MONETARY BOARD
CENTRAL BANK OF SRI LANKA

09 December 2021 | BANKING ACT DIRECTIONS | No. 16 of 2021

Regulatory Framework on Technology Risk Management and Resilience for Licensed Banks

In the exercise of the powers conferred by Sections 46(1) and 76(J)(1) of the Banking Act, No. 30 of 1988, as amended, the Monetary Board hereby issues the following Directions on Regulatory Framework on Technology Risk Management and Resilience for licensed commercial banks and licensed specialised banks, hereinafter referred to as licensed banks, with a view to further strengthening the technology risk management and resilience in licensed banks.

1. Empowerment

1.1 In terms of Section 46(1) of the Banking Act, in order to ensure the soundness of the banking system, the Monetary Board is empowered to issue Directions to all licensed commercial banks, regarding the manner in which any aspect of the business of such bank or banks is to be conducted.

1.2 In terms of Section 76(J)(1) of the Banking Act, the Monetary Board is empowered to give Directions to licensed specialised banks or to any category of licensed specialised banks, regarding the manner in which any aspect of the business of such banks is to be conducted.

2. Scope and Applicability

2.1 These Directions shall be applicable to all licensed banks including operations conducted through agents and third-party service providers.

3. Regulatory Framework on Technology Risk Management and Resilience

3.1 All licensed banks shall ensure compliance with the requirements imposed by the regulatory framework on technology risk management and resilience in the Schedule I to these Directions (hereinafter referred to as regulatory framework).

3.2 Requirements in the regulatory framework shall be applicable to the entire operations of licensed banks including operations conducted through agents and third-party service providers.

4. Responsibilities of the Board

4.1 The Board of Directors of licensed banks shall establish adequate oversight measures to ensure implementation of the technology risk management and resilience requirements specified in the regulatory framework by the licensed banks.

5. Governance Framework

5.1 Licensed banks shall establish an effective governance framework approved by the Board of Directors of the licensed bank in compliance with the requirements specified in Section 4 of the regulatory framework, to ensure prudent management of technology risks.

6. Assessment of Technology Risk under Supervisory Review Process

6.1 Licensed banks shall ensure technology risk is assessed as a part of the comprehensive assessment of risks in the bank's Internal Capital Adequacy Assessment Process (ICAAP) and adequate level of capital is held to meet any potential technology risk.

7. Role of the Internal Audit

7.1 The internal audit function of the licensed banks shall ensure that compliance with regulatory requirements on technology risk management is assessed and reported to the Board of Directors of the licensed bank through the Board Audit Committee, at least annually.

8. Steps to Secure Compliance

8.1 Licensed banks shall ensure all new technology initiatives comply with Section 9 of the regulatory framework on requirements based on information system infrastructure ownership, management, and location from the date of these Directions.

8.2 Licensed banks shall ensure compliance with all other requirements of the regulatory framework as per the timelines set out in Section 10 of the regulatory framework on implementation and transitional arrangements.

8.3 Licensed banks designated as Domestic Systemically Important Banks (D-SIBs) shall ensure compliance with the requirements specifically applicable to D-SIBs within 12 months from the date of notification of being designated as a D-SIB or as per Section 10 of the regulatory framework, whichever falls later.

Nivard Ajith Leslie Cabraal
Chairman of the Monetary Board and
Governor of the Central Bank of Sri Lanka

Banking Act Directions No. 16 of 2021

Regulatory Framework on Technology Risk Management and Resilience for Licensed Banks

SCHEDULE I

Regulatory Framework on Technology Risk Management and Resilience for Licensed Banks

1. Objective

This framework intends to set minimum regulatory requirements on technology risk management and resilience for licensed banks in general as well as based on sensitivity of data, criticality of information systems, and type of information system infrastructure used.

2. Applicability

2.1 Requirements in this framework shall be applicable to entire operations of licensed banks including operations conducted through agents and third-party service providers.

2.2 All information systems and related infrastructure used by licensed banks including primary, disaster recovery, and any other types shall comply with the requirements specified in this framework.

3. Definitions

Following definitions shall be applicable for the purposes of this framework.

3.1 Data

3.1.1 Public data

Data that is freely available to everyone to use and republish without any restriction.

3.1.2 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.

3.1.3 De-identified customer data

Intentionally altered customer data that cannot be used alone or in combination with any other data to identify the customer to whom the data was originally related to.

3.1.4 Confidential non-customer data

Any non-public data that do not fall within the definition of customer data and can cause significant financial or reputational loss if used maliciously or leaked, including the licensed bank's financial transactions, submissions to the Board of Directors and management, sensitive employee data, and any other data as determined by the licensed bank.

3.2 Critical information system

Any information system that is essential to the functioning of the financial system of the country and/or to the functioning of the licensed bank as identified by the Board of Directors of the licensed bank, including information systems of the licensed bank and relevant information systems of third-party service providers and agents.

3.3 Third-party service provider

A service provider with whom the licensed bank has entered into an outsourcing arrangement as defined in the Banking Act Direction No. 2 of 2012 on Outsourcing of Business Operations of a Licensed Commercial Bank and a Licensed Specialised Bank, or any succeeding Direction.

3.4 Agent

An agent or sub-agent as defined in the Banking Act Direction No. 2 of 2018 on Appointment of Agents of Licensed Banks, or any succeeding Direction.

3.5 Accredited certification body

A management system certification body accredited for the specified ISO standard by the Sri Lanka Accreditation Board for Conformity Assessment (SLAB) or by an accreditation body which is a member of International Accreditation Forum (IAF).

3.6 Domestic Systemically Important Bank (D-SIB)

Any licensed bank designated as a D-SIB as per the Banking Act Directions No. 10 of 2019 on Framework for Dealing with Domestic Systemically Important Banks, or any succeeding Direction.

3.7 Board of Directors

For licensed banks incorporated in Sri Lanka, this shall mean the Board of Directors of the bank. For licensed banks incorporated outside Sri Lanka, this shall mean the senior most management level committee in Sri Lanka together with the head office executive responsible for Sri Lanka operations or any appropriate higher-level committee at the head office.

3.8 Board Integrated Risk Management Committee (BIRMC)

For licensed banks incorporated in Sri Lanka, this shall mean the integrated risk management committee of the Board of Directors of the bank. For licensed banks incorporated outside Sri Lanka, this shall mean the local risk management committee or in the absence of such committee head of risk management, together with the risk management function in head office or any appropriate higher-level committee at the head office.

3.9 Board Audit Committee (BAC)

For licensed banks incorporated in Sri Lanka, this shall mean the audit committee of the Board of Directors of the bank. For licensed banks incorporated outside Sri Lanka, this shall mean the head of internal audit in Sri Lanka together with the internal audit function in head office or any appropriate higher-level committee at the head office.

