

## STATEMENT ON SHARIAH GOVERNANCE FOR SIMPANAN SHARIAH

### SAC HONORARIUM AND ALLOWANCES

The SAC members are paid a monthly honorarium and allowance for each meeting attended in 2019 as follows:

- (a) Honorarium (per month): RM5,000.00
- (b) Meeting Attendance: RM1,500.00

### ACCESS TO INFORMATION AND DOCUMENTS

To assist the SAC in discharging its functions, the EPF Management provides the SAC access to all necessary information and documents, and the SAC shall safeguard the confidentiality of such information and documents.

### SAC EFFECTIVENESS EVALUATION

The EPF carries out SAC Effectiveness Evaluation to assess the performance of the SAC. The review is carried out once in every two years by an independent professional body.

### SAC ENGAGEMENT WITH THE BOARD AND INVESTMENT PANEL

The SAC is involved in various discussions with the Board and Investment Panel on matters related to Simpanan Shariah.

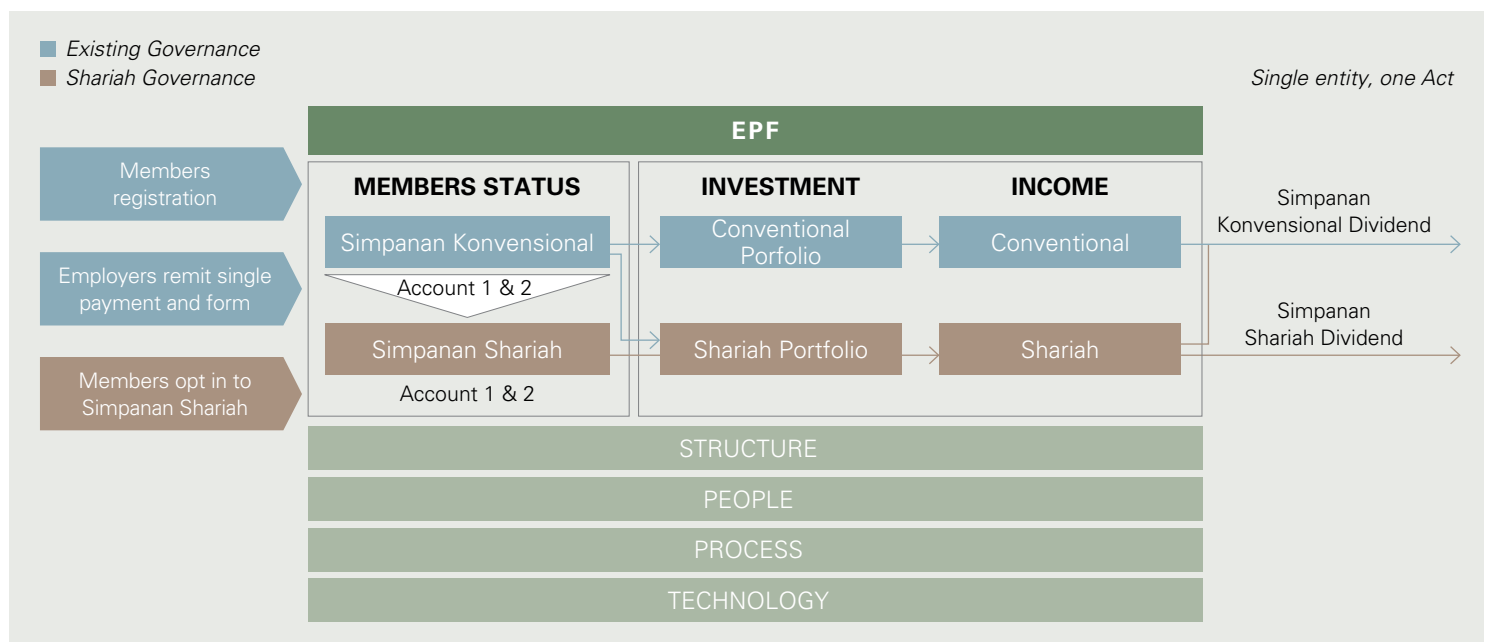
### SAC REPORT

For each financial year, a Shariah Compliance Report in relation to the management of the Simpanan Shariah and approved by the SAC, is presented in the EPF Annual Report.

### SHARIAH POLICIES FOR SIMPANAN SHARIAH

The Shariah governance framework is supported by detailed policies and procedures to ensure that every Shariah-compliant transaction complies with Shariah requirements. The SAC has formulated Shariah policies for Simpanan Shariah with respect to its operations, investment, finance, and treatment of Shariah non-compliant income, which among others are as follows:

#### 1. Operating Model of Simpanan Shariah



## STATEMENT ON SHARIAH GOVERNANCE FOR SIMPANAN SHARIAH

Simpanan Shariah adopts a portfolio-based management model as follows:

- (a) Simpanan Shariah and Simpanan Konvensional co-exist under one fund and managed by the Board.
- (b) EPF members opting for Simpanan Shariah are bound by the *Wakalah* contract, where members agree to appoint the Board as representative and trustee to manage and invest all credit (savings) in members' account in accordance with Shariah principles.
- (c) In addition to the EPF's corporate governance, Simpanan Shariah is also subject to the Shariah governance framework and Shariah policies relating to the operations and investment, as determined by the SAC from time to time.
- (d) The EPF's investment assets are segregated into two portfolios, namely the Shariah portfolio and conventional portfolio. Simpanan Shariah will only invest in the Shariah portfolio.
- (e) Simpanan Shariah leverages on the existing structures, resources, with some enhancement to the legal framework of EPF, operational processes, and IT systems to meet the Shariah requirements as prescribed by the SAC.

### 2. Shariah-compliant Investment

In addition to ethical investment practices, which prohibits from investing in sectors that manufacture and promote alcohol, gambling, adult entertainment, tobacco and military weapons, among others, all EPF's investment assets will undergo Shariah screening process based on Shariah criteria and guidelines set by the SAC. These serve to eliminate Shariah non-compliant elements such as *riba* (interest/usury), *gharar* (uncertainty in contract), *maysir* (gambling), and other prohibited elements such as non-halal goods and services.

Shariah policies on compliance and monitoring aspects of EPF's Shariah investments have also been set out by the SAC, and the policies will be updated from time to time.

As at 31 December 2019, 37.1% or RM342.96 billion of the EPF's investment assets are Shariah-compliant. As Simpanan Shariah members' savings balance is smaller than the total

EPF's Shariah-compliant investment assets in the Shariah portfolio, both Simpanan Shariah and Simpanan Konvensional will jointly invest in the Shariah portfolio. The Shariah income derived from the Shariah portfolio is allocated to Simpanan Shariah in proportion to its share in the said portfolio.

### 3. Reclassification Of Shariah-compliant Investment

The EPF's investments in both listed and private equities, real estates, and infrastructure are subject to periodic Shariah screening to review the Shariah compliance status of such investments.

For listed equities, Shariah classification will be reviewed periodically based on Shariah screening conducted by the Shariah Advisory Council of the Securities Commission Malaysia (SAC SC) for the domestic market and the relevant Shariah index providers subscribed by the EPF for global markets.

Shariah screening for investments in private equities, real estates, and infrastructure, will be conducted internally on an annual basis based on Shariah screening criteria and guidelines set by the SAC.

If any of the above investments fail the Shariah screening, the investment will be reclassified as Shariah non-compliant and will be transferred to the conventional portfolio.

Similarly, if any of the above investments in the conventional portfolio passed the Shariah screening, the investment will be reclassified as Shariah-compliant investment and will be transferred to the Shariah portfolio.

For Shariah mandates managed by external fund managers, any Shariah-compliant instruments being reclassified as Shariah non-compliant will be disposed of in accordance to the guidelines set by the SAC SC.

### 4. Treatment Of Shariah Non-compliant Income

In 2019, the Shariah non-compliant income was mainly derived from the late payment charges imposed on employers for late contributions; and the excess gain due to reclassification of Shariah-compliant equities into Shariah non-compliant equities.

## STATEMENT ON SHARIAH GOVERNANCE FOR SIMPANAN SHARIAH

The late payment charges and/or dividends are imposed on employers and other parties for late payment of contributions and/or any financial obligation due and payable to the EPF, to safeguard the interest of members.

With regards to the Simpanan Shariah, the SAC allows the charges to be imposed as deterrent and penalty to defaulters either in the form of *ta'widh* (compensation) or *gharamah* (penalty at the rate above the *ta'widh* rate). The *ta'widh* amount as endorsed by the SAC, may be recognised as Shariah-compliant income, while any excess amount will be recorded as Shariah non-compliant income.

Any transactions suspected to be Shariah non-compliant will be reported to the SAC to determine the Shariah status of the transactions, including any income therefrom.

The SAC had resolved that the Shariah non-compliant income can only be utilised for allowable expenses through charitable activities, such as payment of statutory charges (death benefit, incapacitation benefit and invocation cost), and any excess Shariah non-compliant income (if any) may be utilised for operating expenditure and indirect investment expenditure.

For the financial year ended 31 December 2019, total Shariah non-compliant income was RM41.92 million and had been utilised for members' welfare through payment of statutory charges.

## 5. Dividend

The dividend policy for Simpanan Shariah is presented to the SAC for deliberation and Shariah endorsement.

