Statement on Risk Management and Internal Control

INTRODUCTION

The Board affirms its overall responsibility for the Group's system of internal control and risk management and for reviewing the adequacy and effectiveness of the system. The Board is pleased to share the main features of the Group's risk management and internal control system in respect of the financial year ended 31 December 2016.

In discharging its stewardship responsibilities, the Group has established a sound risk management framework and procedures of internal control. These procedures, which are embedded into the culture, processes and structures of the Group are subject to regular review by the Board, provide an ongoing process for identifying, evaluating and managing the significant risks faced by the Group that may affect the achievement of its business objectives and strategies. The Group's risk management framework and internal control procedures, in all material aspects, are consistent with the guidance provided to Directors as set out in the "Statement on Risk Management and Internal Control: Guidelines for Directors of Listed Issuers".

BOARD RESPONSIBILITY

The Board of Maxis, in discharging its responsibilities, is fully committed to articulating, implementing and reviewing a sound risk management and internal control environment. The Board is responsible for determining the Group's level of risk tolerance and in conjunction with Management, to actively identify, assess and monitor key business risks in order to safeguard shareholders' investments and the Group's assets.

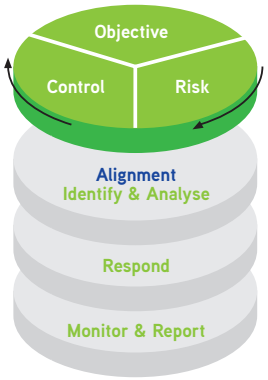
The risk management and internal control systems are designed to identify, assess and manage risks that may impede the achievement of the Group's business objectives and strategies rather than to eliminate these risks. They can only provide reasonable and not absolute assurance against fraud, material misstatement or loss, and this is achieved through a combination of preventive, detective and corrective measures.

RISK MANAGEMENT

The Board regards risk management as an integral part of the Group's business operations and has oversight over this critical area through the Audit Committee. The Audit Committee, supported by the Internal Audit department, provides an independent assessment of the effectiveness of the Maxis Enterprise Risk Management ("ERM") framework and reports to the Board on a yearly basis.

The Maxis ERM framework is consistent with the ERM framework of the Committee of Sponsoring Organisations ("COSO") and involves systematically identifying, analysing, measuring, monitoring and reporting on the risks that may affect the achievement of its business objectives. This framework helps to reduce the uncertainties surrounding the Group's internal and external environment, thus allowing it to maximise opportunities and minimise adverse incidences that may arise. The major risks which the Group is exposed to are strategic, operational, regulatory, financial, market, technological, products and reputational risks.

Maxis' Enterprise Risk Management Framework



The ERM process is based on the following principles:

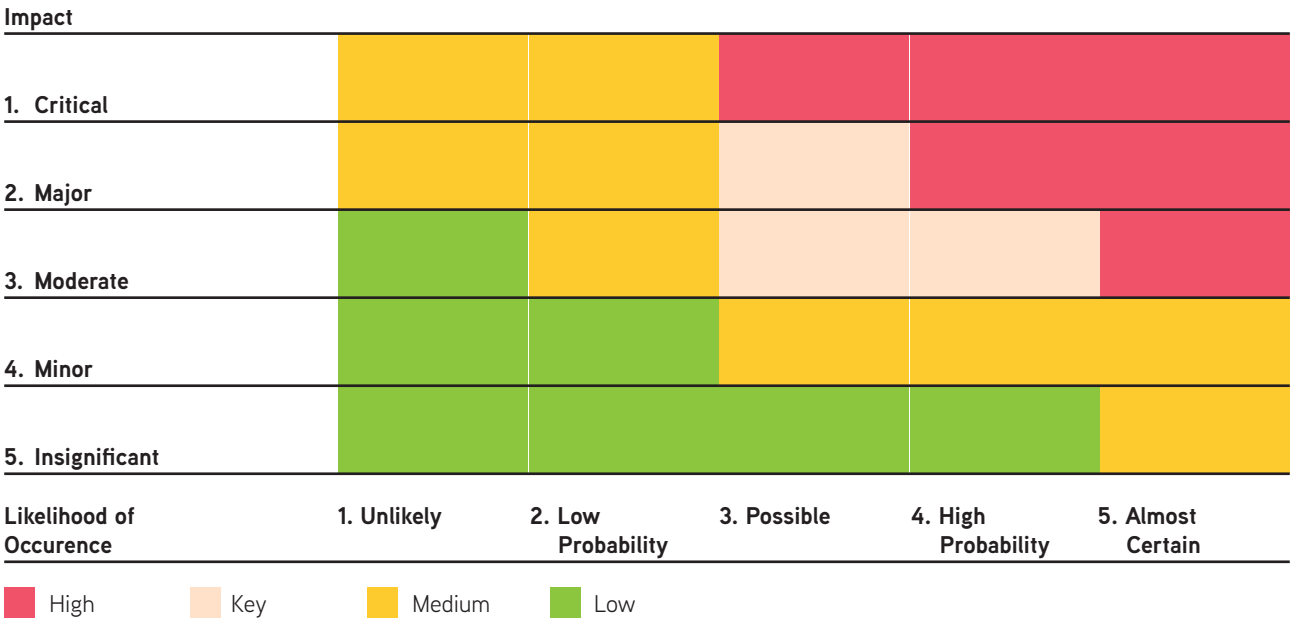
- Consider and manage risks enterprise-wide;
- Integrate risk management into business activities;
- Manage risk in accordance with the ERM framework;
- Tailor responses to business circumstances;
- Regularly assess status of risks and risk responses; and
- Monitor and report compliance with the ERM framework.

