

ALLIANCE BANK MALAYSIA BERHAD

Terms of Reference of Group IT Committee (GITC)

Purpose

The Committee shall be an outcome-based board committee to primarily provide end-to-end oversight for the IT strategy project due to its far-reaching and long-term implications for the Bank. The GITC is responsible for supporting the Board in providing oversight over technology-related matters in accordance with paragraph 8.4 of the BNM policy document on Risk Management in Technology.

The Committee will oversee the end-to-end IT and digital delivery of the Bank's products and services through:

- (i) Supporting the Board in providing oversight over technology-related matters, including establishing and approving the technology risk appetite aligned with the Bank's risk appetite statement.
- (ii) Overseeing the adequacy of the Bank's IT and cybersecurity strategy plans covering a period of no less than three years;
- (iii) Overseeing the effective implementation of a sound and robust technology risk management framework and cyber resilience framework for the Bank's continuity of operations and delivery of financial services.
- (iv) Reviewing regular reporting on the digital ecosystem and overseeing customer experience;
- (v) Providing oversight to the Bank's IT function including IT strategy, enterprise architecture, the alignment of IT function with the Bank's business, system stability, information security and related operations;
- (vi) Overseeing the development and implementation of the Bank's annual IT Programme of Work, being the suite of initiatives and investments to implement the Bank's change programme and to underpin the delivery of the strategic initiatives;
- (vii) Overseeing the investment in the Bank's IT architecture, infrastructure and support systems to underpin the safe and effective delivery of the products and services; and
- (viii) Overseeing alignment between overall business strategy and the IT and digital strategies.

Duties and Responsibilities

The Committee's responsibilities shall include:

1. Strategy

- 1.1 Reviewing updates and where appropriate, demonstrations about emerging technologies and trends and their potential impact on or application within the Bank.
- 1.2 Reviewing reports from Management regarding the Bank's medium to long term (3-5 years) technology strategy and architecture with reference to changes, trends and emerging technologies, and providing feedback on the strategy.

- 1.3 Reviewing business cases for IT projects in support of the implementation of the strategy for endorsement to the Board, based on the balance of the investment and anticipated benefits against cost, project and other associated risks.
- 1.4 Overseeing strategies for the Bank's outsourcing of material technology services, including selection and evaluation of preferred vendors and performance measurement and management of material vendors.
- 1.5 Overseeing the overall Information and Cyber Security strategies and its operational and response posture, ensuring appropriate awareness and continuous engagement across the Bank. Ensuring the Bank allocates the required amount of resources and investment in protection of its digital assets and the prevention of attacks.

2. Customer technology and digital experience

- 2.1 Reviewing regular reporting from management on the customer experience delivered by the Bank's technology and digital eco-system.
- 2.2 Overseeing the establishment of key performance indicators and service level agreements in measuring the performance of IT services delivered or received by the Group.

3. Technology Investment and Expenditure

- 3.1 Reviewing from Management –
 - (i) Regular reporting on the overall health of the Bank's technology portfolio;
 - (ii) Regular reporting, by reference to internal and external benchmarks, on the quality, stability and reliability of the Bank's digital eco-system and IT services;
 - (iii) Regular reporting on the technology elements delivering, or being delivered by, including costs, deliverables, scheduling, implementation risk (including change management and business readiness), and robustness of the technology solution;
 - (iv) Regular reporting on the key (strategic or high risk) individual technology projects, and New Investment Agendas approved by the Group Project Investment Committee; and
 - (v) Post implementation reviews of all key projects to ensure that positive and negative experiences are captured and appropriate processes developed to capture the lessons learned and deliver future process improvements

4 Digital and Technology Staff

- 4.1 Reviewing update on talent management and succession strategy in ensuring sustainable talent pipeline as well as training and development of digital and technology staff (the GITC's input relating to digital and technology staff to be provided to Group Nomination and Remuneration Committee [GNRC]).
- 4.2 Providing feedback during the hiring process and the annual performance of key C Level management for digital and technology to GNRC.

5. Digital and IT Risk and Security

- 5.1 Reviewing and ensuring that key technology related risk areas are identified and mitigated including overseeing the effectiveness of the Bank's IT vulnerability testing and remediation plans.
- 5.2 Reviewing and recommending to the Board for approval at least annually, the Bank's risk tolerances for technology-related events and reviewing the key performance indicators and forward looking risk indicators are in place for an effective oversight of the Bank's technology risk against its approved risk tolerance.
- 5.3 Reviewing and recommending to the Board for approval at least once in every three years or as and when it is deemed necessary by the Committee, the Bank's Information Technology (IT) and cybersecurity strategic plans, technology risk management framework and cyber resilience framework to ensure that the plans/ frameworks are responsive to changes in or expansion of business activities, and developments in the operating environment.
- 5.4 Overseeing the effectiveness of the Bank's Business Continuity and IT Disaster Recovery Plans; and Business Continuity and Disaster Recovery Testing.
- 5.5 Reviewing the risk assessments undertaken in relation to material technology applications submitted to Bank Negara Malaysia are robust and comprehensive.
- 5.6 Reviewing cyber risks and related issues, including the strategic and reputational risks associated with a cyber-incident, supported by input from external experts as appropriate.

Members

To comprise at least three (3) Directors who have the skills, knowledge and experience relevant to the responsibilities of the Committee.

Quorum

Three (3) members shall constitute a quorum at meeting and majority of members present must be Independent Directors.

Decisions

Questions arising at the meeting shall be decided by a majority of votes. In case of equal votes, the Chairman shall have a second or casting vote.

Approving Authority

For IT related CAPEX and OPEX which requires the ABMB EXCO or Board's approval, the Committee's endorsement shall be obtained prior to submission to the EXCO or the Board for approval.

Frequency of Meeting

Monthly or otherwise determined by the Chairman.

To ensure there is an appropriate interface between the Committee and the Group Risk Management Committee ("GRMC"), there shall be at least one joint meeting held annually between the Committee and the GRMC on technology risk-related matters for effective oversight of all risks at the enterprise level.

Secretary

The Company Secretary.

Frequency and Reporting Process

A copy of the relevant minutes shall be circulated to the Board (where relevant) or tabled at the Board meeting for notation.

Update and Review

The Committee shall review and assess the adequacy of the Terms of Reference at two (2) years interval or as and when necessary. Any proposed changes to the Terms of Reference shall be approved by the Board.