राष्ट्रीय
आवास बैंक
NATIONAL
HOUSING BANK

NHB/ND/DRS/ Policy Circular No.90/2017-18
June 15, 2018

All Registered Housing Finance Companies

Madam / Sir,

Information Technology Framework for HFCs

The Housing Finance Companies (HFC) sector has grown in size and complexity over the years. As the housing finance 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, guidelines on IT Framework for the HFC sector that are expected to enhance safety, security, efficiency in processes leading to benefits for HFCs and their customers are enclosed. HFCs may have already implemented or may be implementing some of the requirements indicated in the Circular. HFCs 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 guidelines are categorized into two parts, those which are applicable to public deposit accepting HFCs and HFCs not accepting public deposit with asset size ₹100 crore and above, as per the last audited balance sheet, are provided in Section-A. Guidelines for HFCs not accepting public deposit with asset size below ₹100 crore are provided in Section-B.

4. HFCs may place these guidelines before their Board, together with a gap-analysis vis-à-vis the Guidelines and the proposed action latest by September 30, 2018.

5. HFCs falling in Section- A shall be required to comply with the Guidelines by June 30, 2019 and other HFCs by September 30, 2019.

Yours faithfully,

(V. Vaideswaran)
General Manager
Department of Regulation and Supervision

Enclosure: Information Technology Framework for HFCs- Guidelines

Annexure

Information Technology Framework for HFCs - Guidelines

The Housing Finance Companies (HFC) sector has grown in size and complexity over the years. As the housing finance 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, guidelines on IT Framework for the HFC sector that are expected to enhance safety, security, efficiency in processes leading to benefits for HFCs and their customers are enclosed. HFCs may have already implemented or may be implementing some of the requirements indicated in the Circular. HFCs 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 guidelines are categorized into two parts, those which are applicable to Public deposit accepting HFCs and HFCs not accepting public deposit with asset size of ₹100 crore & above, as per the last audited balance sheet, are provided in Section-A. Guidelines for HFCs not accepting public deposit with asset size below ₹100 crore are provided in Section-B.

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 HFC'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, HFCs may follow relevant aspects of such prudential governance standards that have found acceptability in the finance industry.

1.1 IT Strategy Committee: HFCs 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 HFC's growth and becoming aware about exposure towards IT risks and controls.

IT POLICY

2. HFCs 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 HFC;

b) HFCs 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 HFC, periodic assessment of the IT training requirements should be formulated to ensure that sufficient, competent and capable human resources are available.

d) The HFCs which are currently not using IPv6 platform should migrate to the same as per the National Telecom Policy issued by the Government of India in 2012, as amended from time to time.

INFORMATION AND CYBER SECURITY

3. Information Security

Information is an asset to all HFCs 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. HFCs 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. HFCs 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.), HFCs 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 (e.g. 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. HFC 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. HFCs 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 centre 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. HFCs shall develop and implement processes for preventing, detecting, analysing and responding to information security incidents.

h) Trails- HFCs 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) - HFCs 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

HFCs 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. HFCs 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. HFCs 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. HFCs 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. HFCs 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, HFCs 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 Reporting of information on cyber-security

HFCs shall put in place a suitable mechanism to report all types of unusual security incidents to its IT Steering Committee and the Risk Management Committee.

Incidents involving compromise of the IT systems of the HFC such as data breach, data destruction etc. severely affecting the operations of the company shall be reported to the NHB along with the action take thereon by the HFC, within two working days.

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. HFCs 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. HFCs 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

HFCs 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 HFC 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 HFC and should serve as an input for Information Security auditors.

3.10 Mobile Financial Services

HFCs 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

HFCs 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, HFCs 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. HFCs should identify system deficiencies and defects at the system design, development and testing phases.

HFCs 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 HFCs 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, HFCs 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 HFC 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 HFCs 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, HFCs 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 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 frauds, if any, 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 vis-à-vis reporting under ORMIS /regulatory reporting. Further, it is essential that ""*Read Only*" access be provided to NHB Inspectors or persons authorized by it.

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 HFC. While designing the IS framework, HFCs 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. HFCs shall adopt an IS Audit framework duly approved by their Board. Further, HFCs 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 HFC. In case of inadequate internal skills, HFCs may appoint an outside agency provided that the outside auditor/agency is empanelled with CERT-In. 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 HFCs' 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 HFC but may be conducted at least once in two years. 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 Rotation of IS Auditors- Rotation of IS auditors must be adhered in such a way that an auditor shall not carry out such audit for more than two successive terms if conducted once in two years or for three successive terms if conducted once a year.

5.6 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)

5.7 Compliance – HFCs 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.

5.8 Computer-Assisted Audit Techniques (CAATs): HFCs 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. HFC 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- HFCs 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 HFC's business. The entity shall clearly list the business impact areas in order of priority.

6.2 Recovery strategy/ Contingency Plan- HFCs 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 HFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers.

6.4 HFCs 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 HFC 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 HFC'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 HFC and the Outsourcing service provider should be carefully defined in written agreements and vetted by HFC'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 HFC 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 HFC 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 HFC based on approved requests.

ii. Provide the HFC 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 HFC.

iii. The contractual agreement may include clauses to allow the **National Housing Bank or persons authorized by it to access the HFC'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 HFCs 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 HFC'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) HFC should ensure that their business continuity preparedness is not adversely compromised on account of outsourcing. HFCs are expected to adopt sound business continuity management practices as issued by NHB and seek proactive assurance that the outsourced service provider maintains readiness and preparedness for business continuity on an ongoing basis.

Section-B

Recommendations for HFCs not accepting public deposit with asset size below ₹100 crore

8. HFCs not accepting public deposit with asset size below ₹100 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, 2019. 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 Digital Signature Certificates, Mobile Financial Services and Social Media indicated in para 3.8, 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 NHB (ORMIS);

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 HFC's operations increases.

***