MONETARY BOARD
CENTRAL BANK OF SRI LANKA

28 January 2022 **FINANCE BUSINESS ACT DIRECTIONS** **No. 01 of 2022**

TECHNOLOGY RISK MANAGEMENT AND RESILIENCE

1. Legal provisions

1.1 In terms of the powers conferred by section 12 of the Finance Business Act, No. 42 of 2011, the Monetary Board of Central Bank of Sri Lanka hereby issues these directions on technology risk management and resilience of Licensed Finance Companies (LFCs).

2. Objectives of the directions

2.1 With the adoption of new technology and leveraging technology services to agents and third parties, LFCs embrace technology risk which needs to be integrated into the risk management. These directions intend to set minimum regulatory requirements on technology risk management and resilience for LFCs.

3. Applicability

3.1. Requirements in this framework shall be applicable to entire operations of LFCs including operations performed by agents and third-party service providers.

3.2. The extent and degree to which an LFC implements these directions should be commensurate with the level of risk and complexity of the technologies used and shall be decided by the Board of Directors going beyond the minimum regulatory requirements as may be warranted.

3.3. The provisions of these directions shall be effective from 01.01.2023 subject to the transitional provisions in direction 10.

4. Technology risk governance and oversight

4.1. Role of the Board of Directors

a) Board of Directors shall be responsible to formulate Information Technology (IT) and cyber security strategy in alignment with the potential risks posed by technology, business strategy and minimum regulatory requirements.

b) IT and cyber security strategy shall be supported by the Board approved policies including a well written information security policy, a sound and robust risk management framework with the appropriate Board oversight,

adequate technical resources, institutional arrangement for building awareness on the subject and an independent audit.

c) Engagement with the third parties and agents needs to be evaluated in view of the potential IT and cyber risks they pose to the LFC including the risks arising from the use of cloud services and Fintech.

d) LFCs are encouraged to establish a Board level Information Security Committee (ISC) which is responsible for information security and technology resilience of the LFC.

e) The Board of Directors shall establish adequate oversight measures to ensure effective implementation of the regulatory requirements in the technology risk management and resilience direction.

4.2. Technology Risk Management

a) The focus of the technology risk management should be broadly on identification, protection, detection, responding and recovery functions. Technology risk management should evaluate the adequacy, effectiveness and appropriateness of controls and monitor the same at frequent intervals while keeping the Board informed on any major non-compliances observed.

b) Establish a technology risk management framework with the following functions.

i) Risk identification

Identify the threats and vulnerabilities applicable to IT environment, including information systems maintained or supported by agents or third party service providers.

ii) Risk assessment

Perform an analysis of the potential impact/consequences and likelihood of the IT threats and vulnerabilities on the overall business

and operations. Set criteria for measuring and determining the likelihood and impact of the risk scenarios.

iii) Risk treatment

Develop and implement risk mitigation and control measures that are consistent with the criticality of the information systems and the level of risk tolerance. Assess whether risks have been reduced to an acceptable level after applying the mitigating measures.

iv) Risk monitoring, review and reporting

Establish a process for assessing and monitoring the design and operating effectiveness of IT controls against identified risks.

4.3. Role of Senior Management

a) Implement the Board approved technology risk management framework into specific policies and procedures that are consistent with the approved risk tolerance and supported by effective oversight, reporting, escalation procedures and apprising the Board of Directors of any adverse developments.

b) LFCs shall have a management level ISC headed by the Chief Executive Officer (CEO) to address issues on technology adoption, information security, cyber security, outsourcing and concentration and to support the Board level ISC. The roles and responsibilities of the management level ISC are given in Annexure-I.

c) Ensure the cyber hygiene is maintained within the organization and third party outsourced agencies on an ongoing basis. Awareness programmes need to be conducted based on the role played by the staff and other stakeholders periodically.

d) Establish appropriate controls relating to physical access, logical access, change management, patch management and configuration management, best practices as articulated in various information security

standards/frameworks and such controls should consider the entire life cycle of the information systems.

e) Review the effectiveness and relevance of information security controls periodically and take necessary remedial action on priority.

4.4. Chief Information Security Officer (CISO)

a) LFCs shall appoint a CISO to provide leadership on the requirements of the information security. The main responsibilities of CISO shall be as follows:

i) Develop, manage and operationalize the information security strategy.

ii) Continuously monitor and evaluate the information security practices.

iii) Perform information security audits and risk assessments.

iv) Making the organization compliant with information security regulations.

v) Develop and implement business continuity plans.

vi) Information security risks and strategy related training and awareness.

vii) Manage information security budgets; and

viii) Report to the Board of Directors about the information security.

b) CISO shall be an executive officer of the LFCs' senior management team.

c) CISO shall report to the CEO or have an appropriate reporting line where CEO is at the end of reporting line.

d) CISO shall co-ordinate with risk management and IT functions of the LFC for smooth implementation of the information security activities.

e) LFCs may appoint an executive officer from the LFCs' management

team to simultaneously function as the CISO, provided that the Board of Directors resolve that the magnitude of technology and information security risks faced by the LFCs do not necessitate a dedicated CISO. However, such an officer shall not discharge any function that may conflict with his responsibilities including positions such as Chief Information Officer, Chief Internal Auditor, Chief Risk Officer or Compliance Officer.

4.5. Internal Audit

LFCs shall ensure that compliance with the requirements in these directions through the internal audit at least annually.

5. Information and information system security

5.1. Fair and Ethical Use of Customer Data

a) LFCs shall ensure that customer data would only be used in ways the customers would reasonably expect the LFC to use such data.

b) The Board of Directors shall put in place effective policies and procedures to ensure fair and ethical use of customer data at all times. Further, LFCs shall not disclose such data except for that has been provided by law.

c) LFCs shall ensure the outsourced vendors, including Fintech, abide by the expectations on fair and ethical use of customer data, as if they are subjected to similar regulations, as it pertains to LFC operations.

