GUIDELINES ON DIGITAL GOVERNANCE FRAMEWORK

1.0 Introduction

1.1 The cyber risks emanating from expanding digital and virtual transactions such as IT security failures and system deficiencies have increasingly become key concerns amongst financial institutions as these may lead to business disruptions, financial losses and reputational implications.

1.2 Cyber risk presents a growing challenge for financial institutions as they may be exposed to data and identity theft, extortion, or other unlawful activities. As such, there is a need for financial institutions to strengthen their cyber resilience against the operational disruptions to ensure continuity in servicing their clients and to maintain confidence in Labuan IBFC.

1.3 The *Guidelines on Digital Governance Framework* (the Guidelines) is intended to cater for the expanding Digital Financial Services (DFS) in the Centre and ensure that their business operations are undertaken in a prudent manner. This is in line with the objective of promoting overall market stability as well as the orderly development of the Labuan IBFC.

2.0 Regulatory Requirements

2.1 The Guidelines outlines the regulatory requirements on digital governance to be observed by Labuan financial institutions (LFIs) and this comprised the following key areas:

(i) Digital governance oversight;

(ii) Cyber risk management;

(iii) Management of digital services offered by LFIs;

(iv) External service arrangement;

(v) Maintenance and review; and

(vi) Awareness and training.

2.2 The application and observance of the principles specified under the Guidelines is to be achieved by the LFIs through the minimum requirements of the Guidelines and be complemented by the recommended best practices:

(i) Minimum requirements must be complied with by all LFIs. For completeness, these applications may refer to relevant regulatory requirements of other existing guidelines that have been issued by Labuan FSA, but are included in the Guidelines to ensure cohesiveness in their collective application; and

(ii) The best practices are broad guidance on other advanced applications of the digital governance commonly observed in international markets. This includes standards on areas including information technology and cybersecurity management of the International Organization for Standardization (ISO). Although these best practices are not made mandatory, LFIs are encouraged to adopt them as their business operations grow and mature over time.

2.3 The Guidelines complements and is to be read together with the following guidelines issued by Labuan FSA which are applicable to the relevant LFIs as attached in the **Appendix**:

(i) *Circular on Innovative Financial Services in the Labuan International Business and Financial Centre;*

(ii) *Guidelines on Money Broking Business in Labuan IBFC;*

(iii) *Guidelines on Corporate Governance for Labuan Banks and Labuan (Re)Insurers;*

(iv) *Prudential Framework of Corporate Governance for Labuan Insurance and Insurance-Related Companies;*

(v) *Governance and Conduct Framework for Labuan Trust Companies;*

(vi) *Guidelines on External Service Arrangements for Labuan Financial Institutions;* and

(vii) *Guiding Principles on Business Continuity Management.*

2.4 The Guidelines recognises the benefits of cost-rationalisation and greater efficiency that can be achieved through centralised or intra-Group arrangements. For this purpose, the LFI may leverage on its group or head office's digital governance and cyber risk management policies and procedures as long as the approach meets the minimum requirements of the Guidelines. Notwithstanding this permissibility, the ultimate responsibility remains with the LFI's board of directors in ensuring its compliance to the Guidelines.

3.0 Applicability

3.1 The Guidelines is applicable to the following LFIs:

(i) Labuan banks and Labuan investment banks licensed under Part VI of the Labuan Financial Services and Securities Act 2010 (LFSSA);

(ii) Labuan Islamic banks and Labuan Islamic investment banks licensed under Part VI of the Labuan Islamic Financial Services and Securities Act 2010 (LIFSSA);

(iii) Labuan insurers and reinsurers including Labuan captive insurance business licensed under Part VII of the LFSSA;

(iv) Labuan takaful and retakaful operators including Labuan captive takaful business licensed under Part VII of the LIFSSA;

(v) Labuan insurance managers and Labuan takaful managers licensed under Part VII of the LFSSA and Part VII of the LIFSSA, respectively;

(vi) Labuan underwriting managers and Labuan takaful underwriting managers licensed under Part VII of the LFSSA and Part VII of the LIFSSA, respectively;

(vii) Labuan insurance brokers and Labuan takaful brokers licensed under Part VII of the LFSSA and Part VII of the LIFSSA, respectively;

