Board

It should be realized that managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This will require a high level of awareness among staff at all levels. Top Management and Board should also have a fair degree of awareness of the fine nuances of the threats and appropriate familiarisation may be organized. NBFCs should proactively promote, among their customers, vendors, service providers and other relevant stakeholders an understanding of their cyber resilience objectives, and require and ensure appropriate action to support their synchronised implementation and testing.

3.8 Digital Signatures

A Digital Signature Certificate authenticates entity's identity electronically. It also provides a high level of security for online transactions by ensuring absolute privacy of the information exchanged using a Digital Signature Certificate. NBFCs may consider use of Digital signatures to protect the authenticity and integrity of important electronic documents and also for high value fund transfer.

3.9 IT Risk Assessment

NBFCs should undertake a comprehensive risk assessment of their IT systems at least on a yearly basis. The assessment should make an analysis on the threats and vulnerabilities to the information technology assets of the NBFC and its existing security controls and processes. The outcome of the exercise should be to find out the risks present and to determine the appropriate level of controls necessary for appropriate mitigation of risks. 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.

3.10 Mobile Financial Services

NBFCs that are already using or intending to use Mobile Financial Services should develop a mechanism for safeguarding information assets that are used by mobile applications to provide services to customers. The

technology used for mobile services should ensure confidentiality, integrity, authenticity and must provide for end-to end encryption.

3.11 Social Media Risks

NBFCs using Social Media to market their products should be well equipped in handling social media risks and threats. As Social Media is vulnerable to account takeovers and malware distribution, proper controls, such as encryption and secure connections, should be prevalent to mitigate such risks.

3.12 Training

Human link is the weakest link in the information security chain. Hence, there is a vital need for an initial and ongoing training and information security awareness programme. The programme may be periodically updated keeping in view changes in information technology system, threats/vulnerabilities and/or the information security framework. There needs to be a mechanism to track the effectiveness of training programmes through an assessment / testing process. At any point of time, NBFCs need to maintain an updated status on user training and awareness relating to information security.

IT OPERATIONS

4 IT Operations should support processing and storage of information, such that the required information is available in a timely, reliable, secure and resilient manner. The Board or Senior Management should take into consideration the risk associated with existing and planned IT operations and the risk tolerance and then establish and monitor policies for risk management.

4.1 Acquisition and Development of Information Systems (New Application Software) and Change Management

It has been the experience while implementing IT projects that many systems fail because of poor system design and implementation, as well as inadequate testing. NBFCs should identify system deficiencies and defects at the system design, development and testing phases.

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

4.2 NBFCs are required to realign their IT systems on a regular basis in line with the changing needs of its customers and business. The changes need to be done in such a way that adverse incidents and disruption

to services are minimized while maximizing value for the customers. For this purpose, NBFCs should develop, with the approval of their Board, a Change Management Policy that encompasses the following:

a) prioritizing and responding to change proposals from business,
b) cost benefit analysis of the changes proposed,
c) assessing risks associated with the changes proposed,
d) change implementation, monitoring and reporting.

It should be the responsibility of the senior management to ensure that the Change Management policy is being followed on an ongoing basis.

4.3 IT Enabled Management Information System

The IT function of an NBFC should support a robust and comprehensive Management Information System (MIS) in respect of various business functions as per the needs of the business. A good MIS should take care of information needs at all levels in the business including top management.

4.4 NBFCs may put in place MIS that assist the Top Management as well as the business heads in decision making and also to maintain an oversight over operations of various business verticals. With robust IT systems in place, NBFCs may have the following as part of an effective system generated MIS (indicative list)

a) A dashboard for the Top Management summarising financial position vis-à-vis targets. It may include information on trend on returns on assets across categories, major growth business segments, movement of net-worth etc.
b) System enabled identification and classification of Special Mention Accounts and NPA as well as generation of MIS reports in this regard.
c) The MIS should facilitate pricing of products, especially large ticket loans.
d) The MIS should capture regulatory requirements and their compliance.
e) Financial Reports including operating and non-operating revenues and expenses, cost benefit analysis of segments/verticals, cost of funds, etc. (also regulatory compliance at transaction level)
f) Reports relating to treasury operations.
g) Fraud analysis- Suspicious transaction analysis, embezzlement, theft or suspected money-laundering, misappropriation of assets, manipulation of financial records etc. The regulatory requirement of reporting fraud to RBI should be system driven.
h) Capacity and performance analysis of IT security systems
i) Incident reporting, their impact and steps taken for non -recurrence of such events in the future.