There is an ERM department that administers the ERM process to ensure risks that may affect the achievement of Maxis' business objectives are identified, evaluated and managed. A structured process has been established where on a regular basis, ERM discussions are held between units within department/ section to identify potential risks that might affect the department/section from achieving its business objectives. ERM department participates in such discussions on a quarterly basis. Identified risks are then reported, reviewed and discussed with respective Maxis Management Team ("MMT") and Audit Committee on a quarterly basis to ensure key risks are identified, analysed, monitored and mitigating actions are co-ordinated and implemented on a timely manner.

Statement on Risk Management and Internal Control

All identified risks are displayed on a 5 by 5 risk matrix based on their risk ranking to assist Management in prioritising their efforts and appropriately managing the different classes of risks.

Risk Rating Scale – 5 by 5 Matrix



The Board and Management drive a proactive risk management culture and regular risk awareness and coaching sessions are held to ensure that the Group's employees have a good understanding and application of risk management principles.

The ERM department also works closely with the Group's operational managers to continuously strengthen the risk management initiatives within the Group so that it responds effectively to the constantly changing business environment and thus is able to protect and enhance shareholder value.

CONTROL ENVIRONMENT AND STRUCTURE

The Board and Management have established numerous processes for identifying, evaluating and managing the significant risks faced by the Group. These include periodic testing of the effectiveness and efficiency of the internal control procedures and updating the system of internal controls when there are changes to the business environment or regulatory guidelines. These processes have been in place for the financial year ended 31 December 2016 and up to the date of approval of this Statement on Risk Management and Internal Control for inclusion in the Annual Report.

The key elements of the Group's control environment include:

1. **Organisation Structure**
   The business of the Group is overseen by the Board which provides direction and oversight to the Group and Chief Executive Officer (CEO) who is supported by Management. The Board is supported by a number of established Board committees, namely the Audit, Nomination, Remuneration and Employee Share Option Scheme/Long-Term Incentive Plan Committee, and ad-hoc operational and governance committees formed from time to time, all of which facilitate the Board in the discharge of its duties. Each Committee has clearly defined terms of reference and responsibilities, and activities of each Committee are reported back to the Board for information or decision where relevant (please refer to the Statement of Corporate Governance for further details).

Statement on Risk Management and Internal Control

Responsibility for implementing the Group's strategies, operations and day-to-day business, including implementing the system of risk management and internal control, is delegated to the CEO who is supported by Management. The organisation structure sets out a clear segregation of roles and responsibilities, lines of accountability and limits of authority to ensure effective and independent stewardship.

2. Audit Committee

The Audit Committee comprises five (5) non-executive members of the Board, the majority of whom are Independent Directors. The Audit Committee comprises members who bring with them a wealth of knowledge, expertise and experience from different industries and backgrounds such as telecommunications and media, finance and treasury, human resources and general management. The Audit Committee reviews the Group's financial reporting process, the system of internal controls and management of enterprise risk, the audit process and the Group's process for monitoring compliance with laws and regulations and its own code of business conduct, as well as such other matters, which may be specifically delegated to the Committee by the Board, from time to time. Throughout the financial year, Audit Committee members are briefed on corporate governance practices, updates to Malaysian Financial Reporting Standards, as well as legal and regulatory requirements and updates in addition to key matters affecting the financial statements of the Group.

The Audit Committee also reviews and reports to the Board about the engagement and independence of the external auditors and their audit plan, nature, approach, scope and other examinations of the external audit matters. It also reviews the effectiveness of the internal audit function which is further described in the following section on Internal Audit.

The Audit Committee continues to meet regularly and has full and unimpeded access to the internal and external auditors and all employees of the Group. The Chairman of the Audit Committee provides the Board with reports on all meetings of the Audit Committee. Further details of the activities undertaken by the Audit Committee are set out in the Audit Committee Report on pages 68 to 71.

