Risk Management and Internal Controls

In fulfilling its statutory mandates, the Bank is exposed to a broad range of risks in carrying out its responsibilities and daily operational activities. The Bank manages these risks through an Enterprise Risk Management Framework. The framework provides a comprehensive approach to identify, assess, monitor, and mitigate these risks (Diagram 1). The framework also establishes the oversight, control and discipline needed to drive continuous improvements in the Bank's risk management capabilities and risk culture.

The Bank implements a risk governance structure that reflects a shared responsibility for managing risks between line departments, independent risk management and control functions, and internal audit (Diagram 2).

The Bank's Board, supported by the Board Risk Committee (BRC), oversees the Bank's risk management frameworks and practices. The Board also sets the 'tone from the top' in promoting the desired risk culture across the Bank.

The accountability for implementing sound risk management frameworks and practices across the Bank rests with the Bank's Senior Management. This is operationalised through the Risk Management Committee (RMC) and Reserve Management Committee (ReMC). These committees meet regularly to deliberate the latest strategic and critical risks faced by the Bank, including reputational risk. In turn, the RMC is supported by the Financial Risk Management Committee (FRMC), Operational Risk Management Committee (ORMC) and Crisis Management Team (CMT).

The FRMC and ORMC are responsible for the management of financial and operational risks, respectively. Meanwhile, the CMT provides oversight on the Bank's Business Continuity Management by ensuring crisis preparedness. The CMT also coordinates the Bank's response to operational disruptions.

In formulating and implementing policies under its financial and monetary stability mandates, the Bank is guided by its Policy Development Framework and has in place a well-defined governance process for approving policies. Policy proposals are subjected to cross-functional deliberations within the Bank, as well as external consultation and transparency frameworks. The Bank has several high-level committees that preside over policy making. These include the Management Committee, the Monetary Policy Committee, the Financial Stability Committee and the Financial Stability Executive Committee. Chaired by the Governor, these committees are primarily responsible for approving policies issued and implemented by the Bank to promote financial and monetary stability.

