STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

The Board of Directors ("Board") acknowledges the importance of maintaining a sound system of internal control to safeguard 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 of the Group (excluding associated companies, as the Board does not have full management control over their operations) which was prepared with reference to the applicable statutory requirements and regulatory guidelines including:

- Statement on Risk Management & Internal Control: Guidelines for Directors of Listed Issuers;
- Corporate Disclosure Guide and Corporate Governance Guide (3rd Edition); and
- Bursa Malaysia Securities Berhad Main Market Listing Requirements.

Board Responsibility

The Board affirms its overall responsibility for the Group's internal control system and for reviewing the adequacy and effectiveness of this system which covers governance, enterprise risk management, financial, strategy, organisational, operational, regulatory and compliance controls. However, in view of the inherent limitations in any system, such system of internal control can only provide reasonable and not absolute assurance against material misstatements, frauds or losses and unforeseen emerging risks.

The Board delegates the oversight of internal control and risk management to the Audit and Risk Management Committee ("ARMC"). The ARMC deliberated at its meetings, the adequacy and effectiveness of internal controls based on the findings and outcome of the audits which were conducted and reported by the Group Internal Audit ("GIA") during the financial year. The reports by the GIA described the issues discovered during the audits and actions taken by Management in addressing them. The Chairman of the ARMC thereafter briefed the Board members of the proceedings of the ARMC meetings including highlighting any material matters on internal control or risk management that warranted the Board's attention. Minutes of the ARMC meetings which recorded these deliberations were also presented to the Board for notation.

Key Components of Internal Control System

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

1. Integrity and Ethical Values

- A Code of Business Ethics and Conduct ("CoBEC") which sets out the principles to guide 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. The CoBEC is published on the Company's website at www.lion.com.my/lionfib.

- A groupwide integrity framework that 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 & Fraud Risk Policy which interphases with many of the existing policies adopted within the Group and also addresses fraud reporting and investigation.

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 key operating companies' ("KOCs") 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 in ensuring financial integrity, setting the Group's risk appetite, reviewing and approving material transactions, related party transactions, capital financing and succession planning, and overseeing the implementation of stakeholders communication.

- The Board delegates to the Executive Directors ("EDs"), the authority and powers of executive management of the Company and its businesses within levels of authority specified from time to time. The EDs may delegate aspects of their authorities and powers but remain accountable to the Board for the Company's performance and are 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 EDs 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, EDs and the Board for implementing the framework, 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/Tender Policy 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 method and vendor management.

- A Group Personal Data Protection 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. 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 Framework and Plan which provides the roadmap to enhance Governance and the management of the material Economic, Environmental and Social risks and opportunities as well as stakeholders engagement.

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

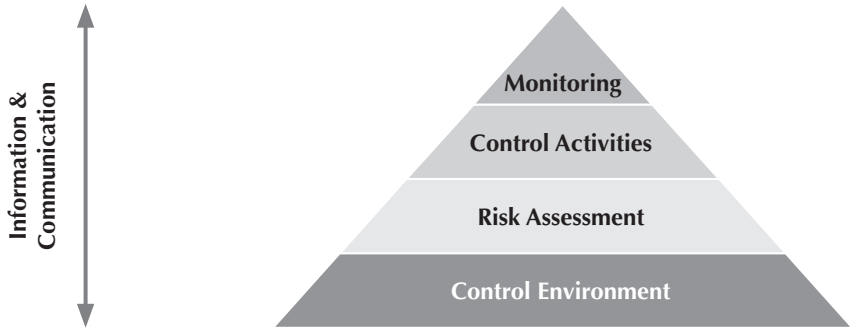
- Internal Audit Charter that is approved by the ARMC articulates the purpose, responsibility and authority of the GIA function as well as the nature of assurance activities provided by the function.

- 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 under the audit scope with regard to risk exposures, compliance towards the approved policies and procedures and relevant laws and regulations and where appropriate, benchmarks against best practices in respective industry.

- Review of business processes and systems of internal control and risk management by the GIA which submits its reports to the ARMC on a quarterly basis. The GIA also established follow-up review to monitor and to ensure that the recommendations of internal audit are effectively implemented.

- Confirmation of the effectiveness of internal control and risk assessment process by the respective Head of KOC and Head of accounts and finance of the KOC (on financial related matters) with the signing off of the Risk Management and Internal Control – Self-Assessment Questionnaire (RMIC-SAQ) on an annual basis.

- The GIA assesses and reports the adequacy and effectiveness of the Group's governance, risk management and internal control system using the Committee of Sponsoring Organisations 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 ISO31000:2009 Risk Management – Principles and Guideline to guide the implementation of a consistent risk management practice 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.