The annual dividend of the Simpanan Shariah is based on the actual performance of the EPF's Shariah-compliant investments in the Shariah portfolio, i.e. realised Shariah-compliant investment income and non-investment income, after netting off expenses, allocated to Simpanan Shariah in proportion to its share in the Shariah portfolio.

Simpanan Shariah dividend declared by the Board for the financial year ended 31 December 2019 was 5.00%.

## 6. Dividend Purification

Muslim members who have opted for Simpanan Shariah, are exempted from the requirement to purify EPF dividends received prior to the offering of Simpanan Shariah, i.e. EPF dividends for financial year 2016 and earlier. Furthermore, any Simpanan Konvensional dividend credited to a member's account after switching to Simpanan Shariah (as the Simpanan Shariah account had not yet been in force) are also exempted from purification, as the member has no right to determine the effective date of the Simpanan Shariah account.

The Special *Muzakarah* of the *Fatwa* Committee of the National Council for Islamic Religious Affairs Malaysia, held on 18 August 2015, had also resolved that EPF is not obliged to purify dividends on EPF savings for all members who opted for Simpanan Shariah.

However, for Muslim members who recently chose to convert their account to Simpanan Shariah, they are advised to purify Simpanan Konvensional dividends as per resolution of the 87th *Muzakarah* of the *Fatwa* Committee of the National Council of Islamic Religious Affairs Malaysia, held on 23-25 June 2009:

*"In Islam, property acquired by means that are not Shariah-compliant, such as usury, ambiguous transaction, gambling, fraud, robbery, plunder, corruption, etc is illegal and cannot be used for personal gain and benefit and must be cleansed through the following methods:*

- (a) channeled to Baitulmal for the general public interest of Muslims such as for funding the construction or maintenance of bridges, roads, toilets, etc; or*
- (b) given to the poor."*

The purification rate for Simpanan Konvensional dividend 2019 is 71% of the total dividends credited to member's account.

# SHARIAH ADVISORY COMMITTEE REPORT

**In the name of Allah, the most Beneficent, the most Merciful.**

**All praise be to Allah and peace be upon the Prophet Muhammad, his family, his companions, and those who followed them.**

We, members of the Shariah Advisory Committee of EPF (SAC), have reviewed the operations and investment of the EPF in relation to Simpanan Shariah for the year ended 31 December 2019, to form an opinion as to whether the scheme has complied with Shariah principles and rulings made by us on all Shariah-related matters. We hereby submit our report for the financial year ended 31 December 2019:

- (a) We have advised the Board and Investment Panel on all Shariah-related matters presented to us by the EPF Management through the Shariah decision made by the SAC, in relation to the operations and investment of Simpanan Shariah, to ensure compliance with Shariah principles as well as the relevant local and global Shariah resolutions and standards as recognised by us.
- (b) The EPF Management is responsible for ensuring that Simpanan Shariah is managed in accordance with Shariah principles by referring to the SAC for advice on any Shariah-related matters and implementing all Shariah rulings and policies set forth by the SAC.
- (c) In advising the EPF on Shariah-related matters, we have obtained all information and explanation from the EPF Management which we consider necessary to form any Shariah rulings. The EPF Management has also arranged for the SAC to visit selected EPF's Shariah-compliant assets.
- (d) We are also supported by the Shariah research and advisory as well as Shariah monitoring and review functions in the day-to-day oversight of Shariah compliance of Simpanan Shariah. In addition, the internal audit evaluates the internal control system and compliance with policies and procedures advised by the SAC, on a regular basis.
- (e) For the financial year ended 31 December 2019, there were 13 SAC meetings held to discuss the following:
  - (i) Shariah screening and issues relating to proposals on Shariah-compliant investment and the existing investment of the EPF, including relevant documents;
  - (ii) Shariah issues relating to the operations of Simpanan Shariah, including the implementation of online Simpanan Shariah via i-Akaun mobile application;
  - (iii) Research on Shariah matters carried out by the Shariah Services Section;
  - (iv) Updates on the Shariah governance framework and Shariah compliance policies and guidelines relating to the investment and operations of Simpanan Shariah, including financial reporting and dividend policy; and
  - (v) Reports on the reclassification of Shariah-compliant investments and Shariah non-compliant income.
- (f) We have also received and deliberated on the Shariah review reports that were presented by the Shariah Services Section on a quarterly basis as per the Shariah monitoring and review plan for 2019, approved by us. This was done for the purpose of continuous assessment on the degree of Shariah compliance of Simpanan Shariah with regards to annual Shariah screening of EPF holdings in alternative investment and initial public offering (IPO) and treatment of non-compliant income.

## SHARIAH ADVISORY COMMITTEE REPORT

- (g) The Internal Audit Department has performed reviews on the operation and investment activities in relation to Simpanan Shariah. Result of the reviews were communicated to the EPF Management and reported to the Board Audit Committee. The Internal Audit Department is continuously monitoring the findings to ascertain action is being taken to resolve the audit observations. The SAC was informed about the audit observations and status of actions taken.
- (h) We acknowledge that appropriate efforts have been taken to rectify the gaps identified, and management actions are taken to prevent similar gaps from recurring.
- (i) In our opinion:
- (i) The contracts, transactions and dealings entered into by the Board in relation to Simpanan Shariah throughout the financial year ended 31 December 2019 that we have reviewed, are in compliance with Shariah principles;
  - (ii) The allocation of profits and losses relating to Simpanan Shariah as disclosed in Note 34.3 to the Financial Statements conforms to the basis that had been endorsed by us in accordance with the Shariah principles; and
  - (iii) All income earned by Simpanan Shariah from sources or means prohibited by the Shariah principles amounting to RM41.93 million as disclosed under Note 34.4 to the Financial Statements have been used for charitable activities such as payment of death benefit, incapacitation benefit, and invocation cost.

We, members of the SAC, hereby confirm that Simpanan Shariah for the financial year ended 31 December 2019 has been managed in conformity with Shariah principles.

On behalf of the SAC,



NAME : **PROF. DR MOHAMAD AKRAM BIN LALDIN**  
TITLE : CHAIRMAN OF THE SAC  
DATE : 1st June 2020

On behalf of the SAC,



NAME : **ASSOC. PROF. DR. AZNAN BIN HASAN**  
TITLE: : DEPUTY CHAIRMAN OF THE SAC  
DATE : 1st June 2020

# STATEMENT ON RISK MANAGEMENT

**Uncertainties about the effects or implications of any one activity (internal or external), coupled with geopolitics, economic slowdown, change in political landscape, and any form of pandemic, requires the understanding of new risks to strengthen EPF's existing risk management process. Exercises like Scenario Analysis/Impact Assessment remain worthwhile to rationally assess some of the new uncertainties. Continuous strengthening of the organisation's governance structure, internal controls, and risk management framework are also key to address additional risks, if any.**

## OVERVIEW

2019 proved to be another challenging year for the EPF with changes in the political landscape, weak ringgit, and economic slowdown contributing to the market volatility that led to various events, which continue to shape the economic, financial, and risk landscape. Acknowledging this, the EPF continues to strengthen and enhance its robust risk management system to remain relevant and resilient ahead of the changing risk landscape to ensure that risks are managed effectively within the organisation.

## THE RISK MANAGEMENT STRUCTURE

The EPF's risk management structure provides clear lines of responsibility and accountability for the risk management processes and outlines the principal risk management and control responsibilities. The EPF Board and Investment Panel oversee the organisation's overall risk management, and are assisted by the Board Risk Management Committee (BRMC) and Investment Panel Risk Committee (IPRC) to oversee all operational risk management activities, recommend the risk appetite, and allocate the risk budget.

## STATEMENT ON RISK MANAGEMENT

**EPF BOARD**

The EPF Board is responsible for the overall organisation's risk management, except for activities related to investment decisions.

**INVESTMENT PANEL (IP)**

The IP is responsible for overseeing risk management pertaining to the EPF's investment decision-making, and defines the level of risks that the EPF is willing to tolerate through its Risk Appetite Statements, which form the basis of fund allocation for investment.

**BOARD RISK MANAGEMENT COMMITTEE AND INVESTMENT PANEL RISK COMMITTEE****BOARD RISK MANAGEMENT COMMITTEE (BRMC)**

The BRMC is responsible for assisting the Board in overseeing all operational risk management activities, except for activities pertaining to making investment decisions, and ensuring that the risk management process is in place and functioning effectively.

**INVESTMENT PANEL RISK COMMITTEE (IPRC)**

The IPRC is responsible for assisting the IP in recommending the risk appetite and appropriate allocation of risk budget. The IPRC is delegated with the responsibility to review and approve appropriate risk measurements, policies, processes, and limits to ensure their continued effectiveness.

**DEDICATED COMMITTEES****MANAGEMENT OPERATIONS RISK COMMITTEE (MORC)**

The MORC oversees, implements, and executes the EPF's operational risk management (which includes strategies, culture, structure, people, and processes) and to ensure that the risk management framework is implemented effectively throughout the organisation.

**INVESTMENT SERVICES DEPARTMENT (ISD)**

The ISD department is responsible for monitoring and compliance of all investment-related risk policies and limits.

**MANAGEMENT RISK COMMITTEE (MRC)**

The MRC is responsible for developing and reviewing risk policies and appropriate limits for managing the EPF's investment risks.