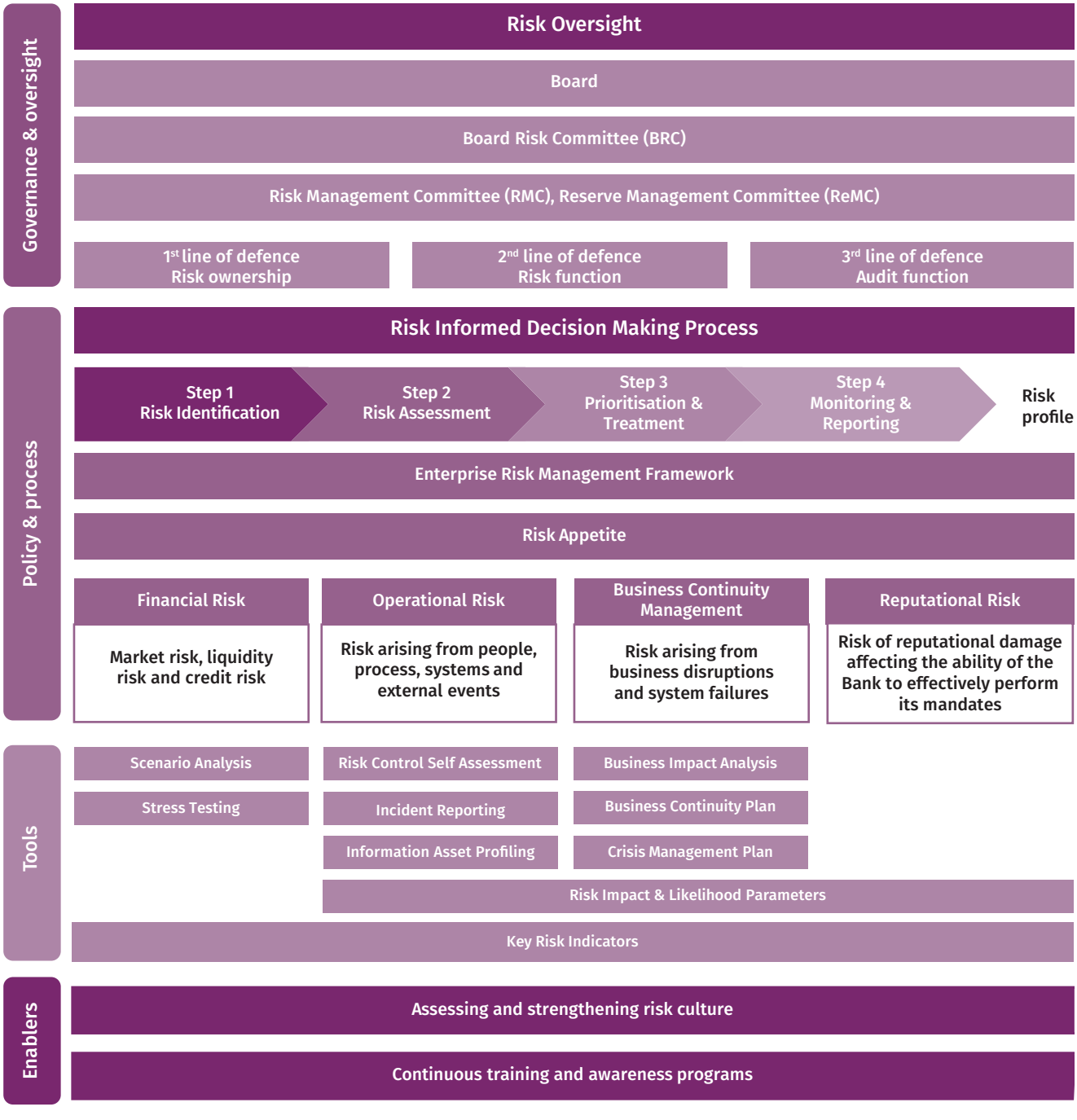
To support effective risk governance, the Bank adopts the 'three lines of defence' model (Diagram 3):

- Business units as the 'first line' of defence are responsible for evaluating their risk environment, establishing controls and ensuring that these controls are implemented effectively.
- The 'second line' function carried out by the Risk Management Department and Treasury Risk Management Section within the Investment Operations and Financial Market Department, facilitates sound risk management practices by business units through appropriate frameworks, policies and tools. The Risk Management Department also supports Senior Management and the Board in monitoring risk developments and issues at an enterprise level.

- The 'third line' of defence – the Internal Audit Department, provides independent assurance of the effectiveness of risk management policies and measures.

The Bank's enterprise risk appetite statements guide the Bank's management of its risks. The statements specify the level and types of risk that the Bank is willing to accept, to achieve its business objectives. The risk appetite statements were refreshed in 2022 to ensure that they remain relevant in light of the changing risk landscape (Diagram 4). The refreshed risk appetite statements provide greater clarity around the boundaries for risk events that the Bank does not tolerate, such as fraud and unethical conduct. The statements also acknowledge that

