MUFG BANK (MALAYSIA) BERHAD

199401016638 (302316-U)

BOARD CHARTER

MUFG Bank (Malaysia) Berhad
199401016638 (302316-U)

<u>BOARD CHARTER</u>

TABLE OF CONTENTS

BOARD CHARTER

1. OBJECTIVE

This board charter ("**Charter**") sets out the key mandate, roles, functions, composition, operations and processes of the Board of Directors ("**Board**") of MUFG Bank (Malaysia) Berhad ("**Bank**"). The Board is committed in ensuring that high standards of corporate governance are practised and applied throughout the Bank.

The mandate of the Board is pursuant to and in accordance with the Bank's Constitution, the Companies Act 2016 ("**CA 2016**"), the Financial Services Act 2013 ("**FSA 2013**"), the Islamic Financial Services Act 2013 ("**IFSA 2013**") and applicable guidelines issued by Bank Negara Malaysia ("**BNM**") as in force for the time being and as amended from time to time.

This Charter is applicable to the Directors of the Bank and serves as a reference to them in executing their duties and responsibilities. The Directors of the Bank are expected to perform their roles and responsibilities with integrity, honesty and in a professional manner.

2. COMPOSITION OF THE BOARD

(a) In accordance with the Bank's Constitution, the number of Directors on the Board shall not be less than four (4).

(b) The Board must not have more than one (1) Executive Director, unless BNM approves otherwise in writing.

(c) The Chairman of the Board must be a non-executive director and must not have served as a Chief Executive Officer ("**CEO**") of the Bank in the past five (5) years. The Chairman of the Board must not chair any of the Board Committees.

(d) The Board must have a majority of independent Directors at all times.

(e) The Board will consist of individuals from differing professional backgrounds and with diverse skill sets, experience and knowledge essential for the governance of the Bank's business operations.

(f) The Board will review its composition and size from time to time to ensure it promotes effective deliberation and encourages active participation of all Directors in order to facilitate the Board's decision making process in an effective and efficient manner.

3. APPOINTMENT, RE-APPOINTMENT, RESIGNATION AND REMOVAL OF DIRECTORS

(a) The Board ensures that it will undertake a clear, formal and transparent vetting process in the selection and appointment of the Directors of the Bank. The Board is encouraged to adopt policies setting out the criteria and requirements in respect of the appointment of the Directors, taking into consideration of, among others, the experience, knowledge and skill set that he can contribute to enhancing the performance of the Board.

(b) The Nomination Committee is tasked with the responsibility of identifying, selecting and recommending suitable candidates for the Board and in the process of its duties, it is guided by the Succession Planning Policy for Directors which was adopted by the Bank and sets out a clear and transparent nomination process. Pursuant to the Succession Planning Policy for Directors, the Nomination Committee will carry out a thorough and comprehensive assessment of the candidate in order to determine if he fulfills the Fit and Proper Policy before a recommendation is made to the Board for approval. In the process, a due diligence on the candidate will be conducted through independent checks on criminal records, bankruptcy and other background searches. Each Director is required to submit the "SELF-ASSESSMENT ON FIT & PROPER" form on an annual basis for purposes of compliance with the relevant requirements under the FSA 2013 or section 68 of the IFSA 2013.

(c) A Director must, during his tenure as a director of the Bank, fulfill the following minimum requirements:

(i) he must not be disqualified under section 59(1) of the FSA 2013 or section 68(1) of the IFSA 2013;

(ii) he must not be involved in competing time commitments that may impair or affect his ability to discharge his duties effectively;

(iii) he must not be an active politician; and

(iv) where a firm has been appointed as the external auditor of the Bank, any officer directly involved in the engagement and any partner of the firm must not be appointed as director of the Bank until at least two (2) years after:

(I) he ceases to be an officer or partner of that firm; or

(II) the firm last served as an auditor of the Bank.

(d) A Director must immediately disclose to the Board if he is aware of any circumstances that may affect his ability to meet the minimum requirements specified under clause 3(c).

(e) The Bank must make an application to BNM and obtain the approval of BNM prior to the appointment of a Director.

(f) Unless the written approval of BNM has been obtained:

(i) the Bank must not publicly announce the proposed appointment of a Director; and

(ii) a Director whose tenure has expired and is being proposed for reappointment must immediately cease to hold office and act in such capacity, including by participating in Board meetings or holding himself out as a director.

(g) An independent director must immediately disclose to the Board any change in his circumstances that may affect his status as an independent director. Upon the Board's review, it will notify BNM in writing of its decision to affirm or change his designation as an independent director. Prior to any resignation and removal[1] of the independent director from the Board, a written approval from BNM must be obtained.