(viii) Labuan trust companies including Labuan managed trust companies licensed under Part V of the LFSSA;

(ix) Labuan money-broking business and Islamic money-broking business licensed under Part VI of the LFSSA and Part VI of the LIFSSA, respectively;

(x) Labuan fund managers licensed under Part III of the LFSSA and Part IV of the LIFSSA;

(xi) Labuan securities licensees and Islamic securities licensees licensed under Part IV of the LFSSA and Part V of the LIFSSA, respectively;

(xii) Labuan credit token business and Islamic credit token business licensed under Part VI of the LFSSA and Part VI of the LIFSSA, respectively; and

(xiii) Labuan exchanges established under Part IX of the LFSSA.

3.2 Notwithstanding paragraph 3.1, Labuan FSA reserves the right to modify the scope to include other LFIs to observe the minimum requirements of the Guidelines which may be specified from time to time.

4.0 Legal Provision

4.1 The Guidelines is issued pursuant to Section 4A of the Labuan Financial Services Authority Act 1996 (LFSAA) to specify the minimum requirements under paragraph 2.2 (i) of the Guidelines.

4.2 The best practices as specified under paragraph 2.2 (ii) are not legally binding as these are intended to be guidance, advice or recommendations that are encouraged to be adopted by LFIs.

5.0 Effective Date

5.1 The Guidelines, which will come into effect on **1 January 2022**, would remain effective and applicable unless amended or revoked. Notwithstanding this, LFIs that wish to early adopt the requirements of the Guidelines are permitted to do so prior to the effective date.

6.0 Definitions

Cyber risk	Threats or vulnerabilities emanating from the connectivity of internal technology infrastructures to external infrastructures, networks or the Internet.
Critical system	Any core application system that supports the provision of banking, investment banking, insurance and insurance-related, takaful and takaful-related, trust company services, fund management, exchanges, money broking, payment services or any digital financial-related businesses[1], where failure of the system has the potential to significantly impair the LFI's provision of financial services to clients or counterparties, business operations, financial position, reputation, or compliance with applicable laws and regulatory requirements.
Digital services	The provision of services by LFIs to clients that is delivered via electronic channels and devices including Internet and mobile devices.
External service provider	An internal group affiliate or external entity providing technology-related functions or services that involve the transmission, processing, storage or handling of confidential information pertaining to the financial institution or its clients. This includes cloud computing software, platform and infrastructure service providers.
Key LFIs	LFIs that are subject to the *Guidelines on External Service Arrangements for Labuan Financial Institutions* i.e. Labuan banks and investment banks, Labuan Islamic banks and Islamic investment banks, Labuan insurers and reinsurers, Labuan takaful and retakaful operators and Labuan fund managers.

[1] The digital financial-related business may include but not limited to digital-banking, insurtech business and digital intermediaries such as Robo-advisors, digital asset exchanges, crypto trading platforms, blockchain tokens as well as e-payment systems.

7.0 Digital Governance Oversight

<u>Principle 1</u>: The board of directors[2] is ultimately responsible in overseeing the LFI's digital governance and cyber risk management. The senior management[3] effects the policies approved by the Board and continuously monitors them to ensure that these remain appropriate to the LFI's business.

Minimum Requirements

7.1 The board of directors is expected to oversee and ensure that:

(i) the digital governance including cyber risk management policies are timely approved to mitigate cyber risks;

(ii) the cyber risks appetite is aligned with the LFI's risk appetite statement;

(iii) the cyber risk management includes the strategic and reputational risks associated with any particular cyber-incident; and

(iv) the critical digital operations which are undertaken by the external service providers engaged by the LFI remain effective.

7.2 The senior management is expected to translate the approved digital governance framework into specific policies and operating procedures. In this regard, the senior management is required to ensure that the LFI:

(i) implements the cyber risk management and cybersecurity policies and procedures to mitigate and manage cyber risks exposures;

(ii) reviews the policies and operating procedures on digital governance and cyber risk management in a periodic manner;

(iii) employs adequate and competent resources to support the implementation of cyber risk management; and

(iv) provides timely updates to the board on key developments which materially affect the LFI including cybersecurity matters.

---

[2] For LFI operating as a branch, any reference made in the Guidelines in relation to the 'board' should refer to the LFI's regional/head office or an equivalent person, whichever is relevant.