4. Governance Framework

4.1 Information Security Committee (ISC)

4.1.1 Licensed banks shall establish an ISC as the apex management level body responsible for information security and technology resilience of the bank. The Committee shall be responsible for both strategic and operational aspects of information security and technology risk management.

4.1.2 ISC shall be chaired by the Chief Executive Officer (CEO) of the bank. The Board of Directors of the licensed bank shall also appoint one or more deputy chairpersons to chair the meetings of ISC when CEO is unable to attend.

4.1.3 The Chief Operating Officer/Head of Operations, Chief Information Security Officer (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 quarterly basis. Participation of any other officers from risk, compliance, or internal audit functions of the bank shall be only on invitation.

4.1.4 Licensed banks incorporated outside Sri Lanka where majority of technology related decisions are made at the head office shall appoint a suitable and sufficiently empowered officer from the head office with seniority equal or higher than the country head of Sri Lankan operations to chair the ISC with the country head as an ex-officio member of ISC.

4.1.5 Licensed banks incorporated outside Sri Lanka shall appoint the relevant officer from the head office to the ISC when any of the officers named in Section 4.1.3 are not in the organization structure of the Sri Lankan branch.

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

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

4.2 Chief Information Security Officer (CISO)

4.2.1 Licensed banks shall appoint a CISO as the executive officer responsible for the licensed bank's information security.

4.2.2 CISO shall be a member of the bank's senior management team and shall be within the immediate two layers below the level of CEO in the organizational structure of the licensed bank.

4.2.3 CISO shall report to the Chief Executive Officer, or Chief Operating Officer (COO) when COO has the overall responsibility for the operational activities of the licensed bank, or to a corporate management member who has a role similar to the role of COO as mentioned above.

4.2.4 D-SIBs shall appoint a dedicated CISO.

4.2.5 As a transitional arrangement for the requirement in 4.2.4, D-SIBs may appoint an officer from the bank's existing senior management team to simultaneously function as the CISO in compliance with the requirements in 4.2.6 up to a period of 2 years.

4.2.6 Licensed banks that are not D-SIBs may appoint an officer from the bank's existing senior 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 licensed bank does not necessitate a dedicated CISO. However, such an officer shall not be Head of Information Technology, Head of Internal Audit, Head of Risk Management, Compliance Officer, or one of their subordinates.

4.2.7 CISO shall be experienced and shall be among the senior most in the licensed bank's organizational hierarchy to ensure effective implementation of information security policies and procedures across the licensed bank and to provide leadership to information security function.

4.2.8 CISO shall possess or acquire eligible qualifications as per requirements in Section 7, within the timelines stipulated under transitional arrangements in Section 10.

4.2.9 Licensed banks incorporated outside Sri Lanka and having information security related decision making handled outside of Sri Lanka, shall designate a sufficiently empowered officer from the head office as the CISO for Sri Lankan operations. Such an officer is exempted from the requirement to possess eligible qualifications as per 4.2.8, but shall possess adequate qualifications in information security as determined by the Head of Human Resources of the bank's head office.

4.2.10 The Board of Directors of licensed bank shall establish appropriate arrangements to fulfill the responsibilities assigned to CISO until a CISO is appointed in accordance with transitional arrangements in Section 10.

4.3 Identification of critical information systems

4.3.1 Board of Directors shall identify information systems falling within the definition of critical information system provided in 3.2, in accordance with requirements in 4.3.2 and 4.3.3.

4.3.2 Critical information systems shall normally include the transaction processing systems, general ledger systems, payment and settlement related systems, delivery channels, systems used for Anti-Money Laundering (AML)/Know Your Customer (KYC) procedures, and any other system that is required to ensure uninterrupted conduct of banking business.

4.3.3 The Board of Directors of a licensed bank may exclude any of the information systems mentioned in 4.3.2 other than transaction processing systems, general ledger systems, and information systems connected to LankaSettle System or are required to fulfill the bank's obligations in the LankaSettle system from being identified as critical, if the concerned information system does not fall within the definition of critical information system in the opinion of the Board of Directors. Such exclusion shall be based on an internally established rational methodology. All such exclusions shall be reviewed at least once every two years and documented in sufficient detail explaining the rationale behind the exclusion.

4.3.4 Licensed banks shall maintain a register recording all the information systems used, including relevant information systems with third-party service providers and agents, clearly identifying whether the information system is a critical information system or not and the type of data the information system is exposed to. Licensed banks may use any existing register/inventory of information systems for this purpose.

4.4 Fair and ethical use of customer data

Licensed banks shall ensure that customer data would only be used in ways the customers would reasonably expect the bank to use such data. 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, licensed banks shall not disclose such data except for as has been provided by law.

4.5 Reporting to Board of Directors

Licensed banks shall establish procedures to regularly report information security and technology risk profile of the bank together with any information security incidents to the Board of Directors through BIRMC using both standard risk indicators and ad-hoc reports.

4.6 Technology risk management function

4.6.1 Licensed banks shall ensure that the bank's risk management function possess a level of maturity in technology risk management that commensurate with the magnitude of technology risk faced by the bank. The level of staff and other resources allocated to the risk management function for technology risk management shall be decided by BIRMC in consultation with the head of risk management.

4.6.2 The Board of Directors shall ensure technology risk appetite is defined through a framework of clearly delineated and measurable technology risk indicators with approved risk tolerance levels.

4.6.3 Licensed banks shall assess technology risk as a part of the comprehensive assessment of risks in the bank's Internal Capital Adequacy Assessment Process (ICAAP).

4.6.4 Licensed banks shall ensure stringent product approval process approved by the Board of Directors and focused on software quality assurance, internal controls, and risk management measures are adhered to, when a new technology driven product or service is introduced or when a change is made to such product or service.

4.6.5 Licensed banks shall ensure that business units responsible for technology driven banking products and services such as payment cards and electronic banking, and information technology and information security related service delivery functions are subjected to quarterly Risk and Control Self-Assessment (RCSA) process implemented and monitored by the risk management function.

4.6.6 Licensed banks shall implement adequate technology risk management and monitoring measures including RCSA processes for third-party service providers and agents that commensurate with the criticality and sensitivity of services carried out by such third-party service providers and agents as approved by BIRMC of the licensed bank.

4.7 Internal audit

4.7.1 Licensed banks shall ensure that compliance with the requirements in this regulatory framework and other CBSL Regulations relating to information security and technology risk management is subjected to an internal audit at least annually.

4.7.2 BAC shall ensure that the licensed bank is complying with the requirement in 4.7.1 even when the internal audit function of the licensed bank is outsourced.