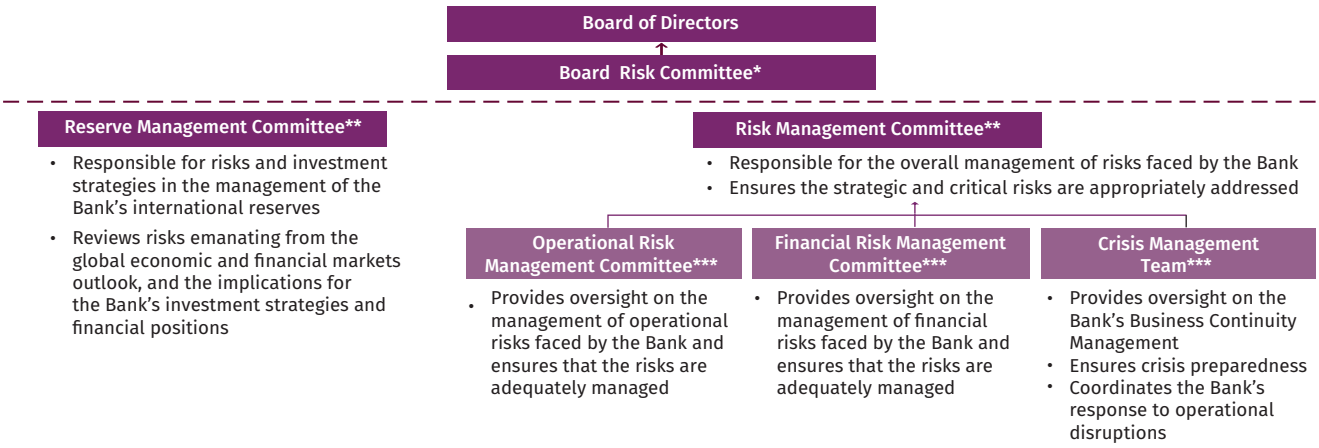
Diagram 1: The Bank's Enterprise Risk Management Framework



Source: Bank Negara Malaysia

there are risks that would be difficult or undesirable to eliminate completely. For example, the costs involved to operate at zero risk could be prohibitive. Tolerance for some level of risk is also necessary to encourage innovation and operational efficiency. As such, the refreshed statements provide flexibility for the Bank to take on measured risks in some areas, with these risks managed through appropriate safeguards. The refreshed risk appetite statements are being embedded into the Bank's processes and culture, to promote consistent, risk informed decision-making aligned with the Bank's strategic goals.

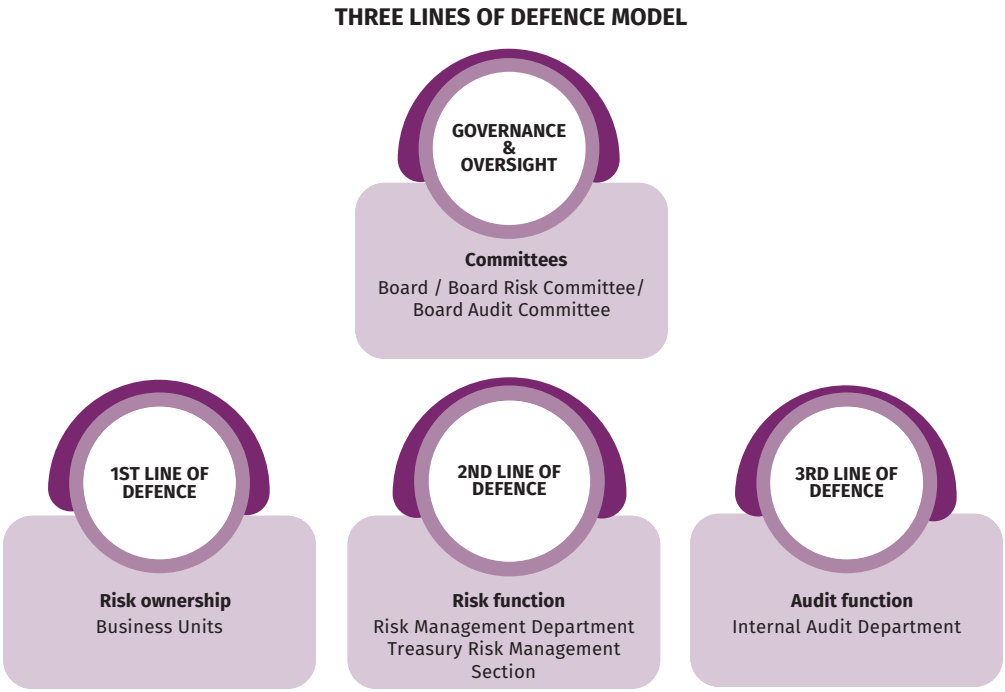
Diagram 2: Risk Management Governance Structure