[3] 'Senior management' should refer to the Principal Officer (PO) of the branch or any officer performing a senior management function in respect of the LFI's operation.

Best Practices

1. In discharging its oversight functions, the board may consider to:

   (i) set performance metrics or indicators, as appropriate to assess the effectiveness of the implementation of cyber policies and procedures by the senior management; and

   (ii) establish a committee to support the board in providing oversight over digital and cyber-related matters.

2. In order to promote effective technology discussions at the board level, the LFI may consider including into its board at least a member with technology experience and competencies.

3. The senior management may designate dedicated staff, who is not engaged in day-to-day technology operations, for the identification, assessment and mitigation of technology risks.

8.0 Cyber Risk Management

<u>Principle 2</u>: An effective cyber risk management entails enterprise-wide strategies to preserve data confidentiality, system security and resilience in a systematic and consistent manner.

Minimum Requirements

8.1 The LFI is required to adopt effective cyber risk management practices and internal controls in relation to its business. This includes assessing the effectiveness of the cyber security in terms of the following parameters:

(i) data confidentiality is preserved;

(ii) system security and reliability is ensured; and

(iii) cyber resilience and recovery arrangement is maintained.

These practices and controls are expected to be integrated within the LFI's culture and business operations over time to maintain operational resilience against cyber threats.

8.2 The LFI's cyber risk management shall be commensurate with its risk profile. The LFI must ensure that comprehensive strategies and measures are developed to manage cyber risk which include, but not limited to the following areas:

(i) Preventive measures

(a) assignment of responsibilities to appropriate officer(s) so that cyber risks are managed effectively across the critical functions;

(b) identification, classification and prioritisation of critical systems, information, assets and interconnectivity to obtain a complete and accurate view of the LFI's information assets, critical systems, interdependencies and cyber risk profile;

(c) risk controls, mitigations and assessment approaches and methodologies for managing cyber risk exposures and threats. This includes controls to validate and monitor all financial transactions to mitigate cyber-attacks, transaction fraud, phishing and compromise of application systems and information;

(ii) Detective measures

(a) monitoring of any potential cyber incidents and breaches within its systems and network;

(b) timely detection of and response to cyber breaches to ensure that any adverse effect of a cyber-incident is properly managed;

(c) adopting layered (defence-in-depth)[4] security controls to protect data, infrastructure and assets against evolving cyber threats;

(iii) Corrective and recovery measures

(a) policies and procedures for incident handling, crisis response management to support the swift recovery from cyber-incidents

[4] Security strategy integrating people, processes and technology to establish a variety of barriers across multiple layers and dimensions of the organisation.

as well as mechanisms to rectify any damage resulting from a cybersecurity breach;

(b) a recovery plan for systems, operations and services arising from a cyber-incident or breach; and

(c) recovery time objective for a cyber-breach on critical systems to ensure uninterrupted provision of important services to clients.

8.3 The LFI is required to incorporate the internal control procedures to protect sensitive or confidential information as part of its cyber risk management framework. These include clear data loss prevention strategy to ensure proprietary, client and counterparty information is identified, classified and secured.

8.4 The LFI's cyber risk management framework would need to include appropriate strategies for handling varying cyber-attack scenarios, crisis management, communication procedures and disaster recovery plan. These strategies can be embedded into the LFI's overall business continuity management which is specified under the *Guiding Principles on Business Continuity Management* and applicable to relevant LFIs.

Best Practices

1. The LFI may consider a more sophisticated protection, encryption and strong access control for sensitive or confidential information stored on LFI's IT systems, servers, and databases.

2. In order to expedite the dissemination of information and improve the communication efficiency in the event of material cyber-incidents, the LFI may consider to establish an automated call tree or system-based platforms to communicate with all relevant internal and external parties including Labuan FSA.

3. The LFI may consider to procure a cyber insurance with adequate coverage that is appropriate to its cyber risk exposure and appetite.

9.0 Management of Digital Services Offered by LFIs

<u>Principle 3</u>: The LFI needs to maintain robust security controls that commensurate with the risk and complexity of digital services rendered to its clients. The LFI ensures that these controls remain relevant and effective at all times.

