STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL FOR THE YEAR ENDED 2021[1]

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.

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.

[1] *As at 24 February 2022*

RISKS FACTORS

The COVID-19 pandemic global public health crisis continues to impact countries worldwide. Whilst there was massive uncertainty and panic 12 months ago, much progress has been achieved in managing this crisis. With vaccinations to combat the virus, countries are looking to inoculate their populations, rein in the spread of the virus and begin loosening restrictions and reopening their economies. However, uncertainty still lingers, as infection continues to increase sporadically, driven by the various mutated variants of the virus. Malaysia is now seeking to hold back and control any surge in COVID-19 cases through further inoculation of its population with a third dose booster vaccination shot. Hence, COVID-19 remains the biggest risk factor affecting our operating environment.

The remote as well as hybrid working arrangements, put in place since the COVID-19 pandemic, increased the areas of exposure and vulnerabilities for cyberattacks on PIDM. This will continue to remain as a threat as we move further into the digital environment.

PIDM also recognises the importance of employees' mental health, well-being and productivity during this period of remote and hybrid working arrangements.

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

2021 RISK RATINGS

The current COVID-19 pandemic and the impact that it continues to have on PIDM's operating environment remain a major component in the assessment of risks. A lot has been learned about the pandemic, and whilst we have made progress in combating its impact, it is now apparent that recovery from COVID-19 is going to be long-drawn, especially with the emergence of the Omicron variant and the potential for future variants to appear. The working environment has as a result pivoted towards a more cyber and digital landscape.

The table below summarises the results of the risk assessment activities performed by Management in 2021.

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 despite volatility in the financial markets, PIDM continues to hold primarily short to medium term Government securities that are held to maturity and no changes are expected to its investment objectives. There was also no indication of any material events that would significantly disrupt PIDM's ability to meet its operational financial obligations.

Risk Category and Definition	Assessment of Risk Areas
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.	With the working environment pivoting towards a more cyber and digital landscape, the main areas of risk within this category relate to cybersecurity and information security, whilst employees' health and security continue to be of concern. Operational Risk is assessed to be on an 'Increasing' trend in view of the shift towards a more cyber and digital working environment, coupled with data that indicates an increase in cyberattacks and attempted data mining.
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 public health and economic crisis caused by the COVID-19 pandemic continues unabated and uncertainties remain as to whether this challenging outlook will have an impact on the safety and soundness of PIDM's member institutions ("MIs"). It is also now apparent that recovery from this pandemic will be long-drawn, with many disruptions anticipated due to the emergence of new variants. Insurance Risk is assessed to be on a 'Stable' trend as although the current economic environment remains uncertain, PIDM's MIs have adequate capital and liquidity buffers to withstand stressed scenarios. Nevertheless, PIDM continues to heighten 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.	The current COVID-19 pandemic operating environment caused PIDM to shift its approach in building stakeholder relations and creating awareness. PIDM continues to leverage on social media and explore other approaches to engage with stakeholders. Reputation Risk is assessed to be on an 'Increasing' trend as the ongoing uncertainties due to COVID-19 continues to cause the public in general to be more anxious about the future outlook. Also the shift in moving its awareness initiatives onto social media platforms continues to expose PIDM to unverified and inaccurate information or negative public sentiment.

Risk Category and Definition	Assessment of Risk Areas
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 take the necessary steps to respond, adjust and adapt to the evolving situation by continuously reviewing the current initiatives to ensure that they remain relevant in light of the changing environment. 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. The impact of the protracted remote working arrangement on the performance, productivity, stress levels and mental health of employees also continues to be a concern to PIDM. 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 2021, PIDM reviewed its earlier approaches from 2020 and revised and adapted these further in light of the shift towards a more cyber and digital operating and working environment. 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 ahead, we expect the global and domestic economy to continue to recover. The ongoing vaccination drive, the advent of antiviral treatments, and more widespread and cheaper testing availability will help countries stay ahead of the virus, keep severe cases in check, and allow the economies to remain open more sustainably. However, uncertainties remain over the path of the virus, its variants, and the impact on businesses and households. The unwinding of accommodative policies globally puts financial markets at risk of higher volatility. Intensifying supply-chain constraints, coupled with ongoing geopolitical and trade tensions, will weigh on global growth. Overall, the Malaysian economy is poised to recover in 2022, but the balance of risks remains tilted towards the downside.

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 is independent of Management and has oversight over the establishment and implementation of internal controls. • The Board's and Management's tone at the top and expectations are expressed through the establishment and regular review of Board-approved codes of conduct, charters, frameworks, and policies. This helps cultivate a strong governance, risk management and internal control culture. • An annual assessment is conducted to evaluate the effectiveness of the Board and the Board Committees. • Structures, reporting lines, and appropriate authorities and responsibilities have been established with the Board's oversight. This includes the evaluation and decision on employees' performance and rewards in carrying out PIDM's mandate and achieving its objectives.
Risk assessment	• PIDM specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to the objectives. • The Risk Appetite Statement, ERM Policy and ERM Procedures are established as a mechanism for the identification and assessment of risks affecting PIDM. • 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. • Robust business continuity and disaster recovery plans and infrastructure are in place and are reviewed regularly.

ICF Components	PIDM's Operations
Control activities	• PIDM selects and develops control activities to mitigate risks in achieving PIDM's objectives to acceptable levels as well as to ensure compliance with laws, regulations, and applicable standards. • 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. • 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, whether obtained externally or internally, 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. • Information relating to the objectives as well as expectations on accountability and responsibilities for internal control is communicated to internal as well as external stakeholders. • 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.
Monitoring activities	• The progress of corporate initiatives and the utilisation of financial resources are continually monitored 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. • The results of risk identification and assessment are reported to the ERM Committee as well as senior management and the Board. • Operational policies and procedures are reviewed and updated as and when there are changes in the respective processes or at specified intervals. • The Communications and Public Affairs Division has a process to monitor mentions about PIDM from external parties as well as to formulate follow-up actions, if required. • The National Audit Department performs an annual financial audit.

REVIEW OF PIDM'S COMPLIANCE WITH LAWS AND INTERNAL CONTROLS FOR 2021

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 2021

In continuing its efforts to respond to the global COVID-19 pandemic, Management has 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 ensured the alignment of these measures with the relevant government regulations required under the Movement Control Order and the 4-phased National Recovery Plan, the 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 continually re-evaluate risks to ensure relevance and that the corresponding controls are being assessed to ensure effectiveness.

During the year, PIDM obtained the Information Security Management System (ISMS) ISO/ IEC 27001 certification to elevate its cybersecurity posture as well as to strengthen its governance, risk management and control processes on information management. PIDM has strengthened its governance structure with the establishment of the Information Governance and Security Management Committee, and a comprehensive and holistic risk assessment on information, information technology and cybersecurity related risks. This has resulted in changes to key strategic and operational policies, processes, practices and tools, which are effective in mitigating relevant evolving risks impacting PIDM's information and information assets.

A Quality Assessment Review (QAR) is carried out periodically 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 conforms to the requirements of the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

CONCLUSION ON INTERNAL CONTROLS

For 2021, 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 www.pidm.gov.my.

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 and reviewed by the Audit and Consulting Services ("ACS") Division; the report from the Human Capital and 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 STATEMENT ON 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 2021 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 2021.

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 five (5) 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 24 February 2022.