

1.0 COMPOSITION OF THE COMMITTEE

- 1.1 The Committee shall consist of only non-executive directors with at least three (3) members, with a majority of whom are independent directors and chaired by an Independent Non-Executive Director;
- 1.2 No alternate directors shall be appointed as a member of the Committee;
- 1.3 The Committee's Chairman shall be designated by the Board or, if it does not do so, the Committee members shall elect a Chairman by vote of a majority of the full Committee;
- 1.4 In the event of any vacancy in the Committee, arising from retirement or resignation, with the result that the number of members is reduced to below three (3), the Board of Directors must fill the vacancy within three (3) months;
- 1.5 The Board may from time to time appoint to the Committee additional members who are Non-Executive Directors as it deems fit and necessary, subject to Section 1.1 above being complied;
- 1.6 The Committee may invite any director, executive, or other person to attend any meeting(s) of the Committee as it may from time to time consider desirable to assist the Committee in the attainment of its objective; and
- 1.7 The Chairman of the Committee is not the Chairman of the Board.

2.0 OBJECTIVE

- 2.1 The duties of the Board is to be aware and ensure the proper oversight of the management of all risks covering credit risk, market risk, liquidity risk, shariah risk, IT risk, operational risk management and compliance risk as well as legal and other risks.
- 2.2 The primary objectives of the Committee are to:-
 - i. Assist the Board in fulfilling its fiduciary responsibilities particularly in management controls;

MBSB BANK BERHAD

Terms of Reference of the Board Risk Management And Compliance Committee (BRMCC)

- ii. Oversee Senior Management's activities in managing credit, market, liquidity, shariah, IT, operational, compliance, legal and other risk and to ensure that the risk management process is in place and functioning;
- iii. Provide focal point for communication between risk managers, Board and Senior Management on matters in connection with reporting, risks and controls and providing a forum for discussion independent of the Management; and
- iv. Undertake additional duties as may be deemed appropriate and necessary to assist the Board.

3.0 RIGHTS

3.1 The Committee shall:-

- i. Have the resources which are required to perform its duties;
- ii. Have full and unrestricted access to any information pertaining to the Bank;
- iii. Have direct communication channels with external auditors, internal auditors and risk managers;
- iv. Be able to obtain independent professional or other advice. All expenses incurred in relation to the abovesaid shall be borne by the Company and approved by the Committee and implemented through the Company Secretary;
- v. Have the authority to make any inquiries on any matter within its terms of reference and to instruct the Internal Auditor to carry out investigations; and
- vi. To review and present to the Board for approval of annual Risk Management Strategic Initiatives.

4.0 DUTIES AND RESPONSIBILITIES

4.1 With regards to Risk Management and Compliance, the Committee is responsible for the following:

- i. Support the Board in overseeing the management of risk and compliance within the Bank;
- ii. Review and recommend risk and compliance policies for Board's approval, including AML/CFT related policies, to facilitate the right risk and compliance culture in the day-to-day business and operational activities;
- iii. Review existing resources for risk management and compliance functions to ensure sufficient staff with competencies and experience in discharging their duties;
- iv. Evaluate the effectiveness of the Bank's risk management and compliance functions;
- v. Review and recommend the Risk Management and Compliance Annual Plans and AML/CFT annual risk assessment to the Board for approval;
- vi. Appoint, transfer or remove the Chief Risk Officer (CRO) and Chief Compliance Officer (CCO). The appraisal of the CRO and CCO would be evaluated by the Committee.
- vii. Ensure that the Chief Risk Officer (CRO) and Chief Compliance Officer (CCO) are provided with direct and unimpeded access to the Board;
- viii. Ensure risk management and compliance functions; CRO and CCO are provided with appropriate standing, authority and independence;
- ix. Ensure infrastructure, resources and systems and other capabilities are in place for risk management and compliance functions and are adequate to maintain a satisfactory level of risk management and compliance disciplines;
- x. Ensure that the risk management and compliance functions are able to secure assistance from other functions with specific expertise, for example, Legal Advisory. In this respect, Risk Management and Compliance Division must have clear authority

to engage with any officers and obtain access to relevant information for purposes of discharging its responsibilities;.