**DIVISIONS, DEPARTMENTS AND BRANCHES**

All divisions, departments, and branches are responsible for managing risks in their respective functions on a day-to-day basis, as well as for escalating significant potential risks to the MORC via the RMD. Among the principal roles and responsibilities of these divisions, departments and branches are:

**MANAGEMENT INVESTMENT COMMITTEE (MIC)**

The MIC is responsible for evaluating and recommending investment proposals to the IP. It also evaluates and recommends investment strategies and performance of external fund managers.

- (a) Identify, assess, and manage risks;
- (b) Constantly review their risk profiles to ensure relevancy and appropriateness;
- (c) Update the risk status and level of risk management and controls;
- (d) Develop and implement action plans to manage risks; and
- (e) Adhere to risk management practices and guidelines

**RISK MANAGEMENT DEPARTMENT (RMD)**

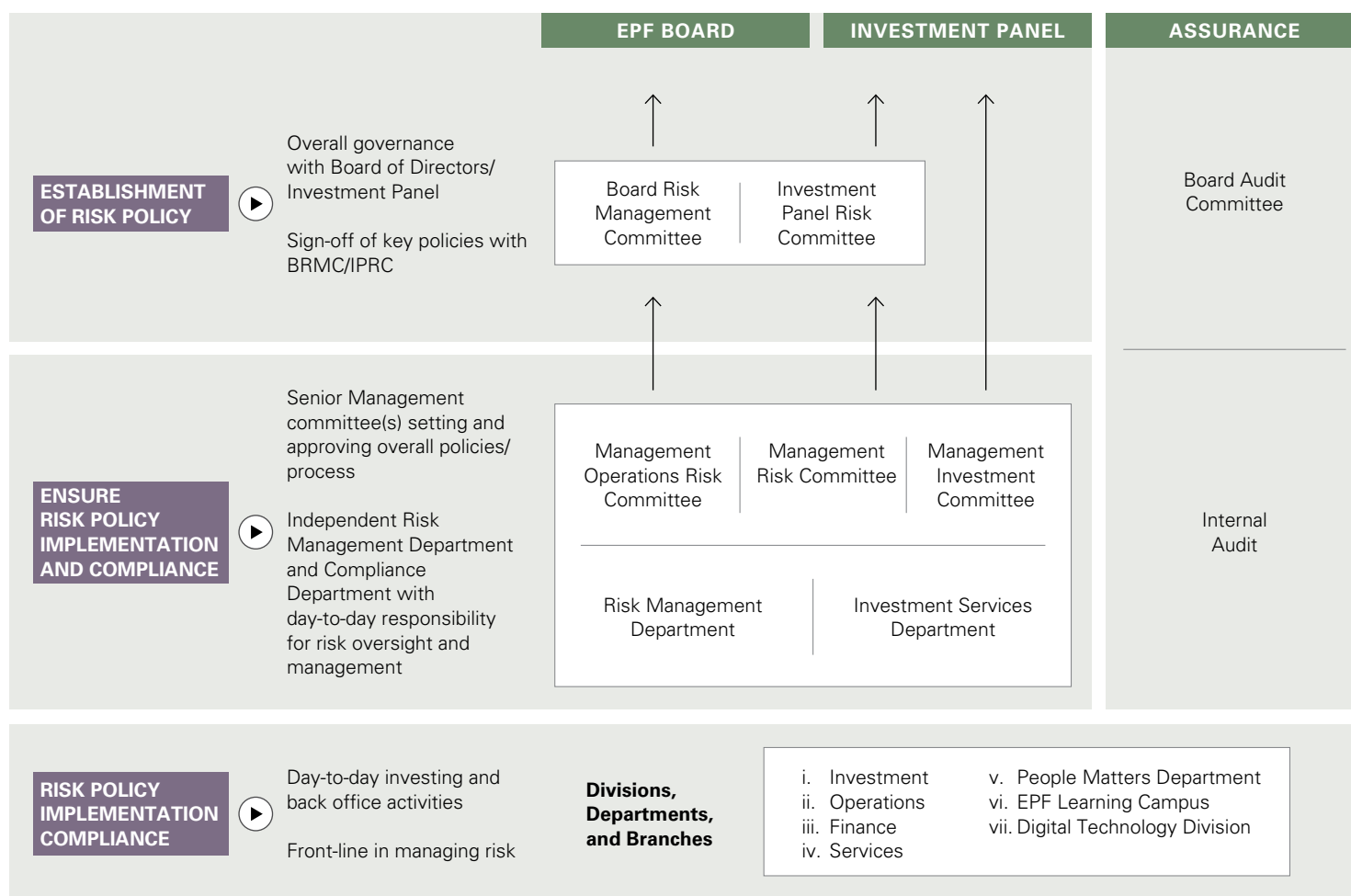
The RMD supports the MIC, MRC, MORC, IPRC, BRMC, and IP in all risk management matters covering investment risk, operational risk, risk measurement, independent assessment, and the monitoring and reporting of risk exposures.

## STATEMENT ON RISK MANAGEMENT

### RISK MANAGEMENT GOVERNANCE

The EPF believes that a strong governance structure is important to ensure an effective and consistent implementation of risk management throughout the entire organisation. In achieving that, the EPF's risk governance places accountability and ownership between three lines of defence where departments, branches, and the Management constantly engage in healthy and productive discussions on key risk matters and processes, thus creating a robust risk-practising culture. To further support its risk governance structure, the EPF has also developed structured policies and procedures to address all key risk areas in the organisation.

The EPF Risk Governance Structure consists of three lines of defence as shown below:



### RISK APPETITE

The EPF's risk appetite defines the amount, level, and type of risk that the EPF is able and willing to accept in pursuit of its strategic objectives. It also sets out the level of risk tolerance and limits to govern, manage, and control the EPF's risk-taking activities.

The Risk Appetite Statements in investment define the level of risks that the EPF is willing to tolerate and form the basis of the allocation of funds for investment. The asset allocation is regularly reviewed to ensure that funds are invested within the EPF's risk appetite.

STATEMENT ON RISK MANAGEMENT

ENTERPRISE RISK MANAGEMENT

Operational Risk Management

The Operational Risk Management (ORM) supports and enhances the EPF’s activities in all of its operational areas as ORM is an integral part of the EPF’s decision making process and corporate culture. The four key areas of the ORM are:

- (a) Operational Risk Management Framework
- (b) Operational Risk Management Methodology and Process
- (c) Corporate Risk Scorecard
- (d) Business Continuity Management

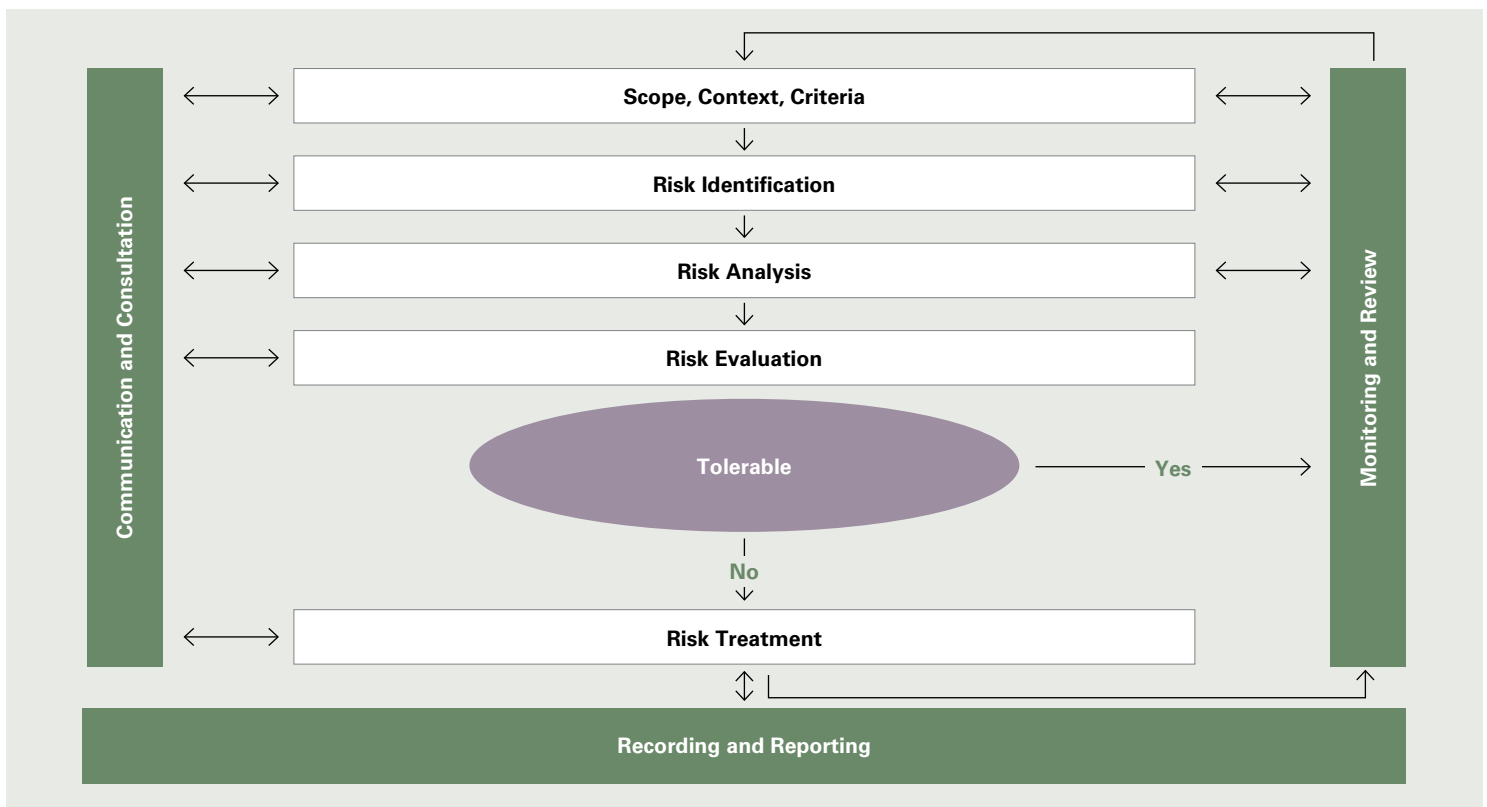
Operational Risk Management Framework

Through the adoption of the ORM framework (MS ISO 31000:2018 Risk Management – Principles and Guidelines) and robust processes, the EPF is able to manage its risks effectively by minimising the impact to an acceptable level. This framework is regularly reviewed to ensure its continuous application and relevance.

