

Statement on Risk Management and Internal Control

INTRODUCTION

Pursuant to Paragraph 15.26(b) of the Main Market Listing Requirements (“**MMLR**”) of Bursa Malaysia Securities Berhad (“**Bursa Malaysia**”), a listed issuer must ensure that its Board of Directors (“**Board**”) includes in its annual report a statement about the state of its risk management and internal controls as a group. In addition, the Malaysian Code on Corporate Governance also stipulates that the Board should maintain a sound system of internal controls, including a review of its effectiveness to safeguard Shareholders’ investments and the Group’s assets.

Set out below is the Board’s Statement on Risk Management and Internal Control in compliance with the MMLR of Bursa Malaysia.

BOARD RESPONSIBILITY

The Board is committed to maintaining a sound system of internal controls and has instituted a risk management framework, as well as good corporate governance measures to monitor the Group’s effectiveness in safeguarding Shareholders’ investments and the Group’s assets.

The Board is responsible for determining key strategies and policies for significant risks and control issues, whereas functional management is responsible for the effective implementation of the Board’s policies by way of identifying, monitoring and managing risks. However, as any system of internal controls will have its inherent limitations, the system has been designed to manage risks rather than provide absolute assurance against material misstatement, fraud or loss.

The Board has also received reasonable assurance from the Group Managing Director and Group Chief Financial and Operations Officer that the Group’s risk management and internal control system is operating adequately and effectively, in all material aspects.

RISK MANAGEMENT AND INTERNAL CONTROL SYSTEM

The Board and Management of the Group are committed to the implementation of an internal control system to manage those risks that could affect the Group’s continued growth and financial viability.

Measures are taken to continuously evaluate changes in the risk profile of the Group and business complexities to assist the Board and Management to anticipate and manage all potential risks and protect Shareholders’ value.

The key elements of the Group’s internal control system include the following:

Risk Management Framework

The risk governance structure in the Enterprise Risk Management Framework defines the roles and responsibilities throughout the organisation to ensure accountability and ownership. It sets out the principles of sound corporate governance to assess and manage risks to ensure that risk-taking activities are aligned with the Group’s capacity to absorb losses and its long-term viability.

The risk management philosophy adopted by the Group is based on the three (3) lines of defence approach. The line management is the first line of defence and is primarily responsible for the day-to-day risk management by identifying the risks, assessing impact and taking appropriate actions to manage and mitigate risks.

The second line of defence is the oversight functions comprising Group Risk Management and Group Regulatory & Corporate Services (“**Group Regulatory**”). They perform independent monitoring of business units, reporting to Management and Board to ensure that the Group is conducting business and operations within internal guidelines and is regulatory compliant.

The third line of defence is Group Internal Audit (“**GIA**”) which provides independent assurance to the Board on the adequacy and effectiveness of system of internal controls, risk management and governance processes.

Governance

The Board, through its appointed committees such as the Group Board Risk Committee (“**GBRC**”) and Group Board Digital Innovation & Technology Committee (“**GBDITC**”), ensures that the Group’s activities are consistent with its approved risk appetite, strategies and policies.