3. Internal Audit

The Internal Audit department continues to independently, objectively and regularly review key processes, check compliance with policies/procedures, evaluate the adequacy and effectiveness of internal control, risk management and governance processes established by Management and/or the Board within the Group. It highlights significant findings and corrective measures in respect of any non-compliance to members of the MMT and Audit Committee on a timely basis. Its work practices are governed by the Internal Audit Charter, which is subject to revision on an annual basis. The annual audit plan, established primarily on a risk-based approach, is reviewed and approved by the Audit Committee annually and an update is given to the Audit Committee every quarter. The Audit Committee oversees the Internal Audit department's function, its independence, scope of work and resources. The Internal Audit department also maintains a quality assurance and improvement programme and continuously monitors its overall effectiveness through internal self-assessments.

The Internal Audit function follows the requirements of the latest International Standards for the Professional Practice of Internal Auditing of the Institute of Internal Auditors Inc. Further activities of the Internal Audit function are set out in the Audit Committee Report on pages 68 to 71.

4. Code of Business Practice

The Group is committed to conducting business fairly, impartially and ethically and in full compliance with all laws and regulations. The Maxis Code of Business Practices ("the Code") stipulates how Directors and employees as well as external parties such as vendors, dealers and business partners should conduct themselves in all business matters. All Directors and employees are required to declare they are in compliance with the Code upon joining the Group. The Directors are required to acknowledge the Code when there are significant changes made to it. Communications are made to all employees on the content of the Code throughout the year to ensure they understand what is expected of them. External parties such as vendors, dealers and business partners who conduct business with the Group are required to sign a declaration that they have read and will adhere to the Code.

To effectively implement the Code, there is an established Office of Business Practice to provide policy guidance and to facilitate compliance. The Office of Business Practice will continuously look at ways to enhance the Group's highest standards of business conduct and ethics, and to benchmark these against best practices. There is also an Ethics Hotline, which serves as a safe and effective channel for employees or parties dealing with us to report any incidence or occurrence which are not in accordance with the Code.

Statement on Risk Management and Internal Control

5. **Revenue Assurance**
The Revenue Assurance team is responsible for the continuous monitoring of potential revenue leakage that may arise from day-to-day operations. This includes performance and examination of regular test calls, reconciliations of chargeable transactions from network and IT systems to the billing systems and independent rating of key services via automated tools. Processes and controls within the revenue cycle are also reviewed regularly to ensure they function effectively and efficiently. Key issues and mitigation actions are reported to the Management monthly and reported to the Audit Committee on a half-yearly basis. The Revenue Assurance department meets key stakeholders on an ongoing basis to address key revenue assurance issues and drive revenue assurance initiatives across the Group.

6. **Subscriber Fraud Management**
The Subscriber Fraud Management ("SFM") function complements the Revenue Assurance function. While the Revenue Assurance function monitors and reviews controls within the revenue cycle as indicated above, the SFM function monitors daily subscriber calls on a near real-time basis. Appropriate actions are taken immediately for suspected fraudulent calls, using an industry developed system to monitor call patterns on a 24/7 basis throughout the financial year and other manual reporting investigations. It also reviews key new services and products for possible fraud risk and recommends counter-measures. Fraud findings with remedial actions taken are reported to the Management on a monthly basis and presented half-yearly to the Audit Committee.

7. **Business Continuity Planning**
The Business Continuity Planning ("BCP") team is responsible for identifying activities and operations that are critical to sustain business operations in the event of a disaster. These include facilitating the building of additional redundancies in network infrastructure, establishing alternate sites where key operational activities can be resumed and mitigating the risk of high-impact loss events through appropriate insurance coverage. A risk-based approach is applied in identifying the key initiatives and their levels of importance by reviewing critical systems and single-point of failures as well as their impact on the business of the Group as a whole. During the financial year, selected critical areas as identified by risk priority were tested to assess the effectiveness of the implemented BCP initiatives. These tests were successfully executed and the progress of these initiatives was presented half-yearly to the Audit Committee. Since January 2014, Maxis is also certified under ISO 22301, the international certification standard for Business Continuity Management systems.

8. **Regulatory**
The Regulatory function ensures compliance with the Communications and Multimedia Act 1998 ("CMA"), and its applicable rules and regulations, which governs the Group's core business in the communications and multimedia sector in Malaysia. As a licensee under the CMA, the Group adheres to its licensing conditions, as well as economic, technical, social and consumer protection regulations embedded in the CMA and its subsidiary legislation. The Group actively participates in new regulatory and industry development consultations initiated by the regulator, MCMC.

The Regulatory function also frequently engages the Malaysian Communications and Multimedia Commission and the Ministry of Communications and Multimedia Malaysia in discussions on pertinent industry issues.