(h) The appointment or re-appointment of Directors is considered and decided by the Board as a whole, based on the recommendation of the Nomination Committee and is subject to the written approval of BNM.

(i) Upon the appointment, a new Director shall undergo the Director's Orientation Programme and will be briefed on the terms of his roles and responsibilities, including those arising from his membership in any Board Committee of the Bank.

[1] This excludes terminations in accordance with statutory requirements

4. TENURE OF DIRECTORSHIP

(a) The maximum tenure for which an individual can serve as an independent director shall not exceed nine (9) years.

(b) Pursuant to the Succession Planning Policy for Directors, the tenure for the position of CEO / Executive Director or Non-Independent Non-Executive Director will be limited to a maximum of five (5) years or less depending on the Parent Bank's discretion.

(c) In accordance with the Bank's Constitution, one third (1/3) of the Directors for the time being (excluding Managing Director) shall retire in every year or if the number is not three (3) or a multiple of three (3), the number nearest to one third (1/3) shall retire from office at the conclusion~~s~~ of annual general meeting. A retiring director shall be eligible for re-election. All Directors (excluding Managing Director) should be required to submit themselves for re-election at regular intervals.

(d) A director shall, during the tenure of his appointment, be always subject to the provisions relating to rotation, retirement, appointment and re-appointment of Directors as well as provisions relating to vacation of the office or removal of Directors in the prescribed circumstances as set out in the CA 2016, FSA 2013, IFSA 2013, the Bank's Constitution, the guidelines issued by BNM, the Charter, and/or any other laws, regulations, rules and bylaws in force in Malaysia.

5. BOARD MEETINGS

(a) The Board shall hold a Board Meeting in accordance with the provisions of the Bank's Constitution and Terms of Reference ("**TOR**") of the Board.

(a) The Board shall meet regularly and shall hold a minimum of six (6) meetings in a financial year. Members of the Management and Managers who are not Directors may be invited to attend and speak at meetings on matters relating to their scope of responsibility.

(c) A Director must attend at least 75% of the Board meetings held in each financial year, and must not appoint another person to attend or participate in a Board meeting on his behalf.

(d) The notice, agenda and Board papers shall be circulated to all Directors in advance of each Board meeting to ensure that the Directors are well informed and have the opportunity to seek additional information or further clarification as required.

(e) The quorum for Board meetings must require at least half of the Board members to be present.

(f) The Bank will ensure that attendance at a Board meeting, by way other than physical presence, remains the exception rather than the norm, and is subject to appropriate safeguards to preserve the confidentiality of deliberations.

(g) All matters of the Board shall be decided by way of a majority of votes of the Directors present and voting. In the event of equality of votes, the Chairman of the Board shall be entitled to a second or casting vote. Where a Board member has a vested interest in the issue being discussed, he should recuse himself from the discussions to avoid conflict of interests.

(h) The Board shall ensure that clear and accurate minutes of Board meetings are maintained to record the decisions of the Board, including the key deliberations, rationale for each decision made, and any significant concerns or dissenting views. The minutes must indicate whether any Director abstained from voting or excused himself from deliberating on a particular matter. Such minutes shall be signed by the Chairman of the meeting and the Board shall procure the Company Secretary to cause the minutes to be entered into the relevant books of the Board.

(i) In accordance with the Bank's Constitution, a resolution in writing signed by all the Directors for the time being entitled to receive notice of a meeting of the Directors who may at the time be present in Malaysia and who are sufficient to form a quorum, shall be as valid and effectual as if it had been passed at a meeting of the Directors duly convened and held on the day of the resolution in writing was signed and at the time at which the resolution in writing was last signed by a Director.

6. DUTIES AND RESPONSIBILITIES

In discharging its duties, the Board shall be constantly mindful of the need to safeguard the interests of its shareholders and other stakeholders. The Board assumes, amongst others, the following duties and responsibilities:

(a) to review and approve strategies, business plans, other initiatives including but not limited to outsourcing plan and material outsourcing engagement which would singularly, or cumulatively, have a material impact on the Bank's risk profile, significant policies and to monitor management's performance in implementing them;

(b) to ensure that the Bank establishes comprehensive risk management policies, processes infrastructure and resources, to manage the various types of risks;

(c) to ensure the effectiveness of Risk Management Framework by taking into consideration the changes in business environment to control the Bank's risk-taking activities. Also, to provide constructive challenge on the credibility and robustness of the framework;

(d) to establish periodic review on quantity and quality of the Risk Management reporting;