Operational Risk Management Methodology and Process

The main elements of the ORM process are as follows:

- (a) **Establishing the context:** Articulates the organisation’s objectives, and defines the external and internal parameters to be taken into account when managing risks.
- (b) **Risk assessment:** The overall process of risk identification, risk analysis, and risk evaluation.
- (c) **Risk treatment:** Actions to be taken to prevent, detect, or manage the Net Risks to an acceptable level.
- (d) **Communication and consultation:** The two-way communication between Risk Management Department and stakeholders about the existence, nature, form, severity, or acceptability of risks.
- (e) **Monitoring and review:** Both activities are planned and are an integral part of the risk management process that involve regular checking or surveillance.
- (f) **Recording and reporting:** Risk management process where risks, its details, and minutes of meetings are recorded and reported periodically.



## STATEMENT ON RISK MANAGEMENT

### Corporate Risk Scorecard (CRS)

The CRS methodology incorporates the Risk and Control Self-Assessment (RCSA) module which allows employees to self-assess and update their risk profiles. The CRS is implemented through the Operational Risk Management (ORM) System that records the ownership and details of risks, controls, management actions, and incorporates changes to the risk scorecard. All business units use the risk scorecard as a tool to manage their risks effectively.

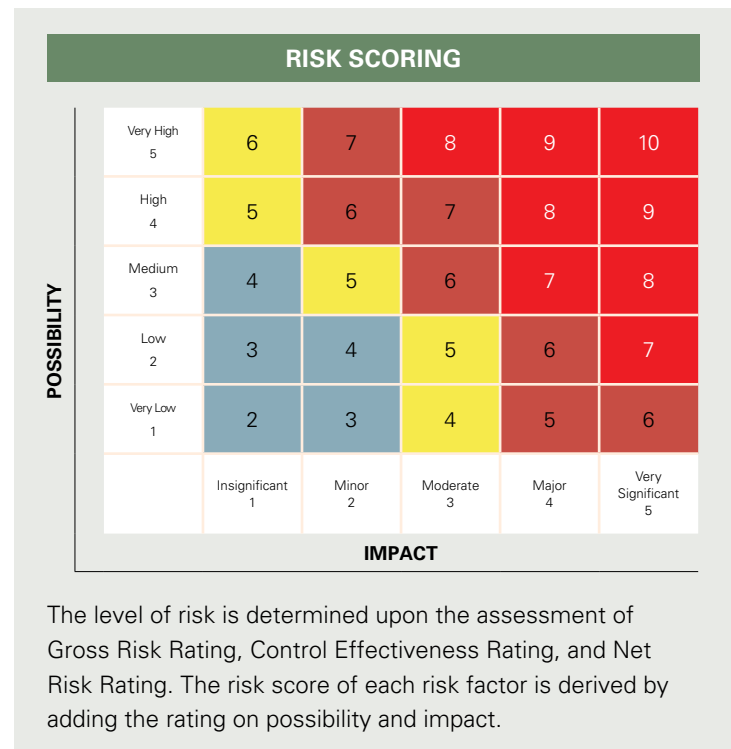
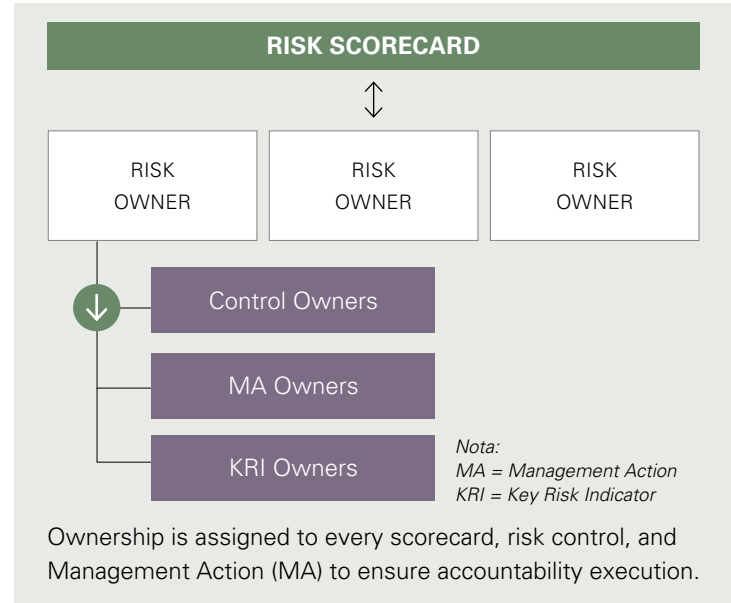
Access to the ORM system is provided on an enterprise-wide basis so that all Risk Scorecard Owners, Risk Owners, Control Owners, and Management Action (MA) Owners can undertake RCSA activities effectively. A total of 107 risk scorecards were established in 2019, comprising risk scorecards for C-Suites – Chief Executive Officer, Deputy Chief Executive Officer, Chief Investment Officer, Chief Strategy Officer, Chief Financial Officer, Chief Digital Technology Officer, 33 departments, and 68 branches. Risks in the EPF are monitored and managed through ownership from the line management, and the assurance process is implemented through the Corporate Digital Assurance (CDA) process.

Owners of scorecard, risk, control, and MA are required to provide digital assurance four times a year to the Management to give assurance that they have been managing risks within their risk profiles appropriately.

Key Risk Indicators (KRIs) identified in the risk scorecards act as an early warning system, enabling the EPF to monitor potential risks before they escalate into serious concerns.

The Risk Management Department reports and highlights risk management related issues in the Management Operations Risk Committee (MORC), Board Risk Management Committee (BRMC), and the EPF Board for their information and/or decision making on a periodic basis.

The methodology, which underlies our Corporate Risk Scorecard, is shown in the chart below:



STATEMENT ON RISK MANAGEMENT

**BUSINESS CONTINUITY MANAGEMENT (BCM)**

The implementation of BCM in the EPF is based on these three components:

(a) **Human Resource Readiness**

This refers to the development of knowledge and skills in managing disasters. The implementation is carried out through awareness trainings, tutorials, walkthroughs, call trees, crisis simulation exercises, and BCM i-learning.

(b) **Infrastructure Readiness**

The system and equipment at the disaster recovery centre are tested to ensure optimal readiness and functionality in the event of a disaster, and that the infrastructure is adequate, to cater to the business continuity activities.