4.5 MIS for Supervisory requirements - The MIS that help management in taking strategic decisions shall also assist in generating the required information/returns for the supervisor. The present structure of

reporting system (to the supervisor) needs to be kept in view while designing the MIS. All regulatory/supervisory returns should be system driven; there should be seamless integration between MIS system of the NBFC and reporting under COSMOS. Further, it is essential that *""Read Only"* access be provided to RBI Inspectors.

IS AUDIT

5. Policy for Information System Audit (IS Audit).

The objective of the IS Audit is to provide an insight on the effectiveness of controls that are in place to ensure confidentiality, integrity and availability of the organization's IT infrastructure. IS Audit shall identify risks and methods to mitigate risk arising out of IT infrastructure such as server architecture, local and wide area networks, physical and information security, telecommunications etc.

5.1 IS Audit should form an integral part of Internal Audit system of the NBFC. While designing the IS framework, NBFCs shall refer to guidance issued by Professional bodies like ISACA, IIA, ICAI in this regard. ICAI has published "Standard on Internal Audit (SIA) 14: Internal Audit in an Information Technology Environment" on the subject. NBFCs shall adopt an IS Audit framework duly approved by their Board. Further, NBFCs shall have adequately skilled personnel in Audit Committee who can understand the results of the IS Audit.

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

5.3 Personnel – IS Audit may be conducted by an internal team of the NBFC. In case of inadequate internal skills, NBFCs may appoint an outside agency having enough expertise in area of IT/IS audit for the purpose. There should be a right mix of skills and understanding of legal and regulatory requirements so as to assess the efficacy of the framework vis-à-vis these standards. IS Auditors 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.

5.4 Periodicity - The 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. IS Audit should be undertaken preferably prior to the statutory

audit so that IS audit reports are available to the statutory auditors well in time for examination and for incorporating comments, if any, in the audit reports.

5.5 Reporting – The framework should clearly prescribe the reporting framework, whether to the Board or a Committee of the Board viz. Audit Committee of the Board (ACB)

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

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

Business Continuity Planning

6. Business Continuity Planning (BCP) and Disaster Recovery

BCP forms a significant part of an organisation's overall Business Continuity Management plan, which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes. BCP shall be designed to minimise the operational, financial, legal, reputational and other material consequences arising from a disaster. NBFC should adopt a Board approved BCP Policy. The functioning of BCP shall be monitored by the Board by way of periodic reports. The CIO shall be responsible for formulation, review and monitoring of BCP to ensure continued effectiveness. The BCP may have the following salient features:

6.1 Business Impact Analysis- 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.

6.2 Recovery strategy/ Contingency Plan- NBFCs shall try to fully understand the vulnerabilities associated with interrelationships between various systems, departments and business processes. The BCP

should come up with the probabilities of various failure scenarios. Evaluation of various options should be done for recovery and the most cost-effective, practical strategy should be selected to minimize losses in case of a disaster.

6.3 NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers.

6.4 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.

IT SERVICES OUTSOURCING

7. Policy for IT Services Outsourcing

Outsourcing of IT related business process can provide an NBFC the opportunity to realise valuable strategic and economic benefits. However, prior to commencement of any outsourcing arrangement, careful consideration of risks, threats of contractual arrangements and regulatory compliance obligations must take place. Companies usually outsource their IT related business process to a third party vendor because of higher efficiency, inadequate resources and lack of specialized knowledge. The NBFC's decision to outsource IT Services should fit into the institution's overall strategic plan and corporate objectives.