- xi. To evaluate, review or access the performance of the CRO, CCO and Head of Integrity and Governance unit (IGU) and to recommend the same to the Board Nominating & Remuneration Committee (BNRC) for further recommendations to the BOARD on the remuneration packages.

4.2 With regards to Risk Management specifically, the Committee is responsible for the following:

- i. Review operational policies of the Bank and to formulate new ones where appropriate to improve efficiency, cost effectiveness and control over the resources;
- ii. Review, monitor, mitigate and report the significant risks as identified by the Risk Management Division and their impact on the operations;
- iii. Review and propose the setting of the risk appetite / tolerance of the Bank and to ensure risk exposures are within the parameters set by the Board by:
 - a. Reviewing and recommending changes to the Risk Appetite annually based on the macroeconomic environment, regulatory landscape, the Bank's liquidity and capital profile, etc.;
 - b. Providing oversight on the compliance of the approved Risk Appetite which is reported annually;
 - c. Being apprised of action plans in cases where there is non-compliance with the Risk Appetite in accordance with approved policies and procedures;
 - d. Recommending the annual Risk Appetite Statement for Board approval.
- iv. Review the allocation of risk-adjusted capital and broad-based limits across the Bank covering market, credit and operational risk;
- v. Ensure oversight of the Internal Capital Adequacy Assessment Process ("ICAAP")

MBSB BANK BERHAD

Terms of Reference of the Board Risk Management And Compliance Committee (BRMCC)

by:

- a. Ensuring adequacy of the capital management framework and policies in line with capital strategy and regulatory requirements;
- b. Ensuring risk and capital management frameworks and policies are operating effectively and complied with;
- c. Providing oversight on the risk and capital positions of the Bank which are reported on a quarterly basis
- d. Assisting the Board to oversee the managing of ICAAP of the Bank by:
 - Ensuring that all relevant risks have been captured and there are sufficient capital resources in place;
 - Ensuring that the impact of any material event has been incorporated and, where appropriate, being apprised of the suitability of the risk assessment; and
 - Ensuring that the overall stress test programme is carried out.
- vi. Ensure oversight of risk management disclosures by approving all disclosures, disclosure policies and internal controls over the disclosure process in line with regulatory requirements;
- vii. Ensure that there are clear and independent reporting lines and responsibilities for the overall business activities and risk management functions;
- viii. Inculcate risk management culture within the Bank so that risk management processes and controls are applied and embedded in the day-to-day business and operational activities;
- ix. Review and recommend risk policies, methodologies and strategies for measuring and managing risks arising from the Bank's business and operational activities, for Board's approval;

MBSB BANK BERHAD

Terms of Reference of the Board Risk Management And Compliance Committee (BRMCC)

- x. Review new products and services to be submitted for Board's approval and highlighting the risk aspects to the Board;
- xi. Review and assess the adequacy of risk management policies and framework (including processes, systems and internal controls), in identifying, measuring, monitoring and controlling risk and the extent to which these are operating effectively;
- xii. Review management's periodic reports on risk exposure, risk portfolio composition and risk management activities;
- xiii. Review contingency plans for dealing with various extreme internal/ external events and disasters;
- xiv. Support the Board in meeting the expectations on risk management as set out in BNM's policy document on Risk Governance;
- xv. In assisting the implementation of a sound remuneration system, examine whether incentives provided by the remuneration system take into consideration risks, capital, liquidity and the likelihood and timing of earnings, without prejudice to the tasks of the Board Nominating and Remuneration Committee (BNRC);
- xvi. Review and deliberate on Composite Risk Rating (CRR) issues raised by BNM prior to reporting to Board;
- xvii. Review and deliberate on any Supervisory Assessment report by BNM as delegated by Board, prior to onward reporting to Board;
- xviii. Review and sanction any reply / responses / updating of reply or responses to BNM in respect of CRR issues outstanding raised by BNM;
- xix. To provide oversight on the following, in relation to the Independent Credit Review ("ICR") function:-
 - Review the adequacy of the scope, procedures, frequency, functions, resources and competency of the Independent Credit Review Department and that it has the necessary authority to carry out its duties. The credit review

assessment will be as per the scope stated in Credit Risk Guideline issued by Bank Negara Malaysia.