5.2. Information Classification and Labelling

a) LFCs shall have an information classification policy approved by the Board of Directors based on the recommendations of the Board Integrated Risk Management Committee (BIRMC) and ISC.

b) All electronically maintained data shall be classified based on information security level and labelled with assigned classification as per the information classification policy.

5.3. Identification of Critical Information Systems

a) A critical information system refers to any information system that supports the provisions of the critical LFC activities or payment services, where failure of the system has the potential to significantly impair the financial institution's provisions of financial services to its customers or counterparties, business operations, financial position, reputation, or compliance with applicable laws and regulatory requirements.

b) A critical information system shall include, but not limited to, the transaction processing systems, general ledger systems, payment and settlement systems, delivery channels, systems used for Anti-Money Laundering (AML)/Know Your Customer (KYC) procedures, and any other system that is required to ensure the uninterrupted conduct of finance business. Any information system exclusion from the above shall be based on an internally established policy. All such exclusions shall be reviewed at least every two years.

c) The Board of Directors shall identify information systems falling within the definition of critical information system on the recommendations of BIRMC and ISC.

5.4. User Access Management

a) User access control shall be applicable to critical information systems and information systems exposed to customer data.

b) The Board of Directors shall decide on the need to apply the user access control requirements similar to critical information systems for non-critical information systems exposed to confidential non-customer data in consultation with BIRMC and ISC.

c) LFCs shall implement an industry standard user access and identity management system(s) to manage all users including the privileged users.

d) In the event of an industry standard user access and identity management system(s) are not feasible or appropriate, LFCs may use alternative controls implementing a suitable control, for any existing information system subject to the approval of the Board of Directors on the recommendation of BIRMC and ISC.

e) The privileged user access shall be provided only on "need-to-have" basis and the highest level of access shall only be provided for a limited time when such access is required. Activities of these accounts should be logged and reviewed as a part of the LFC's ongoing monitoring.

f) The LFCs shall conduct user access reviews as per following frequencies:

i) At least on a monthly basis for the critical information systems.

ii) At least on a quarterly basis for the non-critical information systems exposed to customer data and confidential non-customer data.

iii) At least on an annual basis for all the other information systems.

iv) At least on a bi-annual basis for customers and their authorized representatives registered to use any information system of the LFC including the electronic delivery channels, using an appropriate methodology in accordance with the operating instructions of the linked accounts.

g) LFCs shall adopt appropriate methodologies to conduct user access privilege reviews as approved by ISC.

h) When conducting the user access privilege reviews, LFCs must implement an appropriate mechanism to review the identification, authentication and authorization of internal and external users such as the third-party service providers.

5.5. Computer Security and User Activity Log Management

a) LFCs shall implement a log management policy to manage computer

security and user activity logs of critical information systems and customer data information systems. Such policy may be extended to the other information systems at the discretion of BIRMC.

b) The policy shall be approved by the Board of Directors based on the recommendations of BIRMC and ISC.

c) The policy shall include types of logs to be maintained, retention period, frequency of review, method of review and tools to be used, event identification and response, and responsibilities for the maintenance and review of logs.

d) Computer security logs to be generated by security software, operating systems and applications. Computer security and user activity logs maintained shall be adequate to successfully identify and investigate information security incidents.

e) Logs of the privileged users shall be given a higher importance and reviewed on a near real time basis using appropriate tools and methods.

5.6. Data Encryption

5.6.1 Customer Data Encryption

a) Customer data shall be protected using encryption.

b) Encryption shall be applicable to customer data maintained with LFCs, agents, and the third-party service providers.

c) Levels of data encryption,

i) Data-at-rest encryption

Customer data shall be subjected to database encryption or file level encryption at rest.

ii) Data-in-transit encryption

Whenever a file containing customer data is transmitted, it shall remain encrypted at file level.

iii) Full disk encryption for endpoint devices and removable media

All endpoint devices and removable media that store customer data of LFCs, either permanently or temporarily, including such devices of the third-party service providers and agents shall be subject to full disk encryption.

d) LFCs shall use industry standard encryption methods. Selection of such methods shall be subjected to the approval of the Board of Directors on the recommendation of BIRMC and ISC.

e) When industry standard encryption methods are not feasible or appropriate, LFCs may use alternative controls to protect customer data subject to the approval of the Board of Directors on the recommendation of BIRMC and ISC.

5.6.2 Confidential Non-Customer Data Encryption

Encryption requirements shall be applicable to confidential non-customer data as well, except for the categories of confidential non-customer data that will only pose negligible adverse impact to LFCs if subjected to a data leakage or any other adverse information security incident that could have been prevented with encryption as determined by BIRMC.

5.7. Security Operations Center (SOC)

All LFCs offering electronic delivery channels (e.g., internet banking, mobile apps, customer/third-party integrations, etc.) shall implement a SOC as per the minimum requirements in Annexure II.

5.8. Data Loss Prevention (DLP)

a) LFCs shall implement industry standard DLP tools to minimize the risk of data leakages. Scope of implementation shall cover the entire LFC, any third- party service providers and agents exposed to customer data.

b) In case of the third-party service providers and agents, LFCs may allow them to implement DLP tools as per minimum requirements specified

by the LFCs.

c) LFCs shall conduct at least an annual review of such implementations by the third-party service providers and agents to ensure adequate DLP measures are in place.

d) When industry standard DLP tools are not feasible or appropriate, LFCs may use alternative controls to protect customer data subject to the approval of the Board of Directors on the recommendation of BIRMC and ISC.

5.9. Information Security Incident Response and Recovery

5.9.1 Incident Response Plan (IRP)

a) LFCs shall have an up to-date IRP approved by Board of Directors, including procedures for incident escalation, remediation, recovery, and communication with internal and external stakeholders.

b) IRP shall include specific procedures to deal with commonly known types of information security incidents, including but not limited to cyber security incidents.

5.9.2 Incident Response and Recovery Testing

Incident response and recovery capabilities shall be tested at least annually using scenarios close to the real life as much as possible to determine the LFC's incident response readiness. Results of such test shall be reported to the Board of Directors through BIRMC by ISC.