(e) to oversee and approve the recovery and resolution as well as business continuity plans' maximum tolerable downtime (MTD), recovery time objective (RTO) of critical business function (CBF) for the Bank to restore its financial strength, and maintain or preserve critical operations and critical services when it comes under stress;

(f) to set up an effective internal audit department, staffed with qualified internal audit personnel to perform internal audit functions, covering the financial and management audit;

(g) to establish a rigorous process for the appointment and removal of Directors;

(h) to oversee the selection, performance, remuneration and succession plans of ~~the~~ CEO, control function heads and other members of Senior Management, such that the Board is satisfied with the collective competence of Senior Management to effectively lead the operations of the Bank;

(i) to establish a written policy to address Directors' actual and potential conflict of interest;

(j) to establish and ensure the effective functioning of various Board Committees;

(k) to promote Shariah compliance in accordance with expectations set out in BNM's Shariah Governance Policy Document and ensure its integration with the Bank's business and risk strategies;

(l) to ensure the effective management of the Bank's capital and capital adequacy levels to ensure fulfillment of regulatory and internal requirements;

(m) to ensure that the relevant stakeholders discharge their responsibilities for the development and effective implementation of the Bank's capital management policies and processes;

(n) to approve credit transactions to connected parties based on Guidelines on Credit Transactions and Exposures with Connected Parties;

(o) to approve the appointment, remuneration and termination of Chief Compliance Officer ("**CCO**");

(p) to approve the establishment of the compliance function and the position of the CCO, and ensure that the compliance function and the CCO are provided with appropriate standing, authority and independence;

(q) to ensure that the CCO has sufficient stature to allow for effective engagement with the CEO and other members of senior management;

(r) to engage with the CCO on a regular basis to provide the opportunity for the CCO to discuss issues faced by the compliance function. The Board should also consider engaging the CCO without the presence of other members of Senior Management from time to time;

(s) to provide the CCO with direct and unimpeded access to the Board;

(t) to ensure that the CCO is supported with sufficient resources, including competent officers, to perform his duties effectively;

(u) to oversee the implementation of the Bank's governance framework and internal control environment, and periodically review whether these remain appropriate in the light of material changes to the size, nature and complexity of the Bank's operations;

(v) to promote, together with Senior Management, a sound corporate culture within the Bank which reinforces ethical, prudent and professional behaviour;

(w) to promote sustainability through appropriate environmental, social and governance considerations in the Bank's business strategies;

(x) to promote timely and effective communication between the Bank and BNM on matters affecting or that may affect the safety and soundness of the Bank;

(y) to undertake the Board's duties and responsibilities as well as oversight functions as stipulated in the CA 2016; FSA 2013, IFSA 2013, BNM Policy Documents and Guidelines; and any other regulations for directives issued by BNM from time to time;

(z) Undertake the Board's duties and responsibilities and oversight functions as stipulated in paragraph 11.2 of the BNM's Policy Document on Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financing Sanctions for Financial Institutions (AML/CFT and TFS for FI) as per Appendix 1;

(aa) Undertake and exercise the Board's duties, responsibilities and oversight functions as stipulated in BNM's Risk Management in Technology (RMiT) Policy Documents as per Appendix 2;

(bb) Exercise oversight accountability over Shariah governance and compliance to ensure the processes reflect the integration of Shariah governance considerations within the business and risk strategies of the Bank as per outlined under the BNM's Shariah Governance Policy Document or any other regulations or directives issued by BNM from time to time.

(cc) To provide board veto clearance for large exposures based on the Credit Policy of the Bank. Where such veto clearance was obtained via circulation the loan / financing exposures to be collectively deliberated and ratified in the subsequent Board meeting.

The Directors are aware and shall at all times observe and comply with the provisions of the CA 2016, FSA 2013, IFSA 2013 and other applicable laws, guidelines and regulations, in the performance of their duties.

Chairman

(a) The Chairman shall be a Non-Executive Director.

(b) The roles of the Chairman and the CEO are separate to ensure that there is a balance of power and authority.

(c) The Chairman is responsible for the leadership, effectiveness, conduct and governance of the Board and assumes, amongst others, the following duties and responsibilities:

  (i) to ensure that appropriate procedures are in place to govern the Board's effective operation;

  (ii) to ensure that decisions are taken on a sound and well-informed basis, including by ensuring that all strategic and critical issues are considered by the Board, and that Directors receive the relevant information on a timely basis;

  (iii) to encourage healthy discussion and ensure that dissenting views can be freely expressed and discussed; and

  (iv) to lead efforts to address the Board's developmental needs.

