

STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

INTRODUCTION

Pursuant to Paragraph 15.26(b) of the Listing Requirements of Bursa Malaysia Securities Berhad, the Board of Directors ("**Board**") is pleased to provide the following Risk Management and Internal Control Statement (the "**Statement**") which outlines the nature and scope of risk management and internal controls of the Group during the financial year ended 31 December 2017.

For the purpose of disclosure, this Statement is guided by the Statement on Risk Management & Internal Control: Guidelines for Directors of Listed Issuers. The Board is committed and acknowledges its responsibility to oversee the system of risk management and internal controls within the Group including reviewing its adequacy, integrity and effectiveness to safeguard shareholders' investments and the Group's assets.

The Board has received assurance from BHB's CEO and the Group Chief Financial Officer that the Group's risk management and internal control systems are operating adequately and effectively, in all material aspects, during the financial year under review and up to the date of this Statement.

Taking into consideration the assurance from the Management and the input from the relevant assurance providers, the Board is of the view that the systems of risk management and internal control are performing satisfactorily and are adequate to safeguard the shareholders' investments, customers' interest and the Group's assets. The Group will continue to implement new measures to strengthen the internal control and risk management environment.

BOARD RESPONSIBILITY

The Board recognises that a sound system of internal control and risk management practices are essential in ensuring good corporate governance. Such a system is designed to manage an acceptable risk profile rather than eliminate the risk of failure to achieve the business objectives of the BHB Group; and can only provide reasonable and not absolute assurance against material misstatement, fraud or loss.

As a financial holding company ("**FHC**"), continuous enhancements are being made to the system of internal control in line with the Board's commitment to improve the Group's governance, risk management and internal control framework and control culture. The environment for the proper control of the Group's business operations is also in line with Bank Negara Malaysia's ("**BNM**") regulatory framework.

At BHB level, the internal control oversight responsibilities were initially carried out by the following committees:-

- **Audit & Examination Committee ("**AEC**")**

The main responsibility of the AEC is to assist the Board in assessing the effectiveness of the Group's internal control systems and overseeing the accounting system's internal control. This is to ensure that appropriate methods and procedures are in place to obtain the level of assurance required by the Board. The AEC also review the quarterly reports relating to regulatory developments, compliance and operational deficiencies identified within the Company. The AEC also assists the Board to review the adequacy and effectiveness of the accounting system's internal control and ensures that appropriate methods and procedures are in place to obtain the level of assurance required by the Board. The minutes of the AEC is escalated to the Board for information.

The Terms of Reference is available on the Company's website www.bimbholdings.com; About us – Corporate Governance – Board Committees – Audit & Examination Committee – Terms of Reference

STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

- **Board Risk Committee (“BRC”)**

The BRC is responsible to assist the Board on risk management and oversee the Management’s activities in managing significant risk areas and to ensure that the risk management framework is in place and functioning effectively. At the Management level, the BRC is supported by the Group Risk Management Committee (“**GRMC**”) to oversee the risk management matters relating to the Group risk management activities. The minutes of the BRC is escalated to the Board for information.

The Terms of Reference is available on the Company’s website www.bimbholdings.com; About us – Corporate Governance – Board Committees – Board Risk Committee – Terms of Reference

In respect of the key operating subsidiaries, in particular Bank Islam Malaysia Berhad (“**Bank Islam**”) and Syarikat Takaful Malaysia Berhad (“**Takaful Malaysia**”), the internal control oversight function is carried out by the respective subsidiaries’ BRC. At BIMB Securities Sdn Bhd (“**BIMB Securities**”), the risk management and internal control oversight function is carried out by its AEC.

The risk management control structure and processes which have been instituted throughout the BHB Group are reviewed from time to time to cater for the changes in the business environment. BHB’s AEC and BRC together with the respective AEC/BRC at the key operating subsidiaries regularly reviews and monitors the Management’s approach and actions in addressing key risks at Company and subsidiaries level. It also provides the Board and the Management with the platform to anticipate and manage both the existing and potential risks, taking into consideration changing risk profile and risk appetite. This process has been in place and continued to be BHB Group’s practice for the financial year under review and up to the date of approval of this Statement for inclusion in this Integrated Annual Report.

MANAGEMENT RESPONSIBILITY

The Management is accountable for implementing the Board’s policies and procedures on risks and control and its roles includes but not limited to:-

- Identify the risks relevant to the business, implementation of strategies and the achievement of its objectives;
- Implement regular risk management reporting, monitoring and review as part of its risk management framework;
- Identify changes to risks or emerging risks, take actions as appropriate, and promptly bring these to the attention of the Board;
- Discuss the tolerance level for each of the operational business and ensuring that they are within accepted parameter by the relevant regulatory bodies; and
- Report in a timely manner to the Board any changes to the risk and any corrective action taken.