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

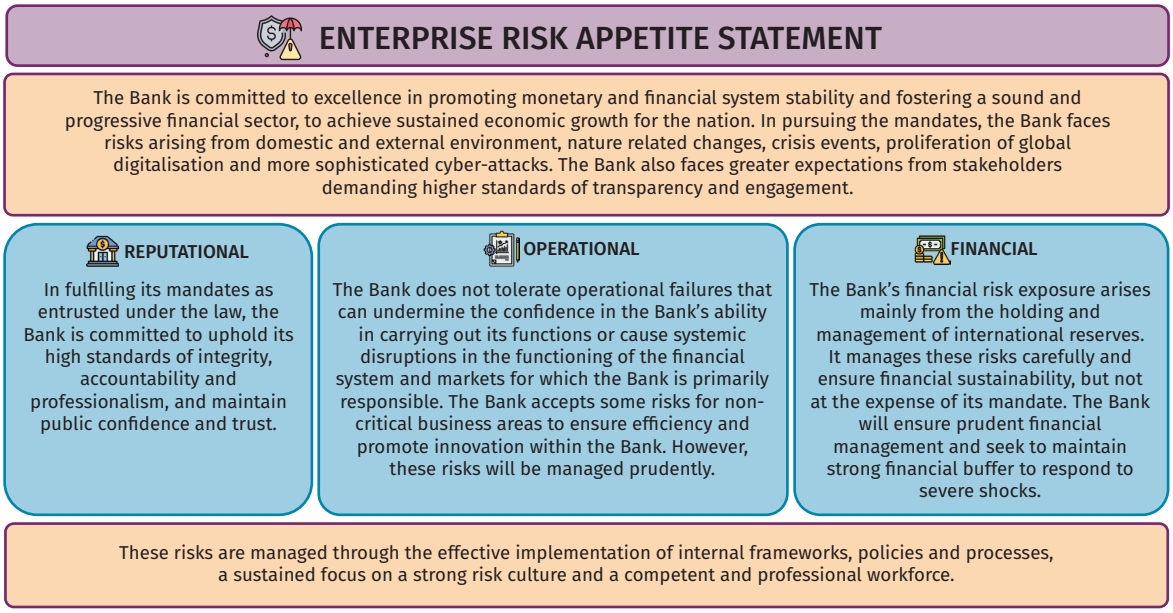
Source: Bank Negara Malaysia

Diagram 3: Three Lines of Defence Model



Source: Bank Negara Malaysia

Diagram 4: Bank Negara Malaysia's Risk Appetite Statements



Source: Bank Negara Malaysia

Managing the Bank's key organisational risks

To manage financial risk, the Bank monitors market, liquidity, and credit risk exposures, via risk limits and controls. The Bank's international reserves portfolio investments are driven by a Board-approved investment benchmark that sets the appetite for long-term risk and returns. Any deviation from the benchmark is controlled using risk limits, investment guidelines and designated approving authorities. During the year, the Bank revised its investment benchmark for international reserves. The benchmark is reviewed every three to five years to reflect significant changes in the global investment landscape. In the area of credit risk, the Bank maintains a stringent credit policy to ensure credit exposures undertaken through the Bank's investment activities remain within acceptable levels.

In managing non-treasury financial risks, controls are also in place to ensure that the Bank allocates its expenditures and manages its finances prudently. These include policies and procedures for procurements and payments, as well as a robust budgeting and management accounting process that involves careful planning, forecasting and analysis. The budget is also monitored and adjusted on an on-going basis as new information becomes available. This is accompanied by regular reporting to management. On the procurement front, effort has been put into strengthening the governance and efficiency of the Bank's procurement processes. This includes the establishment of a Centralised Procurement Department.