- Reviewing key independent credit review reports and ensuring the senior management is taking necessary corrective actions in a timely manner to address control weaknesses, non-compliance with laws, regulatory requirements, policies and other problems identified by the independent credit review and other control functions.
 - Ensure the independence of the independent credit review function.
 - To ensure the independent credit review function is well placed to undertake review on behalf of BRMCC, thus independent credit reviewers should have an appropriate standing within the institution.
 - The outcomes and recommendations arising from the review will be escalated to the Board Audit Committee (BAC) and Board Risk Management and Compliance Committee (BRMCC) for deliberation.
 - The independent credit review will be subject to internal audit assessments.
- xx. Receive Asset Liability Committee (ALCO) and Capital Management Committee (CMC) minutes for notation; and
- xxi. To undertake any other activities as authorised by the Board.

4.3 With regards to Compliance specifically, the Committee is responsible for the following:

- i. Review management reporting to the Board on compliance risk issues and any material incidences of non-compliance (for example, failures that may attract a significant risk of legal or regulatory sanction) to ensure such issues are resolve efficiently and expeditiously; and
- ii. Review and recommend to Board for approval on all engagement with external expertise to undertake compliance assessment in specific areas.

4.4 With regards to oversight roles on the activities of Integrity and Governance Unit (IGU) and issues on bribery, corruption and abuse of power, the Committee is responsible for the following:

- i. Assist the Board to oversee and manage the risks of bribery, corruption and abuse of power as part of the enterprise risk management within the Bank;
- ii. Monitor the activities and performance of the Head of Integrity and Governance Unit based on its core functions; and
- iii. The Committee shall attend related training on ethics, integrity, anti-bribery, corruption and abuse of power once in two (2) years.

4.5 Meetings

- i. The Committee meets every quarter or more frequently either face to face (physically) or accessed online (video conferencing) basis, as circumstances may dictate. In the event face to face or accessed online meeting is not possible, a resolution by circulation can also be passed for urgent issues;
- ii. The quorum for a meeting shall be majority of the committee members whereby the members present must be Independent Non-Executive Directors and the quorum must be maintained throughout the meeting. As part of its duty to foster communication, the Chief Executive Officer (CEO), the Management Team, Chief Internal Auditor (CIA) and Chief Compliance Officer (CCO) or any other person(s) who may be requested by the Committee are invited to attend the meetings for the purpose of briefing the Committee on the activities involving their areas of responsibilities;
- iii. Apart from the scheduled meetings, the Chairman of the Committee may call for additional meetings whenever necessary or shall call a meeting if requested to do so by the Board, or any Committee member or can be based on the advice of the Chief

MBSB BANK BERHAD

Terms of Reference of the Board Risk Management And Compliance Committee (BRMCC)

Executive Officer (CEO), the Chief Risk Officer (CRO) or the Chief Compliance Officer (CCO).

- iv. While the Committee may invite any person to be in attendance to assist it in its deliberations, the Committee should also ensure that the Members meet exclusively when necessary.
- v. The Chairman and the Committee shall report and update the Board on significant issues and concerns discussed during the Committee meetings and where appropriate, make the necessary recommendations to the Board;
- vi. The Chairman and the Committee should engage on continuous basis with Senior Management in order to be kept informed of matters affecting the Bank and the Group; and
- vii. The CRO shall be the Secretary of the Committee and the Head of Company Secretarial Department shall be the Recording Secretary to the Committee.

Note: The position of CEO in this context shall include Acting CEO. For clarification, the position of Deputy CEO is not a permanent position and was specifically established only for succession planning purposes.

4.6 Modus Operandi

- ii. The Committee, through the Company Secretary, is to keep proper records of all decisions/ recommendations made for each Meeting, in which case minutes of each Meeting must be confirmed by the Chairman and retained by the Committee's recording secretary as the Committee's records. A copy of the confirmed minutes of Meeting of the Committee must be presented to the Board for the latter's notation.

4.7 Resolution of the Committee

- i. Questions arising at any Meeting of the Committee shall be decided by a majority of votes by members present at said Meeting.
- ii. Circular Resolution in Writing

A resolution in writing circulated in hard copy or electronic form signed physically or digitally signed and approved by all members of the Committee for the time being in Malaysia shall be effective for all purpose as a resolution of the Committee passed at a Meeting duly convened and constituted.

*** End ***