Minimum Requirements

9.1 As provided under paragraph 8.0 of the Guidelines, the LFI that provides digital services is expected to have robust digital security controls as part of its cyber risk management. These security controls would need to ensure the following objectives are met:

(i) Confidentiality and integrity of client and counterparty information and transactions;

(ii) Reliability of services delivered via channels and devices with minimum disruption to services;

(iii) Proper authentication of users or devices and authorisation of transactions;

(iv) Sufficient audit trail and monitoring of anomalous transactions; and

(v) Strong physical control and logical control measures.

9.2 LFIs that use advanced technology to authenticate and deliver digital services such as biometrics, tokenisation and contactless communication must ensure compliance with internationally recognised standards, where available.

9.3 Sufficient number of backup copies of critical data, the updated version of the operating system software, production programs, system utilities, all master and transaction files and event logs are maintained by the LFI.

9.4 The LFI shall have a reliable and secure enterprise network infrastructure that is able to support its business activities as well as protect its critical systems against potential network faults and cyber threats. A reliable and secure network infrastructure can be achieved by implementing measures

to safeguard the confidentiality, integrity and availability of data, amongst others, by having the following:

(i) Network security measures such as firewalls to secure the network between the LFI and the internet, as well as connections with external parties;

(ii) Network intrusion prevention systems that are deployed in the LFI's network to detect and block malicious network traffic; and

(iii) Network access controls to detect and prevent unauthorised devices from connecting to the LFI's network.

Best Practices

1. Where third party software is used, the LFI may rely on relevant independent reports provided such reliance is consistent with its risk appetite and tolerance, and the nature of digital services provided by the LFI which leverage on the technologies and algorithms.

2. In order to enhance security controls for its digital services, the LFI may consider developing a robust and resilience cryptography policy to promote the adoption of strong cryptographic controls for protection of important data and information.

10.0 External Service Arrangement

<u>Principle 4</u>: The LFI 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.

Minimum Requirements

10.1 The LFI needs to address any risks and vulnerabilities arising from the engagement of any external service provider to manage or render services relating to its critical IT systems.

10.2 The LFI is required to undertake a proper due diligence on the external service provider's competency, system infrastructure and financial viability prior to engaging its services.

10.3 The service level agreement shall specify the obligations between the LFI and the external service provider.

10.4 The LFI must validate the external service provider's recovery and resumption capability and provisions to facilitate an orderly exit by ensuring that LFI has ready access to all its records and information in the event of failure or unsatisfactory performance by the external service provider, as practicable.

10.5 The LFI needs to ensure that the external service provider provides sufficient notice to the LFI before any changes are undertaken that may impact its IT systems and digital services arrangement. Such notification would need to be incorporated in the service level agreement to ensure that it is a contractual obligation.

10.6 The LFI is required to conduct an appropriate risk assessment prior to adopting cloud services. This assessment would include the inherent architecture of cloud services that leverages on the sharing of resources and services across multiple tenants over the Internet.

10.7 For key LFIs, they are required to adhere and read Paragraph 10 together with the requirements of the *Guidelines on External Service Arrangements for Labuan Financial Institutions.*

Best Practices

1. In conducting risk assessment for cloud adoption, the LFI may consider the risks associated with cloud services as follows:

   (i) sophistication of the deployment model;

   (ii) migration of existing systems to cloud infrastructure;

   (iii) multi-tenancy or data co-mingling;

   (iv) vendor lock-in and application portability or interoperability;

(v) ability to customise security configurations of the cloud infrastructure to ensure a high level of data and technology system protection;

(vi) exposure to cyber-attacks via cloud service providers;

(vii) termination of a cloud service provider including the ability to secure the LFI's data following the termination;

(viii) demarcation of responsibilities, limitations and liability of the service provider; and

(ix) ability to meet regulatory requirements and international standards on cloud computing on a continuing basis.

11.0 Maintenance and Review

<u>Principle 5</u>: 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.

Minimum Requirements

11.1 The LFI is required to ensure that a periodic assessment on its critical network infrastructure as well as security testing on platforms, applications and critical systems is undertaken to identity vulnerabilities. The frequency of the assessment is to be determined based on the LFI's risk appetite and its own risk experience. For instance, if the LFI recorded a cyber risk incident in a particular period, then it would be appropriate for the LFI to subsequently undertake a more frequent assessment of its critical network infrastructure. The assessment is expected to be undertaken by the LFI's own IT expertise or external IT professionals engaged by the LFI.

