

# STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

This Statement on Risk Management and Internal Control (“Statement”) is made pursuant to Paragraph 15.26(b) of Bursa Malaysia Listing Requirements and in accordance with the guidance set out in the Statement on Risk Management and Internal Control Guide 2025 : Guidelines for Directors of Listed Companies. It sets out the key features, adequacy and effectiveness of Pavilion REIT’s risk management and internal control system for the financial year and up to the date of approval of this Statement by the Board.

## Governance & Oversight Structure

The Board retains the overall responsibility for risk management and internal control systems, including setting the risk appetite and fostering a culture of proactive risk management to ensure their effectiveness in managing Pavilion REIT. The Risk Management Committee (“RMC”), comprising mainly Independent Non-Executive Directors assist the Board members to oversee the risk management framework and policies. Management’s Risk Management Working Committee (“RMWC”), led by the CEO and supported by senior personnel, coordinates bottom-up risk identification and validation by Risk Owners, before escalation to the RMC. The CEO is responsible for ensuring that the structure of risk management operates effectively. Risk Owners are responsible for ensuring that their respective functions or business units within Pavilion REIT are managed efficiently by identifying, assessing and implementing mitigation plans to address the risks arising from their functions. Internal Audit provides independent assurance and reports on the adequacy and effectiveness of internal controls and reports directly to the Audit Committee. Pavilion REIT adopts the Institute of Internal Auditors (“IIA”)’s Three Lines Model: first line owns and manages risk in day-to-day operations, second line provides oversight and guidance to ensure risks remain within appetite, and third line offers independent assurance through internal audit.

## Risk Management Process

Pavilion REIT’s Enterprise Risk Management (ERM) Procedure aligns with ISO 31000:2018 and integrates risk management into objectives, processes and decision-making. Its risk assessment process is a systematic 12-step assessment that

- 1) defines processes / activities / objectives,
- 2) determine risk parameter,
- 3) identify risks,
- 4) root cause analysis,
- 5) determine consequences (insignificant, minor, moderate, major, catastrophic),
- 6) define likelihood (remote, unlikely, possible, likely, almost certain),
- 7) establish gross risk rating (low, medium, significant, high),
- 8) identify controls,
- 9) determine control effectiveness,
- 10) challenge / revise ratings,
- 11) determine risk residual and
- 12) develop risk profile, supported by standard templates (risk registers, risk maps, flash reports).

The framework explicitly covers material Environment, Social and Governance (ESG) and climate-related risks (including environment management, flood, data privacy & cybersecurity, and human capital) and sets out risk treatment options of termination, reduction, acceptance or pass on risk to third parties.

RMWC meets at least half-yearly or as and when required to review detailed risk registers with Risk Owners. RMC meetings are held at least half-yearly to oversee the Pavilion REIT’s key residual risks of medium to high rating on the risk map.

There is an established structure with defined lines of authority, responsibility and accountability to meet Pavilion REIT’s mission, vision and purpose within a realistic and coordinated environment. Policies on anti-bribery and corruption, code of conduct and ethics, environmental, human rights occupational health and safety, sustainability, vendor code of conduct and whistleblowing are in place to provide transparency and guidance.

Discretionary authority limit for various activities, including investments and divestments, acceptance of credit facilities or medium-term notes, annual budget, transactions of capital in nature and non-capital expenditure, leasing and income generating matters and human resource matters have been adopted. Transactions exceeding certain limit requires Board approval, while authority for transactions within certain threshold are delegated to authorized personnel to ensure operational efficiency. Only authorized personnel are empowered to approve transactions. The annual budget, tabled to the Board for approval will be monitored against actual performance.

# STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

Cont'd

Standard operating procedures pertaining to operations and maintenance of Pavilion REIT's properties as well as acquisition and divestment of properties are also reviewed regularly. Business continuity planning activities will continue to be undertaken across Pavilion REIT properties as part of ongoing efforts to strengthen operational resilience and crisis preparedness.

Anti-bribery and corruption assessments are conducted prior to engaging new tenants / customers or renewing expired tenants. Measures to mitigate money laundering as well as combating the financing of terrorism have also been formalised with training provided. The Compliance Officer is responsible for adherence with applicable regulatory and legal requirements. As we continue to leverage on information technology for business operations and in light of ongoing concerns regarding data security breaches and privacy protection, training was provided to increase employees' awareness levels on cyber security threats such as malware and ransomware attacks, password security, using public wi-fi networks, securing mobile devices and cyber security best practices. Simulated phishing emails are also regularly sent to staff to gauge their alertness.

## Review and Actions

BDO Governance Advisory Sdn Bhd (BDO), as the internal auditor of Pavilion REIT, reports directly to the Audit Committee. As an independent service provider, BDO's annual audit objectives are to :-

- i) assess the adequacy and test the integrity of the system of internal controls
- ii) assess compliance with policies and procedures and recommended best practices
- iii) identify any potential areas for improvement in the effectiveness and efficiency of the processes (if any)

BDO will present their internal control review plan to the AC for consideration and approval. Subsequent to internal control review, recommendations made by BDO will be considered by Management for improvement with follow-up thereafter by BDO. The Audit Committee and Board will continue to monitor the recommendations and action plan on an on-going basis.

## Adequacy and Effectiveness

The Board, through the RMC, is satisfied that the risk management and internal control system is adequate and effective to provide reasonable assurance that Pavilion REIT's objectives will be achieved.

The respective risk owners have also provided their assurances that they have reviewed and considered, to the best of their knowledge, the following :-

- The adequacy and effectiveness of risk management practices and internal control systems within their respective areas
- That all mitigation plans have been implemented as stated in each risk owner's risk register
- That any emerging risks have been identified, evaluated and appropriately highlighted
- That RMWC has reviewed and concurred with the latest risk management report

## Joint Ventures and Associates

This Statement encompasses Pavilion REIT and its subsidiaries only as Pavilion REIT does not have any joint ventures or associates.

## Review of the Statement by External Auditors

This Statement on Risk Management and Internal Control ("Statement") has been reviewed by external auditors as required by Paragraph 15.23 of Bursa Listing Requirements. The external auditors have performed limited assurance procedures on the Statement in accordance with Malaysian Approved Standard on Assurance Engagements, ISAE 3000 (Revised), Assurance Engagements Other than Audits or Reviews of Historical Financial Information and Audit and Assurance Practice Guide 3, Guidance for Auditors on Engagements to Report on the Statement on Risk Management and Internal Control Included in the Integrated Annual Report.

Based on the limited assurance procedures performed, the external auditors have reported to the Board that nothing has come to their attention which causes them to believe this Statement is not prepared, in all material aspects, in accordance with the disclosures required of the Guidelines, nor is factually inaccurate.

# STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

Cont'd

## **CEO and Board Assurances**

The RMC and the Board have received assurance from the CEO that the risk management and internal control system is operating sufficiently and effectively, in all material aspects for the year under review and up to the date of approval of this Statement.

The Board is of the view that the risk management and internal control system in place for the year under review up to the date of approval of this Statement is adequate and effective. Nevertheless, it will continue to be reviewed and improved in line with changes in the operating environment and strengthen ESG and sustainability risk integration. There was no material control failure or weakness that would have material adverse effect to Pavilion REIT's mission.

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