1

STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL FOR THE YEAR ENDED 2020

Risk management is an integral part of PIDM's day-to-day operations and decision-making processes. PIDM has established appropriate policies and internal controls to mitigate key risk areas that could prevent it from achieving its objectives.

The Board of Directors, in discharging its responsibilities, is fully committed to PIDM maintaining a sound system of risk management and internal control, as well as to review its adequacy, integrity and effectiveness. PIDM's Management, led by the Chief Executive Officer (CEO), has established processes and controls to ensure a high level of governance within the organisation. The accountabilities and responsibilities for risk management and internal control are illustrated in the table below:

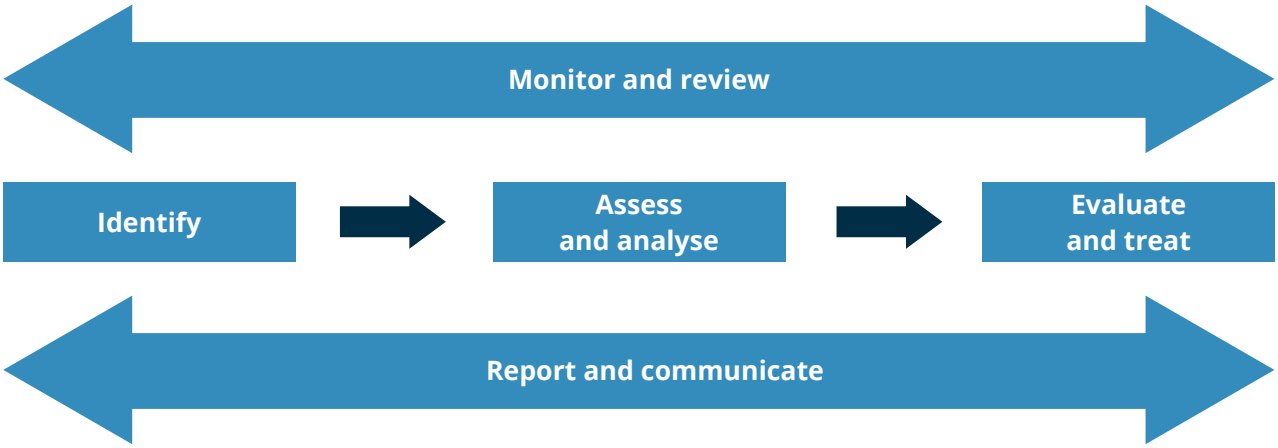
Systems relating to:	Role of the Board	Role of Management
Risk Management	• Ensures that there is an appropriate enterprise risk management (ERM) process to manage risks, reviews the ERM process and oversees its implementation. • Provides oversight of ERM activities through the Audit Committee.	• Assumes ultimate responsibility for the implementation of the risk management processes.
Internal Control	• Ensures that auditing, accounting principles and practices are in line with international and Malaysian best practices and conform to all legislative requirements. • Ensures that there is a control environment that enables the Board to seek reasonable assurance regarding the state of internal control and that appropriate action is being taken to address any significant weaknesses.	• Designs, develops, implements and maintains effective controls and sound business and governance processes to manage risks to PIDM.

RISK MANAGEMENT FRAMEWORK

PIDM's ERM Framework assists PIDM to manage risks on an integrated, enterprise-wide basis and supports the proactive identification and management of risks that could prevent or distract PIDM from achieving its mission, goals and objectives.

PIDM's ERM Framework is benchmarked against the Committee of Sponsoring Organizations of the Treadway Commission's ERM – Integrated Framework and the International Organization for Standardization 31000:2018 (Risk Management - Guidelines).

PIDM's Risk Management Process



The risk management process is as follows:

a. **identify, assess and review** significant risks faced by PIDM that could prevent it from achieving its objectives, mission, vision and strategic initiatives;
b. **formulate** action plans and incorporate these into initiatives in the management of significant risks, and monitor their progress and effectiveness; and
c. **provide** risk reports to the Audit Committee and Board of Directors to facilitate their understanding of significant risks faced by PIDM.

Risks Factors

The unequivocal risk driver in the assessment of risk for 2020 has been the COVID-19 health crises, which has resulted in temporary shutdowns and other containment measures that have led to economic crises in many countries around the world.

Following government restrictions on the freedom of movement around the world, organisations have had to adopt work-from-home arrangements or reorganise their business premises for health and safety reasons. Operational processes were forced onto virtual platforms, increasing their vulnerabilities to cyberattacks.

