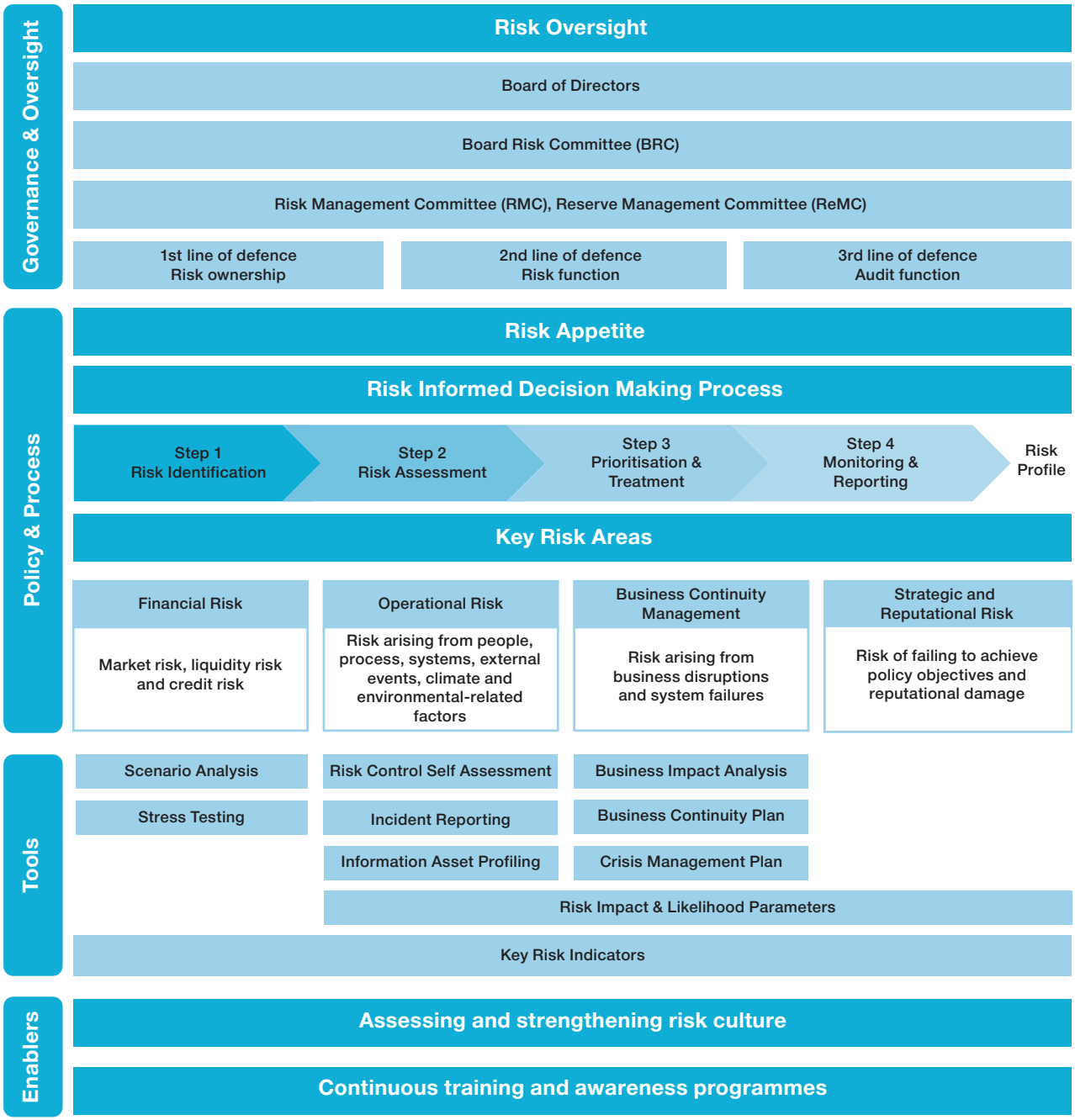
Risk Management and Internal Controls

BNM applies its Enterprise Risk Management (ERM) Framework (Diagram 1) to provide a structured approach for identifying, assessing, monitoring and managing risks. The framework also fosters a strong risk culture and ensures consistent risk strategies across the organisation.