CEO

The CEO, in leading Senior Management bears primary responsibility over the day-to-day management of the Bank. The responsibilities of Senior Management include:

(a) implementing the business and risk strategies, remuneration and other policies in accordance with the direction given by the Board;

(b) establishing a management structure that promotes accountability and transparency throughout the Bank's operations, and preserves the effectiveness and independence of control functions;

(c) promoting, together with the Board, a sound corporate culture within the Bank which reinforces ethical, prudent and professional behaviour;

(d) addressing actual or suspected breaches of regulatory requirements or internal policies in a timely and appropriate manner; and

(e) regularly updating the Board with the material information, the Board needs to carry out its oversight responsibilities, particularly on matters relating to–

(i) the performance, financial condition and operating environment of the Bank;

(ii) internal control failures, including breaches of risk limits; and

(iii) legal and regulatory obligations, including supervisory concerns and the remedial actions taken to address them.

Independent Director

Independent Directors should ensure a strong element of independence on the Board both in thought and actions. The effective participation of Independent Directors is to enhance the accountability in the Board's decision making process. The responsibilities of an Independent Director include the following:

(a) to provide and enhance the necessary independence and objectivity on the Board

(b) to ensure effective checks and balances on the Board,

(c) to mitigate any possible conflict of interest between the policy-making process and the day-to-day management of the Bank,

(d) to constructively challenge and contribute to the development of business strategy and direction of the Bank and

(e) to ensure that adequate systems and controls to safeguard the interests of the Bank are in place.

7. MATTERS RESERVED FOR THE BOARD'S DECISION

The responsibilities and procedures of the Board and Board Committees are set out in their respective TOR.

Matters reserved for the Board's decision, supported by any recommendations and may be made from time to time by the Board Committees and/or Management include, amongst others, the following:

(a) business direction, strategies and plan
(b) financial matters
(c) structure and capital
(d) company's operation
(e) financial reporting and controls
(f) board structure; appointment of Shariah Committee members and key responsible persons
(g) remuneration matters
(h) delegation of authority
(i) related party transactions of a material nature
(j) others such as policies; any decisions likely to have a material impact on the Bank from any perspective
(k) matters which exceed the Board Committees' approval authorities delegated by the Board

8. REPORTS

The Board is responsible for ensuring the production of the following reports on an annual / quarterly basis:

(a) Financial statements (including annual audited accounts and interim unaudited accounts)
(b) Annual Report
(c) Corporate Governance Statement
(d) Business Plan and Strategies as well as Budget
(e) Any other periodic reports as required by the regulators from time to time

9. AUTHORITY

With the exception of specific corporate decisions stated in the CA 2016, FSA 2013, IFSA 2013 and the Bank's Constitution, which require the approval of the Minister of Finance/BNM or which require the passing of ordinary or special resolutions by shareholder, the Board shall have full authority to make all decisions.

The Board may delegate any of their powers to a committee or committees consisting of such members of their body as they think fit; any committee so formed shall in the exercise of the powers so delegated conform to any directions that may be imposed on it by the Directors and a power so exercised shall be deemed to have been exercised by the Directors.

The Bank must provide the Board with access to advice from third party experts on any matter deliberated by the Board as and when required, and the cost of such advice shall be borne by the Bank.

10. BOARD COMMITTEES AND INDEPENDENT COMMITTEE

(a) The Board needs to establish specialized Board Committees and Independent Committee i.e. Shariah Committee to oversee critical or major functional areas and to address matters, which require detailed review or in-depth consideration. Although the Board may delegate certain duties to the Board Committees and Shariah Committee, it remains fully accountable for any authority the Board has delegated.

(b) The Board must provide the Board Committees and Shariah Committee with sufficient support and resources required to investigate any matter within their mandates.

(c) The Board appoints the following Board Committees and Shariah Committee to assist it in carrying out its duties and responsibilities and to facilitate efficient decision making:

- Audit Committee;
- Risk Management Committee;
- Nomination Committee;
- Remuneration Committee; and
- Shariah Committee

(d) The Board Committees operate within their own clearly defined roles and responsibilities as set out in their respective TORs approved by the Board and below is a brief description of each of the Board Committees and Independent Committee:

(i) Audit Committee

The Audit Committee was established to support the Board to ensure that there is a reliable and transparent financial reporting process within the Bank. The AC is primarily responsible for reviewing and monitoring the integrity of the Bank's financial reporting process, accounting records, risk management process and system of internal controls.