5. Information Security

5.1 Information security training and certification

5.1.1 Training and awareness to Board of Directors

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

(ii) 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 licensed bank.

(iii) Responsibilities of Board of Directors and Board committees in terms of 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.

(iv) 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.

(v) The Board Secretary of the licensed bank shall ensure compliance with the above requirements on training and awareness to Board of Directors.

5.1.2 Information security awareness training and certification requirement for staff

(i) Licensed banks shall ensure that the staff of the licensed bank, 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 following requirements:

(a) Required persons shall complete an information security awareness training program based on the information security policies and procedures of the licensed bank;

(b) Such program as per 5.1.2(i)(a) shall commensurate with the information security responsibilities of the trainee and shall be updated regularly and whenever the bank's information security policies are updated; and

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

(ii) The Board of Directors of a licensed bank may exclude staff of agents and third-party service providers from the requirements in 5.1.2(i), if adequate and comparable information security awareness measures have been implemented by such agents and third-party service providers.

5.2 User access management

5.2.1 Scope

(i) Requirements in 5.2.2 and 5.2.3 on user access management shall be applicable to critical information systems and information systems exposed to customer data.

(ii) Board of Directors shall decide on the need to apply the requirements imposed by 5.2.2 and 5.2.3 for non-critical information systems exposed to confidential non-customer data in consultation with BIRMC and ISC.

(iii) Requirements in 5.2.4 shall be applicable to all information systems as specified.

5.2.2 User access and identity management system

(i) Licensed banks shall implement an industry standard user access and identity management system(s) to manage all users including privileged users.

(ii) Licensed banks may deviate from the requirement in 5.2.2(i) and implement suitable compensating controls, for any existing information system when implementation of industry standard user access and identity management system is not feasible. All such information systems shall be subjected to user access privilege reviews as per the frequency specified in 5.2.4.(i)(a).

5.2.3 Privileged users

Privileged user access shall be provided only on "need-to-have" basis and highest level of access shall only be provided for a limited time when such access is required.

5.2.4 User access privilege reviews

(i) Licensed banks shall conduct user access privilege reviews as follows:

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

(b) At least on quarterly basis for non-critical information systems exposed to customer data and confidential non-customer data.

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

(d) At least on annual basis for all other information systems.

(ii) The objective of user access privilege reviews shall be to establish that all users and their user profiles in an information system are having a valid authorisation for the privileges and status assigned.

(iii) Licensed banks shall adopt appropriate methodologies to conduct user access privilege reviews as approved by ISC.

(iv) User access privilege reviews shall be conducted independently from the user access management function responsible for the creation, alteration, and deletion of user access in information systems.

(v) Risk management department shall conduct a root-cause analysis on discrepancies identified during user access privilege reviews and suggest appropriate internal control enhancements to ISC at least on annual basis.

5.3 Computer security and user activity log management

5.3.1 Licensed banks shall implement a computer security and user activity log management policy adhering to the requirements in 5.3.2 to 5.3.7, to manage computer security and user activity logs of critical information systems and information systems exposed to customer data. Such policy may be extended to other information systems at the discretion of the bank's Board of Directors.

5.3.2 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.

5.3.3 Computer security logs shall include logs generated by security software, operating systems, and applications.

5.3.4 Computer security logs maintained shall be adequate to successfully identify and investigate information security incidents.

5.3.5 User activity logs maintained shall be adequate to establish accountability without repudiation for any access or modification to customer data or critical information systems.

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

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

5.4 Information classification and labelling

5.4.1 All electronically maintained data shall be classified based on information security sensitivity and labelled with assigned classification, as per an information classification policy approved by the Board of Directors.

5.4.2 Licensed banks shall establish an appropriate mechanism to effectively determine the data category to which any piece of data will belong to as per definitions given in 3.1.

5.5 Data encryption

5.5.1 Customer data encryption

(i) Customer data shall normally be protected using encryption as recommended in 5.5.1(ii). This requirement shall be applicable to customer data maintained with the licensed bank, agents, and third-party service providers. However, licensed banks may use alternative controls to protect customer data in accordance with 5.5.1(iv) when encryption is not feasible or appropriate.

(ii) Recommended levels of encryption

(a) **Data-at-rest encryption**

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

(b) **Data-in-transit encryption**

Data-in-transit encryption shall be implemented for customer data. Further, whenever a file containing such data is transmitted it shall remain encrypted at file level.

(c) **Full disk encryption for endpoint devices and removable media**

Endpoint devices and removable media that store customer data of the licensed bank, either permanently or temporarily, including such devices of third-party service providers and agents shall be subject to full disk encryption. The licensed bank may exclude any end point device that is usually non-movable and the risk of data leakage is negligible, from this requirement based on an exclusion criterion approved by the Board of Directors of the licensed bank.

(iii) Types of encryption to be used

Licensed bank shall use industry standard encryption methods. Selection of such methods shall be subjected to the approval of the licensed bank's Board of Directors on the recommendation of BIRMC and ISC.

(iv) Deviations from customer data encryption requirement

(a) Licensed banks may decide to deviate from customer data encryption requirements mentioned in 5.5.1 (ii) for specific scenarios at the discretion of the bank's Board of Directors, when it is not feasible or appropriate to protect customer data using encryption in the given scenario.

(b) The Board of Directors shall ensure adequate compensating controls and monitoring measures are enforced to minimise the risks arising due to customer data not being encrypted, whenever a deviation is approved as per 5.5.1(iv)(a).

(c) All deviations as per Section 5.5.1(iv)(a) together with compensating controls shall be recommended by the ISC through BIRMC for the approval by Board of Directors.

(d) All deviations approved as per 5.5.1(iv)(a) together with associated compensating controls and monitoring measures shall be reviewed at least once in every two years to determine whether data can now be protected with encryption or better compensating controls and monitoring mechanisms can be introduced.

5.5.2 Confidential non-customer data encryption

Encryption requirements for customer data specified in 5.5.1 shall be applicable to confidential non-customer data as well, except with respect to categories of confidential non-customer data that will only pose negligible adverse impact to the licensed bank if subjected to a data leakage or any other adverse information security incident that could have been prevented with encryption as determined by the Board of Directors of the licensed bank.

5.6 Security Operations Center (SOC)

5.6.1 Applicability

All licensed commercial banks, licensed specialised banks that are D-SIBs, and other licensed specialised banks offering electronic delivery channels other than automated teller machines (e.g., internet banking, mobile apps, customer/third-party integrations, etc.) shall implement a SOC as per the requirements in this regulatory framework. Implementation of a Data Loss Prevention (DLP) tool as per 5.6.7(iii) is mandatory for all licensed banks.

5.6.2 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.

