STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

The Board of Directors ("Board") acknowledges its overall responsibility for maintaining a sound system of risk management and internal control ("RMIC") and for reviewing its adequacy and effectiveness in safeguarding the interests of stakeholders (including shareholders' investments) and the Group's assets. The Board is pleased to present the Statement on Risk Management and Internal Control ("Statement") of the Group covering key subsidiaries, which outlines the nature and scope of its internal control and risk management during the financial period under review.

This Statement has been prepared in accordance with the requirements of the Bursa Malaysia Securities Berhad Main Market Listing Requirements ("Listing Requirements"), the Statement on Risk Management and Internal Control Guide 2025 ("SORMIC Guide 2025"), the Corporate Governance Guide (4th Edition), the Malaysian Code on Corporate Governance 2021 and the Audit and Assurance Practice Guide 3 ("AAPG 3") issued by the Malaysian Institute of Accountants ("MIA").

The Statement outlines the governance framework and processes established by the Board to ensure the adequacy and effectiveness of the Group's RMIC systems. It also describes the mechanisms for which the Board, supported by its committees and assurance functions, maintains effective oversight of the Group's governance, risk and control environment.

Board Responsibility and Oversight

The Board affirms its responsibility for the Group's overall risk management and internal control framework. This includes establishing appropriate governance and organisational structures, defining the Group's risk appetite, strategic direction and control environment; ensuring that management identifies and manages key and emerging risks; and reviewing the adequacy and effectiveness of the internal control system on an ongoing basis.

To assist in fulfilling its oversight responsibilities, the Board is supported by the Audit and Risk Management Committee ("ARMC") which provides oversight on governance, risk management and internal control processes across the Group. The ARMC ensures that these processes remain robust, effective and aligned with the Group's strategic objectives and regulatory expectations, in accordance with the principles outlined in the SORMIC Guide 2025.

The ARMC is further supported by the Group Internal Audit ("GIA") and Group Risk Management and Compliance ("GRC") functions, both of which operate independently to provide objective assurance and continuous monitoring of the adequacy and effectiveness of the Group's risk management and internal control aspect as follows:

- GIA performs independent reviews and evaluations on the design and operational effectiveness of the internal control systems, ensuring that key risks are properly identified, managed and mitigated.
- GRC facilitates the implementation and continuous enhancement of the enterprise-wide risk management framework, promotes a culture of risk awareness and compliance, and ensures adherence to applicable laws, regulations and internal policies.

Both GIA and GRC report directly to the ARMC and provide regular updates on risk exposures, control effectiveness and compliance matters. The Chairman of the ARMC thereafter briefs the Board members on the proceedings of the ARMC meetings including highlighting any material matters on internal control or risk management that warrant the Board's attention. Minutes of the ARMC meetings which recorded these deliberations are also presented to the Board for notation.

Key Components of RMIC System

The Group's key components of RMIC system are as follows:

1. Integrity and Ethical Values

- A Code of Business Ethics and Conduct ("CoBEC") which sets out the principles to guide Directors' and employees' conduct to the highest standards of personal and corporate integrity. The CoBEC covers areas such as conflict of interest, use of company assets, confidentiality of proprietary information, acceptance of gifts and business courtesies, prohibition of kickbacks as well as provisions which cover personal data protection, competition, anti-money laundering and anti-terrorism financing.

- A groupwide integrity framework which accentuates the Group's commitment to uphold integrity in all manner of conduct by its employees at all times in their interaction with various stakeholders, both internal and external. This framework includes Integrity and Fraud Risk Policy which interphases with many of the existing policies adopted within the Group and also addresses fraud reporting and investigation.

- An Anti-Bribery and Corruption Policy ("ABC Policy") which reflects the Group's stand of zero tolerance against all forms of bribery, fraud and corruption, and its commitment to lawful and ethical conduct at all times. The ABC Policy elaborates on the Group's core principles set out in the CoBEC and the Employee Code of Conduct, providing information and guidance to all directors, employees and other stakeholders of the Group concerning how to deal with improper solicitation, bribery and other corrupt activities and issues that may arise in the course of business.

- Annual e-declarations on Conflict of Interest and acknowledgement on the understanding and compliance with the ABC Policy among executive employees being part of the Group's effort in creating awareness and ensuring that the employees understand, observe and uphold high integrity and ethical values in all their business dealings.