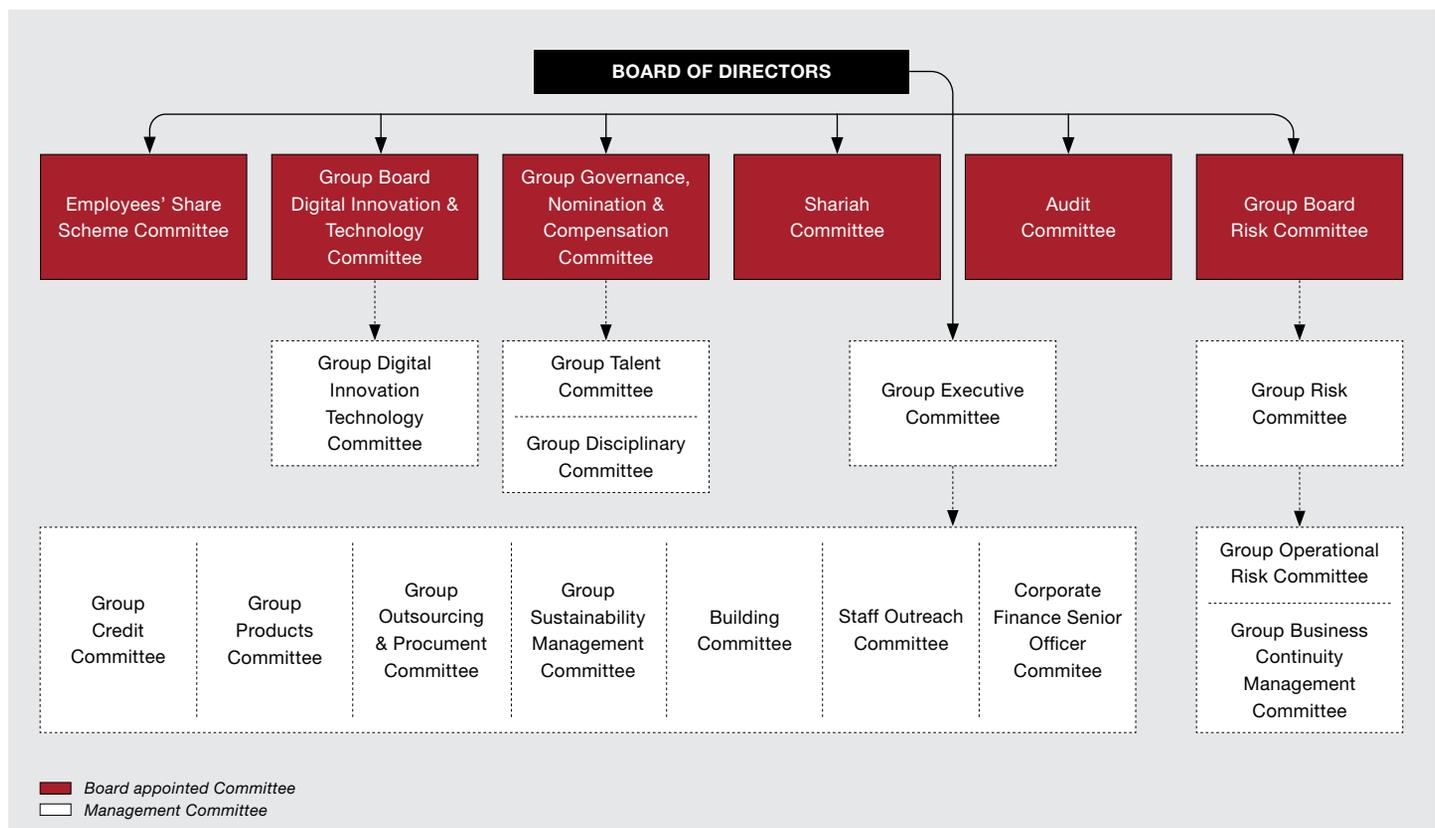
The GBRC is supported by the Group Risk Committee (“**GRC**”) that provides a forum to address and review the management of credit, operational, market, liquidity, technology and other significant risks to enable effective oversight, accountability and responsibilities for risk-taking decisions. Assisting the GRC is the Group Operational Risk Committee and the Group Business Continuity Management Committee.

The GBDITC focuses on technologies and IT risk of the Group at the Board level and is supported by the Group Digital Innovation Technology Committee (formerly known as Group Information Technology Steering Committee) which covers the Group’s technology plans and projects.

Quarterly meetings are held by the Audit Committee (“**AC**”) together with Management to review issues highlighted in the reports by internal and external auditors, as well as audits conducted by

regulators such as Bank Negara Malaysia (“**BNM**”), the Securities Commission Malaysia (“**SC**”) and Bursa Malaysia, in particular the actions taken to address issues. If required, the internal auditors will also assist the AC to periodically review the measures taken to address the AC’s concerns on any internal control system.