5.6.3 Reporting line

The Board of Directors of the licensed bank shall establish an appropriate line of reporting for the SOC. Such a reporting line shall ensure both the bank's CIO/Head of Information Technology and CISO has 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.

5.6.4 Operating hours

SOC shall be operational on 24 X 7 basis. Licensed banks shall decide on staffing levels at different times of the day/week based on activity levels and threat profile.

5.6.5 Human resources, artificial intelligence, and automation

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

(ii) Licensed banks shall rationally decide on the exact staffing level required at each level and on any other types of staff required in the SOC.

(iii) Licensed banks may use artificial intelligence or other automation technologies instead of humans for any of the above roles, except for the role of SOC manager.

5.6.6 Processes

(i) Clearly defined and documented processes

SOC shall have clearly defined and documented processes for event classification and prioritisation, analysis, remediation and recovery, post incident assessment, and forensics. Such processes shall clearly identify the steps to be followed and responsible people for each step.

(ii) 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 suspicious activity from normal activity.

5.6.7 Tools

(i) Monitoring and detection tools

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

(ii) Security Information and Event Management (SIEM) tools

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

(iii) Data Loss Prevention (DLP) tools

(a) Licensed banks shall implement industry standard DLP tools to minimise the risk of data leakages. Scope of implementation shall cover the entire bank, and any third-party service providers and agents exposed to customer data.

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

specified by the licensed bank. Licensed banks shall conduct at least annual reviews of such implementations by third-party service providers and agents to ensure adequate data loss prevention measures are in place.

(c) Licensed banks may exempt third-party service providers from the requirement to implement a DLP tool, if there is no data leakage risk due to the control measures in place when sharing data with the third-party service provider. Such exemption shall be approved by the Board of Directors of the licensed bank based on independent assessments provided by the head of relevant business/operational function, CIO/Head of Information Technology, CISO and Head of Risk Management. All such exemptions shall be reviewed by the Board of Directors at least once in every two years.

5.6.8 Threat information and intelligence

Licensed banks shall implement mechanisms to obtain threat information and threat intelligence from relevant sources. The SOC's staff, processes, and tools shall be capable of aggregating, analysing, and operationalising threat information and threat intelligence received.

5.6.9 Outsourcing of SOC

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

(ii) All decisions to outsource SOC functions shall be made after the Board of Directors evaluating the information security threats posed by such outsourcing, including threats/vulnerabilities that could arise due to any other products or services provided by the SOC service provider to the licensed bank. Such evaluations shall be based on independent assessments submitted to the Board of Directors by CIO/Head of Information Technology, CISO, Head of Legal, and Head of Risk Management.

(iii) Licensed banks shall ensure that third party service providers of SOC services to whom the bank'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 the SOC services provided to the licensed bank.

(iv) Licensed bank shall have a non-disclosure agreement approved by the Board of Directors of the bank with the third-party service provider of the SOC.

(v) All staff allocated by the third-party service providers of SOC to whom the bank's non-public data may be exposed shall be subjected to enhanced background checks by the bank or by the third-party service provider of the SOC through a specialized background checking service acceptable to the bank.

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

(vii) The rights of the Sri Lankan judiciary to request and obtain any information or data relating to the services provided to the licensed bank by any SOC service provider located outside Sri Lanka shall be ensured through contractual agreements between the licensed bank and the SOC service provider.

(viii) Licensed banks shall appoint an officer with sufficient seniority and authority as the SOC Coordinator to coordinate between the licensed bank and the outsourced SOC.

5.6.10 SOC coverage for information systems operated by agents and third-party service providers

Licensed banks shall ensure any critical information systems operated by agents or third-party service providers are covered by a SOC in compliance with the above requirements. In such scenarios the licensed bank shall require the respective agent or third-party service provider to have their own SOC, or subscribe to a third party SOC that fulfills the applicable requirements specified in 5.6.9, or be covered by the bank's SOC as appropriate. Further, licensed banks shall decide the need for coverage of SOC for all non-critical information systems operated by agents and third-party service providers based on an internal risk assessment.

5.7 Information security incident response and recovery

5.7.1 Incident Response Plan (IRP)

Licensed banks shall have an up to date and Board of Directors approved IRP, detailing procedures for incident escalation, remediation, recovery, and communication with internal and external stakeholders. IRP shall include specific procedures to deal with commonly known types of information security incidents, including but not limited to cyber security incidents.

5.7.2 Incident response and recovery testing

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

5.8 Information security testing

5.8.1 Pre-implementation information security testing

(i) Scope

(a) Critical information systems and information systems exposed to customer data shall be subjected 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.

(b) 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 in consultation with BIRMC and ISC, based on the importance of each such information system.

(c) 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 and approval of ISC at the time of implementation of the specific minor modification that need to be excluded.

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

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

(b) Dynamic Application Security Testing (DAST) to detect application level vulnerabilities an attacker could exploit;

(c) Quality assurance testing on computing and networking infrastructure hardening to ensure compliance with internal hardening policies; and

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

(iii) Pre-implementation tests shall be conducted by a team independent of the team responsible for the development and/or implementation of the information system. Licensed banks shall ensure that qualifying information systems operated by agents or third-party service providers are subjected to pre-implementation tests by a suitable internal team of the agent/third-party service or by an external service provider acceptable to the licensed bank.

(iv) Licensed banks may adopt suitable alternative security evaluation methodologies when procuring off-the-shelf software if conducting pre-implementation tests as per 5.8.1(ii) is not possible.

(v) Licensed banks may rely on an assurance provided by an independent third-party, mutually acceptable to both the licensed bank and the information system provider, as an alternative to 5.8.1(ii)(a) in case of information systems provided by external vendors.

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

5.8.2 Vulnerability assessments

(i) Critical information systems and information systems exposed to customer data shall be subject to vulnerability assessments at least quarterly.

(ii) Vulnerability assessments shall focus on both infrastructure vulnerabilities and application vulnerabilities.

(iii) Vulnerability assessments shall be performed on production environments.

(iv) Vulnerability assessments can be performed by the licensed bank's internal information security staff or external experts.

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

5.8.3 Penetration tests by independent external experts

(i) Objective

Licensed banks 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 bank'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.

(ii) Scope and frequency

(a) Critical information systems, information systems exposed to customer data, and repositories of customer data with the licensed bank, agents, and third-party service providers shall be subjected to penetration tests by independent external penetration testing experts.

(b) Critical information systems shall be subjected to penetration tests at least annually while all other qualifying information systems and repositories of customer data as per 5.8.3(ii)(a) shall be subjected to penetration tests at least once in every two years.

(c) The Board of Directors of a licensed bank may require the qualifying agents and third-party service providers of the licensed bank to conduct penetration tests for applicable information systems and customer data with them in accordance with these requirements and report to the bank, instead of being included in the scope of the penetration tests commissioned by the bank. 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 objective of penetration testing is achieved.

