

# Risk Management and Internal Controls

## Risk management

The Bank is exposed to a range of risks that may affect our ability to deliver on our mandates.

As the country's central bank, the Bank's financial risk exposure comes from activities and operations that impact our balance sheet, such as our holding and management of international reserves. These include exposure to market risk whereby movements in exchange rates, interest rates and other market prices have the potential to adversely affect the value of our investments. The Bank is also exposed to credit risk, the potential for loss arising from default of an issuer or a counterparty.

We are exposed to non-financial risks arising from our day-to-day operations and a wide range of external factors. These include operational events that can disrupt our operations, or cause systemic implications. The Bank is also exposed to reputational risk from the conduct of staff, engagement with stakeholders and events relating to our operations and policy decisions.

To systematically address these risks, the Bank has put in place a risk management framework (Diagram 1) that helps ensure that we conduct our operations and activities prudently and responsibly. We adopt an integrated and cohesive approach towards risk management, ensuring that significant risks confronting the organisation are identified, assessed, monitored and managed effectively.

In addition to formal structures and processes, the Bank emphasises a strong risk culture that promotes risk awareness and open communication on risk. Our aim is for all staff – at all levels and from all across the organisation – to be able and willing to identify, understand, escalate and act on risks facing the Bank.

Our risk governance structure emphasises a shared responsibility for risk that begins with business units and is reinforced through strong risk management and control functions.

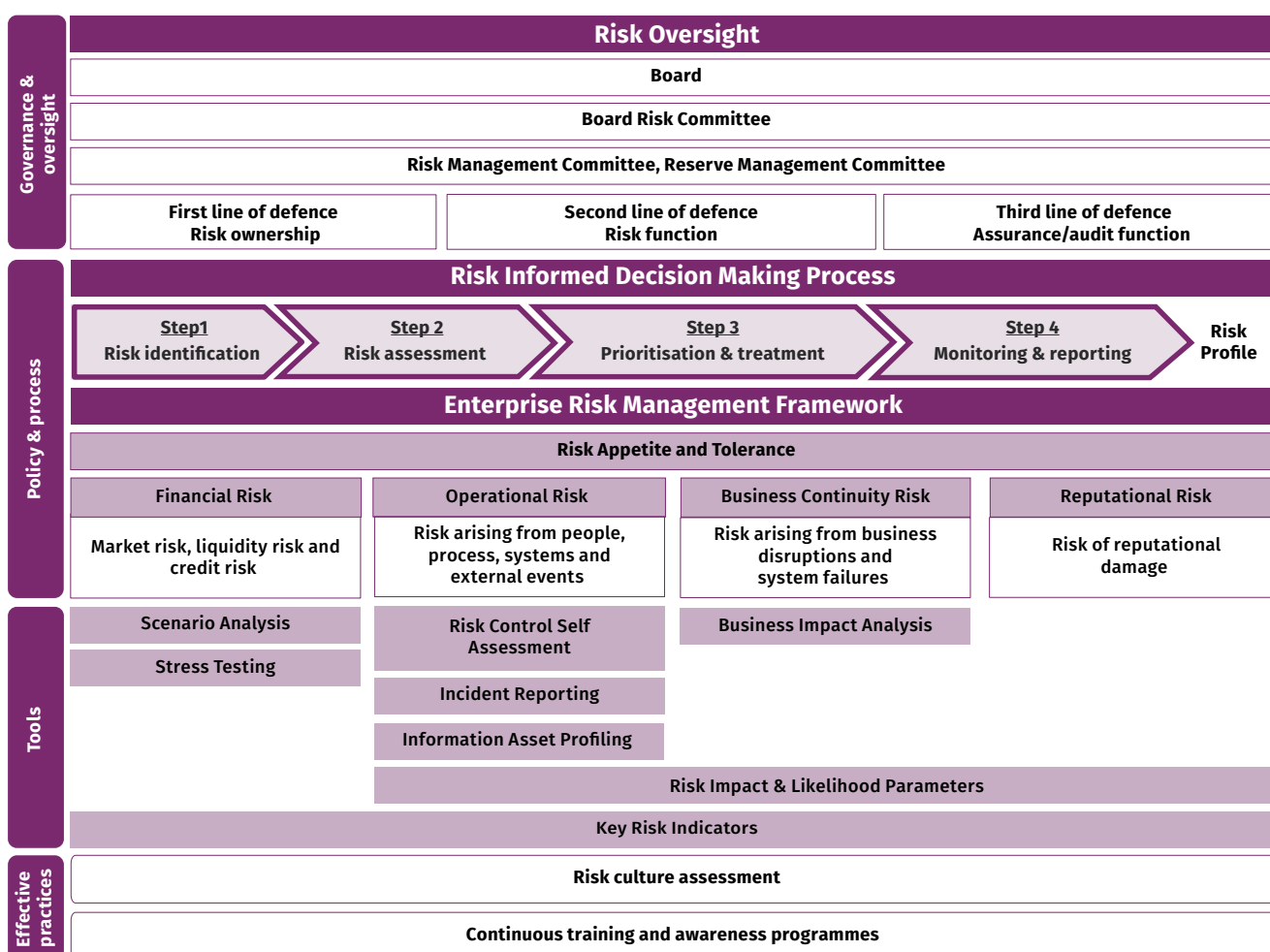
At the top, the Board – supported by the Board Risk Committee – has overall responsibility on risk governance and oversight. The Board also sets the “tone at the top” in fostering a sound risk culture.

