

# STATEMENT OF RISK MANAGEMENT AND INTERNAL CONTROL

The Manager realises the significance of establishing a sufficient and effective risk management and internal control system, and has attended to this under the Pavilion REIT Operation Manual approved by the Board. Such process has been in place for the past years under review, including up to the date of approval of this statement for inclusion in the annual report.

There is a policy in place pertaining to the level of authority required for transactions and standard operating procedures pertaining to operations and maintenance of Pavilion REIT's properties as well as acquisitions and divestments of property.

The Audit Committee and Board meet at least once every quarter to review the financial performance of Pavilion REIT against the approved budget. The Board also reviews the business risk of Pavilion REIT, where identified by the CEO, internal auditor and external auditor and acts accordingly, where deemed appropriate. Board's approval is required for any proposed acquisition or disposal of investment property, which would be evaluated from the aspect of economic, environment, financial and risks relevant to the property industry or sector. The CEO meets the management regularly to review, monitor and manage risks identified by the management and thereafter, update the Audit Committee as required.

Standard operating procedures for management of Pavilion REIT properties have been adopted, which comprise operational guide, control and monitoring procedures. Enterprise risk management committee, policy and procedures have also been formalized during the year.

BDO Governance Advisory Sdn Bhd ("BDO GA") has been appointed as internal auditor whereby they had performed internal control review of the following areas:-

- i) corporate governance review of board charter, terms of reference, reporting, policies and procedures as well as whistle-blowing; and
- ii) compliance review on anti-bribery and corruption policies, procedures, training, communication with business partners and reporting.

With digitalization being a necessity to business operations with data security and privacy protection being risk factors, BDO Consulting Sdn Bhd ("BDO Consulting") was engaged to review the design and implementation of information security controls by using relevant areas of the ISO/IEC 27001 standard on Information Security Management System (as a baseline). Areas covered included policies, system acquisition, development and maintenance, supplier relationship, information security incident management and aspects of business continuity management. Security from aspects of organisation, human resource, physical and environment control, operations as well as communication were also reviewed.

The execution strategies that both BDO GA and BDO Consulting adopts are one that is risk-based and process life cycle focused. Risk-based approach allows for prioritisation of audit on functions or processes that are of the highest concern, or which will have significant impact to Pavilion REIT in the event of control failures.

A process life cycle approach allows for :

- i) understanding and evaluation of business processes and related business controls from a risk perspective along the entire life cycle;
- ii) identification of control inadequacies within the processes and recommend feasible or best practices; and
- iii) consider the effectiveness and efficiency of processes and controls, ie not just in terms of integrity but also in terms of process improvement opportunities

The Audit Committee has reviewed the findings presented by BDO GA and BDO Consulting during the year. Recommendations made have been rectified and adhered to and the Audit Committee and Board will continue to monitor the recommendations on an on-going basis.

The Board has received assurance from the CEO that the risk management and internal control system is operating sufficiently and effectively, in all material aspects.

The Board is of the view that the risk management and internal control system in place for the year under review is adequate and effective. Nevertheless, it will always be improved and updated in line with changes in the operating environment.

Due to inherent restrictions as well as the ever-changing risk landscape, the controls which are employed are intended to cope with and are not expected to eliminate all risks of failure to achieve business objectives. Established controls can only provide realistic and not total assurance against material misstatement of management and financial information or against financial losses and fraud.