7.1 The terms and conditions governing the contract between the NBFC and the Outsourcing service provider should be carefully defined in written agreements and vetted by NBFC's legal counsel on their legal effect and enforceability. The contractual agreement may have the following provisions.

a) **Monitoring and Oversight***:* Provide for continuous monitoring and assessment by the NBFC of the service provider so that any necessary corrective measure can be taken immediately. Outsourcing service provider should have adequate systems and procedures in place to ensure protection of data/application outsourced.

b) **Access to books and records / Audit and Inspection***:* This would include :

   i. Ensure that the NBFC has the ability to access all books, records and information relevant to the outsourced activity available with the service provider. For technology outsourcing, requisite audit trails and logs for administrative activities should be retained and accessible to the NBFC based on approved requests.

ii. Provide the NBFC with the right to conduct audits on the service provider whether by its internal or external auditors, or by external specialists appointed to act on its behalf and to obtain copies of any audit or review reports and findings made on the service provider in conjunction with the services performed for the NBFC.

iii. The contractual agreement may include clauses to allow the **Reserve Bank of India or persons authorized by it to access the NBFC's documents**, records of transactions, and other necessary information given to, stored or processed by the service provider within a reasonable time. This includes information maintained in paper and electronic formats.

7.2 The Board and senior management are ultimately responsible for 'outsourcing operations' and for managing risks inherent in such outsourcing relationships. The Board of Directors of NBFCs is responsible for effective due diligence, oversight and management of outsourcing and accountability for all outsourcing decisions. The Board and IT Strategy committee have the responsibility to institute an effective governance mechanism and risk management process for all IT outsourced operations.

7.3 The Role of IT Strategy committee in respect of outsourced operations shall include

a) Instituting an appropriate governance mechanism for outsourced processes, comprising of risk based policies and procedures, to effectively identify, measure, monitor and control risks associated with outsourcing in an end to end manner;
b) Defining approval authorities for outsourcing depending on nature of risks and materiality of outsourcing;
c) Developing sound and responsive outsourcing risk management policies and procedures commensurate with the nature, scope, and complexity of outsourcing arrangements;
d) Undertaking a periodic review of outsourcing strategies and all existing material outsourcing arrangements;
e) Evaluating the risks and materiality of all prospective outsourcing based on the framework developed by the Board;
f) Periodically reviewing the effectiveness of policies and procedures;
g) Communicating significant risks in outsourcing to the NBFC's Board on a periodic basis;
h) Ensuring an independent review and audit in accordance with approved policies and procedures;
i) Ensuring that contingency plans have been developed and tested adequately;
j) NBFC should ensure that their business continuity preparedness is not adversely compromised on account of outsourcing. NBFCs are expected to adopt sound business continuity management practices as issued by RBI and seek proactive assurance that the outsourced service provider maintains readiness and preparedness for business continuity on an ongoing basis.

Section-B

Recommendations for NBFCs with asset size below ₹ 500 crore

8. It is recommended that smaller NBFCs may start with developing basic IT systems mainly for maintaining the database. NBFCs having asset size below ₹ 500 crore shall have a Board approved Information Technology policy/Information system policy. This policy may be designed considering the undermentioned basic standards and the same shall be put in place by September 30, 2018. The IT systems shall have:

I. Basic security aspects such as physical/ logical access controls and well defined password policy;
II. A well-defined user role;
III. A Maker-checker concept to reduce the risk of error and misuse and to ensure reliability of data/information;
IV. Information Security and Cyber Security;
V. Requirements as regards Mobile Financial Services, Social Media and Digital Signature Certificates as indicated in para 3.18, 3.10 & 3.11 above;
VI. System generated reports for Top Management summarising financial position including operating and non-operating revenues and expenses, cost benefit analysis of segments/verticals, cost of funds, etc.;
VII. Adequacy to file regulatory returns to RBI (COSMOS Returns);
VIII. A BCP policy duly approved by the Board ensuring regular oversight of the Board by way of periodic reports (at least once every year);
IX. Arrangement for backup of data with periodic testing.