(ii) Risk Management Committee

The RMC is primarily responsible for the oversight of risk management policies and practices of the Bank. RMC reviews and assesses the adequacy of risk management function to identify, measure, monitor, and manage all material risks faced by the Bank. RMC ensures that the Bank's business activities are conducted in a safe and sound manner, in line the highest standards of professionalism, consistent with the Bank's overall business strategy, risk appetite and good corporate governance.

(iii) Nomination Committee

The Nomination Committee is primarily responsible for establishing the minimum requirements and criteria for the selection of the Board members, Shariah Committee members, Senior Management and Company Secretary. It also determines and assesses the Board's composition, nomination of new Directors, Shariah Committee members, Board Committee members, as well as nominees for the Senior Management and Company Secretary. In addition, it recommends to the Board the removal of the Director, Shariah Committee member, Senior Management and Company Secretary if they are ineffective, errant or negligent in discharging their responsibilities. It also assesses and ensures the independence of a director.

(iv) Remuneration Committee

The Remuneration Committee (RC) shall support the Board of Directors (Board) in actively overseeing the design and operation of the Bank's remuneration system in accordance with the Bank Negara Malaysia (BNM) Guidelines on Corporate Governance. It is primarily responsible for reviewing and recommending to the Board the overall remuneration policy for Directors, Shariah Committee members, Senior Management and others material risk takers to ensure the remuneration policy attracts, retains and motivates key talents. RC's overarching aim to create fair, competitive, and transparent employment and compensation practices, avoiding conflict of interest and maintaining a balance between competitive and equitable compensation aligned with the Bank's corporate strategies and business objectives.

(v) Shariah Committee

The Shariah Committee is primarily responsible to provide objective and sound advice to the Islamic financial business and operation covering International Business Unit (ICBU), Islamic Banking Window (IBW) and all other approved Islamic financial business by BNM under the Bank's license to ensure that its aims and operations, business, affairs, and activities are in compliance with Shariah. Its responsibilities also include to perform an oversight role on Shariah compliance related to the Bank's Islamic banking operations including assessing the work carried out by Shariah Review and Shariah Audit to ensure Shariah compliance.

(e) Reference shall be made to the TOR of the respective Board Committees and Independent Committee for further details including their roles and responsibilities, requirement membership and frequency of meeting.

10. ACCESS TO INFORMATION AND INDEPENDENT ADVICE

In carrying out its duties and responsibilities, the Board shall have the following powers:

(a) full and unrestricted access to any information, records, properties and personnel of the Bank;

(b) to obtain independent professional advice and expertise necessary for the performance of its duties; and

(c) all Directors shall have access to the advice and services of the Company Secretary.

11. BOARD EVALUATION

The Board, through Nomination Committee, must carry out evaluation on the effectiveness and the performance of the Board, Board Committees, and individual Directors on an annual basis. This is to enable the Board to identify areas for professional development and process improvements, having regard to the changing needs of the Bank.

12. DIRECTORS' TRAINING AND CONTINUING EDUCATION

(a) All newly appointed directors are required to attend and complete the mandatory "Financial Institutions Directors' Education" (FIDE) Core programme (Modules A and B) within one (1) year from the date of their appointment and any other mandatory training for directors under the local regulation within the stipulated timeline.

(b) The Bank will conduct an in-house orientation and education programme for newly appointed Directors; and internal trainings to all Directors to gain insights and keep abreast with the development in the banking industry from time to time.

(c) The Directors shall continue to update and enhance their knowledge and skills by attending appropriate training to enable them to discharge their duties effectively.

(d) The Board shall evaluate and determine the training needs of the Directors from time to time.

13. CONFLICTS OF INTEREST

(a) A director is required under section 58 of the FSA 2013 and section 67 of the IFSA 2013 to disclose to the Board the nature and extent of his interest in a material transaction or material arrangement, and, if such material transaction or material arrangement is being deliberated during a Board meeting, to be absent from the meeting during such deliberations.

(b) For the purposes of section 58(4) of the FSA 2013 and section 67(4) of the IFSA 2013:

(i) an existing or proposed transaction or arrangement will be considered "material" if it is one which a director is required to declare under section 221 of the CA 2016 unless the Director or any person linked to him cannot reasonably be expected to derive a benefit or suffer a detriment from the transaction or arrangement in a way that will place the Director in a position of conflict; and

(ii) an interested Director must make the disclosure by way of a written notice to all members of the Board and the Company Secretary–

(I) as soon as practicable after being aware of his interest in the material transaction or arrangement; and

(II) if the material transaction or arrangement is being deliberated at a Board meeting, before the commencement of that deliberation.