- Pursuant to Section 17A of the Malaysian Anti-Corruption Commission ("MACC") Act 2009 which imposes corporate liability on companies for the corrupt practices of its employees and/or any person associated with the companies in cases where such corrupt practices are carried out for the companies' benefit or advantage, the Group had conducted a series of trainings and workshops to brief employees on the adequate procedures (as per guidelines issued under MACC Act 2009) that had been put in place and to equip them with the required understanding of their duties, responsibilities and obligations under this section. The Board and the Management will continue to strengthen the adequate procedures to prevent acts of corruption related to the organisation.

The CoBEC and the ABC Policy are published on the Company's website at www.lion.com.my/lionpsim.

2. Authority and Responsibility

- The Board establishes the vision and strategic objectives of the Group and is entrusted with the responsibility in leading and directing the Group towards achieving its strategic goals and realising long-term shareholders' value. The Group's business strategic directions are also reflected in the respective operating companies' ("OCs") Corporate Performance Scorecard ("CPS") which are reviewed half-yearly. The Board retains full and effective control of the Group's strategic plans, overseeing the conduct of the Group's businesses, setting policies, implementing, reviewing and maintaining an appropriate system of risk, control and compliance management and ensuring the adequacy and integrity of the Group's system of internal control. The Board is also responsible for ensuring financial integrity, reviewing and approving material transactions, related party transactions, capital financing and succession planning and overseeing the implementation of stakeholder communication.

- The Board recognises that prudent risk management is essential to achieving the Group's strategic objectives and sustaining long-term value for stakeholders, and it defines the Group's risk appetite as the level and type of risk that the Group is willing to accept in pursuit of its strategic and operational goals. This definition takes into account the Group's business model, market conditions, stakeholder expectations and applicable regulatory requirements. The Group's risk appetite had been established and subject to be periodically reviewed to ensure continued alignment with its strategic direction, changing business environment and emerging risk landscape.

- The Board delegates to the Executive Director ("ED"), the authority and powers of executive management of the Company and its businesses within levels of authority specified from time to time. The ED may delegate aspects of her authority and powers but remains accountable to the Board for the Company's performance and is required to report regularly to the Board on the progress being made by the Company's business units and operations. Delegation of responsibilities and accountability by the ED further down the structure of the Group is communicated and formalised via respective operational structure and organisational chart as well as the authority matrix.

- Board Committees which are guided by respective Terms of Reference were set up to fulfil certain responsibilities delegated by the Board. These Committees assist the Board in promoting governance and accountability as well as overseeing internal controls, Board effectiveness, and nomination and remuneration of Directors and key positions:

  – Audit and Risk Management Committee
  – Nomination Committee
  – Remuneration Committee

- The Management of each operating company is responsible and accountable to the Senior Management, ED and the Board for implementing the frameworks, policies and procedures on risk and internal control as approved or directed by the Board.

3. Organisation Structure

- An operational structure and organisational chart which defines the lines of responsibility and delegation of authority together with a hierarchical structure of reporting and accountability.

- The authority matrix outlines the decision areas and the persons empowered to requisite, authorise and approve the expenditure/commitment. Delegated authority carries with it the obligation to exercise sound judgement, good business sense and accountability.

4. Frameworks, Policies and Procedures

- A set of Group level internal policies and procedures which is maintained centrally and accessible to employees via the intranet. The policies and procedures at both Group level and business or operational level are regularly reviewed for updates to resolve operational deficiencies and to meet new compliance requirements. Enhancement efforts to streamline local policies, guidelines or procedures at business or operational level to key Group Policies and Procedures are continuing.

- A Group Procurement Framework which provides a fairly standardised, uniform and consistent set of controls by promoting accountability, ownership and transparency. This increases the ability of the Group to develop a pool of reliable and competent vendors through proper governance, selection of appropriate procurement methods and vendor management.

- A Group Personal Data Protection Compliance Framework which provides guidelines on implementation of controls in business and operations processes in meeting the requirements of data protection principles of Personal Data Protection Act 2010.

- Other key policies such as Competition Policy and Sexual Harassment Policy which complement the Group's CoBEC and ABC Policy. These policies direct the employees to behave ethically and professionally in ensuring compliance with relevant laws and creation of a conducive working environment.