Diagram 1: Bank Negara Malaysia's Enterprise Risk Management Framework



Source: Bank Negara Malaysia

Ensuring Robust and Effective Risk Oversight and Governance

Risk management is a collective responsibility at BNM, with responsibilities shared across departments, independent risk and control functions, as well as internal audit. With the support of the Board Risk Committee (BRC), the Board of Directors oversees BNM's risk management frameworks and practices, ensuring sound governance and effective risk oversight. They are also responsible for setting the tone from the top, setting the risk appetite, and reinforcing a strong organisation-wide risk culture.

At the management level, we exercise our risk management responsibility through two key governance structures, the Risk Management Committee (RMC) and the Reserve Management Committee (ReMC). The RMC deliberates enterprise risks and is supported by functional committees (Diagram 2), while the ReMC focuses on strategies and risks related to the management of international reserves.

BNM adopts the 'Three Lines of Defence' model (Diagram 3). Business units act as our first line of defence. They are responsible for assessing risks, setting appropriate controls and ensuring their effective implementation. To reinforce this role, some business units have introduced a '1.5 line of defence' – where dedicated risk and control functions are embedded within their operations. This structure strengthens risk awareness and proactive management at the operational level.

The Risk Management Department (RMD) serves as the second line of defence, providing independent assessments and monitoring of risks across the organisation. The RMD also supports management in maintaining oversight of overall risk trends and issues at the organisational level. Its direct reporting line to the BRC also enables independent judgement and timely escalation, strengthening oversight and effective monitoring of risk developments. Meanwhile, the Treasury Risk Management Section, part of the Treasury Risk and Infrastructure Unit, looks at investment risks for international reserves, reporting directly to a Deputy Governor. These structures enhance safeguards and promote sound risk practices throughout BNM.

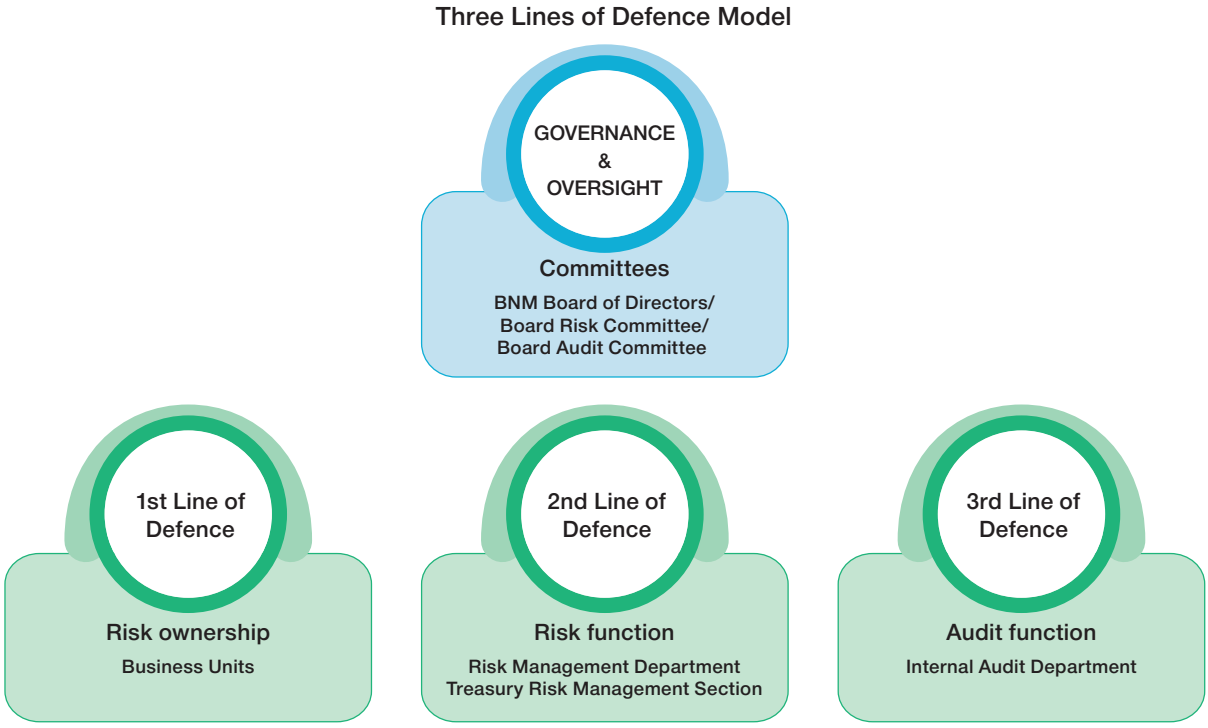
Reporting directly to the Board Audit Committee (BAC), the Internal Audit Department (IAD) forms the third line of defence, providing independent assurance through comprehensive audits and reviews on the effectiveness of controls and governance.

