GUIDELINES ON TECHNOLOGY MANAGEMENT

1.0 Introduction

1.1 The global financial landscape has been significantly transformed by the rapid technological innovations particularly in the post pandemic environment. With the strong synergy between technology and financial intermediation, managing the changes brought by the former will become a critical factor in sustaining and driving the expansion of digital financial services (DFS).

1.2 As the DFS offering continues to expand, it is expected for technology to be appropriately adopted, managed, and deployed to ensure that the digital financial business operations remain sound and viable. Prudent governance and risk management practices needs to be continuously promoted amongst digital financial intermediaries which typically have smaller and simpler business setups. In this regard, it is imperative that suitable technologies be adopted and implemented by these institutions in line with their business nature, scale, complexity and risk profile.

1.3 In this regard, *Guidelines on Technology Management* (the Guidelines) provide the minimum requirements to be adhered by financial intermediaries that undertake DFS in Labuan IBFC [i.e. referred to as Labuan Digital Financial Intermediaries (DFIs)].

2.0 Applicability

2.1 The Guidelines is applicable to any DFI licensed and approved by Labuan Financial Services Authority (Labuan FSA) as follows:

(i) Labuan money-broking business and Islamic money-broking business licensed under Part VI of the Labuan Financial Services and Securities Act 2010 (LFSSA) and Part VI of the Labuan Islamic Financial Services and Securities Act 2010 (LIFSSA), respectively;

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

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

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

(v) Labuan exchanges established under Part IX of the LFSSA; and

(vi) Labuan payment system established under Part XI of the LFSSA.

2.2 Labuan FSA may specify and direct other Labuan financial institutions that undertake DFS to observe the requirements of the Guidelines where relevant.

2.3 The Guidelines are 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 implemented by the DFI.

3.2 Any person who fails to comply with the Guidelines may be subject to an administrative penalty and/or other enforcement actions provided under the following legal provisions:

(i) Section 36B and Section 36G of the LFSAA; and

(ii) Section 187 and Section 194 of the LFSSA; or Section 148 and Section 154 of the LIFSSA.

4.0 Regulatory Requirements

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

(i) Minimum requirements must be complied with by all DFIs. 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 management practices observed in international markets. Although these best practices are not made mandatory, DFIs are encouraged to adopt them as their digital financial business operations grow and mature over time.

5.0 Effective Date

5.1 The Guidelines shall come into effect on **1 January 2024**, and would remain effective and applicable unless amended or revoked. Notwithstanding this, DFIs 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 DFI operating as a branch, any reference made in the Guidelines in relation to the "board" refers to the regional/head office of the DFI; or any equivalent person or body with the authority to oversee the DFI, 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 DFI'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.

Digital Financial Services (DFS)	The provision of services by Labuan Financial Institutions 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 DFI. The information assets also include those that are entrusted to the DFI by clients or third parties, rented or leased by the DFI, and those that are used by service providers to deliver their services to the DFI.
Digital Financial Intermediaries (DFIs)	Refers to Labuan Financial Institutions listed under paragraph 2.1 that are undertaking or providing DFS to their clients including dealing with digital assets.
Senior Management	Refers to the principal officer, any officer(s) or committee performing a senior management function who are principally accountable for: (a) Making decisions that affect the whole, or a substantial part of, the DFI's business; (b) Implementing and enforcing policies and strategies approved by the Board including Head of Department or any equivalent designated person; or (c) Internal controls or other key functionaries of the DFI which include compliance, AML/CFT compliance, Shariah advisory, internal audit and risk management.
Technology Management Framework (TMF)	The set of internal policies that comprise IT strategic plan and the requirements on IT infrastructure, data and system of the organisation to support its digital financial business.

7.0 TECHNOLOGY OVERSIGHT

<u>Principle 1:</u> The Board and senior management play critical roles in overseeing the technology management of the DFI in order to ensure that the information technology (IT) strategies, planning, infrastructure and system are adequate and appropriate to the organisational needs.

Minimum Requirements

7.1 The Board and senior management ensure that the technology management practices and internal controls are implemented effectively to safeguard the DFI's IT infrastructure and system. This includes ensuring that the technology adoption remains up-to-date and able to cater for future expansion.

<u>The Board</u>

7.2 The duties and responsibilities of the Board include:

(i) Setting the organisational risk appetite for the technology adoption of the DFI;

(ii) Assessing the adequacy of the TMF vis-à-vis the organisation's technology risk appetite, complexity of its operations and business environment; and

(iii) Approving the TMF for business implementation and ensure that it remains relevant to suit the organisation's strategies and business operations.

Question 2:

Do you foresee any challenges for your board in discharging the responsibilities stipulated in paragraph 7.2? If yes, please provide details.

Senior Management

7.3 The duties and responsibilities of the senior management include:

(i) Developing and implementing the TMF as mandated by the Board;

(ii) Establishing and effecting sound and prudent policies, standards and procedures that are consistent with the approved TMF;

(iii) Reviewing the TMF periodically for at least once in every three years to ensure continuous relevancy to the DFI;

(iv) Notifying the Board in a timely manner on any salient and adverse technology developments and incidents that could potentially have major impact on the DFI's digital financial services;

(v) Ensuring adequate allocation of resources with appropriate skills and competencies to maintain robust technology infrastructure and systems management. This includes providing clear roles and responsibilities of staff that oversees technology management of the organisation; and

(vi) Providing regular updates to the Board on key technology matters to facilitate strategic decision-making.

Question 3:

In relation to paragraph 7.3(iii), 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.

Best Practices

1. A DFI may establish a board-level committee to support the Board in providing oversight over technology-related matters as well as the review of the technology-related frameworks for approval.

