October 2021

REGULATORY BRIEF

STRENGTHENING CYBER RESILIENCE OF LICENSED OPERATORS

Labuan IBFC
International Business and Financial Centre, Malaysia

The cyber risks emanating from expanding digital and virtual transactions such as security failures and system deficiencies related to information technology have increasingly become key concerns amongst financial institutions, potentially leading to business disruptions, financial losses and reputational implications.

Resulting from the growing challenge in cyber risks, the Labuan Financial Services Authority (Labuan FSA) has issued Guidelines on Digital Governance Framework (Guidelines) with the aim of strengthening the cyber resilience of Labuan Financial institutions (LFIs) through the adoption of good governance and risk management practices to ensure operational robustness and efficiency.

Labuan FSA encourages digital innovation tailored to current market needs, whilst ensuring business is conducted in a conducive and safe operating environment.

The Guidelines provides with six principles of regulatory requirements that need to be observed by LFIs and are complemented by recommended internal and global best practices. The Guidelines will take effect from 1 January 2022.

PRINCIPLE 1:
Digital Governance Oversight

The board of directors (BOD) is ultimately responsible in overseeing the LFI's digital governance and cyber risk management. The senior management effects the policies approved by the BOD and continuously monitors these policies to ensure that these remain appropriate to the LFI's business and changing industry landscape.

PRINCIPLE 2:
Cyber Risk Management

An effective cyber risk management entails enterprise-wide strategies to preserve data confidentiality, system security and resilience in a systematic and consistent manner.

STRENGTHENING CYBER RESILIENCE OF LICENSED OPERATORS

PRINCIPLE 3:
Management of Digital Services Offered by LFIs

The LFI needs to maintain robust security controls that commensurate with the risk and complexity of digital services rendered to its clients. The LFI must ensure that these controls always remain relevant and effective.

PRINCIPLE 4:
External Service Arrangement

The LFIs needs to ensure that all risks from external service arrangements are appropriately identified and managed. The obligations of the service provider and the LFI's expectation on the services to be rendered would need to be sufficiently captured in the service level agreement.

PRINCIPLE 5:
Maintenance and Review

Periodic assessments, testing and maintenance of critical IT systems are essential to minimise and mitigate any potential threats in a timely manner. These would provide assurance to the LFI on the adequacy and effectiveness of its IT systems and cybersecurity internal controls.

PRINCIPLE 6:
Awareness and Training

The LFI must conduct awareness programmes and participate in trainings on emerging cyber risks and digital related issues to mitigate cyber threats and vulnerabilities.

REFERENCE

The Guidelines are available at the following link:

VIEW PDF

A Frequently Asked Questions (FAQs) has also been published to provide further clarification on the Guidelines. The FAQs are available at the following link:

VIEW PDF