GUIDELINES ON TECHNOLOGY AND CYBER RISK MANAGEMENT FOR LABUAN BANKS AND LABUAN (RE)INSURERS

1.0 Introduction

1.1 In today's increasingly interconnected and technology-driven world, financial institutions face numerous challenges when it comes to safeguarding their digital assets. The rapid evolution of technology has brought forth a multitude of opportunities, but it has also exposed businesses to a wide array of risks, particularly in the realm of cybersecurity. Additionally, the extensive reliance on technology in the provision of financial services poses a significant technology risk, which may arise from system failures, cyber threats, data breaches and other technology vulnerabilities. Effective technology risk management and cyber risk management practices have become crucial for financial institutions to ensure the protection of their valuable data, systems, and reputation.

1.2 Technology risk management refers to the systematic identification, assessment, and mitigation of risks associated with the use of technology within the financial institution. It encompasses a broad spectrum of risks, including operational, financial, legal, and reputational risks that can arise from the use, implementation, and reliance on technology infrastructure, systems, and processes. Cyber risk management is a subset of technology risk management that specifically focuses on the identification, assessment, and mitigation of risks related to cybersecurity.

1.3 In this regard, Labuan FSA expects the Labuan Financial Institutions (LFIs) that undertake digital financial services to adhere with the minimum standards set out in the *Guidelines on Technology and Cyber Risk Management for Labuan Banks and Labuan (Re)Insurers* (the Guidelines) to strengthen their technology and cyber resilience against operational disruptions to maintain confidence in the financial system.

2.0 Applicability

2.1 The Guidelines is applicable to the following LFIs:

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

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

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

(iv) Labuan takaful and retakaful operators licensed under Part VII of the LIFSSA, excluding Labuan captive takaful business.

2.2 Notwithstanding paragraph 2.1, 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.

2.3 The Guidelines is to be read together with the requirements under relevant guidelines issued by Labuan FSA as set out in **Appendix I**.

3.0 Legal Provision

3.1 The Guidelines is issued pursuant to Section 4A of the Labuan Financial Services Authority Act 1996 (LFSAA) to specify the minimum prudential standards to be observed by LFIs.

3.2 Any person who fails to comply with the Guidelines may be subject to an administrative penalty and/or other enforcement actions under Section 36B and Section 36G of the LFSAA.

4.0 Regulatory Requirements

4.1 The application and observance of the principles specified under the Guidelines is to be achieved by a LFI through the minimum requirements and to 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 that have been issued by Labuan FSA as set out in **Appendix I**; and

(ii) The best practices are broad guidance on other more advanced technology and cyber risk management practices observed in international markets. Although these best practices are not made mandatory, LFIs are encouraged to adopt them as their financial business operations grow and mature over time.

5.0 Effective Date

5.1 The Guidelines shall come into effect on **1 January 2025** and would remain effective and applicable unless amended or revoked. Notwithstanding this, LFIs which intend to early adopt the requirements of the Guidelines are permitted to do so prior to the effective date.

Question 1:

Do you foresee any challenges with the effective date of the Guidelines vis-à-vis the compliance to its requirements? If yes, please provide details.

6.0 Definitions

Board of the Directors (Board)	For LFI operating as a branch, any reference made in the Guidelines in relation to the "Board" refers to the regional/head office of the LFI; or any equivalent person or body with the authority to oversee the LFI, whichever is relevant.
Configuration Management	Refers to the process of maintaining key information (e.g. model, version, specifications, etc.) about the configuration of the hardware and software that makes up each IT system.
Critical System	Any core application system that supports the provision of LFI's digital financial services, where failure of the system has the potential to significantly impair its services to clients or counterparties, business operations, financial position, reputation or compliance with applicable laws and regulatory requirements.
Cryptography	Refers to a method of securing data and information from unauthorised access which allows only the sender and intended recipient to access the data and information.
Cyber Risk	Refers to threats or vulnerabilities emanating from the connectivity of internal technology infrastructure to external networks or the Internet.
Digital Financial Services	The provision of services by LFI to clients that is delivered via electronic channels including the Internet and mobile devices.
Information Assets	Information assets include data, hardware and software which are not limited to those that are owned by the LFI. The information assets also include those that are entrusted to the LFI by clients or third parties, rented or leased by the LFI, and those that are used by service providers to deliver their services to the LFI.