Management is responsible for implementing sound risk management frameworks and practices across the functions and operations of the Bank. This is discharged through the Risk Management Committee and Reserve Management Committee (Diagram 2). These committees meet regularly to deliberate on strategic and critical risk issues faced by the Bank.

To support the Board and Management in discharging their oversight over risk, responsibility within the organisation for addressing and managing risk is clearly assigned through a “three lines of defence” model. Each of the three lines has an important part to play:

- Line departments, as the first line of defence, own the risk. They are responsible for identifying and assessing the risk of activities within their business areas, and for putting in place controls and to ensure that they are effective.
- As the second line of defence, the Risk Management Department acts as an independent and central risk management function that measures, monitors and reports risk on an enterprise-wide basis. It also develops and oversees the implementation of risk frameworks and policies.
- As the third line of defence, the Internal Audit Department provides independent assurance to the Board, Board Audit Committee and Management on the effectiveness of risk management practices and internal controls within the organisation.

Diagram 1: Enterprise risk management approach



Source: Bank Negara Malaysia

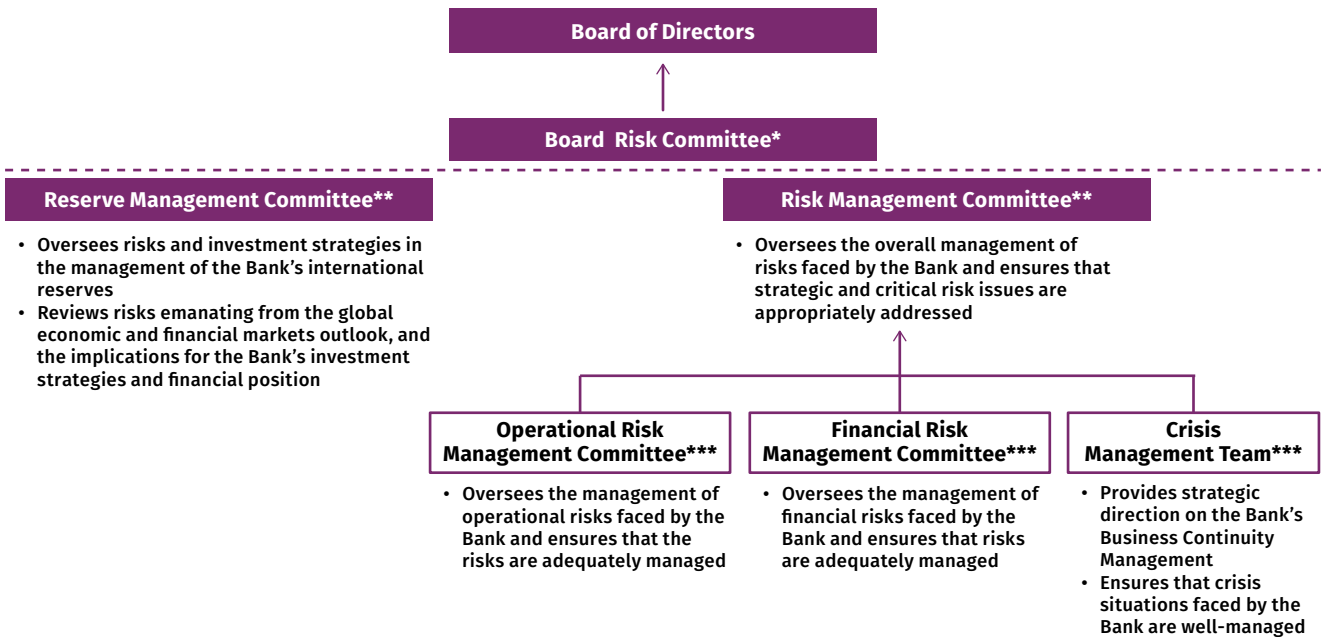
Delivering on our mandates requires the Bank to take on risks. We recognise that we cannot eliminate all risks. Rather, we seek to operate within our Board-approved risk appetite and tolerance. We also evaluate the costs, benefits and other trade-offs involved in controlling or mitigating risks. For this purpose, a process for identifying, assessing, prioritising, reporting and monitoring our financial, operational and reputational risk exposures is in place.