5.10. Information Security Testing

5.10.1 Pre-Implementation Information Security Testing

a) **Scope**

i) Critical information systems and information systems exposed to customer data shall be subject to pre-implementation information security tests. Any other information system that could potentially make any critical information system or any information system exposed to customer data vulnerable shall also be subjected to pre-implementation information security tests.

ii) The Board of Directors shall decide on the need to conduct pre-implementation information security testing for non-critical information systems exposed to confidential non-customer data on the recommendation of BIRMC and ISC.

iii) Pre-implementation information security tests shall be conducted prior to initial implementation and prior to implementation of modifications. Minor modifications could be excluded from pre-implementation information security tests based on an exclusion policy approved by the Board of Directors. In the event of any specific minor modification needs to be excluded, the approval of ISC is required at the time of implementation.

b) Following types of pre-implementation tests shall be carried out as applicable to the given implementation:

i) Static Application Security Testing (SAST) or source code reviews to detect any malicious or unsafe code.

ii) Dynamic Application Security Testing (DAST) to detect application-level vulnerabilities an attacker could exploit.

iii) Quality assurance testing on computing and networking infrastructure hardening to ensure compliance with internal hardening policies, and

iv) Infrastructure vulnerability assessments to identify vulnerabilities in computing and networking infrastructure.

c) Pre-implementation tests shall be conducted by a team independent from the team responsible for the development and/or implementation of the information system.

d) LFCs shall adopt suitable alternative security evaluation methodologies when procuring off-the-shelf software if conducting pre-implementation tests as per 5.10.1(b) is not possible.

e) LFCs may rely on an assurance provided by an independent third-party, mutually acceptable to both the LFC and the information system provider, as an alternative to 5.10.1(b)(i) in case of information systems provided by external vendors.

f) LFCs shall implement industry standard controls to ensure the malicious code will not be injected when source code is moved to production environment after completion of relevant pre-implementation tests.

5.10.2 Vulnerability Assessments (VA)

a) Critical information systems and information systems exposed to customer data shall be subject to VA at least bi-annually or whenever there is a change to the IT infrastructure and system modifications.

b) VA shall focus on both infrastructure and application vulnerabilities.

c) VA shall be performed on production environments.

d) VA may be performed by the LFC's internal information security staff or external experts.

e) Vulnerabilities identified shall be remediated within a time period approved by the ISC.

5.10.3 Penetration Testing (PT)

a) LFCs shall conduct PT using an independent external expert to determine,

i) The ability of tested information systems to withstand real-world style attacks.

ii) The required level of sophistication and persistence an attacker should possess to successfully compromise the tested information systems.

iii) Ability of the LFC's information security, operational, and leadership teams to detect and appropriately respond to such attacks.

iv) Any enhancements required to mitigate such threats in the future.

b) Critical information systems, information systems exposed to customer data, and repositories of customer data with the LFC, agents, and third-party service providers shall be subject to PT by an independent external penetration testing expert, at least annually. An indicative guidance on the conduct of PT is given in Annexure - III.

c) LFCs that are mature and have complex technologies supporting their business activities could conduct red team exercises as an extension of PT. An indicative guidance on how to conduct red team exercises are given in Annexure - IV.

5.11. Information Security Training and Certification

5.11.1 Training and Awareness to Board of Directors

a) LFCs shall implement a comprehensive annual training and awareness program on information security and technology risk management for Board of Directors, in accordance with the requirements below.

i) The objective of such program shall be to enable the Board of Directors to have effective oversight on the adequacy and effectiveness of information security and technology risk management policies and procedures of the LFC.

ii) Responsibilities of the Board of Directors and Board Committees in terms of the requirements in this regulatory framework and other applicable laws and regulations relating to information security and technology risk management shall also be covered through such programs.

iii) Such training shall consist of at least one annual structured training program and one or more awareness sessions by information security and technology risk management experts every year.

iv) The Board Secretary of the LFC shall ensure compliance with the above requirements on training and awareness to the Board of Directors.

5.11.2 Information Security Awareness Training and Certification Requirement for Staff

a) LFCs shall ensure the staff of the LFC, agents, and third-party service providers exposed to or can potentially be exposed to critical information systems, customer data, or confidential non-

customer data are trained and certified on information security, in accordance with the following requirements.

i) Required persons shall complete an information security awareness training program based on the information security policies and procedures of the LFC.

ii) Such program as per 5.11.2 (a) (i) shall be commensurate with the information security responsibilities of the trainee and shall be updated regularly and whenever the LFC's information security policies are updated.

iii) Required persons shall complete an internal certification test, based on the information security awareness training, at least annually.

b) The Board of Directors may exclude staff of agents and the third-party service providers from the requirements in 5.11.2 (a) (i), if adequate and comparable information security awareness measures have been implemented by such agents and third-party service providers.

6. Information system availability and disaster recovery

6.1. Scope

Requirements specified in 6.2 to 6.5 shall be applicable to critical information systems.

6.2. System Availability

a) LFCs shall ensure the critical information systems achieve a high level of system availability.

b) The Board of Directors on the recommendation of BIRMC shall establish the system availability targets for each critical information system.

c) BIRMC shall ensure that achievement of system availability targets of

critical information systems are monitored and reported to the Board of Directors.

6.3. Disaster Recovery (DR) Arrangements

a) LFCs shall ensure the availability of DR arrangements for critical information systems with Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) determined by the Board of Directors on the recommendation of BIRMC, confirming to following minimum requirements:

i) RTO of less than 6 hours for critical information systems of LFC; and

ii) RPO of zero (i.e. no data loss during a disaster) or near zero.

6.4. Disaster Recovery (DR) Activation

a) The Board of Directors shall establish DR activation triggers for each critical information system based on recommendations of the BIRMC and ISC.

b) Such activation triggers shall ensure adequate time to activate the DR arrangement in compliance with the RTO target specified in 6.3.

