FREQUENTLY-ASKED QUESTIONS
GUIDELINES ON DIGITAL GOVERNANCE FRAMEWORK

A. REGULATORY REQUIREMENTS

1. What is Labuan FSA's expectation on the compliance with the best practices outlined under the Guidelines on Digital Governance Framework (the Guidelines)?

- As specified under paragraphs 2.2 and 4.0 of the Guidelines, Labuan financial institutions (LFIs) are only required to comply with the minimum requirements. While the LFIs are expected to observe the minimum requirements prescribed by the Guidelines, the nature and extent of measures to be effected by individual LFIs should be proportionate to the specific nature of their business operations.

- While the adoption of the best practices is not mandatory, LFIs are encouraged to adopt them over time so that their digital governance practices commensurate with the growing size and complexities of their business operations. To clarify, any LFI that does not adopt the Guidelines' best practice recommendations would not be considered as regulatory non-compliance.

B. APPLICABILITY

2. What are the regulatory requirements for LFIs that offer digital financial services under the Guidelines?

The Guidelines is applicable to all LFIs specified under paragraph 3.1 of the Guidelines. Notwithstanding this, LFIs that provide digital financial services are required to have more robust digital security controls as part of their cyber risk management pursuant to paragraph 9.0 of the Guidelines.

3. What is the requirement under the Guidelines that would be applicable to a Labuan managed trust company?

- Given that most of its functions are outsourced to the external service provider (e.g. a full-fledged trust company), a Labuan managed trust company is required to adhere to the outsourcing requirements as specified under paragraph 10.0 of the Guidelines.

- The obligations between the LFI and the external service provider would need to be clearly specified within the service level agreement. In addition, Labuan FSA expects that the outsourcing of IT system does not dilute the Labuan managed trust companies' responsibilities in managing cyber risk to ensure the safety and soundness of their own business operations.

C. CYBER RISK MANAGEMENT

4. Are LFIs required to have a separate cyber risk management policy or allowed to incorporate cyber risk management into the enterprise risk management framework?

LFIs are expected to incorporate the cyber risk management policy as part of their overall enterprise risk management (ERM). In this regard, LFIs would need to ensure that their ERM are consistent with the minimum requirements of the Guidelines.

5. In the event of material cyber-incident or cyber-attack, is it compulsory for LFIs to notify and report to Labuan FSA?

- Under the Guidelines, there is no requirement for the LFIs to notify or report to Labuan FSA in the event of any material cyber-incident or cyber-attack.

- Notwithstanding this, where a cyber-incident leads to the activation or execution of the LFIs' business continuity arrangements, the relevant LFIs (i.e. those that are scoped-in under the *Guiding Principles on Business Continuity Management*) are required to notify Labuan FSA's Supervision and Enforcement Department.

D. MANAGEMENT OF DIGITAL SERVICES OFFERED BY LFIs

6. What are the parameters to assess the effectiveness of the LFI's security controls for digital services rendered to its clients?

The effectiveness of security controls is considered appropriate if the LFI fulfils the requirements as well as the parameters specified under paragraph 9.1 of the Guidelines.

E. EXTERNAL SERVICE ARRANGEMENT

7. Do LFIs need to notify Labuan FSA on their registered external service providers?

- Under the Guidelines, there is no requirement for the LFIs to notify Labuan FSA on their external service providers.

- Notwithstanding this, the Guidelines would need to be read together with the *Guidelines on External Service Arrangements for Labuan Financial Institutions* which is applicable to key LFIs (i.e. banks, (re)insurers and fund managers). Under the said Guidelines, the key LFIs are required to ensure compliance with the requirements on the external service arrangements including the submission of information pursuant to the Reporting Guideline on Statistical Data Submission for Labuan Entities.

F. MAINTENANCE AND REVIEW

8. Are there any restrictions on parties that LFIs should engage to undertake the system assessment and security testing?

- The parties undertaking periodic assessment on LFI's critical network infrastructure as well as security testing on its platforms, applications and critical systems would need to be different from those undertaking the audit as specified under paragraph 11.6 of the Guidelines to ensure sufficient impartiality.

- In this regard, the assessment may be undertaken by in-house or external IT professionals.

G. AWARENESS AND TRAINING

9. What are the recommended areas of training to ensure ongoing cyber awareness within the LFI?

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. For instance, these areas may include the LFI's IT setup and infrastructures, IT improvements that have been instituted or planned, new applications that have been adopted e.g. cloud computing, etc., cyber security controls as well as emerging cyber related risks.

10. How frequent does the LFI's staff involved in IT operations, cybersecurity and risk management would need to undergo training?

The LFI may set the training frequency based on its staff training needs such as in terms of minimum number of trainings per year, etc. to enable effective performance of their roles and responsibilities.

H. OTHERS

11. If LFIs pursue the accreditation or certification from recognised bodies e.g. International Organization for Standardization (ISO), would there be any allowance or exemption from the Guidelines?

This initiative is encouraged as an enhancement to LFI's cyber governance and risk management beyond the bare minimum requirements of the Guidelines. In this regard, Labuan FSA considers such good practices as commendable as these provide greater credibility to their digital governance policy and can be deemed as favourable for supervisory assessment of the entities concerned. As such, there is no need for any allowance or exemption from the Guidelines.