Public Cloud	Refers to a fully virtualised environment in which a service provider makes resources such as platforms, applications or storage available to the public over the Internet via a logically separated multi-tenant architecture.
Senior Management	Refers to the principal officer, any officer(s) or committee performing a senior management function who are principally accountable for: (i) Making decisions that affect the whole, or a substantial part of, the LFI's business; (ii) Implementing and enforcing policies and strategies approved by the Board including Head of Department or any equivalent designated person; or (iii) Internal controls or other key functionaries of the LFI which include compliance, AML/CFT compliance, Shariah advisory, internal audit and risk management.
Technology Management Framework (TMF)	The set of internal policies and procedures that comprise IT strategic plan and the requirements on IT infrastructure, data and system of the organisation to support its financial business.

7.0 Technology and Cyber Governance

Principle 1: The Board and senior management are responsible to effectively implement the technology and cyber risk management of the LFI to safeguard the LFI's information technology (IT) infrastructure and system as well as the IT strategies and planning are sufficient and appropriate to the LFI's needs.

Minimum Requirements

7.1 The duties and responsibilities of the Board include:

(i) Developing and approving the LFI's technology risk appetite in alignment with the risk appetite statement of the LFI;

(ii) Overseeing the LFI's technology and cybersecurity strategic plans for a minimum period of three years. This includes determining the infrastructure requirements, implementing control measures to mitigate technology and cyber risk and allocating adequate financial and non-financial resources, which commensurate with the LFI's technology and cyber risk appetite, complexity of its operations and business environment;

(iii) Approving and assessing the adequacy of technology management framework (TMF) for business implementation and ensure that it remains relevant to suit the LFI's strategies and business operations; and

(iv) Devoting sufficient time to discuss cyber risks and related issues, including the strategic and reputational risks associated with a cyber-incident.

7.2 LFI's board audit committee[1] is responsible for ensuring the effectiveness of the internal audit function which includes:

(i) Ensuring adequate competency of the audit staff to perform technology audits;

(ii) Reviewing and ensuring the audit scope, procedures and frequency of the technology audits are appropriate; and

(iii) Ensuring effective oversight over the prompt closure of corrective actions to address technology control gaps.

Question 2:

Do you foresee any challenges for your Board in discharging the responsibilities stipulated in paragraph 7.1? If yes, please provide details.

7.3 The duties and responsibilities of the senior management include:

(i) Developing and implementing the TMF as mandated by the Board. This includes establishing and effecting sound and prudent policies, standards, and procedures that aligns with the approved TMF;

(ii) Conducting periodic reviews of the TMF, at least once every three years. Additionally, the LFI is required to review its TMF whenever there are any significant changes that may affect the provision of financial services to its clients. A report of the review has to be maintained by the LFI as a reference;

[1] This refers to para 9.0 of the *Guidelines on Corporate Governance for Labuan Banks and Labuan (Re)Insurers* which requires Labuan commercial banks and insurers to establish an Audit Committee.

(iii) Promptly notifying the Board on any salient and adverse technology developments and incidents that could potentially have major impact on the LFI's digital financial services;

(iv) Establishing a cross-functional committee comprises of senior management from both technology functions and major business units to support and assist on the LFI's technology plans and operations. The committee's responsibilities include:

(a) Overseeing the formulation and implementation of technology management framework and associated technology policies and procedures;

(b) Providing regular updates to the Board on key technology matters to facilitate strategic decision-making; and

(c) Approving any deviation from technology-related policies after having carefully considered a robust assessment of related risks. Material deviations shall be reported to the Board; and

(v) Ensuring adequate allocation of resources with appropriate skills and competencies to maintain robust technology infrastructure and systems management.

Question 3:

In relation to paragraph 7.3(ii), do you agree for the review of TMF to be undertaken at least once in three-year time? If not, please provide recommendation and justification.

Question 4:

In relation to paragraph 7.3(iv), do you foresee any challenges on the establishment of cross-functional committee in your organisation? If yes, please provide details.

Best Practices

1. LFI may conduct a self-assessment which covers the complexity of the organisation's operations, the number and size of significant business lines and other business considerations that could give rise to technology risk.

8.0 Technology Risk Management

<u>Principle 2:</u> LFI shall develop and implement a technology risk management framework to assess and mitigate potential risks associated with the use of technology within the LFI.