6.5. Disaster Recovery (DR) Testing

a) DR arrangements shall be tested by operating all critical information systems using DR infrastructure for at least one day a year.

b) In addition to testing of DR infrastructure as per 6.5 (a), an annual cycle of DR simulations, shall be implemented to enable the Board of Directors to determine the ability of the LFC to achieve the required RTO and RPO targets under different disaster scenarios and take necessary corrective measures where required.

7. Staff competency requirements

7.1. a) LFCs shall ensure staff with requisite qualifications are employed in information security, technology risk management, and internal audit functions. In addition, the third party service provider's staff members

shall have such qualifications. An indicative guidance regarding recognized qualifications, institutes for respective roles is given in Annexure - V.

b) In the event the LFC is unable to comply with the requirements in section 7.1 (a), the Board of Directors shall resolve to substitute the indicative qualifications for appropriate experience and skills in information security and technology risk management subject to the recommendations of BIRMC and ISC.

8. Third party service provider management

8.1. The Board of Directors and senior management shall exercise effective oversight and address associated risks when engaging third party service providers for critical technology functions and systems. Engagement of third-party service providers, including engagements for independent assessments, does not in any way reduce or eliminate the principal accountabilities and responsibilities of LFCs for the security and reliability of technology functions and systems.

8.2. The Board of Directors shall be responsible for any customer data confidentiality breaches by a third party service provider.

8.3. Third Party Service Provider Assessment

a) LFCs shall conduct proper due diligence on the third-party service provider's competency, system infrastructure and financial viability prior to engaging its services.

b) In addition, an assessment shall be made of the third-party service provider's capabilities in managing the following specific risks,

i) Data leakage including unauthorized disclosure of customer and counterparty information.

ii) Service disruption including capacity performance.

iii) Processing errors.

iv) Physical security breaches.

v) Cyber threats.

vi) Over-reliance on key personnel.

vii) Mishandling of confidential information pertaining to the financial institution or its customers in the course of transmission, processing or storage of such information.

viii) Concentration risk.

c) In the event the third-party service provider exhibits the risks highlighted in 8.3 (b), the LFC shall ensure necessary steps are in place to mitigate such risks.

8.4. Service Level Agreements (SLA)

a) LFCs shall establish an SLA when engaging with third party service providers. At a minimum, SLA shall contain the following:

i) Access rights for the Central Bank of Sri Lanka (CBSL) and any party appointed by the LFC to examine any activity or entity of the LFC. This shall include access to any record, file or data of the LFC, including management information and the minutes of all consultative and decision-making processes.

ii) The rights of the CBSL to examine the third-party service provider and its staff associated with the services provided to the LFC.

iii) Third-party service provider to make available any information or data requested by the Director concerning the services provided to the LFC.

iv) The rights of the Sri Lankan judiciary to request and obtain any information or data relating to the services provided to the LFC.

v) Third party shall ensure the customer data would only be used reasonably and for the purpose the LFC shared the data.

vi) All customer data and confidential non-customer data available with the third-party service provider are permanently deleted

within a pre-agreed time period at the end of the contract.

vii) Third-party service providers to facilitate internal auditing requirements and information security testing requirements given in these directions.

viii) Requirements for the service provider and any sub-contractor to provide sufficient prior notice to the LFC.

ix) A written undertaking by the service provider on compliance with secrecy provisions under relevant legislation. The SLA shall further clearly provide for the service provider to be bound by confidentiality provisions stipulated under the contract even after the engagement has ended.

x) Arrangements for disaster recovery and backup capability.

xi) Ensure the staff assigned by the third party is committed to the non-disruption service and to provide adequate notice of such changes.

xii) Compensation mechanism and rectification procedure for any customer data confidentiality breaches by the third party service provider.

xiii) Critical system availability.

xiv) Arrangements to secure business continuity in the event of exit or termination of the service provider.

b) In the event the LFC is unable to incorporate the conditions stated at 8.4 (a) in the SLA due to nature and the complexities of the third-party arrangement, the Board of Directors shall resolve such exclusions from the SLA with the recommendation of BIRMC and ISC.

8.5. LFCs shall ensure its ability to regularly review the SLA with its third-party service providers to take into account the latest security and technological developments in relation to the services provided.

8.6. LFCs shall ensure its third-party service providers comply with all relevant regulatory requirements prescribed in these directions.

8.7. LFCs shall ensure data residing in third party service providers are recoverable in a timely manner. LFCs shall ensure clearly defined arrangements with the third-party service provider are in place to facilitate the LFC's immediate notification, timely updates to the LFC and other relevant regulatory bodies in the event of a cyber-incident.

8.8. LFCs shall ensure the storage of its data is at least logically segregated from the other clients of the third-party service provider. There shall be proper controls over and periodic review of the access provided to the authorized users.

8.9. LFCs shall ensure any critical system hosted by the third party service providers have strong recovery and resumption capability and provisions to facilitate an orderly exit in the event of failure or unsatisfactory performance by the third-party service provider.

9. Cloud services

9.1. LFCs shall fully understand the inherent risk of adopting cloud services considering the inherent architecture of cloud services that leverages on the sharing of resources and services across multiple tenants over the internet.

9.2. Comprehensive Risk Assessment

a) LFCs shall conduct a risk assessment prior to cloud adoption. The assessment shall address risks associated with the following:

i) Sophistication of the deployment model.

ii) Migration of existing systems to cloud infrastructure.

iii) Location of cloud infrastructure.

iv) Multi-tenancy or data commingling.

v) Vendor lock-in and application portability or interoperability.

vi) Ability to customize security configurations of the cloud infrastructure to ensure a high level of data and technology system

protection.

vii) Exposure to cyber-attacks through cloud service providers.

viii) Termination of a cloud service provider including the ability to secure the financial institution's data following the termination.

ix) Demarcation of responsibilities, limitations and liability of the service provider.

x) Ability to meet regulatory requirements and international standards on cloud computing on a continuous basis.

b) In the event the cloud service provider exhibits the risks highlighted in 9.2 (a), the LFC shall ensure necessary steps are in place to mitigate such risks.