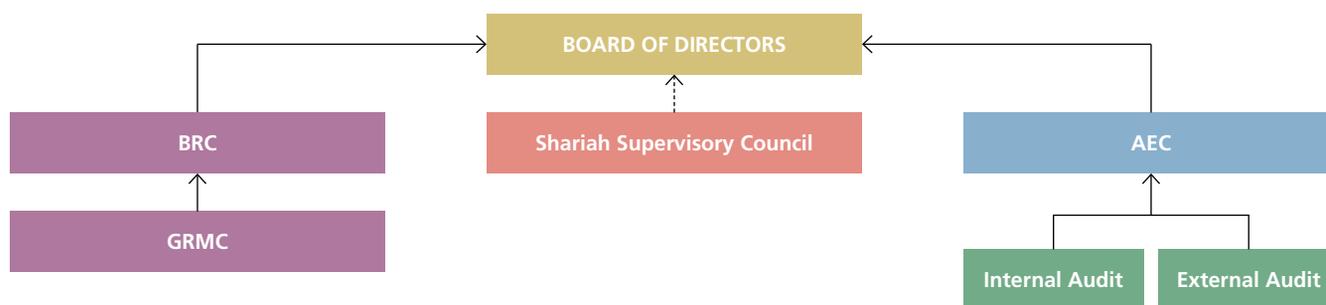
Assurance in relation to the above risk management and internal control are also obtained from the key operating subsidiaries confirming that their risk management and internal control are operating adequately and effectively, in all material aspects. Any material risk management and internal control deficiencies will be presented to the respective subsidiaries’ BRC/AEC and subsequently to the respective Board.

KEY INTERNAL CONTROL STRUCTURE

Key processes that the Board has established in reviewing the adequacy and effectiveness of the system of internal controls include the following:

- **Risk Management Framework**

The Board has established an organisation structure and charter with clear defined lines of responsibility, authority limits and accountability in association with BHB Group's business and operational requirements in order to maintain a sound control environment. The key process that the Board has established in reviewing the adequacy and effectiveness of the system of internal controls is outlined in the diagram below:-



Risk management is considered an integral part of BHB Group's day-to-day operations to facilitate BHB in achieving its objectives as well as to protect its shareholders and stakeholders interest. The risk management is embedded in the Group's key processes and monitored through a Risk Management Dashboard ("RMD") report. The Group's key operating subsidiaries report their risks via RMD at their BRC six (6) times a year. For BIMB Securities, it reports its risks via the RMD at its AEC on quarterly basis.

The Group's risk management framework seeks to ensure that there is an effective on-going process in place to manage risk across the Group. This process is regularly reviewed by the Board through the BRC which provides oversight over the risk management activities for the Group to ensure that the Group's risk management process is functioning effectively. The BRC also assists the Board to review the Group's overall risk management philosophy, frameworks, policies and models. In discharging its overall duties and responsibilities, the BRC is supported by the Group Risk Management Committee which monitors and evaluates the effectiveness of the Group's risk management system on an on-going basis.

In addition to the risk management framework, the Group's key operating subsidiaries had implemented the Internal Capital Adequacy Assessment Process ("ICAAP") framework to ensure that the Group maintains adequate capital levels consistent with the risk profiles including capital buffers to support the Group's current and projected demand for capital under existing and stressed conditions.

The key operating subsidiaries have each appointed a qualified risk officer who is responsible to monitor, assess and manage the risks associated with the business and operations of the respective subsidiaries. The RMD of the respective subsidiaries are tabled at the GRMC and where relevant subsequently tabled at BHB's BRC.

The BRC or the AEC (as the case may be) of the key operating subsidiaries will escalate and update their respective Board on any new regulatory or statutory requirement that could impact the internal control and the risk management principles, policies, procedures and practices of the Companies and its subsidiaries.

STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

- **Risk Appetite**

The BRC, through the Group's key operating subsidiaries establish the risk appetite and risk tolerance for the relevant entities. The defined risk appetite and risk tolerance are periodically reviewed by the respective Management and the respective Board in line with the Group's business strategies and operating environment. Such review includes identifying and setting new risk appetite metrics for business entity or removal of risk appetite metrics that are no longer applicable as well as updates on the risk appetite thresholds to be in line with the Group's business strategy and risk posture. The main risk inherent to the business and operations that were considered in the risk appetite review include regulatory compliance risk, credit risk, market and liquidity.