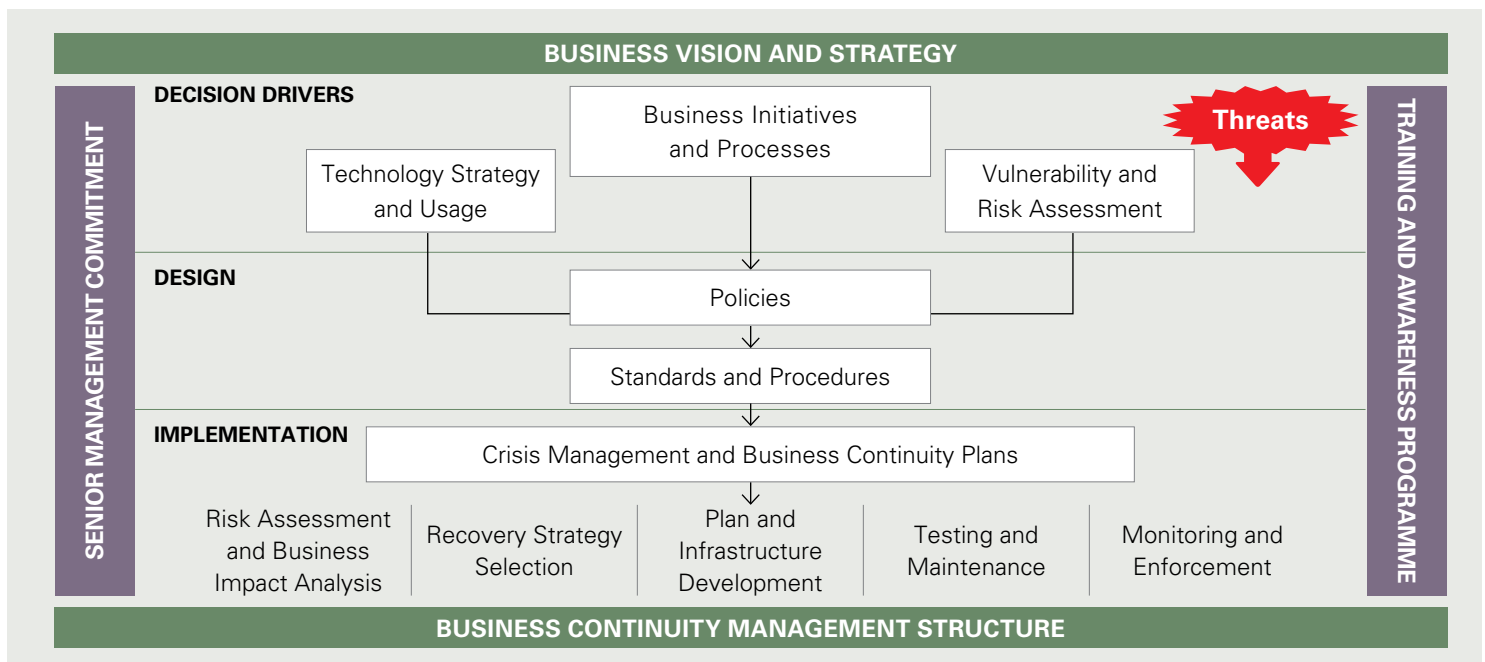
(c) **Plan Readiness**

The Business Continuity Plan (BCP) is regularly updated, based on current work functions, to ensure organisational readiness at all times. It applies to all departments and branches in EPF.

To ensure the EPF’s readiness in facing disasters, unrehearsed crisis simulation exercises are conducted at selected branches annually. In 2019, one crisis simulation exercise was carried out to evaluate the branch’s readiness in scenarios such as handling riots, fire, chemical leakages, cyber-attacks, together with the appropriate communication and relocation to the recovery site. The evaluation of the exercise and key recommendations were presented to the Board and Management, and also shared among EPF staff for their knowledge and learning.

The BCM Framework serves to develop a well-coordinated and consistent BCP that would allow the EPF to respond effectively to business disruptions, resume essential operations within the required time frame, and minimise the cost of damages and interruptions to business operations as a result of the disaster.

The illustration below shows the components of the EPF’s BCM Framework:



## STATEMENT ON RISK MANAGEMENT

### INVESTMENT RISK MANAGEMENT

There are four key areas of investment risk management:

- (a) Investment Risk Management Framework
- (b) Market Risk
- (c) Credit Risk
- (d) Liquidity Risk

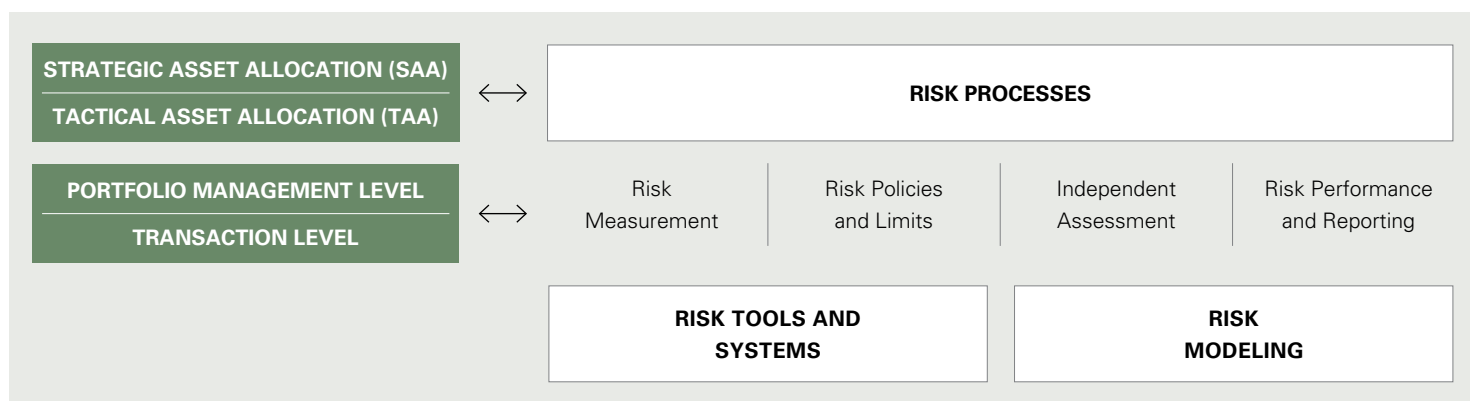
#### Investment Risk Management Framework

The Investment Risk Management Framework governs the EPF's investment processes and ensures that effective risk management

controls and procedures are in place with regards to investment decision-making.

This framework provides an approach to managing and anticipating both existing and potential risks arising from the EPF's investment portfolio, and enables the EPF to have a structured process to measure, assess, monitor, and manage its portfolio risks. This ensures the EPF optimises its returns on risk-taking activities within the risk appetite level as approved by the Board.

The Investment Risk Management framework is illustrated below:



#### Market Risk

Market risk is the risk of loss from changes in the value of portfolios and financial instruments due to movements in interest rates, foreign exchange, and equity prices.

The objective of market risk management in the EPF is to ensure that the risk exposures undertaken by the EPF are within its risk appetite. This is done through an annual review of various policies and limits, periodic reports to monitor market risk at portfolio level for each asset class, and independent validation performed on the underlying risk methodology:

- (a) **Name, ownership, country, and sector concentration limits:** to ensure appropriate diversification of risk exposures.
- (b) **Value-at-Risk (VaR):** a statistical measure of the potential losses that could occur as a result of movements in market rates and prices over a specified time horizon within a given confidence level.
- (c) **Duration:** to manage the sensitivity of the price of a fixed income investment arising from interest rate movement.

- (d) **Tracking error:** a standard deviation of the portfolio's excess returns relative to a benchmark in measuring and benchmarking the performance of the portfolio.
- (e) **Backtesting:** a validation process performed to check the accuracy of the risk methodology used in computing VaR for both fixed income and equity portfolios.
- (f) **Stress testing:** an exercise conducted to capture the potential market risk exposure of 'what-if' scenarios. It incorporates factors such as correlation, volatility, and returns at different levels.

#### Credit Risk

Credit Risk arises when a counterparty's or an obligor's failure to meet its payment obligations results in a loss. EPF's credit risk exposure is in direct correlation towards its investing activities within fixed income instruments, private equity, real estate, and infrastructure asset classes.

The EPF's credit risk management involves detailed credit analysis, in-depth risk assessment methodology, and prudent underwriting

## STATEMENT ON RISK MANAGEMENT

standards. Furthermore, EPF consistently and continuously reviews and updates its risk assessment methodology and credit underwriting standards to ensure consistency with industry or market best practices as well as being at par with other institutional peers.

At the portfolio level, the following credit risk management has been put in place to manage credit risk exposure:

- (a) Credit risk limits and Management Action Triggers (MATs) incorporating minimum broad credit criteria for investment, including name concentration and counterparty exposures;
- (b) Credit portfolio system to measure credit risk of the relevant portfolios using Credit Value-at-Risk (CVaR);
- (c) Periodic review of existing internal credit rating templates for obligors to ensure their relevance; and
- (d) Strong credit awareness or culture across the investment personnel in the EPF through active engagement with the investment personnel at all levels.

At the transaction level, the following credit risk management has been put in place to manage credit risk:

- (a) Independent risk assessment is conducted for every new investment proposal presented to the Management Investment Committee and Investment Panel meetings for decision making;
- (b) Close monitoring of changes to existing investments via assessments on an ad-hoc as well as periodic basis; and
- (c) Credit rating tools to measure the creditworthiness or Probability of Default (PD) of the obligors are as follows:
  - i) **Corporate rating template** which provides internal risk rating for corporate obligors;
  - ii) **Financial institution rating template** which provides internal risk rating for financial institution obligors; and
  - iii) **Credit tool** which measures the Expected Default Frequency (EDF) or Probability of Default (PD) to provide early warning signals for the EPF's close monitoring of respective obligors.

### Liquidity Risk

Liquidity risk relates to the inability of the EPF to meet its financial commitments and obligations when they fall due. The EPF's liquidity risk is limited, as all contributions are mandated by the EPF Act 1991 through the deduction of salaries, and members

are allowed to make withdrawals under the pre-retirement and retirement schemes. The EPF manages its liquidity requirements through:

- (a) Monitoring of its daily cash flow and projecting monthly cash flow on a rolling 12-month basis;
- (b) Allocating 3.00% of its asset's value for short-term instruments in the form of cash and placements in financial institutions in order to meet members' withdrawals and other financial commitments and obligations; and
- (c) Diversifying its investment portfolio by setting the concentration limits on name, sector and asset type.

Over the medium and longer term, the EPF is able to meet its liquidity requirements through its holdings of liquid investments such as publicly traded equities and available-for-sale fixed-income securities. The maturity profile of the EPF's asset and liability is also monitored within a stipulated level. The Group and the EPF's financial liabilities are categorised into relevant maturity groupings based on the remaining period at the Statement of Financial Position date to the contractual maturity date.

