TERMS OF REFERENCE
OF

THE BOARD INFORMATION TECHNOLOGY COMMITTEE
("BITC" or "the Committee")
of Bank Pertanian Malaysia Berhad ("Agrobank" or "the Bank")

Membership	:	At least three (3) directors[1], a majority of whom, including the Chairman should be independent directors.[2]
In Attendance	:	i. President/Chief Executive Officer ii. Chief Finance Officer iii. Chief Information Security Officer iv. Chief Operations Officer v. Chairman is given the discretion to invite any relevant person as and when required. In the event a person is appointed as "Acting" or "Covering" for a particular position, he/she shall attend the meeting in his/her capacityof that position.
Secretary	:	The Company Secretary ("CoSec") or his/her nominee or any person designated by the Committee.
Quorum	:	At least three (3) of the BITC members including the Chairman of the Committee.
Frequency of Meeting	:	The BITC meeting shall be held at least once in every quarter or at such number of time(s) as the Committee requires or deemed necessary to fulfil the Committee's responsibilities.

---

[1] Directors may refer to Independent Non-Executive Directors and Non-Independent Non-Executive Directors
[2] Para 12.3 BNM Policy Document on Corporate Governance ("BNM CG Guidelines")

1.0 OBJECTIVE

The BITC is responsible in assisting the Board in overseeing the implementation of strategies of Information Technology ("IT") and Cyber Security as well as digitalisation activities including e-banking initiatives within Agrobank.

2.0 AUTHORITY

The Committee is authorised by the Board to act within its TOR: -

i.   To deliberate and review for recommendation to the board on matters within its primary duties and responsibilities within these terms of reference or such limits as may be determined by the Board from time to time;

ii. To obtain the resources which it requires including but not limited to obtaining an independent professional advice and expert advice, both internal and external, and to have full and unrestricted access to information to enable the Committee to fulfil its objectives; and

iii. To have a direct communication and on continuous basis with Senior Management to be kept informed of matters affecting the Bank in respect of IT.

3.0 ROLES AND RESPONSIBILITIES

3.1 The role of the Committee is to provide oversight and direction for the Bank's holistic approach to IT. The Committee advises the Bank on IT priorities, makes decisions on strategic issues and drives compliance with agreed actions.

3.2 The responsibilities of the Committee include: -

i.   to provide strategic direction with regard to IT Management and to ensure the IT strategic plan supports the Bank's strategic business plan and IT Management should also be expanded to IT Operation & Strategic IT & Digital;

ii. to review and approve the Bank's key IT strategic investment direction and policies to ensure the effectiveness of internal control systems and the reliability of the management information system;

iii. to ensure the Bank's Management adopts prudent and effective policies and procedures to identify, measure, monitor and control or mitigate IT risks;

iv. to undertake other duties as directed by the Board from time to time; and

v.   to approve the appointment of external consultants and advisors to advise the Committee on risk management system infrastructure and technical matters as and when required.

3.3   Specific Duties:-

i.   to approve periodic management reports and where necessary, recommend appropriate strategic solutions on key IT weaknesses discovered;

ii.   to review, monitor and prioritise major IT programmes and projects;

iii.   to adopt compliance with established IT policies and procedures, and guidelines and circular issued by Bank Negara Malaysia ("BNM");

iv.   to monitor the measures taken to correct weaknesses noted in the internal and external audit reports or BNM's examination reports;

v.   to monitor the performance of IT services delivered to the Bank; and

vi.   to present the minutes and provide brief reports on the decision made to the Board.

3.4   Risk Management in Technology ("RMiT")[3]:-

The Committee shall: -

i.   establish and approve the technology risk appetite which is aligned with the Bank'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 Bank's technology risk against its approved risk tolerance. The Board must ensure the 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;

ii.   ensure and oversee the adequacy of the Bank's IT and cybersecurity strategic plans covering a period of no less than three years. These plans shall address the Bank's requirements on infrastructure, control measures to mitigate IT and cyber risk and financial and non-financial resources, which commensurate the complexity of the Bank'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;

---

[3] Para 8 BNM Policy Document on Risk Management in Technology (RMiT).

iii.   oversee the effective implementation of a sound and robust technology risk management framework ("TRMF") and cyber resilience framework ("CRF") for the Bank to ensure the continuity of operations and delivery of financial services. The TRMF is a framework to safeguard the Bank's information infrastructure, systems and data, whilst the CRF is a framework for ensuring the Bank's cyber resilience. The Committee must ensure that the Bank's TRMF and CRF remain relevant on an ongoing basis. The Committee must also periodically review and affirm the TRMF and CRF, at least once every three years to guide the Bank's management of technology risks;

iv.   review the technology-related frameworks including the requirements spelled out in items 3.4(i) through 3.4(iii), 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;

v.   promote effective technology discussions at the board level, the composition of the committee should include at least a member with technology experience and competencies; and

vi.   Given the rapidly evolving cyber threat landscape, the Committee 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 Committee must also ensure its continuous engagement in cybersecurity preparedness, education and training.

3.5   To accomplish the above roles and responsibilities, and any other specific or ad hoc matters that deemed necessary, the BITC may seek an independent third-party expert's views/advise on the matters determined by the Committee or upon directive from the Board.