(d) 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.

(e) Penetration tests shall be conducted on live/production systems under normal business conditions, subject to 5.8.3(ii)(f) and 5.8.3(viii)(c).

(f) Licensed banks subject to the timelines stipulated under transitional arrangements in Section 10, may initially conduct 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, except when deviations are allowed or necessary.

(g) 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, licensed banks may conduct such exercises with reduced information security as separate or supplementary exercises at the discretion of the Board of Directors.

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

(i) 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.

(j) Both black box penetration testing and gray box penetration testing using bank 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.

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

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

(iii) Leadership team, project manager, and designated point of contact

(a) The Board of Directors of the licensed bank 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 that the penetration testing is conducted in a manner that will best achieve the objective in 5.8.3(i), while ensuring 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 licensed bank's incident escalation chain, who are responsible for informing actual security breaches to external parties including law enforcement authorities and regulators, shall also be members of the leadership team.

(f) The leadership team shall be chaired by the licensed bank's CEO or a management team member who is directly reporting to the CEO, preferably Chief Operating Officer (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.

(iv) 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 licensed bank's risk appetite.

(b) The risk management plan shall include a comprehensive risk assessment and a risk treatment plan detailing risk mitigation strategies 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 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) Licensed banks shall ensure that 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 licensed bank's employees and relevant external parties, will know about the penetration testing exercise until its completion.

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

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

(h) 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) Licensed banks shall ensure the availability of non-disclosure agreement with the penetration testing service provider. Licensed banks shall require the penetration testing service provider to ensure that all personnel deployed by the penetration testing service provider for the penetration testing exercise abide by such non-disclosure agreement.

(v) Selection of penetration testing service provider

(a) Licensed banks shall employ a transparent procurement process with adequate due-diligence measures to select the penetration testing service provider. Such process shall include:

i. Obtaining multiple recent references from previous customers of the service provider who are acceptable to the licensed bank; and

ii. Conducting enhanced background checks for all team members assigned by the service provider to the penetration testing exercise or requiring the service provider to use a mutually acceptable party to conduct such enhanced background checks and submit to the licensed bank.

(b) The penetration testing service providers selected to conduct tests on production systems 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 licensed bank.

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

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

(vi) Threat intelligence and designing of threat scenarios

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

(b) The licensed bank 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 licensed bank. Threat scenarios shall include probable real-life attacks conceptualised from an attacker's point of view.

(d) Threat scenarios of D-SIBs shall normally be designed based on both targeted (bank specific) threat intelligence and generic threat intelligence applicable to banking industry. The Board of Directors of a D-SIB may allow the designing of threat scenarios based only on generic threat intelligence applicable to banking industry if obtaining targeted threat intelligence on the bank is not feasible.

(e) Threat scenarios of non D-SIBs can be designed based only on generic threat intelligence applicable to banking industry, instead of targeted threat intelligence at the discretion of the Board of Directors.

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

(vii) Penetration Test Scope Specification (PTSS)

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

(b) PTSS shall clearly identify the information systems and data subjected 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 licensed bank and threat intelligence obtained, and submit it to the approval of the licensed bank.

(d) Licensed bank shall have final authority over the PTSS.

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

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

(viii) Approval for penetration tests

(a) Commencement of annual penetration tests and finalised PTSS shall be approved by the Board of Directors of the licensed bank, upon

determining that the information systems to be tested should be able to reasonably withstand the vigor of proposed tests.

(b) The Board of Directors of a licensed bank 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 this framework. The Board of Directors shall immediately initiate remediation measures as per 5.8.3(xi) 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 5.8.3 (xi).

(ix) 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 licensed bank 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 that the penetration tests are executed only during such mutually agreed time period.

(c) Licensed banks shall ensure that penetration testing service provider is contractually bound to fulfill their obligations as per 5.8.3(ix)(a) and (b).

(x) Reports of annual penetration testing exercise

(a) Licensed banks 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 mention 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 licensed bank'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 summarise the scope and outcome of the penetration testing exercise, leadership team's assessment on bank's information security and incident response preparedness, and proposed remediation measures in consultation with CIO/Head of Information Technology and CISO.

(xi) 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 of the licensed bank 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 5.8.3(xi)(b) or immediately implement additional control measures to eliminate the risks identified, when the compromise was due to internal penetration testing.

(xii) Internal audit

Annual penetration testing process shall be reviewed by the BAC as soon as it is completed.

(xiii) Reporting to Director of Bank Supervision

(a) Licensed banks shall submit an executive summary on the penetration testing exercise, approved by the Board of Directors of the licensed bank, to the Director of Bank Supervision within 60 days from receiving the penetration testing report from 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.

5.8.4 Red team exercises by independent external experts

(i) Scope and frequency

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

(b) All critical information systems and information systems identified by the licensed bank's Board of Directors as per 5.8.4(i)(c) shall be covered under red team exercises.

(c) The Board of Directors of the licensed bank shall evaluate all non-critical information systems and data repositories to identify any non-critical information systems and repositories of data that could cause substantial adverse impact to the licensed bank due to an information security breach and include those within the scope of red team exercises.

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

(e) Licensed banks shall conduct red team exercises as an extension of penetration tests as per 5.8.3 to human and physical layers of information security.

(f) Red team exercises shall be conducted together with penetration testing exercises as per 5.8.3 during the cycles the licensed banks will be required to conduct red team exercises.

(g) D-SIBs shall conduct red team exercises at least once in every 2 years and licensed banks that are not D-SIBs shall conduct red team exercises at least once in every 3 years.

(ii) Red Teaming Scope Statement (RTSS)

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

(b) RTSS shall clearly identify the information systems and data subjected to test, staff members of the bank and relevant third-party service providers and agents that will be assessed under red teaming, business/operational units and locations that will be assessed under red teaming, techniques and methodologies allowed to be used for red teaming assessments, threat scenarios to be used, targets to be achieved, and time period of the test.

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

(d) Approving authority for RTSS shall be the Board of Directors of the licensed bank.

(e) Licensed banks shall ensure that every red teaming service provider is contractually bound to conduct the penetration testing exercise within the limits specified in RTSS.

(iii) 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 of the licensed bank.

(b) The Board of Directors shall ensure that the licensed bank 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. If 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) Licensed banks shall adopt a board approved procedure to conduct red team exercises that is based on the procedural requirements specified in 5.8.3 with suitable deviations/changes approved by the Board of Directors of the licensed bank.

(iv) Remediation

The Board of Directors of the licensed bank shall implement an action plan to address the weakness identified during red team exercises with regard to human and physical layers of information security in consultation with suitable experts in addition to remediation measures as per 5.8.3(xi) with regard to weaknesses in the technology layer.