8.1 IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases.

Annex - I

Template for reporting Cyber Incidents

1. Security Incident Reporting (SIR) to RBI (within 24 hours):

2. Subsequent update(s) RBI (updates to be provided if the earlier reporting was incomplete i.e. investigation underway or new information pertaining to the incident has been discovered or as per request of RBI):

Basic Information	
1. Particulars of Reporting:	
• Name of the NBFC	
• Date and Time of Reporting to RBI, CERT-IN, other agencies (please mention separately time of reporting to each)	
• Name of Person Reporting	
• Designation/Department	
• Contact details (e.g. official email-id, telephone no, mobile no)	
2. Details of Incident:	
• Date and time of incident detection	
• Type of incidents and systems affected (i) Outage of Critical IT system(s) (e.g. CBS, Treasury Systems, Trade finance systems, Internet banking systems, ATMs, payment systems such as SWIFT, RTGS, NEFT,NACH, IMPS, etc.) (ii) Cyber Security Incident e.g. DDOS, Ransom ware/crypto ware, data breach, data destruction, web defacement, etc.)? [Please complete Annex] (iii) Theft or Loss of Information (e.g. sensitive customer or business information stolen or missing	

or destroyed or corrupted)? (iv) Outage of Infrastructure (e.g. which premises-DC/Central Processing Units, branch, etc. power/utilities supply, telecommunications supply,)? (v) Financial (e.g. liquidity, bank run)? (vi) Unavailability of Staff (e.g. number and percentage on loss of staff/absence of staff from work (vii) Others (e.g. outsourced service providers, business partners, breach of IT Act/any other law and RBI/SEBI regulations. Etc.)?	
• What actions or responses have been taken by the NBFC at the time of first reporting/till the time of subsequent reporting?	
3. Impact Assessment (examples are given but not exhaustive):	
• Business impact including availability of services - Internet banking, Cash Management, Trade Finance, Branches, ATMs, Clearing and Settlement activities, etc.	
• Impact on stakeholders- affected retail/corporate customers, affected participants including operator(s), settlement institution(s), business partners, and service providers, etc.	
• Financial and market impact – Trading activities, transaction volumes and values, monetary losses, liquidity impact, withdrawal of funds etc.	
• Regulatory and Legal impact	
4**. Chronological order of events:**	
• Date of incident, start time and duration.	
• Escalations done including approvals sought on interim measures to mitigate the event, and reasons for taking such measures	
• Stakeholders informed or involved	

• Channels of communications used (e.g. email, internet, sms, press release, website notice, etc.)	
• Rationale on the decision/activation of BCP and/or DR	
5. Root Cause Analysis(RCA):	
• Factors that caused the problem/ Reasons for occurrence, Cause and effects of incident	
• Interim measures to mitigate/resolve the issue, and reasons for taking such measures, and	
• Steps identified or to be taken to address the problem in the longer term. List the remedial measures/corrections affected(one time measure) and/or corrective actions taken to prevent future occurrences of similar types of incident	
6. Date/target date of resolution_____ **(DD/MM/YYYY).**	

Note: All fields are REQUIRED to be filled unless otherwise stated.

CYBER SECURITY INCIDENT REPORTING(CSIR) FORM

General Information Report No:

1. Contact Information: (Please provide if different from what is reported in Basic Information above)

Name of NBFC:

Name of the person reporting and Designation:

Department

Official Email :

Telephone/Mobile :

2. Is this a ☐New incident ☐Update to reported incident?

- For the first update, please indicate "1. If this is an update to a reported incident, please provide the update number for this update. (X.1, X.2, X.3,X.4, etc. where X is the Report No. Update No: Click here to enter text.

3. What severity is this incident being classified as?

Severity 1 ☐ Affected critical system(s)/ customer facing applications/systems, crippled Internal network or a combination of the above	Severity 2 ☐ Incident occurred on system or network that could put the NBFC's network / critical system(s) or a combination of them at risk	

Information about the Incident

4. Please indicate the date and time the incident was reported to the RBI. If it is also reported to Other Agencies (CERT-IN/NCIIP), Law enforcement agencies, separately indicate the date and time of such reporting.