11.2 The outcome of the testing is properly documented and escalated in a timely manner to senior management for relevant responses or plan.

11.3 A periodic cyber drill to test the effectiveness of LFI's cyber crisis plan needs to be conducted to reflect current developments and emerging cyber threat

scenarios. The frequency of the cyber drill should be consistent with the LFI's risk assessment and appetite.

11.4 The LFI would need to ensure that its internal audit oversight includes planned assessments on the effectiveness of its cyber risk internal controls. This would typically include review on the sufficiency of measures for its system's security, IT support that it obtains from service providers as well as digital services that it provides to its clients.

11.5 The scope, frequency and intensity of the internal audit should be in line with the LFI's annual audit plan as well as its own risk assessment and appetite. For LFIs that leverage on their head office or group's cyber risks management, such audit can be undertaken by the group's internal audit.

11.6 For clarity, the internal audit exercise is expected to be conducted by the LFI's internal audit function. This shall be an independent exercise to the periodic network assessment under paragraph 11.1 of the Guidelines.

Best Practices

1. The LFI may consider to obtain an independent assurance from third party expertise on the security and effectiveness of its IT network/system, applications and data recovery planning.

2. In order to enhance its internal audit oversight on digital and cyber risk internal controls, the LFI may consider to have an internal audit function that is adequately resourced with relevant IT and cyber audit competencies.

3. The LFI that undertakes digital financial services may consider to establish a dedicated IT internal audit function to undertake cyber audits.

12.0 Awareness and Training

Principle 6: The LFI must conduct awareness programme and participate in trainings on emerging cyber risks and digital-related issues to mitigate cyber threats and vulnerabilities.

Minimum Requirements

12.1 The LFI is required to conduct periodic awareness programmes for all staff on cybersecurity areas and emerging threats which include the applicable law, regulations, and internal policies and procedures pertaining to the usage, deployment and access to its critical IT resources.

12.2 The LFI's staff that are involved in IT operations, cybersecurity and risk management would need to undergo the needed training in relation to relevant cyber risk areas on periodic basis to enable effective performance of their roles and responsibilities.

Best Practices

1. The LFI may consider to extend the awareness and training programmes to its board members, senior management and external service providers to enhance their understanding on a wide range of cyber threats, incidents and emerging trends affecting the LFI.

2. The LFI may consider to require the staff working on day-to-day IT operations such as IT security, project management and cloud operations are professionally certified.

Labuan Financial Services Authority
13 September 2021

Appendix List of Guidelines to be Read Together with the Guidelines

Guidelines	Applicable LFIs
1. Circular on Innovative Financial Services in the Labuan International Business and Financial Centre	Labuan entities carrying out digital financial services
2. Guidelines on Money Broking Business in Labuan IBFC	Labuan money brokers and Islamic money brokers
3. Guidelines on Corporate Governance for Labuan Banks and Labuan (Re)Insurers	▪ Labuan banks and investment banks ▪ Labuan Islamic banks and Islamic investment banks ▪ Labuan insurers and reinsurers ▪ Labuan takaful and retakaful operators
4. Prudential Framework of Corporate Governance for Labuan Insurance and Insurance-Related Companies	▪ Labuan captive insurance business and Labuan captive takaful business ▪ Labuan insurance-related companies and Labuan takaful-related companies
5. Governance and Conduct Framework for Labuan Trust Companies	Labuan trust companies
6. Guidelines on External Service Arrangements for Labuan Financial Institutions	▪ Labuan banks and investment banks ▪ Labuan Islamic banks and Islamic investment banks ▪ Labuan insurers and reinsurers ▪ Labuan takaful and retakaful operators ▪ Labuan fund managers

Guidelines	Applicable LFIs
7. Guiding Principles on Business Continuity Management	▪ Labuan banks and investment banks ▪ Labuan Islamic banks and Islamic investment banks ▪ Labuan insurers and reinsurers ▪ Labuan takaful and retakaful operators ▪ Labuan captive insurance business and Labuan captive takaful business ▪ Labuan insurance-related companies and Labuan takaful-related companies ▪ Labuan fund managers ▪ Labuan exchanges ▪ Labuan securities licensees and Islamic securities licensees ▪ Labuan trust companies including Labuan managed trust companies