9.3. LFCs shall assess the degree to which the selected cloud configuration adequately addresses the following attributes,

a) Geographical redundancy

b) High availability

c) Scalability

d) Portability

e) Interoperability

f) Strong recovery and resumption capability including appropriate alternate internet path to protect against potential internet faults

9.4. LFCs shall assess the availability of independent, internationally recognized certifications of the cloud service providers, at a minimum, in the following areas:

a) Information security management framework, including cryptographic modules such as used for encryption and decryption of user data.

b) Cloud-specific security controls for protection of customer and counterparty or proprietary information including payment transaction data in use, in storage and in transit.

9.5. LFCs shall separately identify the critical and non-critical systems prior to using any cloud services. The risk assessment as outlined in paragraph 9.2 shall be documented and notified to the Director before the adoption.

9.6. LFCs shall implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorized disclosures and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.

10. Transitional provisions

10.1. The transitional provisions on the direction are as per the Table 1 given below.

Table 1: Timelines for compliance

Reference	Requirement	Date for Compliance
4.3 (b)	Executive level Information Security Committee (ISC)	01.07.2023
4.4	Appointment of a CISO	01.01.2025
5.2	Information classification and labelling	01.07.2023
5.3	Identification of critical information systems	01.07.2023
5.4	User access management	01.01.2024
5.5	Computer security and user activity log management	01.01.2024
5.6	Data Encryption	01.01.2024
5.7	Security Operations Center (SOC)	01.01.2026
5.8	Data Loss Prevention (DLP)	01.01.2024
5.9	Information Security Incident Response and Recovery	01.01.2024
5.10.2 5.10.3	Information Security Testing a) Vulnerability assessments (VA) b) Penetration Testing (PT)	 01.01.2024 01.01.2024
5.11.1 5.11.2	Information Security Training and Certification a) Training and awareness to Board of Directors b) Information security awareness training	01.07.2023

	and certification requirement for staff	01.07.2023
6.2	System availability	01.07.2023
6.3/6.4/6.5	Disaster Recovery	01.07.2023

11. Definitions

11.1. Following definitions shall be applicable for the purposes of these directions.

a) **'Agent'** - An agent or sub-agent is an entity or a person selected by the LFC according to the internal policies approved by the Board of Directors to provide limited finance business activities on behalf of the LFC.

b) **'Confidential non-customer data'** - Any non-public data which do not fall within the definition of customer data and can cause significant financial or reputational loss if they are used maliciously or leaked, including the LFC's financial transactions, submissions to the Board of Directors and management, sensitive employee data, and any other data as determined by the LFC.

c) **'Customer data'** - Any non-public data relating to a past, existing, or potential customer. However, de-identified customer data need not be considered as customer data.

d) **'De-identified customer data'** - Intentionally altered customer data which cannot be used alone or in combination with any other data to identify the customer to whom the data was originally related to.

e) **'Director'** - Director of Department of Supervision of Non-Bank Financial Institutions.

f) **'Public data'** - Data that is freely available to everyone to use and re-publish without any restriction.

g) **'Service provider'** - A service provider with whom the LFC has entered into an outsourcing arrangement as per the Finance Business Act Direction (Outsourcing of Business Operations) No. 7 of 2018 or as amended.

h) **'Senior management'** - Shall have the definition given in the Finance Business Act Direction (Assessment of Fitness and Propriety of Key Responsible Persons) No.06 of 2021 or as amended.

Nivard Ajith Leslie Cabraal

Chairman of the Monetary Board and
Governor of the Central Bank of Sri Lanka

Annexure – I

1. Information Security Committee (ISC)

1.1 LFCs shall establish a management level ISC as the apex management level body responsible for information security and technology resilience of the LFC. The Committee shall be responsible for both strategic and operational aspects of information security and technology risk management.

1.2 ISC shall be chaired by the CEO of the LFC.

1.3 The Chief Operating Officer (COO) /Head of Operations, CISO, Chief Information Officer (CIO)/Head of Information Technology, and Manager of Security Operations Center/ Security Operations Center Coordinator shall be the other ex-officio members of ISC. Head of Legal, Head of Human Resource Management, and Head of Security shall be required to attend as co-opted members whenever a matter relating to their areas is to be discussed. They may be appointed as permanent members at the discretion of the Board of Directors. Head of risk management and Compliance Officer shall be permanent invitees to ISC. Head of Internal Audit shall be invited to present internal audit findings on information security at least on a quarterly basis.

1.4 ISC shall report to the Board of Directors through BIRMC. ISC shall apprise the BIRMC of its proceedings at least on a quarterly basis.

1.5 ISC shall meet at least once in every two months and shall have a quorum and a terms of reference approved by the Board of Directors.

Annexure – II

1. Security Operations Center (SOC)

1.1 Responsibilities

SOC shall be responsible for the prevention, monitoring and detection, incident response, forensics, incident reporting, and knowledge sharing of day-to-day information security threats and incidents.

1.2 Reporting line

a) The Board of Directors shall establish an appropriate line of reporting for the SOC.

b) Such reporting line shall ensure both the LFC's CIO/Head of Information Technology and CISO have adequate oversight over the operations of SOC to carry out their responsibilities effectively, while clearly specifying who has the primary responsibility for the operations of SOC.

1.3 Operating hours

a) SOC shall be operational on a 24 X 7 basis.

b) LFCs shall decide on staffing levels at different times of the day/week based on activity levels and threat profile.

1.4 Human resources, artificial intelligence, and automation

a) Staff roles in SOC shall at least include security analysts (tier 1), incident responders (tier 2), security experts/threat hunters (tier 3), and the SOC manager.

b) LFCs shall rationally decide on the exact staffing level required at each level and on any other types of staff required in the SOC.

c) LFCs may use artificial intelligence or other automation technologies instead of humans for any of the above roles, except for the role of SOC manager.