Diagram 2: Risk Management Governance Structure

[1] Chaired by an Independent Non-Executive Director of BNM.
[2] Chaired by Governor.
[3] Chaired by Deputy Governor.

Source: Bank Negara Malaysia

Diagram 3: Three Lines of Defence Model



Source: Bank Negara Malaysia

Defining Clear Risk Boundaries for Stronger Governance

BNM's enterprise risk appetite statements (Diagram 4) outlines the levels of risk BNM is prepared to take in pursuit of its business objectives. We review the statements periodically so that it remains relevant and practical in line with changes in the risk landscape. We conduct training and engagement sessions regularly across all levels and functions to align operations with the defined risk appetites. We also have an Accountability Framework to deal with incidents of risk breaches, an important

Diagram 4: Bank Negara Malaysia's Risk Appetite Statements

ENTERPRISE RISK APPETITE STATEMENT

BNM is committed to excellence in promoting monetary and financial system stability and fostering a sound and progressive financial sector, to achieve sustained economic growth for the nation. In pursuing the mandates, BNM faces risks arising from domestic and external environment, climate and environmental-related factors, crisis events, proliferation of global digitalisation and more sophisticated cyber attacks. BNM also faces greater expectations from stakeholders demanding higher standards of transparency and engagement.

Reputational

In fulfilling its mandates as entrusted under the law, BNM is committed to uphold its high standards of integrity, accountability and professionalism, and maintain public confidence and trust.

Operational

BNM does not tolerate operational failures that can undermine the confidence in BNM's ability in carrying out its functions or cause systemic disruptions in the functioning of the financial system and markets for which BNM is primarily responsible. BNM accepts some risks for non-critical business areas to ensure efficiency and promote innovation within BNM. However, these risks will be managed prudently.

Financial

BNM's financial risk exposure arises mainly from the holding and management of international reserves. It manages these risks carefully and ensures financial sustainability, but not at the expense of its mandate. BNM will ensure prudent financial management and seeks to maintain strong financial buffers to respond to severe shocks.

These risks are managed through the effective implementation of internal frameworks, policies and processes, a sustained focus on a strong risk culture and a competent and professional workforce.

Source: Bank Negara Malaysia

tool to promote compliance and strengthen accountabilities at all levels. This year, we began to apply the Accountability Framework to better align behaviours and actions with our internal recognition and rewards mechanisms.

Robust Policy Governance, Resilience and Operational Continuity

We adopt a multi-pronged approach to risk management that is underpinned by the three lines of defence. This includes robust policy governance and prudent management of international reserves. We complement this with disciplined oversight of technology, cybersecurity and business continuity to support resilient operations.

Sound policymaking and governance

BNM is committed to sound policymaking practices. The Policy Development Framework provides clear governance for the development, review and approval of policies. As part of its governance, all policies undergo rigorous technical discussions before being deliberated and approved by the Management Committee, Financial Stability Committee, or Financial Development Committee. Monetary policy decisions are made by the Monetary Policy Committee and supported by rigorous technical analysis and discussions. As part of its policy development process, BNM also conducts external consultations for non-monetary policy areas to ensure the views and concerns of its key stakeholders are duly considered. This allows for more informed policy design and practical application.