As countries cautiously attempt to re-open their economy, governments have imposed standard operating procedures on individuals and organisations to minimise the spread of the virus, and these requirements remain a challenge for most organisations.

In coming up with its risk ratings, PIDM has taken these factors into account.

2020 Risk Ratings

A "new normal" has emerged from the current COVID-19 pandemic and uncertainties continue to prevail. These risk factors were considered across the various risk categories, and, looking forward, great uncertainty remains as to how much longer the COVID-19 pandemic will last, as well as its impact on economies.

The table below summarises the results of the risk assessment activities performed by Management in 2020.

Risk Category and Definition	Assessment of Risk Areas
Financial Risk in relation to adverse movements in the value of PIDM's financial assets and liabilities, both on and off balance sheet, and in relation to its ability to fulfil its financial obligations.	PIDM's exposure to market risk remains minimal as it is guided by a conservative investment approach and continues to invest only in low-risk, short-to-medium-term investment securities that are held to maturity. PIDM is able to meet its ongoing operating cash requirements to support its day-to-day operations. Financial risk is assessed as being on a 'Stable' trend, as no changes are expected to its investment objectives (primarily the preservation of capital and maintenance of liquid assets). There was also no indication of any material events that would significantly disrupt PIDM's ability to meet its operational financial obligations.
Operational Risk in relation to PIDM's day-to-day operations including inadequate or failed internal processes and systems that could affect our ability to carry out our mandate.	The COVID-19 pandemic has caused a significant change in the operating environment of PIDM. With employees required to work from home, remote access arrangements had to be established, increasing the potential for cyber vulnerabilities. Some of the existing operational processes and procedures had to be adapted, and safety and health remained a priority for those who were needed at the office to deal with business continuity and other matters. Operational risk is assessed to be on an 'Increasing' trend as the COVID-19 pandemic persists. There also remains the ongoing threat of a resurgence of infections as countries attempt to remove lockdown restrictions and borders slowly reopen. We assess cyberattacks to remain an increasing threat. At the same time, we continue to consider ways to digitise the rest of our processes for efficiencies and effectiveness in a virtual work environment.

Risk Category and Definition	Assessment of Risk Areas
Insurance Risk in relation to the assessment, monitoring, intervention and failure resolution of member institutions, and other related risks inherent in providing the DIS and TIPS.	The COVID-19 pandemic-related risks include uncertainties about the recovery of the global and Malaysian economy and its impact on the public and businesses. Insurance risk is assessed to be on an 'Increasing' trend as the current economic environment remains uncertain. PIDM has heightened its investment in preparedness, communicating closely with other financial safety net players so that it can help contribute towards financial system stability as it is mandated to do.
Reputation Risk in relation to PIDM's reputation including stakeholders' trust and confidence in PIDM and its ability to carry out its mandate.	In view of COVID-19, PIDM increased the use of alternative platforms for stakeholder engagement through virtual channels beyond its original plans. Social media monitoring continues to be carried out to determine if there is unverified or inaccurate information, or negative public sentiment, circulating among the public. Reputation risk is assessed to be on an 'Increasing' trend as general anxiety among members of the public heightens and possible responses become more unpredictable.
Strategic Risk in relation to PIDM's strategy and governance in achieving its mandate, vision, mission, objectives or initiatives.	PIDM reprioritised its initiatives to adapt to the current COVID-19 operating and economic environment. As uncertainties continue to prevail, PIDM continues to monitor the situation and its possible impact on its strategic objectives. Strategic risk is assessed to be on an 'Increasing' trend as the operating and economic environment continues to evolve.
People Risk in relation to our people and how we manage them.	With the COVID-19 pandemic, communications and engagement activities were for the large part of the year virtual, including to provide support for employee morale and performance. People risk is assessed to be on an 'Increasing' trend as we continue to monitor the long-term implications of the current COVID-19 environment on the morale and performance levels.

In 2020, in view of the turn of events, PIDM reformulated its approaches towards achieving PIDM's strategic objectives, reprioritising initiatives as needed to deal with changes or volatility in the environment or to support the industry and its strategic partners. Going forward, ongoing monitoring will continue to ensure that its plans and initiatives are appropriately prioritised and aligned with any immediate needs to support the stability of the financial system.