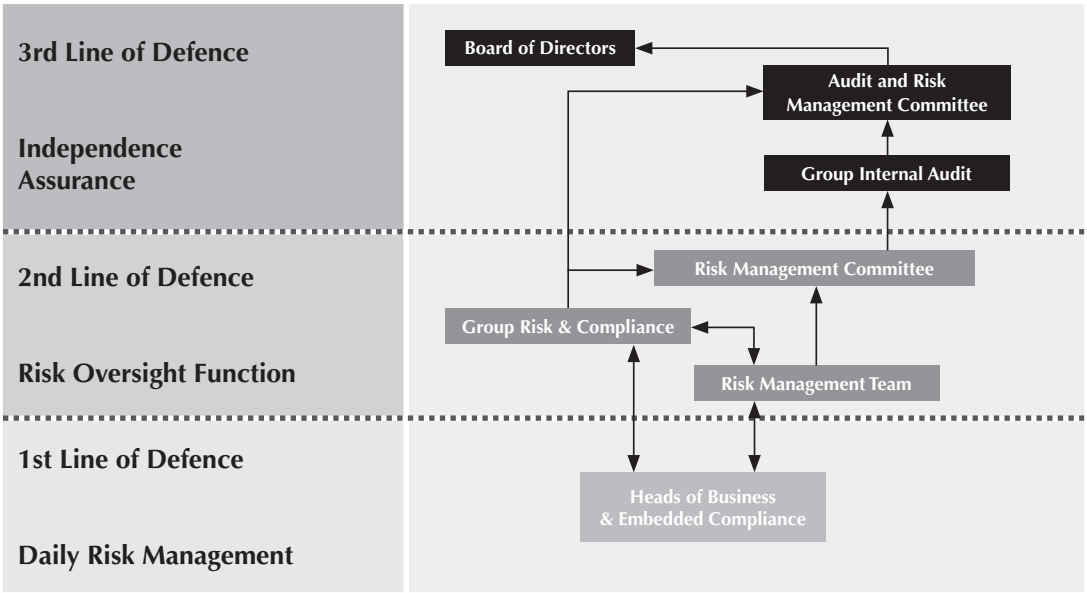
- The ERM Framework provides guidelines on the risk governance, risk management process, risk reporting and generic tools to be used by the Group. The design of the risk governance structure therein is premised on 3 lines of defence concept with clear functional responsibilities and accountabilities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

  - The first line of defence under the framework is found at the KOCs level where the Head of each KOC assumes the overall accountability for the respective KOC's risk management implementation. Each KOC's Heads of department would provide support to the Head of KOC and supervision of risk management practices in key processes under their respective areas of responsibilities. The Heads of KOC, 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 KOC's Risk Management Team ("RMT") and Risk Management Committee ("RMC") both of which are supported by the Group Risk and Compliance ("GRC") department. The RMTs establish their strategy roadmap for every financial year 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 KOC's scorecards development or updates with KOCs' risk representatives. The RMC receives and reviews the scorecards reports from KOCs 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, sets the overall risk appetite for the Group.

- 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:

RISK UNIVERSE

- Most KOCs 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 revision 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 process.

- 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 on-going changes and implementations in the legislative and regulatory requirements affecting the Group.

9. Safety and Hazards Management

- Operations and safety and hazards action plans of operating companies for business resilience and robustness in contingencies, crisis management and disaster recovery management.

- A Crisis Management and Communication Policy and process established under the Corporate Communications Function to guide the handling of external communications in the event of any crisis/disaster.

10. Information and Communication Technology/Management Information System

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

- A set of Group IT Policies is in place to govern the operations of IT within the Group. Due to the diversity of businesses, each operating company 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 data losses. An annual Disaster Recovery test is carried out to ensure service quality as per the agreed Service Level Agreement (SLA).

- As part of the Lion Group Cyber Security Strategy, the Group has issued Cyber Security Policy to be adopted by all its operating companies.

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. Whistle-Blowing

- 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 & Fraud Risk Policy.

Risk Management Process

The KOCs' 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 KOCs' 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 KOCs.

In establishing a bottom-up reporting of the risk profile of the KOCs, the RMT in the respective KOCs identified possible and actual risks faced by the KOC 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 review 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 KOCs for improvement and implementation.

The CPS and CRS were presented by the RMT and RMC to the ARMC on a half-yearly basis for review 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 KOCs on further mitigations, where required.

The Heads of the KOCs, at the half-yearly reporting, had confirmed that the respective KOC's RMT 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 KOC for the 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.

Conclusion

The Board is of the view that the system of risk management and internal control in place throughout the Group for the year 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 taken to strengthen the system of risk management and internal control so as to safeguard shareholders' investments and the Group's assets.

Review by External Auditors

The External Auditors have performed limited assurance procedures on this Statement on Risk Management and Internal Control pursuant to the scopes set out in Audit and Assurance Practice Guide ("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 Malaysian Institute of Accountants for inclusion in the Annual Report of the Group for the financial year ended 30 June 2018, and reported to the Board that nothing has come to their attention that has caused them to believe the Statement on Risk Management and Internal Control intended to be included in the Annual Report has not been prepared, in all material respects, 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, Corporate Disclosure Guide and Corporate Governance Guide (3rd Edition), nor is the Statement factually inaccurate.

AAPG 3 does not require the External Auditors to consider whether the 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 and 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 Bursa Malaysia Securities Berhad Main Market Listing Requirements and for no other purposes or parties.