6. Information system availability and disaster recovery

6.1 Scope

Requirements specified in 6.2 to 6.6 shall be applicable to critical information systems.

6.2 High availability

6.2.1 Licensed banks shall ensure that critical information systems achieve a high level of system availability.

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

6.2.3 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 arrangements

6.3.1 Licensed banks shall ensure Disaster Recovery (DR) arrangements for critical information systems comply 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 4 hours for critical information systems of licensed banks that are D-SIBs and RTO of less than 6 hours for critical information systems of licensed banks that are not D-SIBs; and

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

6.3.2 Licensed banks shall ensure that RTO and RPO targets determined under 6.3.1 for any information system are in compliance with any stringent RTO or RPO targets imposed on such information systems by any other law or regulation.

6.4 Disaster recovery activation

6.4.1 The Board of Directors of licensed banks shall establish disaster recovery activation triggers for each critical information system based on recommendations of the BIRMC and ISC.

6.4.2 Such activation triggers shall ensure that the licensed bank is having adequate time to activate the DR arrangement in compliance with the RTO target specified in 6.3.

6.5 Disaster recovery testing

6.5.1 Disaster recovery arrangements shall be tested by operating all critical information systems using DR infrastructure for a continuous period of 7 days or more at least once a year.

6.5.2 An annual cycle of DR simulations, in addition to testing of DR infrastructure as per 6.5.1, shall also be implemented to enable the Board of Directors to determine the ability of the licensed bank to achieve the required RTO and RPO targets under different disaster scenarios and take necessary corrective measures where required.

6.6 Backup and recovery policies

Licensed banks shall ensure backup and recovery policies and procedures applicable to critical information systems are properly documented and approved by the Board of Directors. Such policies shall be in line with industry best practices applicable to critical information systems and shall provide for off-line and off-site backups or suitable alternative mechanisms that will achieve the objectives of maintaining such backups.

7. Staff Competency Requirements

Licensed banks shall ensure at least a minimum number of staff with eligible qualifications are employed in information security, technology risk management, and internal audit functions as required by 7.1 to 7.5.

7.1 Recognized qualifications

Academic and professional qualifications as per tables 1 and 2 below from institutes specified in 7.1.1 and 7.1.2 are recognized as eligible qualifications.

7.1.1 Academic qualifications

Masters and Bachelors level degree programs awarded by a university or degree awarding institute recognised 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).

7.1.2 Recognised entities for professional qualifications

Professional qualifications from following professional bodies:

(i) ISACA;

(ii) $(ISC)^2$; and

(iii) Global Information Assurance Certification (GIAC).

7.1.3 In the event of discontinuation of any of the recognised professional qualifications, any succeeding or alternative professional qualification by the same or succeeding professional body shall be considered as an eligible qualification.

7.1.4 Licensed banks incorporated outside Sri Lanka and having information security operations handled outside Sri Lanka may designate similar international qualifications as determined by the Head of Human Resources of the head office as alternative qualifications for staff located outside Sri Lanka.

7.2 Competency requirements for CISO

CISO of a licensed bank that is required to set up a SOC shall possess at least one qualification from eligible qualifications listed in 7.4.

7.3 Minimum number of qualified staff

Licensed banks shall employ staff members possessing at least one eligible qualification for both analyst/executive and managerial levels of information security operations, risk management, and internal audit functions. Minimum number of staff required for each function and eligible qualifications shall be as per 7.4. In case of outsourced services, third party service provider's staff members allocated to the bank with eligible qualifications shall count towards this requirement.

7.4 Eligible qualifications and minimum number of qualified staff

7.4.1 CISO and managerial level

Table 1: Eligible qualifications and minimum number of qualified staff for CISO and managerial level

No.	Qualification/ Bank Category	CISO	Information Security Operations (including SOC)	Risk Management	Internal Audit
1.	**Eligible qualifications:**				
1.1	$(ISC)^2$ Certified Information Systems Security Professional (CISSP)	X	X	X	X
1.2	GIAC Strategic Planning, Policy, and Leadership (GSTRT)	X			
1.3	GIAC Information Security Professional (GISP)	X	X	X	X
1.4	ISACA Certified Information Systems Auditor (CISA)	X			X
1.5	ISACA Certified Information Security Manager (CISM)	X		X	
1.6	ISACA Certified in Risk and Information Systems Control (CRISC)	X		X	
1.7	Masters Degree in Information Security or Masters Degree in Computer Science/Information Technology specialising in Information Security	X	X	X	X
2.	**Minimum number of staff with an eligible qualification:**				
2.1	D-SIBs	1	2	1	2
2.2	Non D-SIBs required to setup a SOC	1	1	-	1
2.3	Non D-SIBs not required to setup a SOC	-*	-	-	-

* No mandatory qualification requirement for CISOs of banks not required to setup a SOC.

7.4.2 Analyst/executive level

Table 2: Eligible qualifications and minimum number of qualified staff for analyst/executive level

No.	Qualification/ Bank Category	Information Security Operations (including SOC)	Risk Management	Internal Audit
1.	**Eligible qualifications:**			
1.1	$(ISC)^2$ Systems Security Certified Practitioner (SSCP)	X	X	X
1.2	ISACA CSX Practitioner Certificate (CSXP)	X	X	X
1.3	GIAC Security Essentials (GSEC)	X	X	X
1.4	Bachelors Degree in Information Security or Bachelors Degree in Computer Science/Information Technology specialising in Information Security	X	X	X
1.5	Relevant managerial level qualification	X	X	X
2.	**Minimum number of staff with an eligible qualification:**			
2.1	D-SIBs	5	1	3
2.2	Non D-SIBs required to setup a SOC	2	1	2
2.3	Non D-SIBs not required to setup a SOC	1	-	1

7.5 Continuous Professional Development (CPD) requirement

7.5.1 Staff possessing eligible professional qualifications

Staff members possessing an eligible professional qualification must complete CPD requirements of the professional qualification or 20 CPD hours annually, whichever is higher. Staff members possessing eligible academic qualifications shall complete at least 20 CPD hours by completing CPD qualifying programs offered by relevant eligible professional qualifications listed above.

7.5.2 Other staff

All other staff employed in information security operations, technology/information security risk management, and information security audit shall complete at least 20 CPD hours annually by completing CPD programs approved by the BIRMC on the recommendation of ISC.

7.5.3 Staff members possessing eligible qualifications but failing to fulfill CPD requirements shall not be considered when determining the number of staff with eligible qualifications.