### TECHNOLOGY RISK MANAGEMENT

The EPF understands the need to manage technology risk, given the increasing compliance and regulatory requirements in the technology and digital landscape. In this respect, the EPF continues to ensure the necessary technology risk management

The Technology Risk Management (TRM) not only provides technical support and integrates robust investment risk systems to continuously enhance risk analytical and reporting capability within the user community, but also provides independent risk assessments to enterprise-wide IT systems and projects, and recommends effective security controls to mitigate risks for better protection of mission-critical IT systems that store, process, and transmit sensitive information.

It is also a part of the Cyber Security Maturity Programme that monitors and provides assistance from the risk perspective for Information Risk Management and Business Continuity Management.

# STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

**This Statement is in accordance with the Statement on Risk Management and Internal Control – Guidelines for Directors of Listed Issuers (the Guidelines) issued by an industry-led task force supported by Bursa Malaysia and the Securities Commission Malaysia.**

**The Guidelines are also in accordance with Principle B of the Malaysian Code on Corporate Governance issued in April 2017, which states that the Board should establish an effective risk management and internal control framework.**

**It is with the EPF's intention to promote good corporate governance, that this statement outlines our risk management and internal control framework during the year under review.**

## BOARD RESPONSIBILITY

The Board acknowledges its overall responsibility to ensure the adequacy and effectiveness of the EPF's risk management and internal control framework so that the organisation's objectives are achieved.

The framework is designed to identify, analyse and evaluate significant risks, thus providing insights to the Board, which plays a pivotal role as a risk oversight in ensuring these risks are properly mitigated. Accordingly, the internal control system is in place to manage rather than to eliminate those risks. It can, therefore, provide reasonable but not absolute assurance.

In order to effectively carry out the oversight responsibilities, three committees have been established:

- (a) The Board Audit Committee (BAC) on the internal controls, governance processes and risk management, except for risk management activities related to investment decision making;
- (b) The Board Risk Management Committee (BRMC) on the risk management activities, except for activities in making investment decisions; and
- (c) The Investment Panel Risk Committee (IPRC) on investment risk management matters covering risk appetite, risk measurement, policies limits, except for activities involving investment operations.

More information on IPRC is provided in the Statement on Investment Risk Management in this Annual Report.

## Management Responsibility

The Management is responsible for implementing the Board's policies and procedures on risk and control, comprising of these roles:

- (a) Identifying relevant risks in achieving the EPF's objectives and strategies;
- (b) Designing, implementing and monitoring the risk management and internal control framework in accordance with the EPF's strategic vision and overall risk appetite; and
- (c) Identifying changes to risks or emerging risks, taking appropriate action and keeping the Board informed on a timely basis.

## RISK MANAGEMENT AND INTERNAL CONTROL FRAMEWORK

The EPF has in place an effective risk management and internal control framework as part of good corporate governance practice.

It adopts the Three Lines of Defence Model. The first line is represented by departments and branches, which are responsible for establishing a risk control and incorporating all risk controls in their day-to-day operations.

## STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

The second line of defence is represented by the Risk Management Department, which develops the risk management framework, policy, methodologies, and tools for the management of key risks in the organisation.

The Internal Audit Department, being the third line of defence, reviews the key activities of the EPF's businesses, and evaluates the effectiveness and adequacy of the internal control system, operational risk management, and governance processes.

The key systems and processes that the Board has established for the purpose of reviewing the adequacy and effectiveness of the risk management and internal control framework are as follows:

### Risk Management Framework

The Board has adopted an Operational Risk Management (ORM) Framework based on the ISO 31000:2018 Risk Management – Guidelines, which outlines the principles, policies, and processes in managing the EPF's enterprise risks.

Clear lines of responsibility and accountability has been established for the risk management process. The principal risk and control responsibilities under the risk management structure comprise of:

- (a) The Board Risk Management Committee (BRMC), overseeing all operational risk management activities and ensures that appropriate risk management processes are in place and functioning effectively. The Committee reviews and

recommends risk management strategies and assesses the adequacy of the risk management framework.

- (b) The BRMC is assisted by the Management Operational Risk Committee (MORC), which reviews the risk management framework and ensures that it is implemented effectively throughout the organisation.

### Internal Control Framework

The EPF adopts guiding principles for its internal control mechanism based on the COSO Internal Control Integrated Framework, which outlines the five interrelated control components - control environment, risk assessment, control activities, information and communication, and monitoring.

The Internal Audit Department provides the BAC with an independent and reasonable assurance on the adequacy and effectiveness of the risk management and internal control framework. The Committee is responsible for reviewing internal control issues identified in reports prepared by both the internal and external auditors.

The BAC also further reviews the internal audit function, with particular emphasis on the internal audit's independence, scope, resources and quality of internal audits.

Details of the activities undertaken by the Committee are further described in the Board Audit Committee (BAC) Report and the Statement on Internal Audit in this Annual Report.

## KEY ELEMENTS OF INTERNAL CONTROL

### CONTROL ENVIRONMENT

The control environment sets the tone of an organisation, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Key activities include:

#### Terms of Reference

Clearly defined terms of reference on the roles and responsibilities of all EPF Board committees and the Investment Panel, as stated in the Statement on Corporate Governance.

#### Organisational Structure

The EPF organisational structure has clearly-defined lines of accountability, delegation of responsibility, and levels of authorisation for all aspects of the business. Management

committees meet on a regular basis to identify, discuss and resolve operational, financial, investment and key management issues, and periodically report to the Board, Investment Panel, and its respective committees.

In 2019, several changes in the organisational structure of the EPF were made. Under the Investment Division, the Department of Investment Operations was established in January, comprising of Investment Services, Investment Transformation, and Shariah Services.

## STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

### KEY ELEMENTS OF INTERNAL CONTROL

With the advent of the Fourth Industrial Revolution, the EPF formed the EPF EVO project team to develop a digital blueprint for the organisation. The blueprint serves as an antecedent to strengthen organisational strategy and digital capabilities so that the EPF remains relevant and prepared to meet future customers' expectations.

To support this endeavour, the Information Technology Department had been expanded into a division with various key specification areas, comprising four departments and two sections.

#### **Human Resource Policies and Procedures**

Proper guidelines outlining procedures involving the hiring and termination of employees, implementation of training programmes, annual employee performance appraisals, and other relevant procedures, are established to ensure that employees are adequately trained and own a certain level of competencies to carry out their tasks and responsibilities.

#### **Culture of Integrity**

Entrusted with managing members' savings, various programmes and initiatives are in place to inculcate and uphold the culture of integrity, such as timely declarations of assets by staff, declarations of conflict of interest in both procurement and investment processes as well as a no-gift policy.

The Corporate Integrity Pledge is a commitment by the EPF to uphold integrity, which is essential to create a business and operating environment that is transparent and in line with global best practices in governance.

The EPF has adopted an Anti-Corruption Statement and implemented a zero-tolerance policy on corruption and unethical behaviour in its operations.

In 2019, the Corruption Risk Management (CRM) process was introduced as an additional measure to monitor activities that have high exposure to potential corruption risks. The CRM helps to identify structural weaknesses that may lead to corruption, provides a framework for all staff to take part in identifying risk factors and treatments, and embeds corruption prevention in the organisation.

#### **Code of Ethics**

The EPF Code of Ethics provides guidance for employees to carry out their duties and responsibilities that are consistent with the EPF's Vision, Mission, and Shared Values. The Code serves to clarify ethical behaviours that are in accordance with the relevant laws, policies and procedures.

### RISK ASSESSMENT

Risk assessment involves a dynamic and ongoing process of identifying and assessing risks that may impede the achievement of objectives. Key activities include:

#### **Corporate Risk Scorecard (CRS)**

The Corporate Risk Scorecard (CRS) methodology is a detailed risk management approach where risks are identified based on internal and external sources, and are analysed, evaluated, treated, monitored, and reported.

The CRS allows for continuous Risk and Control Self-Assessment (RCSA) to be performed so employees can self-assess and update their risk profiles.

## STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

**CONTROL ACTIVITIES**

Control activities are policies and procedures that ensure management directives are carried out effectively. This include necessary actions taken to mitigate the risks that impede the achievement of the organisation's objectives. Key activities include:

**Business Performance Management**

The EPF uses the Balanced Scorecard (BSC) methodology to operationalise its strategies aligned to its Vision and Mission, and to drive performance. The business performance is measured through a set of Key Performance Indicators (KPIs), integrated with risk management to enable the EPF to identify and monitor key risks impacting its business objectives.

**Three-Year Rolling Plan**

The EPF's Three-Year Rolling Plan incorporates pertinent outcomes, key priorities, and strategic initiatives to be implemented for the next three years to meet both the immediate and medium- to long-term objectives of the organisation. It is reviewed by the relevant management committees and approved by the Board.

**Risk Culture Index**

To enhance risk management practices in the EPF, the Risk Culture Index is incorporated as KPI for all departments and branches.

**Policies and Procedures**

Policies and procedures are set out in guidelines, directives, operation manuals, and work instruction documents issued by the EPF to ensure compliance with internal controls such as segregation of duties, independent checks, verification processes and system access controls.

These are updated regularly and signed off by the respective Heads of Departments, Heads of Divisions and the Chief Executive Officer. Policy guidelines and delegated authority limits are also imposed on the Management with regards to day-to-day operations.