- A Group Sustainability Policy that outlines the Group's commitment to responsible and sustainable business practices across its operations. The Policy provides a framework for managing material environmental, social and governance (ESG) matters, integrating sustainability considerations into strategic planning, risk management and daily operations.

5. Planning, Monitoring and Reporting

- An annual exercise involving all business units to prepare a comprehensive budget and business plan which includes development of business strategies and the establishment of key performance indicators against which the overall performance of the companies within the Group can be measured and evaluated.

- Review of key business variables and the monitoring of the achievements of the Group's performance on a quarterly basis by the Board and the ARMC.

6. Internal Audit

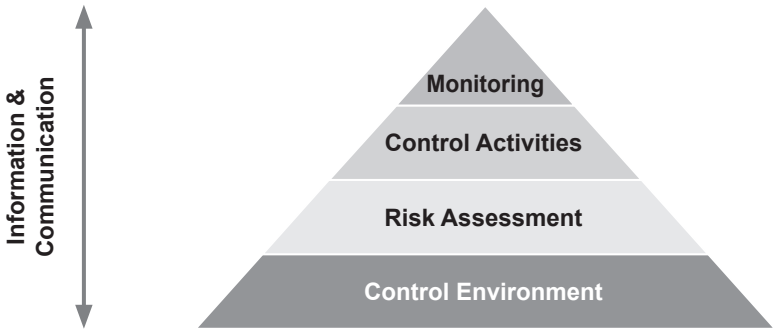
- Internal Audit Charter that is approved by the ARMC articulates the purpose, responsibility and authority of the GIA function as well as the nature of assurance activities provided by the function.

- Annual Audit Plan that is approved by the ARMC provides a basis for audit engagements which also considers feedback from the Management. The GIA adopts a risk-based audit approach, assesses the selected areas within the audit scope for risk exposures, compliance with approved policies and procedures, adherence to relevant laws and regulations and where applicable, benchmarking against industry best practices.

- The GIA reviews business processes and internal control and risk management system, submitting reports to the ARMC quarterly. The GIA also conducts follow-up reviews to ensure effective implementation of internal audit recommendations.

- Confirmation of the effectiveness of internal control and risk assessment process by the respective Heads of OC and Heads of Accounts and Finance of the OC (on financial related matters) through the signing off of the Risk Management and Internal Control – Self-Assessment Questionnaire ("RMIC-SAQ") on an annual basis.

- The GIA assesses and reports on the adequacy and effectiveness of the Group's governance, risk management, and internal control systems in accordance with the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control – Integrated Framework. The following 5 inter-related COSO components are considered during the assessment:



7. Risk Management

- The Group has in place a risk management framework, Enterprise Risk Management ("ERM") Framework that is modelled after the widely adopted standard ISO31000 Risk Management – Principles and Guidelines to guide the implementation of consistent risk management practices across the Group by both the Board and the Management. It recognises that risks are inherent in businesses and views them within the context of risk as an opportunity, uncertainty or hazard. The framework also incorporates sustainability and climate-related risks, cybersecurity risks and other emerging risks to ensure resilience and long-term value creation.

- The ERM Framework provides guidelines on risk governance, risk management process, risk reporting and generic tools to be used by the Group. The design of the risk governance structure therein is premised on a 3 lines of defence model with clear functional responsibilities and accountabilities for the management of risk:

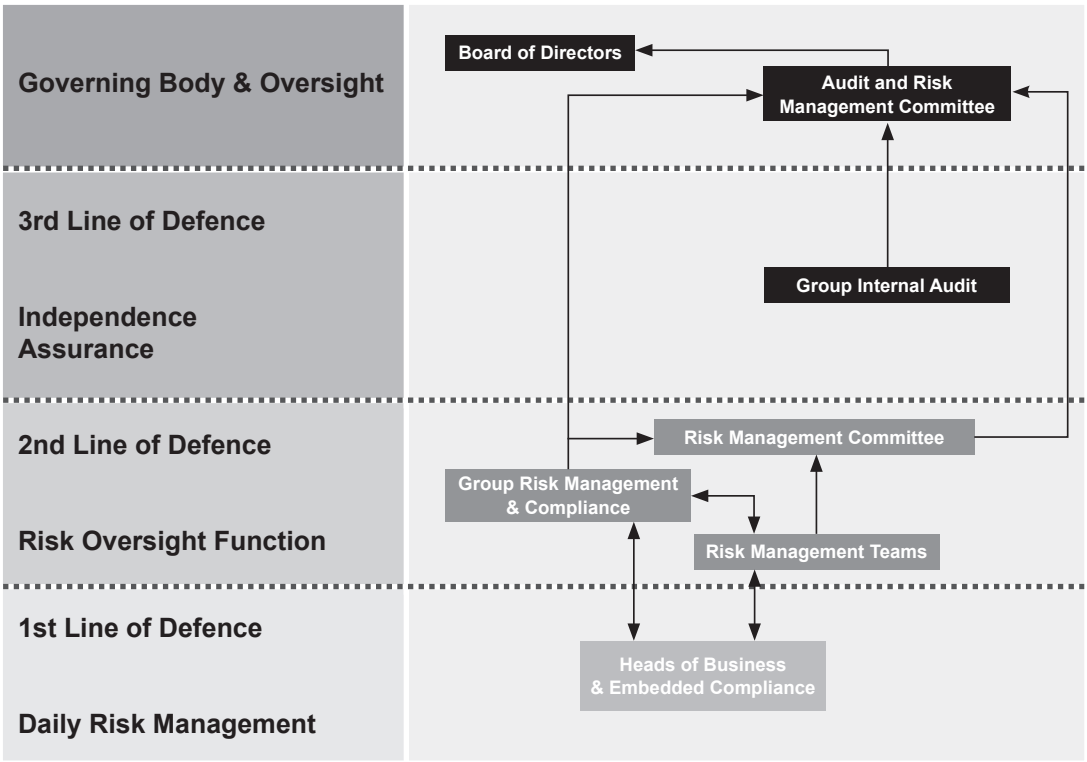
  – The first line of defence under the framework is found at the OCs level where the Head of each OC assumes the overall accountability for the respective OCs' risk management implementation. Each OC's Heads of department would provide support to the Head of OC and supervision of risk management practices in key processes under their respective areas of responsibilities. The Heads of OC, in their half-yearly updates and reporting of respective CPS and Corporate Risk Scorecard ("CRS"), provided confirmation that the risk management process with regard to identification of material issues together with relevant controls and management actions have been adequately complied with.

  – The second line of defence provides oversight function via the establishment and roles vested in the OC's Risk Management Team ("RMT") and Risk Management Committee ("RMC") both of which are supported by the GRC department. The RMTs monitored and reported their Key Performance Indicators via the CPS and identified, analysed and reported risks to the RMC and ARMC via the CRS. The GRC provides the reporting templates, updated tools, maintenance of Q-Radar system and facilitation or review of OC's scorecards development or updates with OCs' risk representatives. The RMC receives and reviews the scorecards reports from OCs together with the ARMC.

  – The third line of defence is realised through the provision of objective and independent challenge by GIA with regard to the level of assurance as provided by business operations and oversight functions.

  – The Board, through the deliberations and recommendations of the ARMC, serves as the Group's Governing Body, providing oversight on the effectiveness of governance, risk management and internal controls.

- The risk management organisational structure adopted by the Group is illustrated as follows:



- The Group employs a Risk Universe Listing to facilitate identification of risk across 4 risk themes which are Strategic, Business, Financial and Operational as shown in the illustration below:



- Most OCs of the Group have set risk tolerance ranges, either qualitative or semi-quantitative, for selected result areas via a self-defined risk impact severity table. Such table is referred to together with a risk matrix which provides measurement scales on possibility of risk occurrence and impact. The use of these tools facilitates the measurement of each risk analysed and evaluated at 3 different levels; Inherent, Nett and Target, thereby enabling the RMTs to focus more on the management of high risk areas in line with their risk tolerance.

8. Compliance Management

- Half-yearly Compliance Risk Self-Assessment (CRSA) exercises with mitigations identified to address breaches or material non-compliances.

- Joint review of existing operational practices and selected policies or procedures for possible and appropriate control enhancements. Such exercises may result in revisions of relevant policies or procedures, new policies or procedures, introduction of control tools such as standard templates/ forms and even development of special purpose automated processes.