(c) The Director shall be entitled to have other business interests other than those of the Bank subject to his compliance, at all material times, of the requirements under the following and Section 58(1) of CA 2016 which prescribes that where there is a change in the prescribed particulars of a Director, a notification of change in the Register of Directors, Managers and Secretaries should be submitted to the Registrar (Companies Commission of Malaysia) within fourteen (14) days from the date of change:

(i) the Director shall be permitted to accept other board appointments or have other interests in other companies or entities PROVIDED ALWAYS THAT such appointment or interest shall not conflict or compete with or harm in any way the interests of the Bank and shall not materially affect the performance of his duties or otherwise compromise his fiduciary duties to the Bank. All other appointments must be informed to the Board.

(ii) the Director shall duly inform and update the Company Secretary of the Bank as soon as possible of his interests as a shareholder, director, officer, trustee or any other interests in other companies or entities including any changes to such interests or of any actual or potential conflict with the interest of the Bank so that the Directors’ interests register can be maintained up to date.

(iii) A Director shall not hold more than five (5) directorships in a public listed company and 15 directorships in non-listed companies (include public and private companies) to ensure that his commitment in his time and resources will not be affected in discharging his duties effectively as a director.

14. COMPANY SECRETARY

(a) The Company Secretary shall be responsible for supporting the effective functioning of the Board. In discharging this role, the Company Secretary provides counsel to the Board on governance matters and facilitates effective information flows between the Board, the Board Committees and Senior Management.

(b) The Company Secretary shall keep confidential the affairs of the Bank and its officers at all times. If the Company Secretary also serves as Company Secretary for the Bank’s affiliates, she shall not disclose the affairs of the Bank or its officers to the affiliates except with the knowledge and consent of the Bank.

(c) The Company Secretary must not have competing time commitments that may impair his ability to discharge her duties effectively. Unless the Bank approves otherwise in writing, the Company Secretary must devote the whole of her professional time to the affairs of the Bank and its affiliates.

(d) The appointment and removal of the Company Secretary are a matter for the Board to decide and approve to ensure that only qualified and suitable individual is appointed.

(e) All Directors particularly the Chairman shall have access to the advice and services of the Company Secretary for the purposes of the Board's affairs and the business.

15. REVIEW OF THE BOARD CHARTER

The Charter has been adopted by the Board on 19 April 2017. The Board may review this Charter from time to time as may be necessary to ensure its effectiveness and relevance to the current laws and regulations in Malaysia as well as the changing environment of the business operation of the Bank.

The Charter is made available for reference in the Bank's website at http://www.bk.mufg.jp/global/malaysia/

Board of Directors' approval
First approval on 19 April 2017
Revised on 20 May 2020
Revised on 23 June 2022
Revised on 23 January 2024

Appendix 1

BANK NEGARA MALAYSIA's Policy Document on Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Financial Institutions (AML/CFT and TFS for FIs)

11. 2 Board

General

11.2.1 Board members must understand their roles and responsibilities in managing ML/TF risks identified by the reporting institution

11.2.2 Board members must be cognisant of the ML/TF risks associated with business strategies, delivery channels and geographical coverage of its business products and services.

11.2.3 Board members must understand the AML/CFT measures required by the relevant laws, instruments issued under the AMLA, as well as industry's standards and best practices in implementing AML/CFT measures.

Roles and Responsibilities

11.2.4 The Board has the following roles and responsibilities:

(a) maintain accountability and oversight for establishing AML/CFT policies and minimum standards;

(b) approve policies regarding AML/CFT measures within the reporting institution, including those required for risk assessment, mitigation and profiling, CDD, record keeping, on-going due diligence, suspicious transaction report and combating the financing of terrorism;

(c) approve appropriate mechanisms to ensure the AML/CFT policies are periodically reviewed and assessed in line with changes and developments in the reporting institution's products and services, technology as well as trends in ML/TF;

(d) approve an effective internal control system for AML/CFT and maintain adequate oversight of the overall AML/CFT measures undertaken by the reporting institution;

(e) define the lines of authority and responsibility for implementing AML/CFT measures and ensure that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls;

(f) ensure effective internal audit function in assessing and evaluating the robustness and adequacy of controls implemented to prevent ML/TF;

(g) assess the implementation of the approved AML/CFT policies through regular reporting and updates by the Senior Management and Audit Committee; and

(h) establish a Management Information System (MIS) that is reflective of the nature of the reporting institution's operations, size of business, complexity of business operations and structure, risk profiles of products and services offered and geographical coverage.