(Please specify in Indian Local Time (+5.30 GMT))

Reported to RBI - Date: Click here to enter a date.

Reported to CERT-IN Date: Click here to enter a date.

Reported to NCIIP Date: Click here to enter a date.

Reported to ----mention the name of agency Date: Click here to enter a date.

5. Types of Threat/Incident

((Please select more than one, as applicable)

☐ Denial of Service (DoS) ☐ Distributed Denial of Service (DDoS)

☐ Virus/Worm/Trojan/Malware ☐ Intrusion/Hack/Unauthorised access

☐ Website Defacement ☐ Misuse of Systems/Inappropriate usage

☐ APT/0-day attack ☐ Spear phishing/Whaling/Phishing/Wishing/Social engineering attack

☐ Other: Click here to enter text.

6. Is this incident related to another incident previously reported?

Choose an item.

- If “Yes”, provide more information on how both incidents are related.

  Click here to enter text.
- Please provide the reference no. of the previously reported incident.
  Ref no: Click here to enter text.

Incident Details

7. Please provide details of the incident in the box below.

- When was the incident first observed/sighted/detected?
  Click here to enter a date.
- How was the incident first observed/sighted/detected?
  Click here to enter text.
- Who observed?

8. Please provide details of the critical system(s) or network(s) that is/are impacted by this incident. Details should minimally include:

-Location, purpose of this system/ network, affected applications (including hardware manufacturer, software developer, make/ model, etc.) running on the systems/networks, etc.

Click here to enter text.

What security software installed on the system currently?

If known, any TCP or UDP ports involved in the incident.

If known, provide the affected system's IP address If known, provide the attacker's IP address

Where relevant, please indicate the Operating System of the affected critical system(s): Choose an item.

- If others, kindly state the OS: Click here to enter text.

9. What is the impact of the attack? (Tick 'one' checkbox for each column)

Customer Service Delivery	(Loss of) Sensitive Information	Public Confidence and Reputation
☐No Impact	☐No loss	☐No Impact
☐Minor Impact	☐Minor Loss	☐Minor Impact
☐Major Impact	☐Major Loss	☐Major Impact
☐Serious Impact	☐Serious Loss	☐Serious Impact
☐Severe Impact	☐Severe Loss	☐Severe impact

10. Does the affected critical system(s)/ network(s) have potential impact to another critical system/critical asset(s) of the NBFC?

Choose an item.

- If "Yes", please provide more details.
  Click here to enter text.

Incident Status

11. What is/are the type(s) of follow up action(s) that has/have been taken at this time?

Click here to enter text.

12. What is the current status or resolution of this incident?

Choose an item.

If it is not resolved, what is the next course of actions?

Click here to enter text.

13. What is the earliest known date of attack or compromise? (Tick 'checkbox' if unknown)

(Please specify in Indian Local Time +5.30 GMT)

Date: Click here to enter a date. Unknown: ☐

14. What is the source/cause of the incident? ('NIL' OR 'NA' if unknown)

Click here to enter text.

15. Has the incident been reported to CERT-IN/NCIIP/ any law enforcement agency/IBCART? Choose an item.

- If "Yes", specify the agency that is being reported to.

  Click here to enter text..

16. Is chain of custody maintained?

17. Has the NBFC filled chain of custody form?

18. What tools were used for collecting the evidence for the incident?

Attack Vectors

E1. Did the NBFC locate/identify IP addresses, domain names, related to the incident

Whether the Indicators of Compromise, list of IP addresses identified from the incident, involvement of the IP addresses in the incident (ex. Victim, Malware Command & Control Servers, etc.), domain names resolved, involvement of the domain names in the incident. (ex. Drive-by-download Servers, Malware Control & Command Servers, defaced website), email addresses identified and their involvement, malicious files/attachments (file name, size, MD5/SHA1 hash, etc.) etc. have been reported in IB-CART/CERT-IN/NCIIP/Law enforcement agencies

****