To manage financial risks, the Bank closely monitors its market, liquidity and credit risk exposures, and has in place risk limits and controls. In our international reserves portfolio, investments are allocated guided by a Board-approved diversified investment benchmark that outlines the Bank's long term appetite for risk and returns. Deviation from the benchmark is controlled using risk limits, governance arrangements and investment guidelines.

The Bank also has in place a credit risk framework that outlines permissible investments and activities. For the Bank's general operations such as budgeting, procurement and payments, governance and controls are in place to ensure that the Bank allocates its expenditures and manages its finances prudently.

To manage non-financial risks, the Bank has put in place structures to identify and monitor risks on an ex ante or pre-emptive basis. These include tools for the first line to conduct risk surveillance and assessments, monitor risk levels and conduct simulations based on scenarios. These tools aid the Board and Management in ensuring that there are effective and adequate safeguards to mitigate the risks that the Bank is exposed to. An incident reporting system also complements these tools by facilitating systematic escalation of risk incidents, which in turn enables the organisation to respond more quickly to operational incidents, including

Diagram 2: Risk management governance structure



\* Chaired by an Independent Non-Executive Director of the Bank  
 \*\* Chaired by Governor  
 \*\*\* Chaired by a Deputy Governor

Source: Bank Negara Malaysia

business disruptions. Across these different risk tools, a common set of risk impact and likelihood parameters is applied consistently throughout the assessment process including business continuity and crisis management to address risk of disruptions that may have systemic implications.

In 2019, we embarked on a number of efforts to further strengthen our risk management framework and capabilities:

- We worked on strengthening our organisational preparedness for dealing with crisis events. In addition to developing a crisis communication plan, we also started preparations to conduct an industry-wide crisis simulation in 2021. This involved the Bank working closely with various stakeholders in the financial sector to ensure that the business continuity plans of various organisations are aligned, and allow for a coordinated response. We also conducted cyber-drills and refined our existing business continuity plans to ensure that we have clear recovery strategies to restore normalcy speedily after a crisis.
- We enhanced our incident reporting system to allow for incident reports to be processed seamlessly, thus shortening time taken to

escalate, report and manage operational incidents. The enhanced system allows for incidents to be tracked and monitored based on criticality and tolerance levels, and the generation of dashboards to aid prioritisation of response and escalation.

- We embarked on a number of initiatives to better prepare ourselves against cyber risk.
  - We established a Security Operations Centre to facilitate surveillance and rapid response to cyber incidents. The centre monitors the Bank's networks and systems to detect potential cyber threats and undertake appropriate response actions.
  - Recognising that cyber criminals know no borders, we initiated the Cybersecurity Resilience and Information Sharing Platform together with other ASEAN central banks. The platform allows for central banks within the region to share cyber-related information and encourage capacity building.
  - Recognising that our staff form the first line of defence against cyber threats, we rolled out a number of initiatives to improve staff awareness of cybersecurity. We conducted a number of cyber-awareness programmes, and issued advisories to educate staff on ways

to remain vigilant against cyber incidents. We also conducted a series of phishing tests and an online assessment to ascertain the level of cybersecurity understanding of our employees.

As a statutory body committed to ensuring that we are effective in discharging our mandates and responsible in managing our resources, the Bank will continue to strengthen our framework for risk management. This will include embedding more deeply the risk management framework within the organisation to a level where it becomes second nature for all Bank staff to act in ways consistent with the Bank's risk appetite and risk management philosophy. We will also work to strengthen the capacity of control functions in adding value to the business by providing insights to further integrate risk considerations in business operations and strategy.

### Internal audit

The Board Audit Committee is responsible for reviewing the effectiveness of the Bank's internal controls and compliance with legal and regulatory requirements. It provides oversight over the internal audit function of the Bank. It is also responsible for the integrity of our financial statements.

The Internal Audit Department provides independent assurance to the Board Audit Committee on the adequacy and effectiveness of the Bank's

governance, risk management and internal control processes. The department conducts regular assessments on the activities of departments and entities related to the Bank to identify and address risks. An audit plan is developed each year and reviewed quarterly to ensure that audit activities reflect changes in the Bank's risk profile and emerging risks. Apart from providing assurance, the department also participates as an independent observer in several of the Bank's key projects and committees to help ensure that internal controls and governance arrangements are consistently upheld. Audit activities are conducted in conformance to the requirements of the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing. The principles espoused by the Committee of Sponsoring Organizations of the Treadway Commission are embedded in the audit approaches for assessing the Bank's control environment.

The Internal Audit Department also provides the Minister of Finance with an independent quarterly report on our international reserve management activities. This is to assure the Minister that the reserves have been managed in accordance with established policies and guidelines approved by the Board.

Audits conducted in 2019 include those in the areas of the Bank's supervisory, treasury operations, finance operations and settlements, currency management and cybersecurity functions.