**Information Technology Security Management**

Information security management in the EPF is based on ISO 27001, which outlines the appropriate controls and procedures to ensure confidentiality, integrity, and availability of information and application systems.

The EPF security architecture and design are constantly reviewed and improved to strengthen security controls and mitigate key technology and cyber risks. Efforts were already underway in 2019, to develop a Technology Risk Management Framework (TRMF) for the EPF to ensure the adoption of a risk-based approach towards managing technology risk and cyber security. This framework covers areas such as Governance, Risk Management, Audit, Technology Operations, Cyber Resilience, and Employee Awareness.

**Chinese Wall Policy**

The Chinese Wall Policy and its procedures are issued to safeguard against any compromise on the tenets of integrity, transparency and accountability by controlling, restricting, and managing the flow of price sensitive information.

**Business Continuity Management (BCM)**

The BCM plans and systems are regularly monitored, tested, updated, and communicated to all levels to ensure that the EPF is prepared in the event of a crisis or disaster.

**Insurance Coverage**

Adequate insurance coverage of major assets is in place to ensure protection against incidents that could result in material loss.

**Shariah Governance Framework**

The EPF has established a Shariah governance framework since 2016 to ensure strict adherence to Shariah requirements in managing Simpanan Shariah. The establishment of a dedicated Shariah Services Section in the Investment Operations Department, is to undertake Shariah functions related to Shariah research and advisory, Shariah compliance review and monitoring as well as Shariah risk management as part of the first and second lines of defence under the Shariah governance framework. The framework outlines the Shariah governance structure and policies as deliberated under the Statement on Shariah Governance for Simpanan Shariah in the Annual Report.

## STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

### KEY ELEMENTS OF INTERNAL CONTROL

#### INFORMATION AND COMMUNICATION

Information and Communication support all other control components by communicating control responsibilities to employees and by providing information in a form and time frame that allow people to carry out their duties. Key activities include:

##### **Fraud Control Management Plan**

The Fraud Control Management Plan, which includes Fraud Risk Assessment, Anti-Fraud Policy and Whistleblower Protection Policy, outlines the EPF's approach to the prevention, detection, reporting, and handling of fraud.

##### **Communication of Operational Risk Management (ORM)**

The ORM principles, framework, and processes adopted by the EPF are communicated to all employees for better understanding of the practices adopted.

#### MONITORING

Ongoing monitoring and evaluation of the effectiveness of internal control are built into business processes at different levels of the organisation. Key activities include:

##### **Operational Risk Management System**

An integrated operational risk management system is used to monitor and manage the EPF's risk exposure. Key risks are identified and the effectiveness of internal control is assessed and electronically confirmed by the respective departments and branches on a timely basis. If the mitigated risks are not within acceptable levels, individual action plans will be identified and implementation monitored to reduce the gap.

##### **Regular Reporting**

Adequate processes are in place to discuss issues on risk management and internal control deficiencies, which are reported regularly to the Management through various committees. The Management evaluates and communicates

to parties responsible for taking corrective action in a timely manner.

##### **Monitoring Activities by Internal Audit**

The results of all audit engagements are reported to the Board Audit Committee (BAC) and communicated to the Management. The Internal Audit Department maintains a follow-up process to monitor and help ensure all the agreed audit observations and resolutions have been promptly addressed.

##### **Quality Management Standard**

All the EPF's core processes comply with the MS ISO 9001:2015 Quality Management System.

### ASSURANCE ON RISK MANAGEMENT AND INTERNAL CONTROL

The Board is of the opinion that the EPF's risk management and internal control framework are effective to safeguard the interests of EPF members. The Board's review of the effectiveness of the risk management and system of internal control is supported by:

- (a) The Board Risk Management Committee (BRMC), which meets a minimum of four times a year to oversee risk management activities;

- (b) The Board Audit Committee (BAC), which meets a minimum of four times a year, reviews the areas of concerns and recommendations identified by the internal and external auditors;
- (c) The Auditor-General's issuance of the annual audit certificate on the financial statements; and
- (d) The Management's assurance that the EPF's risk management and internal control framework is operating adequately and effectively in all material aspects.

This statement is made in accordance with the resolution of members of the Board dated 29 April 2020.

# BOARD AUDIT COMMITTEE REPORT

## OVERVIEW

The Board Audit Committee is committed to its role in ensuring high corporate governance practices and providing oversight on EPF's financial reporting, risk management, and internal control systems.

## MEMBERSHIP

The Board Audit Committee consists of the following members:

(a) For the term 1 June 2019 to 31 May 2021

Board Audit Committee Members	Representative
Khalid Haji Sufat	Chairman – Professionals
Dato' Siti Zauyah Mohd Desa <i>(Service completed on 14 November 2019)</i> Hazim Jamaluddin (Alternate Member) <i>(Service completed on 14 November 2019)</i>	Deputy Chairman – Government
Datuk Dr. Ting Ding Ing	Employers
Hadah Leen	Employees
Zainal Abidin Mohd Kassim	Professionals

(b) Previous term, from 1 June 2017 to 31 May 2019

Board Audit Committee Members	Representative
Datuk Thomas George M.S. George	Chairman – Professionals
Dato' Siti Zauyah Mohd Desa Hazim Jamaluddin (Alternate Member)	Deputy Chairman – Government
Datuk Abang Haji Abdul Karim Tun Abang Haji Openg	Employers
Hadah Leen	Employees
Khalid Haji Sufat	Professionals

## MEETINGS

During the financial year 2019, the Board Audit Committee met nine times: four Special Board Audit Committee meetings, four Board Audit Committee meetings, and one Board Audit Committee meeting with the Auditor-General.

Deliberations at the Board Audit Committee meetings were robust and detailed. Minutes of the Board Audit Committee meetings held were provided to members of the Board Audit Committee. The Board was briefed on significant matters deliberated during the Board Audit Committee meetings.

Further details on the Board Audit Committee attendance have been set out in the Statement on Corporate Governance.

## TERMS OF REFERENCE

The Board Audit Committee is governed by its own terms of reference. The terms of reference establish the authority, duties, and responsibilities of the Board Audit Committee, which were approved by the Board, and accessible via the EPF's official website at [www.kwsp.gov.my](http://www.kwsp.gov.my).

## BOARD AUDIT COMMITTEE REPORT

### SUMMARY OF PRINCIPAL ACTIVITIES

During the financial year 2019, the Board Audit Committee carried out the following activities:

#### (a) Internal Audit

- (i) Reviewed and approved the annual audit plan to ensure adequate audit scope and comprehensive coverage of the EPF's activities as planned, based on risk assessment conducted;
- (ii) Reviewed and deliberated on internal audit reports tabled during the year, including recommendations made, root causes identified and the Management's response to these recommendations, as well as the timely mitigation actions taken by Management to improve the system of internal controls and its processes on the highlighted areas;
- (iii) Reviewed findings of investigations and other ad-hoc special reviews on specific areas of operations to ascertain the root cause of the issues and effectiveness of corrective actions taken to address weaknesses;
- (iv) Monitored corrective actions taken on outstanding audit issues to ensure all key risks and control lapses had been addressed;
- (v) Reviewed effectiveness of audit process and resource requirements for the year, and assessed the performance of the Internal Audit Department on a half-yearly basis and provided written feedback for improvements; and
- (vi) Reviewed and endorsed disclosures on the Statement on Internal Audit, and Statement of Risk Management and Internal Control for inclusion in the Annual Report.

#### (b) External Audit

- (i) Reviewed all areas of concerns identified by external auditors together with the Management's response to their findings;
- (ii) Met the Auditor-General on 29 April 2019 without the presence of the Management to discuss relevant issues and obtain feedback for improvements; and
- (iii) Met external auditors appointed by Auditor-General for the provision of audit services in the EPF on 26 November 2019, to discuss the scope of work and areas of audit emphasis for the year.

#### (c) Financial Reports

Reviewed quarterly unaudited financial results and annual audited financial statements of the EPF before recommending them for approval by the Board, focusing on:

- (i) The impact from changes in accounting policies and practices, to the financial statements;
- (ii) Significant matters highlighted and how these matters were addressed. These include financial reporting issues, judgements by the Management, and unusual events or transactions; and
- (iii) Compliance with applicable and approved accounting standards in Malaysia, and other legal regulatory requirements.

## BOARD AUDIT COMMITTEE REPORT

**(d) Related Party Transactions**

Reviewed related party transactions as disclosed in the financial statements entered into by the EPF and its subsidiaries.