Operational matters are decided by the Operational Management Committee that comprises both internal members and external experts.

Managing market, credit and liquidity risks

On treasury-related financial risks, our role in managing Malaysia's international reserves exposes BNM to market, credit and liquidity risks. These risks are closely monitored and managed against the investment benchmark and risk controls approved by the Board of Directors. During the year, BNM revised its investment strategic asset allocation (SAA) for international reserves. In line with industry best practices, the SAA is reviewed every three to five years to reflect significant changes in global financial market conditions.

Outcome-focused risk management

Our risk approach is framed by the outcomes we must safeguard – the continuous delivery of critical services, the integrity and confidentiality of data and strong recovery capabilities. As technology adoption accelerates and cyber threats evolve, BNM enhances its frameworks and methodologies to better assess and manage technology and cybersecurity risks. This contributes to stronger protection of its digital assets against potential threats.

The Digital Technology Committee (DTC) provides oversight and strategic direction on technology and digital related matters. The Technology and Cyber Security Working Group oversees technology and cybersecurity risk management, sets priorities for technology initiatives, and ensures IT service efficiency. Independent validation through external assurance, red teaming and third-party assessments provides objective insights on the effectiveness of controls and helps uncover blind spots, enabling targeted and timely remediation.

Continuous compliance and modernisation

Compliance monitoring provides early warning of policy drift. It also helps to detect potential control weaknesses. It is supported by periodic reporting through interactive dashboards and automation. At the same time, ongoing technology upgrades and system modernisation deliver more secure and reliable platforms.

Embedding strategic risk assessment in planning

As in previous years, we emphasise identifying risks that can impact our strategic outcomes and mandates. We do this by systematically embedding risk considerations in our business plan, decision and policy making and departmental actions. For example, we review business plan 'must wins' to surface emerging risks and re-prioritised initiatives, integrating actionable mitigation strategies aligned to organisational priorities. This strengthens delivery of Business Plan outcomes by ensuring key initiatives remain achievable and on track despite emerging risks and changing conditions. Careful monitoring of emerging risk events also enables us to flexibly manage ongoing initiatives and ensure that we stay on course to achieve our strategic priorities.

Leveraging technology for better risk reporting

Standardised taxonomies improve data quality, while interactive dashboards support faster decision-making. They support clearer and consistent risk communication across BNM. This was made possible through enhanced periodic risk reporting. We achieved this by leveraging automation and data visualisation techniques. For example, we use data visualisations such as trend charts, heatmaps and drill-down views (enabled by filters and summary indicators) allowing us to spot changes in patterns, risk levels and key action areas.

Critical market infrastructures

BNM's Real-Time Electronic Transfer of Funds and Securities System (RENTAS) and Fully Automated System for Issuing/Tendering (FAST) systems are critical financial market infrastructures that support Malaysia's payment and settlement networks. The Financial Market Infrastructure Committee (FMIC) provides oversight and sets strategic direction for these systems, including ongoing development and upgrades. FMIC oversees the strategic governance over operational resilience and risk management, ensuring these systems remain safe, efficient and reliable. Amid rapid growth of retail instant payments, we upgraded the real-time gross settlement system to RENTAS+.

Building a stronger, more resilient organisation through a purposeful cyber readiness exercise

This upgrade enabled continuous interbank fund transfers and retail payment settlements 24/7 throughout the year. This marked a major milestone in BNM's multi-year modernisation plan of the RENTAS platform.

Strengthening operational continuity of critical functions

An enhanced ability to respond promptly and effectively during disruptions is critical. In 2025, we conducted mid-day live run tests. We also carried out physical scenario exercises to validate operational readiness. This includes mobilisation to the recovery centre and prolonged manual operations for critical business functions. In addition, we strengthened emergency response and staff safety measures, introducing a rapid-response communication tool to enhance coordination during crises. These exercises confirmed the effectiveness of key recovery procedures and provided practical insights to further refine and strengthen coordination during disruptions.