8. Compliance with International Standards

8.1 The licensed bank shall implement following standards by International Organization for Standardization (ISO) and obtain certification or assurance as outlined below:

Table 3: Mandatory ISO standards

No.	Standard	Scope	Certification/Assurance
8.1.1	**Latest edition of ISO/IEC 27001,** Information security management systems	ISO/IEC 27001 scope shall include business/operational units, locations, and technology infrastructure associated with critical information systems and information systems exposed to customer data and confidential non-customer data. All applicable requirements imposed by this regulatory framework and other CBSL Regulations shall be followed during the implementation of the standard.	**D-SIBs:** Certification from an accredited certification body. **Non D-SIBs:** Certification from an accredited certification body; or assurance from an external auditor approved by the CBSL, if the Board of Directors resolve that the licensed bank's information security risk is minimal and does not require accredited certification. Assurances shall be reviewed at least once every two years.
8.1.2	**Latest edition of ISO/IEC 27035,** Information	ISO/IEC 27035 scope shall include business/operational units, locations, and technology infrastructure	Assurance from the internal audit function of the licensed bank through BAC or external

No.	Standard	Scope	Certification/Assurance
	security incident management	associated with critical information systems and information systems exposed to customer data and confidential non-customer data. All applicable requirements imposed by this regulatory framework and other CBSL regulations shall be followed during the implementation of the standard.	certification/assurance from a suitable party approved by the Board of Directors of the licensed bank. Assurances shall be reviewed at least once every two years.
8.1.3	**Latest edition of ISO/IEC 22301,** Business continuity management systems	ISO/IEC 22301 scope shall include business/operational units, processes, and infrastructure required for the availability of critical information systems. All applicable requirements imposed by this regulatory framework and other CBSL regulations shall be followed during the implementation of the standard.	Assurance from the internal audit function of the licensed bank through BAC or external certification/assurance from a suitable party approved by the Board of Directors of the licensed bank. Assurances shall be reviewed at least once every two years.
8.1.4	**Latest edition of ISO/IEC 20000,** Service management	ISO/IEC 20000 scope shall include information technology and information security related service delivery functions associated with critical information	Assurance from the internal audit function of the licensed bank through BAC or external certification/assurance from a suitable party

No.	Standard	Scope	Certification/Assurance
		systems and information systems exposed to customer data and confidential non-customer data. All applicable requirements imposed by this regulatory framework and other CBSL regulations shall be followed during the implementation of the standard.	approved by the Board of Directors of the licensed bank. Assurances shall be reviewed at least once every two years.

8.2 In the event of discontinuation of any of the above standards by the International Organization for Standardization, the Board of Directors of the licensed bank shall implement relevant succeeding standard or identify and implement an alternative standard if there is no succeeding standard.

9. Requirements based on information system infrastructure ownership, management, and location

9.1 Determination of information system infrastructure ownership, management, and location

9.1.1 Determinants

The ownership and/or management of information system infrastructure shall be determined by the party having ownership and/or responsibility for management of processing, storage, networking, and other fundamental computing resources of an information system. Location will be determined by the place in which all the above components are located.

9.1.2 Criterion to determine ownership

Information system infrastructure shall be considered as 'bank owned' only if the licensed bank holds ownership of all the components referred in 9.1.1 pertaining to an information system. All other ownership arrangements shall be considered as 'third-party service provider owned'.

9.1.3 Criterion to determine management

Information system infrastructure shall be considered as 'bank managed' only if the licensed bank's employees are managing all the components referred in 9.1.1 pertaining to an information system. All other management arrangements shall be considered as 'third-party service provider managed'.

9.1.4 Criterion to determine location

Information system infrastructure shall be considered as 'located in Sri Lanka' only if all the components referred in 9.1.1 pertaining to an information system are in Sri Lanka. All other arrangements shall be considered as 'located outside Sri Lanka'.

9.1.5 Accordingly, following models will be considered within this regulatory framework and requirements in 9.2 to 9.9 shall be applicable based on the model used:

(i) Bank owned and managed, located in Sri Lanka;

(ii) Bank owned and managed, located outside Sri Lanka;

(iii) Bank owned, third-party service provider managed, and located in Sri Lanka;

(iv) Bank owned, third-party service provider managed, and located outside Sri Lanka;

(v) Third-party service provider owned and located in Sri Lanka; and

(vi) Third-party service provider owned and located outside Sri Lanka.

9.2 Bank owned and managed, located in Sri Lanka

No additional requirements are applicable to this model.

9.3 Bank owned and managed, located outside Sri Lanka

9.3.1 Use of this model is normally allowed for licensed banks incorporated outside Sri Lanka when utilising information system infrastructure owned and managed by the head office.

9.3.2 Locally incorporated licensed banks shall not utilise this model, except to facilitate operations of any branch or business unit located outside Sri Lanka where use of information system infrastructure located outside Sri Lanka is essential.

9.3.3 Licensed banks incorporated outside Sri Lanka utilising this model shall ensure the availability of multiple, fully independent telecommunications links, individually capable of serving full workload, with both primary and DR sites from Sri Lanka and between the primary and DR sites.

9.3.4 Licensed banks incorporated outside Sri Lanka that are D-SIBs shall ensure that a fully tested DR arrangement complying with the requirements specified in Section 6 of this regulatory framework is available in Sri Lanka, when this model is utilized for critical information systems.

9.4 Bank owned, third-party service provider managed, and located in Sri Lanka

Licensed banks may utilise this model subject to compliance with requirements specified in 9.8 and 9.9.

9.5 Bank owned, third-party service provider managed, and located outside Sri Lanka

9.5.1 Licensed banks incorporated outside Sri Lanka may utilise this model subject to compliance with requirements in 9.3, 9.8 and 9.9, if this is the model mandated by the head office of such licensed bank.

9.5.2 Locally incorporated licensed banks shall not utilise this model, except to facilitate operations of any branch or business unit located outside Sri Lanka where use of information system infrastructure located outside Sri Lanka is essential.

9.6 Third-party service provider owned and located in Sri Lanka

9.6.1 Licensed banks may utilise this model subject to compliance with requirements in 9.8 and 9.9.

9.6.2 Licensed banks implementing this model for critical information systems shall also comply with the following:

(i) Third-party service provider owned information system infrastructure shall possess a certification for the latest edition of ISO 22301 - Business continuity management systems, from an accredited certification body; and

(ii) Availability of a fully tested DR arrangement, complying with the requirements specified in Section 6 of this regulatory framework, either with the licensed bank or with a different third-party service provider. Such DR arrangement shall be available prior to the commencement of live operations using this model.

(iii) Licensed banks may exclude any non-essential component/service utilizing third-party service provider owned infrastructure and used by a critical information system from DR requirements as per 9.6.2(ii), if non-availability of such component/service either on standalone basis or together with other such components/services will not adversely impact the functioning of the country's financial system or the functioning of the licensed bank.