- **Audit and Examination Committee ("AEC")**

The AEC of BHB reviews the adequacy of internal controls within the company based on the assessment performed by the internal auditors. Similarly the AEC of the key operating subsidiaries reviews relevant matters pertaining to its internal accounting controls on quarterly basis. In addition, the AEC of BHB and its key operating subsidiaries also review and assess the adequacy of the scope and effectiveness of the internal and external audit functions. For the external auditors, the AEC assess their independence and the quality of their resources.

All significant findings by the internal auditors, external auditors and regulators are reported to the AEC for review and deliberation. The AEC reviews and ascertains that mitigation plans are implemented by Management to safeguard the interests of the Group and upkeep proper governance. The risk responses and internal controls that the Management has initiated are documented and recorded in the AEC meeting minutes.

Pursuant to Paragraph 15.17(f) of the Listing Requirements of Bursa Malaysia Securities Berhad, two (2) separate meetings with the external auditors were conducted with the AEC of BHB without the presence of any Management of the Company, to discuss on any issues relating to BHB Group during the financial year ended 31 December 2017.

- **Board Risk Committee ("BRC")**

The Group BRC is kept informed by its subsidiaries on their risk management policy statement and framework including the strategies, policies, the risk tolerance levels, governance and reporting structure.

At the key operating subsidiaries level, reviews and assessments were carried out on the adequacy of the risk management policies and framework in identifying, measuring, monitoring and controlling risks and the extent to which these risks are effectively managed. In addition, they would also review the adequacy of relevant policies at the subsidiaries in meeting the relevant regulatory requirements including capital plan, dividend policy, investment and financing policy, single customer limit, business continuity plan, etc.

- **Group Risk Management Committee ("GRMC")**

The GRMC has been established to identify and review the key risk areas of BHB Group. It ensures that an appropriate risk management system and internal controls are in place and functioning effectively. The GRMC is also responsible for assessing the adequacy of infrastructure, resources and systems for effective risk management, and where necessary to embark on the Group's initiative to share facilities, mobilise resources, etc. In addition, the GRMC reviews the subsidiaries risk management periodic reports presented by the key operating subsidiaries on risk exposure, risk portfolio composition and risk management activities six (6) times a year.

The GRMC is chaired by the Group Chief Strategy Officer and the members consist of the Group Chief Financial Officer of BHB together with the Risk Officer of the key operating subsidiaries.

- **Internal Audit**

The internal audit function of BHB and its subsidiaries (save for Takaful Malaysia) is carried out by the Internal Audit Division of Bank Islam. For Takaful Malaysia, the internal audit function is carried out by its own independent internal audit department.

The Internal Audit assesses compliance with policies and procedures and the effectiveness of the Group's internal control systems. The Internal Audit undertakes regular reviews of BHB and its subsidiaries' operations and business processes. It examines and evaluates the adequacy and efficiency of financial and operating controls and highlights significant risks and non-compliance. Where applicable, the Internal Audit will provide recommendations to improve the management of risks, control and governance processes. The AEC regularly reviews the status of rectification actions on the findings or recommendations by the internal auditors. Further details on the internal audit activities are provided in BHB's AEC report.

Internal audit is performed on all key divisions in BHB Group, providing the respective AEC with an independent assurance on the operational, financial, compliance and risk related activities within the Group. The risk-based internal audit plan is approved by the AEC of the key operating subsidiaries on annual basis. All internal audit observations are highlighted in the internal audit reports and reviewed by the AEC.

- **Shariah Advisory**

It is a fundamental requirement of an Islamic financial institution that its entire business practices and operations are based on Shariah rules and principles. Islamic finance derives its value proposition from the application of Shariah contracts in financial transactions that provide for different risks and return profiles. Adherence to Shariah principles under such distinct contracts preserves the validity and sanctity of any Islamic financial transactions. BHB is committed to upholding these principles via strict observance of the Shariah Governance Framework outlined by Bank Negara Malaysia ("**BNM**").

The Shariah advisory function of BHB and its subsidiaries (save for Takaful Malaysia and BIMB Securities) is carried out by the Shariah Supervisory Council ("**SSC**") of Bank Islam. For Takaful Malaysia and BIMB Securities, the Shariah advisory function is carried out by its own independent Shariah committee.

One of the key responsibilities of the SSC/Shariah committees is to advise its respective Board on Shariah matters in relation to business operations, compliance with Shariah principles at all times, auditing the operational aspect of BHB and endorsing the zakat computation and distribution.