To manage operational risks, the Bank identifies and proactively monitors risks through key risk indicators. These risks include, but are not limited to, information technology, cybersecurity, people, legal, business disruption, and physical security risk. The management of these risks is supported by departments designated as Risk Policy Owners (RPO). RPOs are responsible for the identification, monitoring and reporting of relevant transversal risks – risks that cut across the Bank. RPOs also propose Bank-wide controls and action plans to manage the relevant transversal risks.

On the technology front, the adoption of new systems such as cloud services has facilitated more effective remote and hybrid working arrangements. At the same time, it has also meant that the Bank needs to actively manage increasingly dynamic and varied technology and cyber risks. Thus, emphasis is placed on strengthening the resilience of the Bank's defences against cyber-attacks. This includes instituting stronger technology governance and architecture, improving network resilience and conducting regular cyber monitoring. The Bank also has in place a Cybersecurity Management

Assessment Program (CMAP) to assess and improve the level of the Bank's cyber security maturity. Mandatory training sessions were also conducted throughout the year to help staff stay ahead of cyber threats.

In addition, the Bank has deployed several key measures to safeguard its information assets. This includes the use of technology to detect and prevent information leakages. To inculcate continuous awareness among staff on the Bank's information security policies and measures, the Bank has introduced mandatory attestations by staff on information security management.

Recognising expectations for us to communicate and explain our policies, we have intensified our policy communications and education through tailored engagements. We have also been actively sharing content for public consumption in different formats and across more channels to better engage the general public. For example, we have developed infographics such as the 'Monetary Policy Statement snapshots' and 'BNM Explains'. The infographics are disseminated via the Bank's social media platform to help explain our policy decisions. These initiatives are aimed at helping the Bank close expectation gaps and manage reputational risk in the course of discharging its mandates.[1]

Business Continuity Management

The Bank aims to maintain robust business continuity arrangements. This ensures that core business processes are resilient to a broad range of disruptive event scenarios such as pandemics, cyber-attacks, natural disasters and civil unrest.

During the year, the Bank continued to adapt its relevant risk management procedures and controls to facilitate a safe return to office. This includes implementing stricter COVID-19 testing and isolation requirements on staff performing critical business functions. These measures were aimed at minimising operational disruptions.

The Bank also refreshed its business impact analysis by incorporating new risk event scenarios such as floods and cyber-attacks. Regular crisis simulation exercises, including cyber drills, were also conducted to ensure that the Bank's business continuity plans remain responsive and effective.

Despite the challenges presented by uncertainties in the global risk landscape, continuous strengthening of our risk management capabilities has helped us fulfil our statutory mandates. It has also helped us maintain a risk profile throughout the year that continues to be resilient against material risk events.

Internal Audit

The Board Audit Committee (BAC) provides oversight over the effectiveness of the Bank's internal controls and compliance with legal and regulatory requirements. In discharging this role, the BAC is supported by the Internal Audit Department (IAD).

The IAD provides independent assurance on the adequacy and effectiveness of the Bank's governance and risk controls. The IAD also submits an independent quarterly report to the Minister of Finance on the Bank's international reserve management which provides an assessment on whether international reserves have been managed according to policies and guidelines approved by the Board.

Audit priorities in 2022 were aligned with key organisational risks and the Bank's strategic outcomes for the year, which includes assessments on emerging risks and vulnerabilities (Diagram 5). In setting out these priorities each year, the IAD also draws on the input and assessments of the Risk Management Department.

As part of its advisory function, IAD actively promotes higher risk awareness and sound control practices amongst staff. This is done by providing audit insights and recommendations to further enhance the Bank's control environment.

Increased use of data analytics has enabled more efficient and timely risk identification and in-depth audit assessments. IT capabilities have also been upgraded to enable more effective use of analytic dashboards to support audit practices.