1.5 Processes

a) Clearly defined and documented processes

SOC shall have clearly defined and documented processes for event classification and

prioritization, analysis, remediation and recovery, post incident assessment, and forensics. Such processes shall clearly identify the steps to be followed and responsible staff for each step.

b) **Defined baseline activity level**

SOC shall have defined and updated baseline activity levels for users, applications, and all infrastructure components to enable effective monitoring and detection of suspicious and unusual activities. Baseline activity levels shall be used by SOC to effectively segregate a suspicious activity from a normal activity.

1.6 Tools

a) **Monitoring and detection tools**

SOC shall be equipped with monitoring and detection tools that commensurate the magnitude and complexity of the LFC's technology usage. At minimum, SOC shall have tools for automated asset discovery, database activity monitoring, vulnerability assessment, and intrusion detection.

b) **Security Information and Event Management (SIEM) tools**

LFCs shall equip the SOC with industry standard SIEM tools and supportive systems capable of log consolidation, event correlation, incident management, forensics analysis, and management reporting.

c) **Data loss prevention (DLP) tools**

1.7 Threat information and intelligence

LFCs shall be aware of the emerging threat landscape in terms of cyber and implement mechanisms to obtain threat information and threat intelligence from relevant sources. The SOC's staff, processes and tools shall be capable of aggregating, analyzing and operationalizing threat information and threat intelligence received, where such arrangements are available.

1.8 Outsourcing

a) The Board of Directors may decide to outsource any function of SOC to a third-party service provider.

b) All decisions to outsource SOC functions shall be made after the Board of Directors evaluating the information security threats posed by such outsourcing. Such evaluations shall be based on independent assessments submitted to the Board of Directors by BIRMC and ISC.

c) LFCs shall ensure the third party service providers of SOC services to whom the LFC's non-public data may be exposed possess a certification for the latest edition of ISO 27001 - information security management systems, from an accredited certification body, for SOC services provided to the LFC.

d) All staff allocated by the third-party service providers of SOC to whom the LFC's non-public data may be exposed shall be subject to background checks by the LFC and shall have non-disclosure agreements with the LFC.

e) The rights of CBSL to examine third party SOC and their staff as if it is a LFC's internal SOC shall be ensured through contractual agreements between the LFC and the SOC service provider.

f) The rights of the Sri Lankan judiciary and law enforcement authorities to request and obtain any information or data relating to the services provided to the LFC by any SOC service provider located outside Sri Lanka shall be ensured through contractual agreements between the LFC and the SOC service provider.

g) CISO or a direct report of CISO shall be appointed as the SOC Coordinator to coordinate between the LFC and the outsourced SOC.

Annexure - III

1. Penetration Tests by Independent External Experts

1.1 Objective

LFCs shall conduct penetration tests by independent external experts to determine: the ability of tested information systems to withstand real-world style attacks; the required level of sophistication and persistence an attacker should possess to successfully compromise the tested information systems; ability of the LFC's information security, operational, and leadership teams to detect and appropriately respond to such attacks; and any enhancements required to mitigate such threats in future.

1.2 Scope and frequency

a) Critical information systems, information systems exposed to customer data, repositories of customer data with the LFC, agents and third-party service providers shall be subject to penetration tests by independent external penetration testing experts, at least annually.

b) The Board of Directors may require the qualifying agents and third-party service providers to conduct penetration tests for qualifying information systems and customer data with them in accordance with these requirements and report to the LFC, instead of being included in the scope of the penetration tests commissioned by the LFC. The Board of Directors shall make such a request only after determining that the relevant agent or third-party service provider is capable of conducting a penetration test in accordance with the requirements stipulated in this framework and after ensuring adequate oversight is available to ensure the objective of penetration testing is achieved.

c) Penetration tests shall be controlled exercises to simulate real-world attacks on real systems and data using tools and techniques similar to those used by actual attackers, to identify vulnerabilities that can be successfully exploited, either individually or together with other vulnerabilities, within the same information system or across multiple information systems, to compromise the security of tested information

system.

d) Penetration tests shall be conducted on live/production systems under normal business conditions, subject to 1.2 (e) and 1.8 (c).

e) LFCs may conduct the first two annual cycles of penetration tests on non-production systems that resemble production systems to the best possible extent instead of production systems, in order to gain sufficient maturity to conduct penetration tests on production systems. All other requirements on penetration testing shall be fulfilled even when penetration tests are conducted on such non-production systems.

f) Penetration testing shall be conducted without changing any of the information security measures that are normally in place, in order to determine the true level of sophistication and persistence required by an attacker to penetrate tested information systems or data. However, LFCs may conduct such exercises with reduced information security as separate or supplementary exercises at the discretion of the Board of Directors.

g) Penetration testing shall cover both external and internal threats and vulnerabilities.

h) Penetration tests shall attempt to exploit vulnerabilities in the technology layer including software/application vulnerabilities as well as vulnerabilities in processing, networking, and storage infrastructure of information systems.

i) Both black box penetration testing and gray box penetration testing using LFC provided login credentials for different user categories including customers, managerial and operational level business users, and third-party users shall be conducted. However, gray box penetration testing using privileged user credentials are not necessary.

j) Penetration tests need not attempt to exploit vulnerabilities that may exist in human or physical layers of security.

k) Scope of each penetration testing exercise shall be defined and documented in a Penetration Test Scope Specification (PTSS).

1.3 Leadership team, project manager and designated point of contact

a) The Board of Directors shall appoint a leadership team for the effective conduct of each annual penetration testing exercise.

b) The leadership team shall have full authority and responsibility for the overall conduct of the penetration testing exercise.

c) The leadership team shall ensure the penetration testing is conducted in a manner to achieve the objective in 1.1, while ensuring the risks are appropriately managed.

d) The leadership team shall possess sufficient business, operational, technical, and risk management related knowledge and experience.

e) The leadership team shall mainly comprise of management team members, preferably drawn from the members and observers of ISC, with adequate authority to make critical decisions during the test. The highest decision makers in the LFC's incident escalation chain, who are responsible for informing actual security breaches to external parties including law enforcement authorities and regulators, shall also be the members of the leadership team.

f) The leadership team shall be chaired by the CEO or a management team member who is directly reporting to the CEO, preferably COO/Head of Operations, CIO/Head of Information Technology, or CISO.

g) The leadership team shall designate one of its members as the project manager, for the day-to-day project management of the penetration testing exercise.

h) There shall be designated deputies for both chairperson and project manager due to the critical nature of both the roles.

i) A senior member of the penetration testing service provider with full decision-making authority shall be appointed as the designated point of contact for the leadership team. Leadership team may invite such designated point of contact to attend its meetings.