Appendix 2

BANK NEGARA MALAYSIA RISK MANAGEMENT IN TECHNOLOGY (RMiT) POLICY DOCUMENT

PART B POLICY REQUIREMENTS - 8 GOVERNANCE

Responsibilities of the Board of Directors

8.1 The board must establish and approve the technology risk appetite which is aligned with the financial institution's risk appetite statement. In doing so, the board must approve the corresponding risk tolerances for technology-related events and ensure key performance indicators and forward-looking risk indicators are in place to monitor the financial institution's technology risk against its approved risk tolerance. The board must ensure senior management provides regular updates on the status of these indicators together with sufficiently detailed information on key technology risks and critical technology operations to facilitate strategic decision-making.

8.2 The board must ensure and oversee the adequacy of the financial institution's IT and cybersecurity strategic plans covering a period of no less than three years. These plans shall address the financial institution's requirements on infrastructure, control measures to mitigate IT and cyber risk and financial and non-financial resources, which are commensurate with the complexity of the financial institution's operations and changes in the risk profile as well as the business environment. These plans shall be periodically reviewed, at least once every three years.

8.3 The board shall be responsible to oversee the effective implementation of a sound and robust technology risk management framework (TRMF) and cyber resilience framework (CRF), as required to be developed under paragraphs 9.1 and 11.2, for the financial institution to ensure the continuity of operations and delivery of financial services. The TRMF is a framework to safeguard the financial institution's information infrastructure, systems and data, whilst the CRF is a framework for ensuring the financial institution's cyber resilience. The board must ensure that the financial institution's TRMF and CRF remain relevant on an ongoing basis. The board must also periodically review and affirm the TRMF and CRF, at least once every three years to guide the financial institution's management of technology risks.

8.4 The board must designate a board-level committee[2] which shall be responsible for supporting the board in providing oversight over technology-related matters. Among other things, the committee shall review the technology related frameworks including the requirements spelt out in paragraphs 8.1 through 8.3, for the board's approval, and ensure that risk assessments undertaken in relation to material technology applications submitted to the Bank are robust and comprehensive.

[2] The board of a financial institution may either designate an existing board committee or establish a separate committee for this purpose. Where such a committee is separate from the Board Risk Committee (BRC), there must be appropriate interface between this committee and the BRC on technology risk-related matters to ensure effective oversight of all risks at the enterprise level

8.6 Given the rapidly evolving cyber threat landscape, the board shall allocate sufficient time to discuss cyber risks and related issues, including the strategic and reputational risks associated with a cyber-incident. This shall be supported by input from external experts as appropriate. The board must also ensure its continuous engagement in cybersecurity preparedness, education and training.

8.7 The board audit committee (BAC) is responsible for ensuring the effectiveness of the internal technology audit function. This includes ensuring the adequate competence of the audit staff to perform technology audits. The BAC shall review and ensure appropriate audit scope, procedures and frequency of technology audits. The BAC must also ensure effective oversight over the prompt closure of corrective actions to address technology control gaps.

PART B POLICY REQUIREMENTS - 10 TECHNOLOGY OPERATIONS MANAGEMENT

Technology Project Management

10.3 The board and senior management must receive and review timely reports on the management of these risks on an ongoing basis throughout the implementation of significant projects.

Data Centre Resilience - Data Centre Infrastructure

10.25 A financial institution is required to appoint a technically competent external service provider to carry out a production data centre resilience and risk assessment (DCRA) and set proportionate controls aligned with the financial institution's risk appetite. The assessment must consider all major risks and determine the current level of resilience of the production data centre. A financial institution must ensure the assessment is conducted at least once every three years or whenever there is a material change in the data centre infrastructure, whichever is earlier. The assessment shall, at a minimum, include a consideration of whether the requirements in paragraphs 10.22 to 10.24 have been adhered to. For data centres managed by third party service providers, a financial institution may rely on independent third party assurance reports provided such reliance is consistent with the financial institution's risk appetite and tolerance, and the independent assurance has considered similar risks and meets the expectations in this paragraph for conducting the DCRA. The designated board-level committee must deliberate the outcome of the assessment.

[5] Relevant third party assessments may include the Data Centre Risk Assessment (DCRA), Network Resilience and Risk Assessment (NRA) and independent assurance for introduction of new or enhanced digital services.

Network Resilience

10.40 A financial institution is required to appoint a technically competent external service provider to carry out regular network resilience and risk assessments (NRA) and set proportionate controls aligned with its risk appetite. The assessment must be conducted at least once in three years or whenever there is a material change in the network design. The assessment must consider all major risks and determine the current level of resilience. This shall include an assessment of the financial institution's adherence to the requirements in paragraphs 10.33 to 10.39. The designated board-level committee must deliberate the outcome of the assessment.