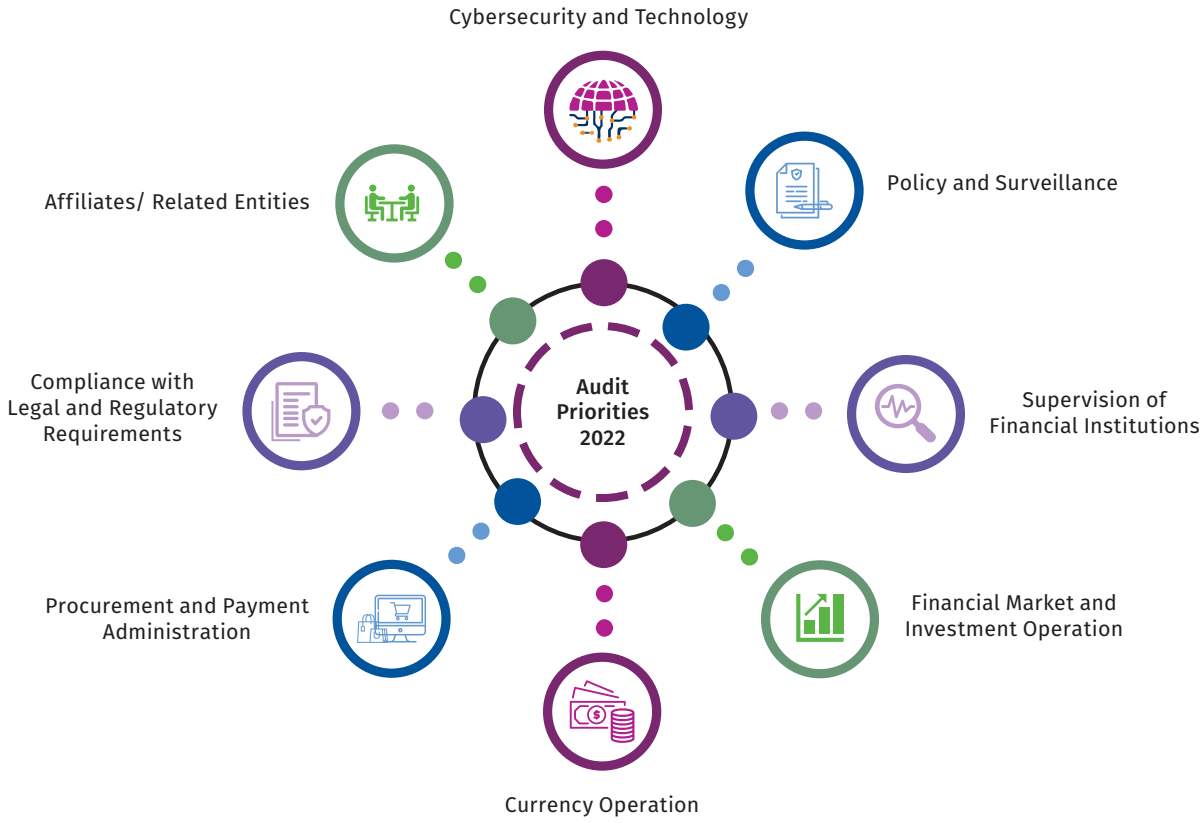
An independent assessment benchmarked against international standards was carried out by the

[1] More information on the Bank's public engagements throughout the year can be found in the 'Engaging Malaysians' chapter of this report.

Institute of Internal Auditors Malaysia in 2022. The evaluation concluded that IAD is operating as a matured and capable audit function. This implies that policies, processes and procedures needed to facilitate an effective internal audit function are in place. Hence, enabling IAD to play a critical role towards the achievement of strategic objectives.

In keeping pace with expectations to strengthen the Bank's control environment, IAD will continue to preserve its agility in response to key organisational and emerging risks. Initiatives to elevate audit competencies will also continue to be prioritised to support sound audit assessments in an increasingly complex operating environment.

Diagram 5: Focus & Coverage of Audits Conducted in 2022



Source: Bank Negara Malaysia