- A compliance programme reviewed by the ARMC on an annual basis addressing key compliance areas of statutory and regulatory requirements, codes and internal ethics/standards/policies and procedures. The results and status of the compliance programme were reported by the Compliance Function on a half-yearly basis to the Compliance Committee to monitor and address ongoing changes and implementations in the legislative and regulatory requirements affecting the Group.

9. Safety and Crisis Management

- The Group is committed to ensuring a safe, healthy and conducive working environment across all operations, in line with our values of care, responsibility and integrity. We recognise that the well-being of our employees and stakeholders is essential to sustainable business performance.

- The Occupational Safety and Health Committee plays a key role in promoting safety and health awareness, identifying potential risks and recommending preventive measures to protect employees' safety, health, and welfare. It also continuously communicates with OCs, recommends precautionary measures to ensure compliance with the Occupational Safety and Health Act, and addresses potential risks through continuous communication and monitoring.

- The Group has also established an action plan in the Group's Human Resource – Occupational Safety and Health Act (HR-OSHA) Manual & Guidelines to manage emergencies such as fire, blackout, bomb threat, earthquake, and civil disorder, ensuring preparedness and business continuity.

- The Group continues to prioritise a safe and healthy workplace for all employees, alongside business continuity concerns. Workplace health and safety procedures, along with the National Security Council's Standard Operating Procedures on preventive measures to mitigate health risks, are in place and communicated to employees, business associates, and other stakeholders.

The following preventive measures have been implemented:

(i) Standard Operating Procedures ("SOPs") on safe work procedures communicated to all employees;

(ii) Established Emergency Response Team (ERT) with SOPs to handle health-related emergencies; and

(iii) SOPs for working at and undertaking construction/renovation works.

- At the Group level, the Issue Management and Communication Policy under the Corporate Communications Function ensures effective handling of internal and external communications in the event of any issue, crisis, or disaster.

10. Information and Communication Technology

- A quarterly IT Steering Committee meeting is held where all IT Managers from various OCs meet. It is a platform which enables collaboration among the OCs, sharing of experiences and consolidation of standard IT platforms.

- A set of Group IT Policies and Guidelines is in place to govern the operations of IT within the Group. Due to the diversity of businesses, each OC has its own set of IT Policy adopting the standard Group IT Policy wherever possible and adding policies that are peculiar to the business they are in.

- The Group Human Resources Management System runs off a cloud infrastructure where a single system is used across the Lion Group of Companies. Cloud infrastructure is hosted offsite to protect the sensitivity of data and is supported by a hot Disaster Recovery site to enable quick recovery of data in the event of any unforeseen incident. An annual Disaster Recovery test is carried out to ensure service quality as per agreed service level agreement.

- As part of Lion Group's Cyber Security strategy to mitigate cyber security risks and threats, Group IT had provided and shall continue to provide Cyber Security Awareness and related initiatives to educate employees with the objective of safeguarding our businesses and employees.

- The Group recognises that a capable and future-ready IT workforce is essential to supporting ongoing growth and transformation. Group IT prioritises continuous learning and development through regular training and knowledge-sharing initiatives, strengthening core technical competencies across key knowledge areas.

11. Insurance

- An insurance programme to safeguard major assets against financial loss resulting from property damage, machinery breakdown, business interruption and general liability, which is reviewed annually.

- A yearly exercise to ensure the adequacy and renewal of the Group's Directors' and Officers' Liability insurance.

12. Whistleblowing

- A Whistleblower Policy which provides the channels to report wrongdoings by employees and/or other stakeholders whilst ensuring the integrity of the process and information and also protecting the rights of informants. The implementation of this policy enables the Group to address such concerns that may adversely affect the reputation and interests of the Group more effectively.

- The oversight by the Board and its engagement with the Management in the handling of reported wrongdoings are also set out in the Integrity and Fraud Risk Policy.

Risk Management Process

The OCs' CPS which are prepared every financial year are updated on a half-yearly basis to provide a clear and proper context within which performance-related risks are to be identified, analysed and managed in line with the respective OCs' strategic direction and business objectives. Key Performance Indicators ("KPI") were assigned to these objectives and their performance were tracked by the KPI owners under the supervision of the Heads of the OC.

In establishing a bottom-up reporting of the risk profile of the OCs, the RMT in the respective OCs identified possible and actual risks faced by the OC together with an analysis of the causes, impact and mitigating actions.