1.4 Risk management

a) The leadership team shall establish a risk management plan, for each annual penetration testing exercise, incorporating appropriate controls, processes, and

procedures to ensure associated risks are identified, assessed, and treated in accordance with the LFC's risk appetite.

b) The risk management plan shall include a comprehensive risk assessment and a risk treatment plan detailing risk mitigation strategy for various risk scenarios including but not limited to denial-of-service incidents, unexpected system crashes, damage to critical live production systems, and the loss, modification or disclosure of data.

c) The leadership team shall also implement processes to continuously monitor the incident escalation procedures to decide the triggering of actions that would be mandatory in the case of a real incident but may not be necessary when the incident is due to penetration testing exercises.

d) The leadership team may order a temporary or complete cessation of the penetration testing exercise, when there is any incident that in the opinion of the leadership team requires such cessation.

e) LFCs shall ensure the number of persons with prior knowledge on penetration testing exercise is kept to a minimum, in order to gain the maximum possible learning experience. Accordingly, the leadership team shall decide who, among the LFC's employees and relevant external parties, will know about the penetration testing exercise until its completion.

f) LFCs shall employ a scheme of code names to identify information systems and data being tested throughout the penetration testing exercise.

g) LFCs shall ensure that only penetration testing service providers possessing sufficient competencies, qualifications, and experience to conduct penetration tests on LFC information systems are engaged.

h) The penetration testing service provider shall be required to maintain comprehensive logs of the entire penetration testing exercise to enable recreation of any step executed during the penetration testing.

i) LFCs shall ensure availability of non-disclosure agreements with every team member of the penetration testing service provider engaged in the penetration exercise.

1.5 Selection of penetration testing service provider

a) LFCs shall employ a transparent procurement process with adequate due-diligence measures to select the penetration testing service provider who are acceptable to the LFC. The due diligence process shall include the recent references from previous customers of the service provider and ensure background checks for all team members assigned by the service provider to the penetration testing exercise.

b) The selected penetration testing service providers shall have their processes and procedures externally assured and preferably be accredited or certified to provide penetration testing services by a recognized body acceptable to the LFC.

c) The selection of the external penetration testing service provider shall be approved by the Board of Directors.

d) LFCs shall change the penetration testing service provider to a different service provider on a frequency decided by the Board of Directors.

1.6 Threat intelligence and designing of threat scenarios

a) Penetration tests shall be threat intelligence-based exercises.

b) The LFC and the penetration testing service provider shall mutually agree on the sources of threat intelligence and threat intelligence provider(s).

c) Penetration tests shall be based on pre-designed and realistic threat scenarios against the LFC. Threat scenarios shall include probable real-life attacks conceptualized from an attacker's point of view.

d) Threat scenarios of LFC can be designed based only on generic threat intelligence applicable to LFC sector, however at the discretion of the Board of Directors targeted threat intelligence could be implemented.

e) There shall be clearly defined targets to be achieved by the penetration testing service provider, to demonstrate a successful compromise, for each threat scenario.

1.7 Penetration Test Scope Specification (PTSS)

a) Every annual penetration testing exercise shall be conducted based on PTSS.

b) PTSS shall clearly identify the information systems and data subject to test, threat

scenarios to be used, targets to be achieved, and time period of the test.

c) Penetration testing service provider shall develop the PTSS based on input from the LFC and threat intelligence sources.

d) LFC shall have final authority over the PTSS.

e) Approving authority for PTSS shall be the Board of Directors.

f) LFCs shall ensure that penetration testing service provider is contractually bound to conduct the penetration testing exercise within the limits specified in PTSS.

1.8 Approval for penetration tests

a) Commencement of annual penetration tests and finalized PTSS shall be approved by the Board of Directors, upon determining the information systems to be tested should be able to reasonably withstand the vigor of proposed tests.

b) The Board of Directors may exclude any information system from being tested in a given annual penetration testing cycle, if the Board of Directors determines that such information system is not adequately secured to withstand a penetration test as required by these directions. The Board of Directors shall immediately initiate remediation measures as per 1.11 for all such information systems.

c) The Board of Directors may direct the leadership team to conduct a mock penetration test on a non-live environment for any of the information systems selected for penetration testing, prior to the conduct of penetration test on the live environment. If such mock penetration test successfully compromises an information system, the Board of Directors may remove such information system from being tested in the live environment and directly initiate remediation measures as per 1.11.

1.9 Execution of penetration tests

a) Execution of penetration tests on live systems and data shall commence only after PTSS is approved and communicated in writing to the penetration testing service provider by the chairperson of the leadership team.

b) Sufficient time, as mutually agreed between the LFC and the penetration testing service provider, shall be allocated to the execution of penetration tests on live

systems to allow a realistic and comprehensive test in which all scenarios are executed, and all targets are attempted to be achieved. Penetration testing service provider shall ensure the penetration tests are executed only during such mutually agreed time period.

c) LFCs shall ensure the penetration testing service provider is contractually bound to fulfill its obligations as per 1.9 (a) and (b).

1.10 Reports of annual penetration testing exercise

a) LFCs shall require the penetration testing service provider to submit a detailed report on the entire penetration testing exercise including how requirements of PTSS were achieved. Such report shall also state whether a compromise was made, what systems and data were compromised and how the compromise was achieved on each information system and threat scenario included in the PTSS.

b) Leadership team upon the completion of testing period shall require the LFC's information security and incident response teams to provide reports on their observations on the incidents detected and responsive measures carried out during the testing period.

c) Leadership team shall prepare a final report on the penetration testing exercise based on the above reports and submit to the Board of Directors through ISC and BIRMC. Such report shall summarize the scope and outcome of the penetration testing exercise, leadership team's assessment on LFC's information security and incident response preparedness, and proposed remediation measures in consultation with CIO/Head of IT and CISO.