Minimum Requirements

A. Technology Management Framework (TMF)

8.1 LFI is required to establish a robust TMF which is essential for supporting IT services and operations, tracking information assets, managing changes, responding to incidents and ensuring the stability of the production of IT environment. The TMF shall include the following:

(i) Clear responsibilities assigned for the management of technology risk at different levels and across functions, with appropriate governance and reporting arrangements;

(ii) Implement a configuration management process to maintain accurate information of its hardware and software. The configuration must be reviewed and verified by the DFI whenever there are changes to ensure it is accurate and up-to-date;

(iii) Monitor the hardware's or software's end-of-support dates to avoid the usage of outdated and unsupported hardware or software which could increase its exposure to security and stability risks;

(iv) Ensure relevant functional and non-functional patches (e.g. fixes for security vulnerabilities and software bugs) are implemented within a timeframe that is commensurate with the criticality of the patches and the LFI's IT systems;

(v) Establish a change management process to ensure changes to information assets are assessed, tested, reviewed and approved before the implementation of changes;

(vi) Conduct backups of the information asset before implementing changes, and establish a rollback plan to revert the information asset to the previous state if a problem arises during or after the change implementation;

(vii) Configure system events or alerts to provide an early indication of issues that may affect its IT systems' performance; and

(viii) Determine and resolve the root cause of incidents to prevent the recurrence of similar incidents. A record of past incidents must be maintained to facilitate the diagnosis and resolution of future incidents with similar characteristics.

B. Technology Management Function

8.2 LFI is required to establish a dedicated technology management function with the following responsibilities:

(i) Overseeing and implementing the TMF and cyber risk management policies;

(ii) Providing advice on critical technology projects and ensuring critical issues that may have an impact on LFI's risk tolerance are adequately deliberated or escalated in a timely manner; and

(iii) Providing independent views to the Board and senior management on third-party assessments, where necessary.

8.3 The technology management function should be designated to an officer [e.g. Chief Information Security Officer (CISO) or Chief Technology Officer (CTO)] that has sufficient authority, independence and resources to carry out his functions as follows:

(i) Be independent from day-to-day technology operations;

(ii) Keep apprised of current and emerging technology developments which could potentially affect the LFI's IT plan and deployment; and

(iii) Be appropriately certified by IT accreditation bodies.

8.4 The designated officer (e.g. CISO or CTO) is responsible for ensuring LFI's information assets and technologies are adequately protected, which includes:

(i) Developing appropriate policies and procedures to ensure effective implementation of the TMF and cyber risk management policies;

(ii) Enforcing compliance with the applicable legislations, regulations and other technology-related regulatory requirements; and

(iii) Advising senior management on technology risk and security matters, including developments in LFI's technology security risk profile in relation to its business and operations.

Question 5:

Do you foresee any challenges on the establishment of a dedicated technology management function in your organisation? If yes, please provide details.

9.0 TECHNOLOGY OPERATIONS MANAGEMENT

<u>Principle 3:</u> LFI shall maintain the technology operations management in an effective manner which includes overseeing the strategic technology planning, implementation, and maintenance of technology infrastructure to ensure seamless functionality across the organisation.

Minimum Requirements

A. Technology Project Management

9.1 LFI is required to implement appropriate governance practices which include project oversight roles and responsibilities, authority and reporting structures as well as risk assessments throughout the project life cycle to ensure the delivery outcomes meet the project objectives and requirements.

9.2 LFI shall conduct risk assessment to identify and address the material risks arising from the implementation of technology projects which could threaten the project implementation or would have impact on its operational capabilities. At a minimum, the risk assessments cover the following:

(i) Adequacy and competency of resources including those of the vendor to effectively implement the project. This includes the number, size and duration of significant technology projects already undertaken concurrently by LFI;

(ii) Complexity of systems to be implemented such as the use of unproven or unfamiliar technology and the corresponding risks of integrating the new technology into existing systems, managing multiple vendor-proprietary technologies, large-scale data migration or cleansing efforts and extensive system customisation;

(iii) Comprehensiveness of the user requirement specifications to mitigate risks from extensive changes in project scope or deficiencies in meeting business needs; and

(iv) Appropriateness of system deployment and fall back strategies to mitigate risks from prolonged system stability issues.

9.3 Throughout the technology projects implementation, LFI is expected to timely report to the Board and senior management on project developments such as key milestones, obstacles and challenges that may impede the progress and completion of the project.

9.4 Any material issues which may have impact to the project deliverables would need to be adequately resolved by LFI in a timely manner.