The Group Governance, Nomination & Compensation Committee (“**GNC**”) was established with the objective, amongst others, to support the Board in the effectiveness and the enhancement of the Group’s governance structure, framework and policies and its compliance with the applicable statutory and regulatory requirements in relation thereof, including but not limited to, the MMLR of Bursa Malaysia, BNM’s Policy Document on Corporate Governance, the Malaysian Code on Corporate Governance and the Malaysian Anti-Corruption Commission Act 2009, as well as the relevant latest developments in the corporate governance area.



Management Committees (“**MC**”) are established to oversee specific responsibilities based on defined terms of references. MC meetings are held regularly to ensure that business operations are executed in accordance with approved strategies, policies and business directions. The MCs are responsible for, amongst others:

- reviewing the actual performance against expectations and budget;
- addressing any internal control issues with the AC, GBRC, GBDITC, GNC, GIA, regulators and the external auditors; and
- addressing any matters arising from the meetings of the Board, AC, GBRC, GBDITC and GNC; and ensuring that actions are taken in relation to these matters.

Risk Management Process and Infrastructure

The risk management process is a combination of both bottom-up and top-down approaches to facilitate decision-making based on available information known at the time and creating opportunities to refine inputs when new information is available.

In addition to establishment of risk policies, tools and methodologies to identify, quantify and manage the risks, Group Risk Management is also responsible for establishing the risk measurement and monitoring process to ensure that the Group's risk profile and portfolio concentration are reported to the various risk committees on a regular basis.

Internal Policies and Procedures

Policies and procedures which set out standard day-to-day operations and managing risks are formulated based on current regulatory requirements and industry best practices.

The adequacy and compliance with regulatory requirements of the policies and procedures are assessed by independent control functions such as risk management, compliance and audit, prior to obtaining approval from the Board or relevant management committee.

Existing policies and procedures are reviewed regularly to ensure improvements and in consideration of emerging or changing risks profile, new products or services as well as new or updated regulatory requirements.

Annual Business Plans and Budgets

The Board reviews and approves the business plans and budgets which are developed in line with the Group's strategies and risk appetite. Actual performances against the approved budgets are escalated to Management and Board on a monthly basis allowing responses and corrective actions to be taken.

Human Capital Management

The organisational structure, which is aligned to business and operational requirements are led by Heads of Departments with accountability in place.

Human Resources' policies and procedures are reviewed regularly to ensure they remain relevant to manage operational and people-related risks.

There are regular trainings and updates for employees on requirements/guidelines of BNM, Bursa Malaysia and the SC, as well as on the importance of corporate governance, risk management and internal control. Various awareness programmes on operational risks, ethics and fraud are also conducted regularly.

Business Continuity Management

Business Continuity Plans and Disaster Recovery Plans are established to ensure non-disruption of business or efficient business resumption. Regular testing or drills are also conducted for the purpose of staff preparedness, readiness of disaster recovery site, effectiveness of communication, escalation and recovery procedures. For effective business continuity management ("BCM"), awareness training is held annually for BCM coordinators and key persons.

Information Technology Security

The use of information technology ("IT") is essential and central to the Group's business. In order to ensure the reliability and resiliency of the business operations to meet the expectations of customers and all stakeholders, and in line with the guidelines of regulators such as BNM's Policy Document on Risk Management in Technology, the Group has established the corporate Cyber Security Policy and implemented the necessary security procedures to protect the confidentiality, integrity and availability of information systems and data.

With the increase in adoption of digitalisation and service delivery via cyberspace, the Group will continue to reinforce its IT security efforts and initiatives to be aligned with the Group's current and envisaged operations, strategies and business environments. The IT security posture of the Group is also continuously reviewed and enhanced to mitigate the risks arising from new and emerging threats. In-house IT security training and security updates on the latest threats are constantly provided to all staff to ensure their awareness on the importance of IT security.

Compliance Function

The Board is unreservedly committed and always strives to adopt the principles and recommendations of the Malaysian Code on Corporate Governance issued by the SC, as well as, other relevant regulatory requirements relating to corporate governance.