9. **Legal**
The Legal department plays a pivotal role in ensuring that the interests of the Group are preserved and safeguarded from a legal perspective. It ensures that the Group's operations and transactions with third parties are in compliance with all laws. It also plays a key role in advising the Board and Management on legal and strategic matters. The Board is also briefed through reports to the Audit Committee on material litigation and any changes in law that would affect the Group's operations.

10. **Company Secretary**
Please refer to Statement on Corporate Governance on pages 54 to 67 of this Annual Report.

11. **Limits of Authority**
A Limits of Authority ("LOA") manual sets out the authorisation limits for various levels of Maxis' Management and staff and also those matters requiring Board approval to ensure accountability, segregation of duties and control over the Group's financial commitments. The LOA manual is reviewed and updated periodically to align with business, operational and structural changes.

12. **Policies and Procedures**
There is extensive documentation of policies, procedures, guidelines and service level agreements on the Group's intranet site including those relating to finance, contract management, marketing, sourcing, human resources, information systems, network operations, legal, system and information security controls. Continuous control enhancements are made to cater for business environment changes and to align with Maxis' new and growing business strategy.

Statement on Risk Management and Internal Control

13. **Financial and Operational Information**
Budgets are prepared by the operating units and presented to the Board before the commencement of a new financial year. Upon approval of the budget, the Group's performance is tracked and measured against the budget on a monthly basis. Reporting systems which highlight significant variances against budget are in place to track and monitor performance. The variances in financial as well as operational performance indices are incorporated in monthly management reports. On a quarterly basis, actual results for the quarter and rolling forecast are reviewed by the Board to enable the Directors to evaluate the Group's performance compared to the budget and prior periods.

14. **Systems and Information Security**
The Systems and Information Security unit has an assurance function and is responsible for continuously monitoring and resolving security threats to the Group both internally and externally. This includes conducting security awareness, vulnerability assessment and penetration test programmes, and compliance audits on the IT systems and networks of Maxis to reduce the impact of service interruption due to malicious activities, cyber-attacks, negligence and malware. The effectiveness of the security programme is validated by auditors and external security consulting companies.

    Apart from the internal security compliance programmes, the unit is also required to maintain and assist in the compliance of the following regulatory and industry security programmes, namely: MS/ISO27001:2013, Payment Card Industry/Data Security Standard, and the Personal Data Protection Act 2010.

    The unit is governed by Security Governance team made up of members of MMT who meet periodically to direct and approve the corporate security policies and standards set by the unit and security projects undertaken by the unit. It is also responsible for updating the Audit Committee at least annually on the Group's security status.

MONITORING AND REVIEW

The processes that monitor and review the effectiveness of the system of risk management and internal controls include:

1. **Management Representations made to the Board** by the CEO and Chief Financial and Strategy Officer ("CFSO"), based on representations made to them by Management on the adequacy and effectiveness of the Group's risk management and internal control system in their respective areas. Any material exceptions identified are highlighted to the Board.

2. **Internal Audit** in their quarterly report to the Audit Committee and members of MMT continues to highlight significant issues and exceptions identified during the course of their review on processes and controls compliance.

3. **The Defalcation Committee** meets and deals regularly on matters pertaining to fraud and unethical practices. All issues arising from work carried out by the investigation team within the Internal Audit department and Management are channelled to this committee for deliberation. Appropriate actions are then taken based on the findings.

4. **Enterprise Risk Management department** reports to the Board on a quarterly basis through the Audit Committee on the risk profile of the Group and the progress of action plans to manage and mitigate the risks.

    Management has taken the necessary actions to remediate weaknesses identified for the period under review. The Board and Management will continue to monitor the effectiveness and take measures to strengthen the risk management and internal control environment.

CONCLUSION

For the financial year under review and up to the date of issuance of the financial statements, the Board is satisfied with the adequacy and effectiveness of the Group's system of risk management and internal control to safeguard the interest of shareholders. No material losses, contingencies or uncertainties have arisen from any inadequacy or failure of the Group's system of internal control that would require separate disclosure in the Group's Annual Report. The CEO and CFSO have provided assurance to the Board that the Group's risk management and internal control system, in all material aspects, is operating adequately and effectively.

REVIEW OF THE STATEMENT BY EXTERNAL AUDITORS

As required by paragraph 15.23 of the Bursa Malaysia Securities Berhad Main Market Listing Requirement, the external auditors have reviewed this Statement on Risk Management and Internal Control. Their limited assurance review was performed in accordance with Recommended Practice Guide ("RPG") 5 (Revised 2015): 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. RPG 5 (Revised 2015) does not require the external auditors to form an opinion on the adequacy and effectiveness of the risk management and internal control systems of the Group.