9.7 Third-party service provider owned and located outside Sri Lanka

9.7.1 Licensed banks may utilise this model subject to compliance with requirements specified in 9.6.

9.7.2 Licensed banks implementing this model for critical information systems shall also comply with the following, in addition to requirements specified in 9.6.2:

(i) Licensed banks that are locally incorporated and licensed banks incorporated outside Sri Lanka that are designated as D-SIBs shall ensure DR arrangement as per Section 9.6.2(ii) is located in Sri Lanka; and

(ii) Availability of multiple fully independent telecommunications links, individually capable of serving full workload, with both primary and DR sites from Sri Lanka and between the primary and DR sites.

9.8 Requirements for using information system infrastructure managed or owned by third-party service providers for any information system

9.8.1 Approval of the Board of Directors of the licensed bank based on a recommendation from the BIRMC of the bank.

9.8.2 Information system infrastructure managed or owned by third-party service providers located outside Sri Lanka shall only be in locations approved by the licensed bank's Board of Directors, having satisfied themselves over the adequacy and effectiveness of legal and regulatory environment in such locations to protect the interests of the licensed bank, its customers, the CBSL, and Sri Lankan judiciary.

9.9 Requirements for using information system infrastructure managed or owned by third-party service providers for critical information systems and for information systems exposed to customer data or confidential non-customer data

9.9.1 Information system infrastructure managed or owned by third-party service providers shall possess a certification for the latest edition of ISO 27001 - Information security management systems, from an accredited certification body.

9.9.2 In the event the third-party service obtained is cloud computing, the cloud computing service provider shall possess a certification for the latest edition of ISO 27017 – Security controls for cloud services, from an accredited certification body.

9.9.3 Customer consent

(i) Explicit customer consent shall be obtained, for exposing customer data to third-party service providers, prior to entering into a new business relationship with either new or existing customer, when a licensed bank is utilising information system infrastructure managed or owned by third-party service providers for information systems exposed to customer data. If information system infrastructure is located outside Sri Lanka, customer's consent shall also be obtained for their data to be located outside of Sri Lanka.

(ii) If any information system exposed to customer data is already utilising information system infrastructure managed or owned by third-party service providers, licensed bank shall inform of such arrangement to all customers whose data are stored or processed in such information systems. Licensed banks shall seek the explicit consent of the customers whose data are stored or processed in an information system utilizing information system infrastructure owned and managed by the bank, whenever such an information system is migrated to information system infrastructure managed or owned by third-party service providers.

(iii) Any customer who fails to respond when consent is requested as per 9.9.3(ii) shall be given at least 3 reminders, at monthly or longer intervals through the preferred communication method registered with the bank.

(iv) Licensed banks may migrate data of existing or past customers who have failed to respond even after 3 reminders as per 9.9.3(iii), to information system infrastructure managed or owned by third-party service providers.

(v) Information about the third-party service provider's involvement together with associated risks and benefits shall be communicated to customers in languages preferred by them when requesting customer consent.

9.9.4 Licensed banks shall ensure the following through contractual agreements with the third-party service provider:

(i) The rights of the CBSL to examine the third-party service provider and its staff associated with the services provided to the licensed bank, as if it is a licensed bank's internal function;

(ii) Third-party service provider to make available any information or data requested by the Director of Bank Supervision concerning the services provided to the licensed bank;

(iii) The rights of the Sri Lankan judiciary to request and obtain any information or data relating to the services provided to the licensed bank either directly or through the licensed bank;

(iv) Third-party service provider to facilitate smooth transfer of data and systems at the end of the contract or whenever demanded by the licensed bank;

(v) 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; and

(vi) Third-party service providers to facilitate internal auditing requirements and information security testing requirements including red team exercises as requirements in this regulatory framework.

10. Implementation and transitional arrangements

10.1 Licensed banks shall ensure all new initiatives comply with the requirements in Section 9 from the date of issue of this regulatory framework.

10.2 Licensed banks shall ensure compliance with all other requirements in this regulatory framework as per table 4 below.

10.3 Licensed banks that are D-SIBs shall ensure compliance with the requirements specifically applicable to D-SIBs within 12 months from the date of notification of being designated as a D-SIB or as per 10.1 and 10.2, whichever falls later.

10.4 The Board of Directors of licensed banks shall monitor the progress made by the licensed bank in achieving the timelines for compliance on quarterly basis from the date of issue of this regulatory framework and take necessary measures to ensure compliance with the given timeline.

Table 4: Timelines for compliance

No.	Ref.	Requirement	Date for Compliance
1.	**General deadline** (All requirements without extended deadlines)		31.12.2022
2.	**Extended deadlines**		
2.1	4.2.1	Appointment of a chief information security officer (CISO)	01.01.2024
2.2	4.2.1 & 4.2.4	Appointment of a dedicated CISO for D-SIBs	01.01.2026

No.	Ref.	Requirement	Date for Compliance
2.3	4.2.7 & 7.2	Qualifications for CISO	31.12.2024
2.4	5.1	Information security training and certification	31.12.2023
2.5	5.2.2	User access and identity management system	31.12.2024
2.6	5.3	Computer security and user activity log management	31.12.2024
2.7	5.5.1	Customer Data encryption	
2.7.1	5.5.1 (ii) (a)	Data-at-rest encryption	31.12.2025
2.7.2	5.5.1(ii) (b)	Data-in-transit encryption	31.12.2024
2.7.3	5.5.1(ii) (c)	Full disk encryption for removable media	31.12.2023
2.7.4	5.5.1(ii) (c)	Full disk encryption for endpoint devices	31.12.2026
2.8	5.5.2	Confidential non-customer data encryption	31.12.2025
2.9	5.6	Security Operations Center (SOC)	31.12.2024
2.10	5.8.1	Pre-implementation information security testing	31.12.2023
2.11	5.8.3	Penetration tests by independent external experts – on non-production systems	31.12.2023
2.12	5.8.3	Penetration tests by independent external experts – on production systems	31.12.2025
2.13	5.8.4	Red team exercises by independent external experts	31.12.2026
2.14	6	Information System Availability and Disaster Recovery	31.12.2024
2.15	7	Staff competency requirements	31.12.2024
2.16	8	Compliance with international standards	
2.16.1	8.1.1	ISO/IEC 27001, Information security management systems	31.12.2024
2.16.2	8.1.2	ISO/IEC 27035, Information security incident management	31.12.2025
2.16.3	8.1.3	ISO/IEC 22301, Business continuity management systems	31.12.2024
2.16.4	8.1.4	ISO/IEC 20000, Service management	31.12.2025
2.17	9	Requirements based on information system infrastructure ownership, management, and location - Compliance for existing arrangements	31.12.2024