Compliance reviews and monitoring are undertaken by Group Regulatory using various tools and approaches based on the framework set by Group Compliance, a department of Group Regulatory. These reviews and monitoring are performed to assess the level of compliance with the relevant regulatory requirements and the respective companies' internal policies and procedures. Any regulatory deviation or compliance breaches will be reported to the respective Boards of operating entities within the Group and the relevant regulators. Pursuant to this, appropriate corrective actions including disciplinary actions will be taken to address the breach with a view to pre-empt and prevent the occurrence of a similar breach.

Aside from Group Compliance, the five (5) other departments of Group Regulatory undertake functions to review and monitor compliance in their respective areas. In this respect, the Group Financial Crime Intelligence, Group Prudential Supervision and Regulatory Affairs, Group Business Ethics and Integrity, Group Legal and Group Company Secretarial provide timely, structured and comprehensive advice and support to the Group in matters relating to the laws, rules and regulations applicable to the Group.

Group Regulatory has also implemented self-assessment framework to facilitate and promote regulatory compliance by the business within the Group. For this purpose, a list of identified laws, regulations and other regulatory instruments applicable to the Group are documented and maintained to facilitate compliance.

Please refer to the 'Ethics and Compliance Statement' for more details on functions, roles and responsibilities of Group Regulatory.

Internal Audit

GIA provides independent and objective assurance to the Board that the established internal controls, risk management and governance processes are adequate and are operating effectively and efficiently. To ensure independence and objectivity, GIA reports independently to the AC of KIBB and has no responsibilities or authority over any of the activities it reviews. GIA's scope of work and activities are guided by the Internal Audit Charter, mandatory elements of The Institute of Internal Auditors' ("IIA")'s International Professional Practices Framework ("IPPF") and relevant regulatory guidelines. In 2021, an external Quality Assessment Review was conducted on GIA to assess its conformity with the IIA's IPPF, of which GIA has been accorded the rating of "Generally Conforms", i.e. GIA has fulfilled its key objectives in accordance with the IPPF.

An Annual Audit Plan based on the appropriate risk-based methodology has been developed and approved by the AC. On a quarterly basis, audit reports and status of internal audit activities including the sufficiency of GIA resources are presented to the AC for review.

Periodic follow up reviews are conducted to ensure adequate and timely implementation of Management's action plans.

Associate and Joint Venture Companies

The Board does not regularly review the internal control systems of associate companies and joint venture companies as the Board does not have any direct control over their operations. Notwithstanding this, the Group's interests are served through representation on the boards of the respective companies via receipt and review of management accounts, periodical reports as well as deliberation on proposals related to these companies. Such representation also

provides the Board with information for decision-making on the continuity of the Group's investments based on the performance of these associate companies and joint venture company.

CONCLUSION

The Board, through the AC and GBRC, confirms that it has reviewed and considered the effectiveness of the Group's risk management and internal control system as adequate during the financial year and has taken into consideration any material developments up to the date of approval of the Annual Report and Audited Financial Statements for the Financial Year Ended 31 December 2021. The main financial risk areas faced by the Group and the guidelines and policies adopted to manage them are provided in detail under Note 50 of the Audited Financial Statements of the Company for the Financial Year Ended 31 December 2021.

The Board is satisfied that there is an effective on-going process for identification, evaluation and management of risks and there are regular reviews to ensure controls are efficient and effective.

REVIEW OF THE STATEMENT BY EXTERNAL AUDITORS

As required by Paragraph 15.23 of the MMLR of Bursa Malaysia, the external auditors have reviewed this Statement on Risk Management and Internal Control. Their review was performed in accordance with the Audit and Assurance Practice Guides ("AAPG") 3, 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. Based on the review, the external auditors have reported to the Board that nothing has come to their attention that causes them to believe that this Statement is inconsistent with their understanding of the process that the Board has adopted in the review of the adequacy and integrity of the internal controls of the Group. AAPG 3 does not require the external auditors to, and they did not, consider whether this Statement covers all risks and controls, or to form an opinion on the effectiveness of the Group's risk and control procedures.

This Statement on Risk Management and Internal Control is made in accordance with the resolution of the Board dated 3 March 2022.