Third Party Service Provider Management

10.41 The board and senior management of the financial institution must exercise effective oversight and address associated risks when engaging third party service providers14 for critical technology functions and systems. Engagement of third party service providers, including engagements for independent assessments, does not in any way reduce or eliminate the principal accountabilities and responsibilities of financial institutions for the security and reliability of technology functions and systems.

PART B POLICY REQUIREMENTS - 11 CYBERSECURITY MANAGEMENT

Cyber Response and Recovery

11.25 A financial institution must conduct an annual cyber drill exercise to test the effectiveness of its CIRP, based on various current and emerging threat scenarios (e.g. social engineering), with the involvement of key stakeholders including members of the board, senior management and relevant third party service providers. The test scenarios must include scenarios designed to test:

(a) the effectiveness of escalation, communication and decision-making processes that correspond to different impact levels of a cyber-incident; and

(b) the readiness and effectiveness of CERT and relevant third party service providers in supporting the recovery process.

PART B POLICY REQUIREMENTS - 13 INTERNAL AWARENESS AND TRAINING

13.4 A financial institution must provide its board members with regular training and information on technology developments to enable the board to effectively discharge its oversight role.

PART C REGULATORY PROCESS - 14 NOTIFICATION FOR TECHNOLOGY-RELATED APPLICATIONS

14.5 For the introduction of new services, and any enhancements to existing services not listed in Appendix 6, the financial institution is required to undertake the following measures prior to notifying the Bank:

(a) engage an independent external party to provide assurance that the financial institution has addressed the technology risks and security controls associated with the e-banking, Internet insurance and Internet takaful services or any material enhancement to the existing e-banking, Internet insurance and Internet takaful services. The format of the assurance shall be as set out in Appendix 7; and

(b) provide a confirmation by the CISO, senior management officer or the chairman of the board or designated board-level committee stipulated in paragraph 8.4 of the financial institution's readiness to provide e-banking, Internet insurance and Internet takaful services or implement any material enhancement to the e-banking, Internet insurance and Internet takaful services. The format of the confirmation shall be as set out in Appendix 8.

PART C REGULATORY PROCESS - 15 CONSULTATION AND NOTIFICATION RELATED TO CLOUD SERVICES

15.1 A financial institution is required to consult the Bank prior to the first-time adoption of public cloud for critical systems. During the consultation, the financial institution must demonstrate that specific risks associated with the use of cloud services have been adequately considered and addressed to the satisfaction of the Bank, in order to proceed with the adoption of the public cloud for critical systems for the first time. The financial institution shall undertake the following prior to consulting the Bank on its adoption of public cloud for critical systems:

(a) conduct a comprehensive risk assessment of the proposed cloud adoption, including the possible impact and measures to address and mitigate the identified risks as outlined in paragraph 10.49 and in Appendix 10. The financial institution shall also adopt the format of the Risk Assessment Report as per Appendix 7;

(b) provide a confirmation by the CISO, senior management officer or the chairman of the board or designated board-level committee stipulated in paragraph 8.4 of the financial institution's readiness to adopt public cloud for critical system. The format of the confirmation shall be as set out in Appendix 8; and

(c) perform a third-party pre-implementation review on public cloud implementation that covers the areas set out in Appendix 10 and Part A of Appendix 9 for higher-risk public cloud services, such as when the cloud services involve the processing or storage of customer information, or if data will be transmitted across borders.

Appendix 10: Key Risks and Control Measures for Cloud Services

This appendix provides additional guidance to financial institutions for the assessment of common key risks and considerations of control measures when financial institutions adopt public cloud for critical systems.

Part A: Cloud Governance

1. Cloud Risk Management

   (a) The board of a financial institution should promote and implement sound governance principles throughout the cloud service lifecycle in line with the financial institution's risk appetite to ensure safety and soundness of the financial institution.

   (b) The senior management of a financial institution should develop and implement a cloud risk management framework that integrates with existing outsourcing risk management framework, technology risk management framework (TRMF) and cyber resilience framework (CRF), for the board's approval, proportionate to the materiality of cloud adoption in its business strategy, to assist in the identification, monitoring and mitigating of risks arising from cloud adoption.

2. Skilled personnel with knowledge on cloud services

   (a) The adoption of cloud services requires commensurate changes to the financial institution's internal resources and process capabilities. In this regard, a financial institution should:
      i. equip its board and senior management with appropriate knowledge to conduct effective oversight over the cloud adoption.

****