B. System Development and Acquisition

9.5 LFI shall incorporate appropriate risk management policies and procedures throughout the system development life cycle which comprises the system design, development, testing, deployment, change management, maintenance and decommissioning. The policies and procedures shall be part of its TMF and this must be reviewed periodically to ensure it remains relevant.

9.6 LFI is required to enhance the resilience of the critical system infrastructure by considering the use of different technology architecture designs and applications, technology platforms and network infrastructure to ensure the critical system infrastructure are not excessively exposed to similar technology risks.

9.7 An appropriate procedure to review and approve system changes would need to be in place. In addition, LFI is also required to establish and test contingency plans in the event of unsuccessful implementation of material changes to minimise any business disruption.

9.8 Prior to deployment, LFI shall establish a sound methodology for rigorous system testing to ensure that the system meets user requirements and performs robustly. The testing may include unit testing, integration testing, user acceptance testing, application security testing, stress and regression testing as well as exception and negative testing, where applicable.

9.9 LFI is required to physically segregate the production environment from the development and testing environment for critical systems. Where the LFI is relying on a cloud environment, the LFI shall ensure that these environments are not running on the same virtual host.

9.10 When decommissioning critical systems, LFI must ensure minimal adverse impact on clients and business operations. This includes establishing and testing contingency plans in the event of unsuccessful system decommissioning.

9.11 Where the IT systems are managed by third-party service providers, LFI ensures, including through contractual obligations, that the third-party service providers provide sufficient notice to the DFI before any material changes are undertaken that may impact the IT systems.

Best Practices

1. To facilitate a more secure systems development, LFI may deploy automated tools for software development, testing, software deployment, change management, code scanning and software version control.

C. Cryptography

9.12 LFI shall establish a robust and resilient cryptography policy to protect the important data and information which, at the minimum, shall covers the following:

(i) The adoption of industry standards for encryption algorithms, message authentication, hash functions, digital signatures and random number generation;

(ii) The adoption of robust and secure processes in managing cryptographic key lifecycles which include generation, distribution, renewal, usage, storage, recovery, revocation and destruction;

(iii) The periodic review, at least every three years, of existing cryptographic standards and algorithms in critical systems, external linked or transactional customer-facing applications to prevent exploitation of weakened algorithms or protocols; and

(iv) The development and testing of compromise-recovery plans in the event of a cryptographic key compromise. This must set out the escalation process, procedures for keys regeneration, interim measures, changes to business-as-usual protocols and containment strategies or options to minimise the impact of a compromise.

9.13 LFI shall ensure clear senior-level roles and responsibilities are assigned for the effective implementation of the cryptographic policy.

D. *Management of Information Assets*

9.14 LFI is required to adopt sound information asset management practices to ensure an accurate and complete view of its IT operating environment which include the following:

(i) Identification of information assets that support the LFI’s business and delivery of financial services;

(ii) Classification of an information asset based on its security classification or criticality;

(iii) Ownership of information assets, and the roles and responsibilities of the staff managing the information assets; and

(iv) Establishment of policies, standards and procedures to manage information assets according to their security classification or criticality.

9.15 An appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third-party service providers) shall also be implemented by the LFI. The access controls policy shall covers the following:

(i) Implement robust authentication processes to ensure the legitimacy of identities being used. The authentication mechanisms should be in line with the criticality of the functions and adopt at least one or more of these three basic authentication factors, namely, something the user knows (e.g. password, PIN), something the user possesses (e.g. smart card, security device) and something the user is (e.g. biometric characteristics, such as a fingerprint or retinal pattern);

(ii) Regularly review and adapt its password practices to strengthen resilience against evolving attacks. This includes the effective and secure generation of passwords. There must be appropriate controls in place to check the strength of the passwords created;

(iii) Establish a user access matrix which includes the access rights, user roles or profiles, and the authorising and approving authorities. This shall be periodically reviewed and updated; and

(iv) Ensure effective management and monitoring of access controls and maintain activity logs for user activities in critical systems for audit and investigation purposes. The activity logs must be maintained for a minimum of three years.