The risk owners were responsible to ensure preventative, detective and corrective controls were in place to address these risks. Gaps in controls and continual improvements were implemented through management action plans. This process was executed by the RMTs and documented in the CRS.

The GRC conducted reviews of the risk profiles, either focusing on specific risk issues or the completeness of the risk assessment process for selected risk profiles. The results of the review were communicated to the administrators of risk scorecards and/or Heads of OC for improvement and implementation.

The CPS and CRS were presented by the RMTs and RMC to the ARMC on a half-yearly basis for reviews on the status of the performance objectives and management action plans implementation. These reviews may result in identification of new risks or re-assessment of reported risks. The ARMC reviewed significant risks, if any, across the risk themes and guided the OCs on further mitigations, where required.

The Heads of the OC, at the half-yearly reporting, had confirmed that the respective OCs' RMTs had reviewed and updated the CPS and CRS with the status of all related material information, controls and management actions and that the risk management process had been complied with and information provided therein fairly reflected the position of the OC for the financial period under review.

In all material transactions such as acquisitions and disposals of assets or business and corporate proposals, risks associated with such transactions as analysed by the project team and RMC are presented to the ARMC and Board for their deliberation and decision making. The ARMC will review the proposals together with the risks associated therewith after which the Board may approve, decline or modify the proposals in line with the Group's risk appetite and the Group's strategic and business directions.

Board Assurance on Adequacy and Effectiveness of RMIC Systems

The Board, through the ARMC had reviewed the adequacy and effectiveness of the Group's risk management and internal control systems for the financial period ended 30 June 2026 and up to the date of approval of this Statement. The Board confirmed that the processes were in place.

This review was supported by the following sources of assurance:

- Reports from the GIA and GRC functions which provided independent assessments of the design and operating effectiveness of the controls in place;
- Annual confirmations by the respective Heads of OC and Heads of Accounts and Finance of the OC (on financial related matters) through the RMIC-SAQ, affirming compliance with the Group's internal control framework and risk management procedures; and
- The External Auditors' limited assurance review, conducted in accordance with the AAPG 3 issued by the MIA.

Continuous Improvement

The Board remains committed to strengthening the Group's overall governance, risk management and internal control environment through continuous improvement initiatives. Key focus areas include:

- Integration of sustainability and climate-related risk considerations into the Group's strategic planning, decision-making and risk assessment processes;
- Enhancement of digital resilience and data protection controls with emphasis on cybersecurity readiness and incident response capabilities;
- Strengthening of compliance and ethical culture through targeted training, leadership accountability, and reinforcement of tone-from-the-top; and
- Ongoing refinement of ERM tools, methodologies and analytics to enhance risk visibility, data-driven insights and informed decision-making.

These continuous improvement efforts reflect the Board's commitment to sustaining a robust, forward-looking, and resilient risk management and internal control framework that supports the Group's long-term value creation and enhances stakeholder confidence.

Conclusion

The Board is of the view that the system of risk management and internal control in place throughout the Group for the financial period under review, and up to the date of approval of this Statement, is sound and effective, providing reasonable assurance that the structure and operation of controls are appropriate for the Group's operations.

Implementation measures are continuously being taken to strengthen the system of risk management and internal control so as to safeguard the Group's assets as well as the shareholders' investments, and the interests of other stakeholders.

Review by External Auditors

The External Auditors have performed limited assurance procedures on this Statement pursuant to the scopes set out in the Audit and Assurance Practice Guide 3 ("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 MIA for inclusion in the Annual Report of the Group for the financial period ended 30 June 2026, and reported to the Board that nothing has come to their attention that has caused them to believe the Statement intended to be included in the Annual Report has not been prepared, in all material respects, in accordance with the disclosures of the SORMIC Guide 2025, Corporate Disclosure Guide, Listing Requirements and Corporate Governance Guide, nor is the Statement factually inaccurate.

AAPG 3 does not require the External Auditors to consider whether the Statement 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 and the Management thereon. The report from the External Auditors was made solely for, and directed solely to the Board of Directors in connection with their compliance with the Listing Requirements and for no other purposes or parties. The External Auditors do not assume responsibility to any person other than the Board in respect of any aspects of this Statement.