Risk Outlook

Looking to the future, although the vaccine rollout has lifted market expectations of global growth, with the resurgence of virus outbreaks and reimposition of movement restrictions, downside risks remain. Uncertainties continue to prevail, and the pandemic's effects continue to impact countries, businesses and individuals, both in terms of health and economically. The external environment also brings with it other issues such as new variants of the virus, issues with the roll-out of vaccines in some countries and increasing cybersecurity threats. Overall, Malaysia's economy is expected to recover, although the outlook remains subject to downside risks.

INTERNAL CONTROL FRAMEWORK

PIDM's Internal Control Framework (ICF) is founded on the internationally recognised Committee of Sponsoring Organizations of the Treadway Commission Internal Controls – Integrated Framework (COSO Framework).

Internal Control Review Process

The review of the state of internal control is carried out based on the following two (2) approaches:

a. specific audits and limited review performed throughout the year; and
b. internal audit observations in executing consulting service activities in various operations within PIDM, mainly through involvements in projects, management and working committees' meeting and discussion sessions, as well as policy and procedures review exercises.

Mapping of ICF Components and PIDM's Operations

ICF Components	PIDM's Operations
Control environment	• The Board's and Management's tone at the top is demonstrated through the establishment and continuous review of the Board-approved charters, frameworks, and policies. • The expectations of the Board and Management are expressed through the establishment of codes of conduct, which are continuously reviewed and updated to cultivate a strong governance, risk management and internal control culture. • There is adequate segregation of functions and proper assignment of authorities and responsibilities. • Human capital frameworks, policies and practices are established and continuously reviewed to attract, employ, develop and retain competent individuals. • Internal control responsibilities are embedded into structures and taken into consideration when evaluating and deciding on employees' performance and rewards.

ICF Components	PIDM's Operations
Risk assessment	• A corporate-wide risk assessment is performed annually to identify, assess and respond to key risks faced by PIDM in meeting its mandate and objectives. • The risks identified will then form the basis for the formulation and prioritisation of initiatives and action plans, which include financial resources planning, to be implemented in order to meet the short and long-term objectives of PIDM. In addition, these risks are considered in formulating the internal audit's annual risk-based assurance plan. • Control processes are in place to ensure compliance with laws and regulations, and that applicable standards are met in accordance with PIDM's risk appetite.
Control activities	• Controls are incorporated in policies and procedures, which are developed, implemented and reviewed on a regular basis to mitigate risks and achieve set objectives. • The IT Governance Framework and the IT Steering Committee provide Management with an oversight of all IT initiatives and activities. • Adequate and robust business continuity and disaster recovery plans and infrastructure are in place. • The adequacy and effectiveness of PIDM's governance, risk management and internal control practices are assessed and validated by the independent internal audit function based on a risk-based assurance plan approved by the Board annually.
Information and communication	• Establishment of structures, methods and approaches to ensure that information is provided to the right employees in a timely manner with sufficient detail to enable them to carry out their roles and functions effectively and efficiently. • Awareness sessions are conducted to communicate key policies and various codes of conduct to employees. • The Corporate Enterprise Portal enables access to corporate-wide information and facilitates secure and effective information sharing across PIDM. • Policies and procedures relating to external parties as well as corporate publications are published and made available in digital format. • The National Audit Department performs an annual financial audit as well as a management audit (Accountability Index audit) based on an agreed interval.
Monitoring activities	• The progress of corporate and divisional initiatives and the utilisation of financial resources are continuously monitored through scorecard reporting, with regular updates provided to the Audit Committee and the Board. • The results of internal and external audits and reviews are evaluated and communicated to responsible parties, including senior management and the Board, as appropriate. Management continues to be responsive to the internal and external auditors' recommendations in maintaining an effective internal control system.

Review of PIDM's Compliance with Laws and Internal Controls for 2020

Management carries out an annual review of PIDM's compliance with internal controls via an annual compliance certification exercise, where all heads of divisions are required to submit their certification of compliance with relevant laws and internal policies for areas under their purview. For the year under review, the results of the assessment of internal controls indicate that overall, Management has ensured that sound internal controls have been established.

Internal Controls Updates for 2020

In responding to the current global COVID-19 pandemic, Management has proactively implemented measures, based on its business continuity management and plan, to ensure the safety and security of employees, the continuity of its operations, the safeguard of critical and confidential information, and effective internal and external communications. Management has also ensured that these measures are implemented in line with the Movement Control Order, regulations, and standard operating procedures issued by the National Security Council and Ministry of Health, the guidelines provided by the Department of Occupational Safety and Health, and the recommendations issued by the World Health Organisation. Steps have been taken to continuously re-evaluate risks to ensure relevance and that the corresponding controls are being assessed to ensure effectiveness. An independent assessment on the business continuity management processes and practices was carried out to validate the effectiveness of controls.