Best Practices

1. LFI may consider the following principles in its access control policy:

(i) Adopt a "deny all" access control policy for users by default unless explicitly authorised;

(ii) Employ "least privilege" access rights or on a 'need-to-have' basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles;

(iii) Employ time-bound access rights which restrict access to a specific period including access rights granted to service providers;

(iv) Employ segregation of incompatible functions where no single person is responsible for an entire operation that may provide the ability to independently modify, circumvent, and disable system security features. This may include a combination of functions such as:

(a) system development and technology operations;

(b) security administration and system administration; and

(c) network operation and network security;

(v) Employ dual control functions which require two or more persons to execute an activity;

(vi) Adopt stronger authentication for critical activities including for remote access;

(vii) Limit and control the use of the same user ID for multiple concurrent sessions;

(viii) Limit and control the sharing of user ID and passwords across multiple users; and

(ix) Control the use of generic user ID naming conventions in favour of more personally identifiable IDs.

E. *Data Centre*

9.16 LFI is responsible for maintaining its production data centre[2] to ensure its optimal functioning. This includes having redundant capacity components and distribution paths serving the computer equipment. Potential data centre failures or disruptions must not significantly degrade the delivery of its digital financial services or impede its internal operations.

9.17 LFI is required to ensure the critical systems are hosted in a dedicated space specifically designed for production data centre usage. The dedicated space must be physically secured from unauthorised access and is not located in a disaster-prone area.

9.18 LFI must eliminate single point of failure in the design and connectivity for critical components of the production data centres, including hardware components, electrical utility, thermal management and data centre infrastructure.

9.19 LFI is required to ensure its capacity needs are well-planned and managed with due regard to its financial business growth plans. This includes ensuring adequate system storage, central processing unit (CPU) power, memory and network bandwidth.

[2] Production data centre is the data centre that is used for day-to-day operations.

9.20 LFI is required to implement real-time monitoring mechanisms to track utilisation and performance of key processes and services[3].

9.21 LFI is required to establish adequate control procedures for its data centre operations, including the deployment of relevant automated tools for batch processing management to ensure timely and accurate batch processes. These control procedures shall also include procedures for implementing changes in the production system, error handling as well as management of other exceptional conditions.

Best Practices

1. In addition to the production data centres as required under paragraph 9.16, LFI should also ensure that the recovery data centres are concurrently maintainable.

2. LFI may undertake an independent risk assessment of its end-to-end backup storage and delivery management to ensure that the existing controls are adequate in protecting sensitive data at all times.

3. LFI may consider appointing a technically competent external service provider to carry out a production data centre and network resilience and risk assessment. This includes setting the proportionate control aligned with its risk appetite and determine the current level of resilience. For data centres managed by third-party service providers, the LFI may rely on independent third-party assurance reports provided such reliance is consistent with the organisation' risk appetite and tolerance. The designated board-level committee may be formed to deliberate the outcome of the assessment.

[3] For example, batch runs and backup processes for the LFI's application systems and infrastructure.

F. *Cloud Services*

9.22 LFI that adopts cloud services is required to assess the inherent risk of such arrangements.

9.23 LFI must implement appropriate safeguards on clients and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access that includes the following:

(i) Retaining ownership, control and management of all data pertaining to clients and counterparty information;

(ii) Proprietary data and services hosted on the cloud; and

(iii) Relevant cryptographic key management.

9.24 For critical systems hosted on public cloud, LFI is required to ensure additional security measures are in place to preserve the confidentiality and integrity of the information assets stored on the cloud at all times.

Best Practices

1. In relation to paragraph 9.22, LFI may assess the risk associated with the use of cloud services for critical systems which may include the following areas:

(i) The availability of independent, internationally recognised certifications of the cloud service providers which covers:

(a) Information security management framework, including cryptographic modules used for encryption and decryption of user data; and

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

(ii) The degree to which the selected cloud configuration adequately addresses the following attributes:

(a) Geographical redundancy;

(b) High availability;

(c) Scalability;

(d) Portability;

(e) Interoperability; and

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

2. In relation to paragraph 9.24, LFI may consider the following common key risks and control measures:

(i) Implement sound governance principles throughout the cloud service lifecycle;

(ii) Implement policies and procedures that articulate the criteria for permitting or prohibiting the hosting of information assets on cloud services, commensurate with the level of criticality of the information asset and the capabilities of the LFI to effectively manage the risks associated with the cloud arrangement;

(iii) Ensure effective oversight over cloud service providers taking into account the fact that the cloud service providers may engage sub-contractor(s) to provide cloud services;

(iv) Ensure its IT and security operations or relevant personnel are appropriately skilled in the areas of cloud design, migration, security configurations, including administrative, monitoring and incident response;

(v) Implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud; and

(vi) Establish a robust cloud exit strategy to prepare for extreme adverse events such as the unplanned failure or termination of cloud service providers.