Cyber incident preparedness and resilience

In 2025, BNM ran a cybersecurity drill simulating real-world threats to test our risk management, internal controls and crisis protocols. This allowed us to affirm our ability to respond to threats in a coordinated and effective manner.

Building shared responsibilities

As we accelerate the use of AI and digital tools, we accord high priority to strengthening security awareness. This is crucial to safeguard BNM's data and assets. In 2025, we rolled out mandatory bank-wide cybersecurity training, covering emerging threats such as AI-enabled attacks and deepfakes. This helped build stronger security resilience in an AI era. We also carried out periodic phishing simulation exercises to help employees recognise suspicious emails in a safe, controlled environment. Insights from these exercises are used to develop targeted training for higher-risk groups and further strengthen internal controls. Furthermore, we expanded organisation-wide awareness outreach. We take this opportunity to share monthly security advisories and campaigns as well as engage with business units. This is intended to keep employees informed on emerging threats and real-world attack trends. It also reinforces best practices to protect our assets, stakeholders and reputation.

Risk governance and industry collaboration

In our efforts to promote strong risk governance and foster a resilient risk culture, we hosted a series of engagements with external parties across key focus areas, such as risk culture, technology and cybersecurity. These included a Regional Risk Dialogue with central banks to discuss emerging risks, Risk Networking Group Roundtable to exchange views on current issues, and RiskX Talk series featuring industry experts on risk management and organisational resilience. We also reviewed our Enterprise Risk Appetite Statements to give greater prominence to climate and environmental risks for physical safety and security, as a start. This enables the organisation to better anticipate, withstand and respond to evolving environmental threats.

Internal Audit

The BAC, supported by IAD, plays a central role in overseeing the adequacy and effectiveness of BNM's internal controls and the integrity of its financial reporting process. IAD's functional and direct reporting to the BAC preserves its independence and objectivity. This ensures that audit priorities and findings are overseen at the highest level of governance at BNM. This reporting line enables the BAC to obtain objective, independent assessments on the effectiveness of governance arrangements, risk management practices and internal control systems. IAD also provides assurance to the Minister of Finance on a quarterly basis, that the international reserves are managed in line with policies and guidelines approved by the Board of Directors.

BNM adopts a risk-based approach in determining audit priorities and engagements. This allows focus on areas of higher significance to BNM's mandates and reputation (Diagram 5). Close engagements with the BAC, Senior Management, RMD and line departments helped refine these priorities. In 2025, we audited 33 departments and affiliates. Audit findings are accompanied by constructive and practical recommendations aimed at strengthening controls, improving efficiency and enhancing governance practices. IAD also monitors the implementation of agreed management actions and provides regular updates to the BAC on pertinent control enhancements, thereby reinforcing accountability and continuous improvements across BNM.

In enhancing audit efficiency, IAD continues to modernise its audit processes through technology

and innovation. Increasingly, we adopt data analytics and GenAI tools such as Optical Character Recognition and Natural Language Processing to enable comprehensive assessments of emerging risks and control effectiveness. These capabilities enhance audit coverage and support timely and insightful assurance. In 2025, we also began to introduce elements of continuous auditing in selected areas to strengthen overall risk management and control environment.

Moving forward, IAD is committed to expanding AI-driven and data-centric audit approaches to stay aligned with enterprise needs and industry benchmarks. Knowledge sharing and exposure to international best practices will be key. We will continue to engage with our counterparts via the ASEAN Central Banks' Heads of Internal Audit Network Meeting, Regulators Internal Audit Roundtable meeting and global professional networks, to support ongoing progress towards a future-ready audit function.

In a rapidly changing environment, it is also crucial that IAD remain focused on delivering independent and practical assurance to support sound decision-making. By strengthening core audit practices, progressive development of staff capabilities and adoption of advanced technology, IAD is able to deliver actionable insights and ensure internal controls are adaptive and resilient in navigating a dynamic risk landscape.

Diagram 5: Coverage of Audits Conducted in 2025

Source: Bank Negara Malaysia