2. In order to promote effective technology discussion at the Board level, the Board composition and the Board-level committee may include at least a member with technology experience and competencies.

3. The senior management may establish a cross-functional committee to assist on the formulation and implementation of the strategic technology plan and associated technology policies and procedures.

4. The senior management may establish a dedicated technology management function to oversee the TMF as well as to provide an independent view of the technology deficiency faced by the DFI. The technology management function should be designated to an officer 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 DFI's IT plan and deployment; and

   (iii) be appropriately certified by IT accreditation bodies.

5. DFI may conduct 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 affect its technology management requirements.

Question 4:

In view that DFIs are operating with high reliance on technology, should the technology management function be made mandatory as a dedicated function for your organisation? Please provide your views and rationale.

8.0 TECHNOLOGY MANAGEMENT FRAMEWORK

<u>Principle 2:</u> DFI is required to maintain a framework that specifies how it plans and implements technological enhancements; manages the technology-related risks in a prudent manner; as well as detailing policies on the proper upkeep of key IT infrastructures.

Minimum Requirements

A. <u>IT Planning</u>

8.1 A DFI is required to establish a robust IT strategic plan which is essential for supporting IT services and operations, tracking information assets, managing changes, responding to incidents and ensuring the stability of the production IT environment.

8.2 The IT strategic plan covers the processes and procedures for IT management activities which include but not limited to the following:

(i) adopting a configuration management process to maintain accurate information of its hardware and software. The configuration must be reviewed and verified by the DFI on a periodic basis to ensure it is accurate and up-to-date;

(ii) monitoring 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;

(iii) ensuring applicable 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 DFI's IT systems;

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

(v) performing a backup of the information asset prior to the change implementation, and establish a rollback plan to revert the information asset to the previous state if a problem arises during or after the change implementation;

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

(vii) determining and resolving 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.

Best Practices

1. A DFI may review and verified its configuration management plan at least once in every three years to ensure continuous relevancy.
2. A DFI may establish a change advisory board, comprising key stakeholders including business and IT management to approve and prioritise the changes after considering the stability and security implications of the changes to the production environment.
3. In identifying commonalities and patterns in the incidents as well as verifing if the root causes to the problems had been properly identified and resolved, DFI may perform trend analysis of past incidents. The analysis may be used to determine if further corrective or preventive measures are necessary.

B. Technology Project Management

8.3 A DFI is expected to adopt an appropriate project management 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.

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

8.5 A DFI must ensure that the risk assessments conducted for technology projects identify and address the material risks 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 the DFI;

(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.

8.6 Throughout the technology projects implementation, a DFI is expected to timely report to the Board and senior management on project developments such as key milestone, obstacle and challenges that may impede the progress and completion of the project.

C. System Development and Acquisition

8.7 A DFI is expected to incorporate an appropriate risk management policies and procedures for 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.

8.8 A DFI 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.

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

8.10 Where the IT systems are managed by third party service providers, the DFI 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.

D. Management of Information Assets

8.11 In order for the DFI to have an accurate and complete view of its IT operating environment, it is required to adopt sound information asset management practices that include the following:

(i) Identification of information assets that support the DFI's business and delivery of digital 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.

Best Practices

1. In order to enhance the security controls on its important data and information, a DFI may establish a robust and resilient cryptography policy which, at the minimum 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 may 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.

E. Data Centre

8.12 A DFI must ensure that its production data centre[1] is well maintained. This includes ensuring that production data centres have redundant capacity components and distribution paths serving the computer equipment.

8.13 A DFI is required to host critical systems in a dedicated space intended for production data centre usage. The dedicated space must be physically secured from unauthorised access and is not located in a disaster-prone area.

8.14 A DFI must also ensure there is no 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.

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

Best Practices

1. In addition to the production of data centres as required under paragraph 8.12, a DFI should also ensure that the recovery data centres are concurrently maintainable.

2. A DFI may consider to appoint a technically competent external service provider to carry out a production data centre resilience and risk assessment and set proportionate controls aligned with its risk appetite. The assessment may include all major risks and determine the current level of resilience of the production data centre. For data centres managed by third party service providers, the DFI may rely on independent third party assurance reports

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

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.

F. Cloud Services

8.16 A DFI that adopts cloud services is required to assess the inherent risk of such arrangements.

8.17 A DFI 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 keys management.

Best Practices

1. In relation to paragraph 8.16, a DFI may assess the risk associated with the use of cloud services for critical system 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 such as 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.

Question 5:

Do you foresee any challenges on the implementation of the above technological management requirements as prescribed under paragraph 8.0? If yes, please provide details.

9.0 CYBER-INCIDENT ALERTS

9.1 A DFI is required to immediately notify Labuan FSA's Supervision and Enforcement Department of any cyber-incidents affecting the DFI. Upon completion of the investigation, DFI is also required to submit a report on the incident as set out in Appendix II 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 6:

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
DD/MM/2022

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

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

   (i) Guidelines on the Establishment of Labuan Fund Manager;

   (ii) Guidelines on the Establishment of Labuan Securities Licensee including Islamic Securities Licensee;

   (iii) Guidelines on Carrying Out Money Broking Business in Labuan IBFC;

   (iv) Guiding Principles on Business Continuity Management;

   (v) Guidelines on Fit and Proper Person Requirements;

   (vi) Guidelines on Compliance Function for Labuan Licensed Entities;

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

   (viii) Guidelines on Digital Governance Framework;

   (ix) Guidelines on Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Labuan Key Reporting Institutions; and

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

APPENDIX II CYBER-INCIDENT REPORTING TEMPLATE

Name of DFI (may include the DFI'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	