Question 6:

Do you foresee any challenges on the implementation of the above technological operations management requirements as prescribed under paragraph 9.0? If yes, please provide details.

10.0 Cybersecurity Management

<u>Principle 4:</u> LFI shall establish clear responsibilities for cybersecurity operations which includes implementing appropriate preventive, detective, corrective and recovery measures.

Minimum Requirements

10.1 LFI is required to ensure its technology systems and infrastructure including critical systems outsourced to or hosted by third-party service providers are adequately protected against all types of distributed denial of service (DDoS) attacks (including volumetric, protocol and application layer attacks) through the following measures:

(i) Subscribing to DDoS mitigation services, which include automatic 'clean pipe' services to filter and divert any potential malicious traffic away from the network bandwidth;

(ii) Regularly assessing the capability of the provider to expand network bandwidth on-demand including upstream provider capability, adequacy of the provider's incident response plan and its responsiveness to an attack; and

(iii) Implementing mechanisms to mitigate against Domain Name Server (DNS) based layer attacks.

10.2 LFI is expected to establish a data loss prevention (DLP) strategy and processes in order to ensure that client and counterparty information and proprietary data is identified, classified and secured. This includes the following:

(i) Ensure that data owners are accountable and responsible for identifying and appropriately classifying data;

(ii) Undertake a data discovery process prior to the development of a data classification scheme and data inventory; and

(iii) Ensure that data accessible by third parties is clearly identified and policies must be implemented to safeguard and control third party access. This includes adequate contractual agreements to protect the interests of the LFI and its clients.

Best Practices

1. LFI may consider purchasing a cyber insurance policy to mitigate the financial losses from a cyber incident. LFI may review the adequacy of its cyber insurance coverage at least annually.

Question 7:

In view that LFI is operating with high reliance on technology, should the cyber insurance policy requirement be made mandatory? Please provide your views and rationale.

11.0 Cyber-Incident Alerts

11.1 LFI is required to immediately notify Labuan FSA's Supervision and Enforcement Department on any cyber-incidents as identified by LFI under paragraph 7.3(iii) through expeditious means (e.g. phone call, email, etc.). Upon completion of the investigation, LFI is also required to submit a report on the incident as set out in **Appendix II** within 48 hours to Labuan FSA as follows:

Director
Supervision and Enforcement Department
Labuan Financial Services Authority
Level 17, Main Office Tower
Financial Park Complex
Jalan Merdeka
87000 Federal Territory of Labuan, Malaysia

Telephone no: 03 8873 2000
Facsimile no: 03 8873 2209
Email: sed@labuanfsa.gov.my

Question 8:

If you have comment(s) / recommendation(s) on any matters relevant to be considered in finalising the proposed Guidelines, please provide details.

Labuan Financial Services Authority
XX XXX XXXX

APPENDIX I LIST OF POLICY DOCUMENTS TO BE READ TOGETHER WITH THE GUIDELINES

1. The Guidelines is to be read together with the following guidelines:

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

(ii) Guidelines on Fit and Proper Person Requirements;

(iii) Guidelines on Shariah Governance for Labuan Islamic Financial Institutions;

(iv) Guidelines on Market Conduct for Labuan Insurance and Insurance-Related Companies;

(v) Guidelines on Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Labuan Key Reporting Institutions (AML/CFT and TFS for Labuan KRIs);

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

(vii) Guiding Principles on Business Continuity Management;

(viii) Guidelines on Digital Governance Framework; and

(ix) Circular on Principles on Electronic Know-Your-Customer (e-KYC) for Digital Financial Services.

APPENDIX II CYBER-INCIDENT REPORTING TEMPLATE

Name of LFI (may include the LFI’s logo) **Cyber-Incident Reporting Template**		
Part A: Contact Information		
(i)	Name & designation of the Reporting Officer	
(ii)	Date of report	
Part B: Details of Incident		
(i)	Nature of incident	
(ii)	Immediate actions or responses taken	
Part C: Impact Assessment		
(i)	Impact to business/ operations	
(ii)	Impact to stakeholders	
Part D: Root Cause Analysis		
(i)	Factors/ gaps that have contributed to the incident	
(ii)	Actions taken/ enhancement or rectification identified to prevent future incidents	