CENTRAL BANK OF SRI LANKA

08 December 2023 BANKING ACT DIRECTIONS No. 05 of 2023

AMENDMENTS TO THE BANKING ACT DIRECTIONS NO. 16 OF 2021 ON REGULATORY FRAMEWORK ON TECHNOLOGY RISK MANAGEMENT AND RESILIENCE FOR LICENSED BANKS

In the exercise of the powers conferred by Sections 46(l) and 76(J)(1) of the Banking Act, No. 30 of 1988, as amended, the Central Bank of Sri Lanka hereby issues the following amendments to the Schedule 1 of the Banking Act Directions No. 16 of 2021 on Regulatory Framework on Technology Risk Management and Resilience for Licensed Banks.

1. Section 3.3 shall be replaced with the following:

Third-party service provider

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

However, a service provider of a locally incorporated licensed bank that is a subsidiary of the licensed bank and is operating to provide services exclusively to the licensed bank/group, and a service provider of a licensed bank incorporated outside Sri Lanka that is either the licensed bank's head office, a branch of the head office, or a subsidiary that is operating to provide services exclusively to the head office and its branches/group, can be excluded from being considered as a third party service provider for the purposes of this regulatory framework at the discretion of the Board of Directors of the licensed bank, provided such operations comply with the requirements of this regulatory framework applicable to the licensed bank.

2. Section 4.3.3 shall be replaced with the following:

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 and general ledger systems used for banking transactions and information systems connected to LankaSettle System or systems that are required to full fill 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 with sufficient details explaining the rationale behind the exclusion.

3. Section 4.6.5 shall be replaced with the following:

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 Risk and Control Self-Assessment (RCSA) process implemented and monitored by the risk management function with at least sample-based control testing on a quarterly basis while conducting comprehensive RCSA exercises at a frequency determined by the Board of Directors of the licensed bank.

4. Section 5.2.4 (i) shall be replaced with the following:

(i) Licensed banks shall conduct user access privilege reviews as follows:
   (a) At least on quarterly basis for critical information systems.
   (b) At least on bi-annual basis for non-critical information systems exposed to customer data and confidential non-customer data.
   (c) At a frequency decided and approved by the Board of Directors of the licensed bank, for a sample of 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.

5. Section 5.8.3 (ix)(d) shall be inserted immediately after Section 5.8.3 (ix)(c):

The licensed banks incorporated outside Sri Lanka may use penetration test teams from their head office/branches, to conduct the penetration tests.

6. Section 6.5.1 shall be replaced with the following:

Disaster recovery arrangements shall be tested by operating all critical information systems using DR infrastructure for a continuous period of 5 days or more at least once a year.

7. Section 9.1.2 shall be replaced with the following:

Criterion to determine ownership

(i) 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' subject to (ii) below.

(ii) Information system infrastructure of locally incorporated licensed banks owned by the subsidiaries of the bank that are operating to provide services exclusively to the licensed bank/group and information system infrastructure of licensed banks incorporated outside Sri Lanka owned by its head office, branches of the head office, and subsidiaries that are operating to provide services exclusively to the head office and its branches/group can be considered as bank owned at the discretion of the Board of Directors of the licensed bank, provided such arrangements comply with the requirements of this regulatory framework applicable to the licensed bank.

8. Section 9.1.3 shall be replaced with the following:

Criterion to determine management

(i) 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' subject to (ii) below.

(ii) Information system infrastructure of locally incorporated licensed banks managed by the subsidiaries of the bank that are operating to provide services exclusively to the licensed bank/group and information system infrastructure of licensed banks incorporated outside Sri Lanka managed by its head office, branches of the head office, and subsidiaries that are operating to provide services exclusively to the head

office and its branches/group can be considered as bank managed at the discretion of the Board of Directors of the licensed bank, provided such arrangements comply with the requirements of this regulatory framework applicable to the licensed bank.

9. The Timeline for compliance given in Section 10.4 shall be amended as follows:

Table 4: Timelines for compliance

No.	Ref.	Item	Date for Compliance
1	General deadline (for all requirements without extended deadlines)		31.03.2024
2.5	5.2.2	User access and identity management system	31.12.2026
2.7.2	5.5.1 (ii) (b)	Data-in-transit encryption	31.12.2026
2.10	5.8.1	Pre-implementation information security testing	31.12.2025
2.12	5.8.3	Penetration tests by independent external experts – on production system	31.12.2028

Dr. P Nandalal Weerasinghe
Chairman of the Governing Board and the
Governor of the Central Bank of Sri Lanka