OTHER KEY ELEMENTS OF INTERNAL CONTROL

The other key elements of the internal control systems are described below:

- **Board Meetings**

At a minimum, the Board meets six (6) times a year and has a formal agenda on matters for discussion. The CEO leads the presentation of board papers and provides explanation on pertinent issues. A thorough deliberation and discussion by the Board is a prerequisite before arriving at any decision. In addition, the Board is kept updated on the Group's activities and operations on a timely and regular basis.

- **Group Organisation Structure**

The Board has established an organisation structure with clearly defined lines of responsibilities, authority limits, and accountability aligned to business and operations requirements which support the maintenance of a strong control environment.

STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

- **Limit of Authority Matrix**

The Group has clearly defined lines of authorities to facilitate prompt responses in the continuously evolving business environment, effective supervision of day-to-day business conducts and accountability. The establishment of Limit of Authority (“**LoA**”) matrix clearly outlines the Board and Management’s limits and approval authorities across various key processes. The LoA is duly approved by the Board and subject to regular review and enhancement to ensure it reflects changes in accountability and risk appetite of the Group.

- **Standard Operating Procedures**

Documented Standard Operating Procedures (“**SOPs**”) for all departments of BHB and its subsidiaries were approved by the respective Management. The SOPs serves as a day-to-day operational guide to ensure compliance with financial and operational controls as well as the applicable laws and regulations. All SOPs are reviewed and updated regularly to reflect current risks, new regulatory requirements and current operations.

- **Human Resources Policies and Procedures**

The Human Resources policies and procedures of BHB and its subsidiaries encompasses areas of human resources management such as the recruitment of new employees based on “fit and proper” criteria, performance appraisals, training and development.

- **Annual Business Plan and Budgeting Process**

The Group’s budget is prepared based on the annual business plans of BHB’s key operating subsidiaries. The budget and business plan are approved by the respective Board and subsequently endorsed by BHB’s Board. Actual performances of the subsidiaries are reviewed against the targeted results on a quarterly basis allowing for timely response and corrective actions to be taken to ensure the business targets are met.

The subsidiaries’ performances are assessed against the budget, business plans and relevant key financial indicators.

- **Information Technology (“IT”) System**

IT is key in supporting the service efficiency and delivery systems of the Group. The IT Risk Framework was developed to ensure that risks are correctly identified and mitigated accordingly. Bank Islam and Takaful Malaysia have developed their IT policies to address issues of security and risk related to IT. The subsidiaries continue to upgrade their IT systems to enhance efficiency of their business operations and services.

- **Performance Review**

The Board receives and reviews reports from the Management on the Group’s financial and operational performance, risk management as well as legal and regulatory matters on a quarterly basis. The financial performance presented highlights the key financial indicators of which include amongst others the ratio on profitability, capital adequacy and asset quality.

The actual performance of BHB and its key operating subsidiaries are assessed against approved budgets and business plans, key financial indicators as well as industry’s benchmark. The assessment enables the Management to identify any significant deviations and gaps for remedial measures to be implemented where necessary.

- **Whistle Blowing Policy**

There is an established process for reporting anyone suspected found to be abusing or circumventing processes and controls. All staff are accorded the opportunity to report via the whistle-blowing mechanism with the assurance that the report will be dealt with confidentially and that the reporter’s identity will be protected.

REVIEW OF THE STATEMENT BY EXTERNAL AUDITORS

The external auditors have reviewed this Statement on Risk Management and Internal Control pursuant to the scope set out in the Audit and Assurance Practice Guide 3 (“**AAPG 3**”) (Revised 2018), Guidance for Auditors on Engagements to Report on the Statement on Risk Management and Internal Control included in the Annual Report issued by the Malaysian Institute of Accountants (“**MIA**”) for inclusion in the Annual Report of the Group for the financial year ended 31 December 2017.

Based on the review conducted, the external auditors have reported to the Board that nothing has come to their attention that cause them to believe that this statement intended to be included in the Integrated Annual Report of the Group, in all material respect:

- (a) has not been prepared in accordance with the disclosures required by paragraphs 41 and 42 of the Statement on Risk Management and Internal Control: Guidelines for Directors of Listed Issuers, or
- (b) is factually inaccurate.

AAPG 3 (Revised 2018) does not require the external auditors to consider whether the Directors’ Statement on Risk Management and Internal Control covers all risks and controls, or to form an opinion on the adequacy and effectiveness of the Group’s risk management and internal control system including the assessment and opinion by the Board of Directors and Management thereon. The auditors are also not required to consider whether the processes described to deal with material internal control aspects of any significant problems disclosed in the Annual Report will, in fact, remedy the problems.

This statement is made in accordance with the resolution of the Board dated 28 March 2018.