FREQUENTLY-ASKED QUESTIONS
GUIDELINES ON TECHNOLOGY AND CYBER RISK MANAGEMENT FOR LABUAN BANKING AND INSURANCE BUSINESS

A. APPLICABILITY

1. Is a Labuan Financial Institutions (LFIs) allowed to outsource its Technology Management Function?

LFIs may outsource their Technology Management Function provided that they meet the requirements specified under the existing Guidelines on External Services Arrangements for Labuan Financial Institutions.

In addition, it is expected that any outsourcing would not result in any delegation or dilution of oversight and responsibilities over the outsourced functions. As such, the board and senior management of the LFI shall remain fully responsible and accountable for overseeing the outsourced functions.

B. TECHNOLOGY AND CYBER GOVERNANCE

2. In relation to paragraph 7.1(iv), LFI's Board is required to devote sufficient time to discuss cyber risks and related issues, including the strategic and reputational risks associated with a cyber-incident. How does LFI ensure that the requirement on "devoting sufficient time" is met?

This shall be based on the LFI's discretion where LFI is required to allocate adequate and appropriate amount of time to discuss cyber risks and related issues comprehensively as well as to ensure all aspect has been covered including strategic and reputational risks associated with a cyber-incident. This may be reflected as part of LFI's periodic Board meeting agenda.

3. **In relation to paragraph 7.3(ii), LFI is required to review its Technology Management Framework whenever there are any significant changes that may affect the provision of financial services to its clients. How are "significant changes" defined?**

   "Significant changes" refers to any substantial modifications or developments that may affect the LFI's ability to provide digital financial services to its clients.

4. **In relation to paragraph 7.3(iii), LFI is required to promptly notify the Board of any salient and adverse technology developments and incidents that could potentially have major impact on the LFI's digital financial services. How is "promptly" defined?**

   LFI should endeavor to notify its Board as soon as practicable without delay or hesitation.

C. TECHNOLOGY MANAGEMENT FRAMEWORK

5. **In relation to paragraph 8.2(iii), LFI's technology management function is required to provide independent views to the Board and senior management on third-party assessments, where necessary. Does the "third-party assessment" include assessment by Group/Head Office?**

   The "third-party assessment" refers to the assessment undertaken by any external service providers who are independent from the LFI. In this regard, Group/Head Office assessment is excluded from third-party assessment".

6. **What are Labuan FSA's expectations for LFI that is part of a group of companies which manages all technology risks within the group at the holding company level?**

   In the situation where the LFI's technology risks are managed by its Group, the LFI may leverage on its group's Technology Management Framework (TMF), provided that the framework is comprehensive and addresses areas specified in the Guidelines. The arrangement is considered as an outsourcing arrangement under the Guidelines, and hence, the LFI and its board remain responsible for the outsourced functions.

7. In relation to paragraph 8.3, what are the responsibilities of the dedicated officer for the Technology Management Function and certifications needed?

The dedicated officer is required to formulate and facilitate the effective implementation of TMF, advise senior management on technology risk and security matters, including developments in the LFI's technology risk in relation to its business and operations. In relation to the certifications needed, the dedicated officer must have an appropriate and related certification on information security and technology.

8. What is the appropriate reporting structure for the dedicated officer?

The dedicated officer must be independent from day-to-day technology operations. Ideally, the dedicated officer should be placed within the second line of defense function (i.e. risk management function and compliance function), nevertheless LFIs have the flexibility to position the dedicated officer where they deem equally suitable to meet the requirements under the Guidelines. LFIs must demonstrate that the dedicated officer has sufficient authority and is not inhibited in providing independent views.

9. Are LFIs allowed to leverage on Head Office's dedicated officer for Technology Management Function?

The dedicated officer may take guidance from the expertise of their Group-level. Notwithstanding this, there must be an officer at the entity level who will serve as the point of contact for any technology-related matters as well as the responsible person for ensuring the LFI's information assets and technologies are adequately protected to preserve operational integrity and business continuity.

D. CYBER-INCIDENT ALERTS

10. In relation to paragraph 11.1, LFIs are required to immediately notify Labuan FSA's Supervision Department on any major cyber-incidents. How is "immediately" defined?

"Immediately" refers to as soon as practicable in no less than 24 hours from the occurrence of cyber incident.

11. What constitutes a cyber-incident?

Cyber-incident refers to any unauthorised or action that compromises the confidentiality, integrity or availability of system, networks and database. These incidents can encompass a wide range of activities, including but not limited to:

(i) Malware Attacks;
(ii) Phishing;
(iii) Denial of Service (DoS) or Distributed Denial of Service (DDoS) Attacks; or
(iv) Hardware or Software Failures.