In view of the dynamic nature of information, information technology and cybersecurity related risks, which have been further escalated by the global COVID-19 pandemic, Management has strengthened its governance structure to safeguard its information asset, by establishing a dedicated information management and security office (IMSO). IMSO acts as the second line of defense, to ensure effective implementation of information management and information security related control processes and practices. Management has also formulated plans to elevate PIDM's cybersecurity posture based on the results of a cybersecurity maturity level assessment which was carried out by an independent external assessor.

A Quality Assessment Review (QAR) was carried out to assess the effectiveness of the internal audit activity performed by PIDM's internal audit function. A QAR helps organisations enhance the effectiveness, quality and value received from their internal audit function. PIDM's internal audit function obtained a general conformance rating, confirming that its internal audit activity conforms to the requirements of the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

Conclusion on Internal Controls

For 2020, based on the assessment performed by the internal audit on the state of internal controls, there were no reported incidents of significant weaknesses or deficiencies in the adequacy and integrity of risk management and internal controls embedded in PIDM's systems, policies, practices and processes. For the work performed in relation to internal controls, refer to the summary report of the Audit Committee's key areas of work in the Statement on Governance at https://www.pidm.gov.my/en/pidm/corporate-governance/governance-reports/.

THE BOARD'S REVIEW OF THE SYSTEM OF RISK MANAGEMENT AND INTERNAL CONTROL

The Board reviewed the effectiveness of PIDM's systems, policies, practices and processes based on the reports from the Board Committees and Management, and its review included the following:

a. The Board considered the reports of the Board Committees on a regular basis. These included the Audit Committee's report on the review of PIDM's financial statements; its compliance with laws and ethics; the effectiveness of controls embedded in systems or processes audited by the Audit and Consulting Services (ACS) Division; the report from the Remuneration Committee on PIDM's compliance with key human capital policies and related laws; and the report from the Governance Committee on PIDM's compliance with key governance policies.

b. The Board considered, on a semi-annual basis:

- PIDM's financial reports, including the utilisation of resources, compared to the approved budget; and
- the update and progress of Management's overall performance against the approved initiatives and targets in the Corporate Plan, as well as Management's assessment of internal and external factors that may impair the performance of the Corporate Plan.

c. In addition, the views of the Chairman of the Board and Chairman of the Audit Committee were also obtained on the current strength of PIDM's internal control environment.

THE BOARD'S REVIEW OF THE SYSTEM OF RISK MANAGEMENT AND INTERNAL CONTROL

Representations

The Chief Risk Officer (CRO) provides the Board with an annual ERM representation letter confirming that PIDM's risks are being managed and that the relevant policies and ERM process continue to be effective and relevant. An annual ERM representation letter from each head of division is also provided to the CRO to confirm that each Division's risks are being managed and that the Division meets the Board's expectations with regard to the Division's responsibilities in mitigating the risks as well as to instil Management accountability.

The effectiveness of PIDM's internal controls as at 31 December 2020 has been assessed by Management via compliance assessment and where applicable, validated by the ACS Division through its planned audit and consultancy engagements. The Chief Internal Auditor (CIA) provides an annual representation letter to the Audit Committee and the Board, which sets out the assessment results on PIDM's system of internal controls that cover the areas in the ACS Division's risk-based assurance plan. These include those pertaining to PIDM's financial management and reporting, i.e., the controls that support the preparation of the financial statements and verify the accuracy and validity of the financial statements as at 31 December 2020.

The CIA and CRO report functionally to the Board through the Audit Committee and administratively to the CEO, and have unrestricted access to the Audit Committee and the Board. This ensures their independence and ability to fulfil their responsibilities effectively. There are seven (7) personnel in the ACS Division and to the Board's knowledge, the personnel are free from any relationships or conflicts of interest that could impair their objectivity and independence.

Based on these assessments and the effectiveness of PIDM's frameworks, systems, policies, processes and procedures that have been implemented and maintained, the Board is of the view that a sound system of risk management and internal control has been established and maintained.

This Statement is approved by the Board on 25 February 2021.