1.11 Remediation

a) Information systems and repositories of data that were compromised during penetration tests or excluded from the penetration testing scope shall be remediated immediately.

b) The Board of Directors shall actively consider replacing or shutting down any information system or repository of data that was excluded from penetration testing

or compromised due to any form of external penetration testing, if it cannot be adequately remediated to withstand the penetration tests during next penetration testing exercise. Enhanced and sufficient monitoring and control measures approved by the Board of Directors shall be implemented immediately, until such a system is improved, replaced or shut down.

c) The Board of Directors shall either implement measures as per 1.11 (b) or immediately implement additional control measures to eliminate the risks identified, when the compromise was due to internal penetration testing.

1.12 Internal audit

Annual penetration testing process shall be reviewed by the Board Audit Committee as soon as it is completed.

1.13 Reporting to Director

a) LFCs shall submit an executive summary on the penetration testing exercise, approved by the Board of Directors, to the Director within 60 days from receiving the penetration testing report from the penetration testing service provider.

b) Such executive summary shall indicate number of systems subjected to tests, number of systems excluded, number of systems compromised, whether adequate remediation measures have already been implemented or timeline for the implementation of remediation measures, internal audit assurance on the compliance of penetration testing exercise with the requirements in this regulatory framework, and a brief profile of the penetration testing service provider.

Annexure – IV

1. Red teaming - red team exercises by independent external experts

1.1 Scope and frequency

a) LFCs shall conduct red team exercises that simulate real world adversary scenarios to gain a holistic understanding of the LFC's information security capabilities.

b) All critical information systems and the Board of Directors identified non-critical information systems and repositories of data that could cause substantial adverse impact to LFC due to an information security breach shall be covered under red team exercises.

c) Red team exercises shall be the maximum effort attempts to compromise information systems and data by breaching all layers of the information security including human, physical and technology layers.

d) LFCs shall conduct red team exercises as an extension of penetration tests as per Annexure III to human and physical layers of information security.

e) Red team exercises shall be conducted together with annual penetration testing exercises as per Annexure III during the annual cycles the LFC will be required to conduct red team exercises.

f) All information systems and repositories of data that need to be subjected to penetration tests as per Annexure III shall be subject to red team exercises as well.

g) LFCs shall conduct red team exercises at least once in every 3 years.

1.2 Red Teaming Scope Statement (RTSS)

a) Red teaming exercises shall be conducted based on RTSS.

b) Requirements applicable to PTSS as per Annexure III, 1.7 shall be applicable to RTSS.

c) RTSS shall also define the limits applicable to the red teaming service provider when attempting to breach the human and physical layers of security. The service provider shall be allowed to conduct only the tasks explicitly permitted in RTSS.

1.3 Approval and procedure for the conduct of red team exercises

a) The scope including RTSS, service provider(s), commencement, and time period for the conduct of red team exercises shall be approved by the Board of Directors.

b) The Board of Directors shall ensure the LFC has achieved a sufficient level of information security maturity with respect to all 3 layers of security to be tested through red team exercises, prior to the commencement of red team exercises. In the event, the Board of Directors determine the level of information security maturity is inadequate, the Board shall initiate appropriate remediation measures and defer red team exercises by a maximum period of 12 months.

c) LFCs shall adhere to the procedural requirements specified in Annexure III when conducting red team exercises.

1.4 Remediation

The Board of Directors shall implement an action plan to address the weaknesses identified during red team exercises with regard to the human and physical layers of information security in consultation with the suitable experts in addition to the remediation measures as per Annexure III, 1.11 relating to the weaknesses in the technology layer.

Annexure – V

1. Staff competency requirements

1.1 Recognized qualifications

Academic and professional qualifications as per Tables 1 and 2 below from the institutes specified in 1.2 and 1.3 are recognized as eligible qualifications.

1.2 Academic qualifications

Masters and bachelor's level degree programs awarded by an university or degree awarding institute recognized by the University Grants Commission of Sri Lanka, or masters and bachelors level degree programs accredited by an accreditation body supported by the Institute of Electrical and Electronics Engineers (IEEE).

1.3 Professional qualifications

Professional qualifications from following professional bodies:

a) ISACA

b) $(ISC)^2$; and

c) Global Information Assurance Certification (GIAC)

1.4 Competency requirements

LFCs that are required to set up SOC shall possess at least one qualification from eligible qualifications listed below.

Table 1: Eligible qualifications for the Board and senior managerial level

No.	Qualification/ LFC Category	Board /CISO	Information Security Operations (including SOC)	Risk Management	Internal Audit
1	$(ISC)^2$ Certified Information Systems Security Professional (CISSP)	X	X	X	X
2	GIAC Strategic Planning, Policy, and Leadership (GSTRT)	X			

3	GIAC Information Security Professional (GISP)	X	X	X	X
4	ISACA Certified Information Systems Auditor (CISA)	X			X
5	ISACA Certified Information Security Manager (CISM)	X		X	
6	ISACA Certified in Risk and Information Systems Control (CRISC)	X		X	
7	Master's degree in information security or master's degree in Computer Science/Information Technology specializing in Information Security	X	X	X	X

1.5 Analyst/executive level

Table 2: Eligible qualifications for analyst/executive level

No.	Qualification/ LFC Category	Information Security Operations (Including SOC)	Risk Management	Internal Audit
1	$(ISC)^2$ Systems Security Certified Practitioner (SSCP)	X	X	X
2	ISACA CSX Practitioner Certificate (CSXP)	X	X	X
3	GIAC Security Essentials (GSEC)	X	X	X
4	Bachelor's Degree in Information Security or bachelor's degree in Computer Science/Information Technology specializing in Information Security	X	X	X
5	Relevant managerial level qualification	X	X	X