**TRAINING**

During the year, members of the Board Audit Committee attended the following training programmes, conferences, and seminars:

Course
Audit Committee Conference 2019: Meeting The New Expectations
IIA Malaysia National Conference 2019 – GRC 4.0: Are You Ready?
PNB Leadership Forum: Organisational Excellence From Governance To Performance
International Social Well-Being Conference 2019: Shaping Destiny - Between Hope and Extinction
International Directors Summit 2019: The Trust Compass – Resetting the Course
EPF Investment Seminar 2019: Inspiring A Greater Tomorrow
EPF Thought Leadership: FutureFit 2019
MIA International Accountants Conference 2019: Trust and Sustainability In A Digital Economy
Islamic Finance For Board of Directors (IF4BoD)
Financial Institution Directors Education (FIDE) Forum: Rethinking Strategy
FIDE Forum 4th Distinguished Board Leadership Series: Digital To The Core
BNM-FIDE Forum: Masterclass on Cybersecurity – Unseen Threats
FIDE Forum Dinner Talk: Digital Assets – Global Trends Legal Requirements and Opportunities for Financial Institutions
Corporate Liability Under MACC Act 2018: New Amendments – Implication to Directors
Corporate Governance: Enhancement – MACC Act Section 17A
Value-Based Intermediation
Board Strategy Session 2019

**INTERNAL AUDIT FUNCTION**

- (a) The Board Audit Committee is supported by the Internal Audit Department in the discharge of its duties and responsibilities. The Internal Audit Department reports directly to the Board Audit Committee on its activities based on the approved annual internal audit plan.
- (b) The Internal Audit Department provides independent, objective assurance and consulting services designed to improve and add value to the EPF's operations. The Internal Audit Department helps the EPF accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, internal control, and governance processes.
- (c) Further details on internal audit function have been set out in the Statement on Internal Audit.

# STATEMENT ON INTERNAL AUDIT

**The Internal Audit Department provides independent, objective assurance, and consulting services designed to improve and add value to the EPF's operations. The department helps the EPF accomplish its objectives by bringing a systematic and disciplined approach to evaluate and improve the effectiveness of risk management, internal control, and governance processes.**

## INDEPENDENCE AND OBJECTIVITY

The Head of Internal Audit Department reports functionally to the Board Audit Committee and administratively to the Chief Executive Officer. The internal audit activities are free from interference in determining the scope of internal auditing, performance of work and communication of results.

In the interest of protecting its independence, the department has no executive or managerial powers, authority, functions or duties except those relating to the management of internal audit functions. The department is also not responsible for the detailed development or implementation of new systems, plans, regulations, policies, or procedures.

## SCOPE OF WORK

The Internal Audit Department's functions include the auditing of the financials, operations, compliance, and management of the EPF. Its scope of work, primarily, is to determine whether the EPF's risk management, internal control systems, management information systems and governance processes, as designed and represented by the Management, are adequate and functioning in a manner which ensures:

- (a) Risks are appropriately identified and managed;
- (b) Resources are acquired economically, and employed effectively and efficiently;
- (c) Assets are safeguarded;
- (d) Significant management, financial and operating information are accurate, reliable and timely;
- (e) Applicable laws and regulations, policies, standards and procedures are complied with; and
- (f) Established objectives and goals are achieved.

The Internal Audit Department's secondary scope of work encompasses the following:

- (a) Carrying out special investigations as requested by the Management / Board Audit Committee;
- (b) Coordinating with external auditors to ensure adequate audit coverage and minimal duplication of work; and
- (c) Participating as an observer in management committees set up to develop or implement new systems or processes. Such participation is limited to providing advice on control matters and does not preclude the Internal Audit Department from auditing the systems or processes.

## STATEMENT ON INTERNAL AUDIT

The Internal Audit Department continues to adopt a risk-based audit plan approach, prioritising the internal audit activities according to the audit risk level. Audit engagements carried out have been prioritised based on the assessment of inherent risks, control risks and detection risks for each operation, function and information technology system.

In 2019, a total of 119 reports were presented to the Board Audit Committee.

Status of outstanding audit findings are reported to the Management on a quarterly basis and to the Board Audit Committee on a half-yearly basis. The Internal Audit Department continues to monitor the implementation of action plans as agreed by the Management.

**INTERNAL AUDIT RESOURCES**

The Board Audit Committee reviews and approves the department's human resource requirements to ensure the department is adequately equipped with competent internal auditors. As at 31 December 2019, the Internal Audit Department had a staff strength of 89 individuals from diverse background and qualifications, as follows:

Field of Expertise	No. of Auditors	Percentage
Finance and Accounting	59	66%
Information Technology	14	16%
Business Administration	14	16%
Engineering / Quantity Surveying	2	2%
<b>Total</b>	<b>89</b>	<b>100%</b>

**PROFESSIONAL QUALIFICATIONS AND CONTINUOUS COMPETENCY DEVELOPMENT**

The Internal Audit Department is committed to equip its auditors with sufficient knowledge, skills and competencies to discharge their duties and responsibilities. The internal auditors are also encouraged to obtain appropriate professional certifications and qualifications. To date, 19 of the internal auditors hold a total of 27 professional certifications and qualifications, such as Association of Chartered Certified Accountants (ACCA), Certified Practising Accountants (CPA) Australia, Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA) and Certified Fraud Examiner (CFE). These qualifications and professional memberships have been awarded by various recognised professional bodies.

## STATEMENT ON INTERNAL AUDIT

During the year, the auditors underwent continuous training programmes to equip themselves with the requisite audit and product knowledge, soft skills on leadership, communication and negotiation skills to enhance their job performance and career prospects. The list of courses attended are as follows:

Course
<b>(A) In-House Training</b>
Certified Internal Auditor (Part 2)
Implementing Data Analytics in Internal Audit
MFRS 9 – Financial Instruments
Internal Audit Department Teambuilding
<b>(B) External Training</b>
IIA Malaysia National Conference 2019 – GRC 4.0: Are You Ready?
Cybersecurity, IT Assurance And Governance Conference (CIAG) 2019
Forensic Investigation And Fraud Analytics Conference
International Social Well-Being Conference 2019
Leadership Energy Summit Asia 2019
EPF Thought Leadership: FutureFit 2019
ICLIF's Women Of The World – Be The Change
Attachment Program at Aztec Financial Services (Luxembourg)
100 Common Problems In Construction Contract
Applied Data Analytics
Balanced Scorecard Refresher
Data Storytelling For Business
Effective IT Audit Techniques
Forex Derivatives
Global Fixed Income Academy
ISO 9001:2015 Internal Audit Training
Leadership Signature
Masterclass On Integrated Cybersecurity Management
MFRS 16 Leases – Transforming Assets and Liabilities
MFRS Update And Refresher
Management Conference 2019
Premier Shariah RFP Capstone Programme
Private Equity Academy
Real Estate Academy
Seminar On ISO/IEC 20000:2018 IT Service Management System (ITSMS) – Upgrading
Shaping Shared Leadership
Shariah RFP Course
Tea Talk Session: Project Management Review
The Art Of Storytelling
The Risk Management Audit
Winning In The Open Source World

## QUALITY AND IMPROVEMENT PROGRAMMES

- (a) The Internal Audit Department has established and maintained a quality assurance and improvement programme designed to evaluate the operations of the department. This programme includes periodic internal and external quality assessments and ongoing internal monitoring.

The internal assessments include:

- (i) Ongoing reviews of the performance of internal audit activities; and
  - (ii) Peer reviews of the audit processes, procedures and documentation on a periodic basis.
- (b) The Internal Audit Charter stipulates that a Quality Assurance Review by a qualified independent reviewer is required at least once every five (5) years.
- (c) Based on the review by KPMG Management & Risk Consulting Sdn. Bhd., in 2014, the Internal Audit Department has generally conformed with all of the International Standards for the Professional Practice of Internal Auditing (IIA Standards) promulgated by the Institute of Internal Auditors.
- (d) PricewaterhouseCoopers Risk Services Sdn. Bhd. was appointed to conduct Quality Assurance Review of the Internal Audit Department in February 2020.

# STATEMENT ON INVESTMENT RISK MANAGEMENT

## RESPONSIBILITY

In accordance with Section 18 (1) of the Employees Provident Fund Act 1991, the Investment Panel (IP) is responsible for matters pertaining to the EPF's investments and acknowledges responsibility for the investment risk management framework. The framework is designed to provide reasonable assurance and to mitigate rather than to eliminate the risk of misstatement or loss in carrying out the organisation's investment policies and objectives.

## INVESTMENT RISK MANAGEMENT FRAMEWORK

The EPF's investment risk management framework encompasses the organisation's governance structure, risk appetite, asset allocation, policies and processes. It is reviewed regularly to ensure relevance and effectiveness.

## INVESTMENT RISK MANAGEMENT STRUCTURE

The Investment Panel is responsible for overseeing risk management pertaining to the EPF's investment decision making.

The Investment Panel Risk Committee (IPRC) is responsible for assisting the IP in recommending the risk appetite and appropriate allocation of the risk 'budget'. The IPRC regularly reviews the risk measurement, policies, processes, and limits to ensure their continued effectiveness.

The IPRC is assisted by the Management Risk Committee (MRC) to monitor and review risk management activities.

The Risk Management Department supports the MRC, IPRC and IP in risk management related matters covering independent measurement and credit assessment, monitoring and reporting of the EPF's investment risk exposures.

## RISK CONTROLS

The Risk Appetite Statements, as approved by the IP, broadly outline the levels of risk that the EPF is willing to tolerate and form the basis of the allocation of funds for investment. Asset allocation reviews are regularly conducted to ensure funds are invested within the EPF's risk appetite.

Various policies and limits are in place to ensure risks are adequately mitigated for each asset class. Risk and Performance Systems have been installed and continuously enhanced to ensure that risks are systematically measured and monitored.

## CONCLUSION

The IP is of the opinion that the investment risk management practices in place are effective to safeguard the EPF's investments. The IP is supported by the IPRC, which meets a minimum of two times a year to review the risk and compliance reports from the Management.

This statement has been made in accordance with the resolution of members of the Investment Panel dated 29 April 2020.