



Risk Management Framework



The
Scottish
National
Investment
Bank



The Bank's Risk Management Framework (RMF) summarises the approach the Bank will take to the management of all risk and compliance matters across the Bank, and the management and mitigation of their potential impacts.

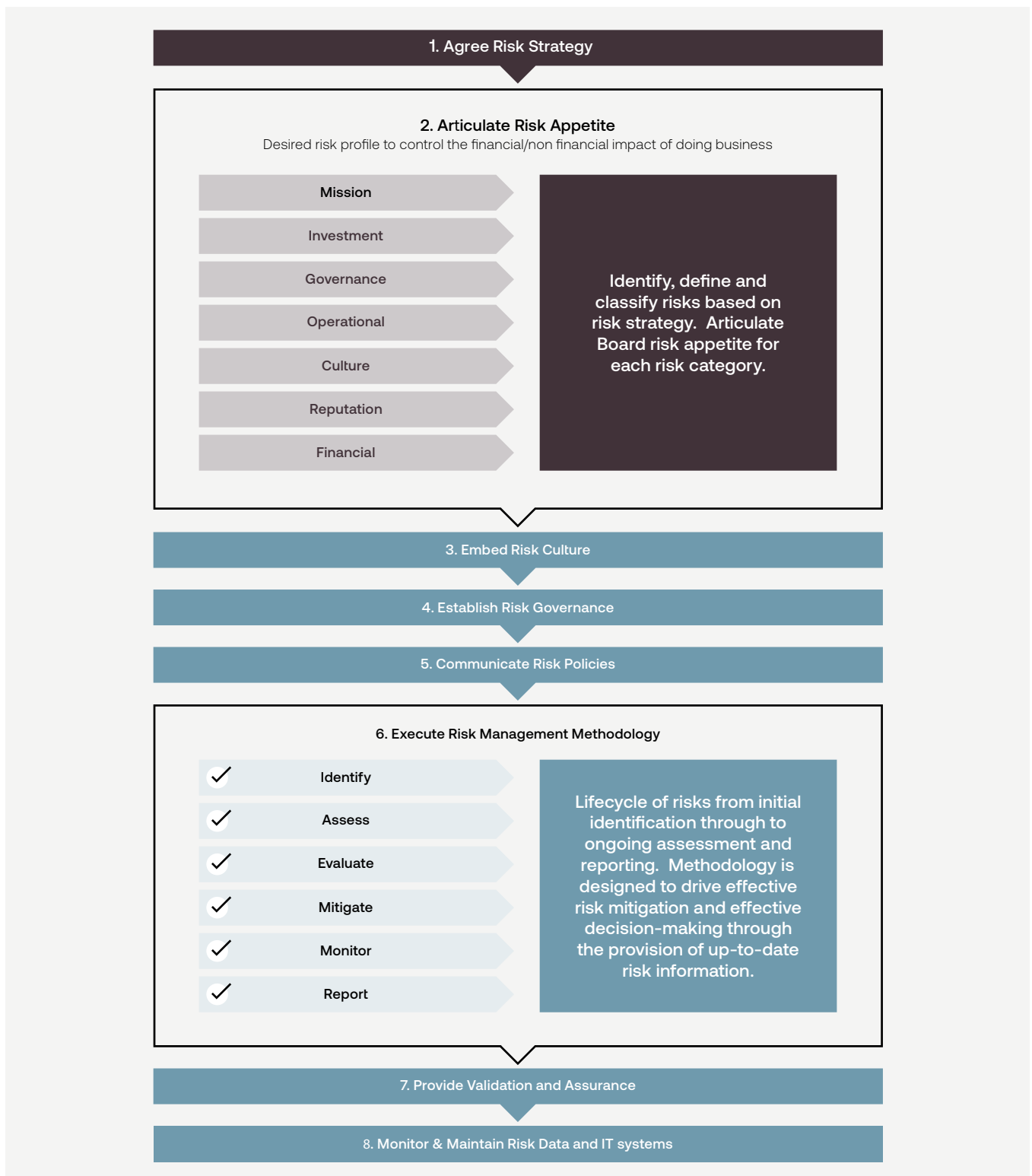
The RMF is designed to:

- ◆ Establish common principles and standards for the management and control of all risks.
- ◆ Guide behaviour across the organisation.
- ◆ Provide a shared framework to improve awareness and understanding of the Bank's risk management processes.
- ◆ Provide clear accountability and responsibility for risk management across the Bank.



Overview of the Bank's Risk Management Framework

The RMF supports the Bank to identify, assess, evaluate, mitigate, monitor and report the risks the Bank faces.





1. Risk Strategy

The Bank's Risk Strategy is guided by and supports the delivery of the Bank's missions, Business Plan and Investment Strategy.

The Bank's internal risk team supports the Bank by providing independent and objective challenge to ensure that the Bank has an effective control framework and operates according to the Bank's Risk Appetite. The Bank will achieve this by adopting a collaborative approach that values:

- ◆ Positive engagement
- ◆ Constructive challenge
- ◆ Independent monitoring
- ◆ Objective assessments of risk
- ◆ Efficient support



2. Risk Appetite

2.1 Risk Definition and Categorisation

As part of the overall risk management strategy, risks are monitored and reported to ensure that the Bank has a complete and robust understanding of all the risks it faces. The definitions for all the Level 1 risks are defined in Table 1 below. The Bank uses Level 1 risk types as a basis for comprehensive and consistent identification of risks, wherever they may arise, as well as for reporting purposes.

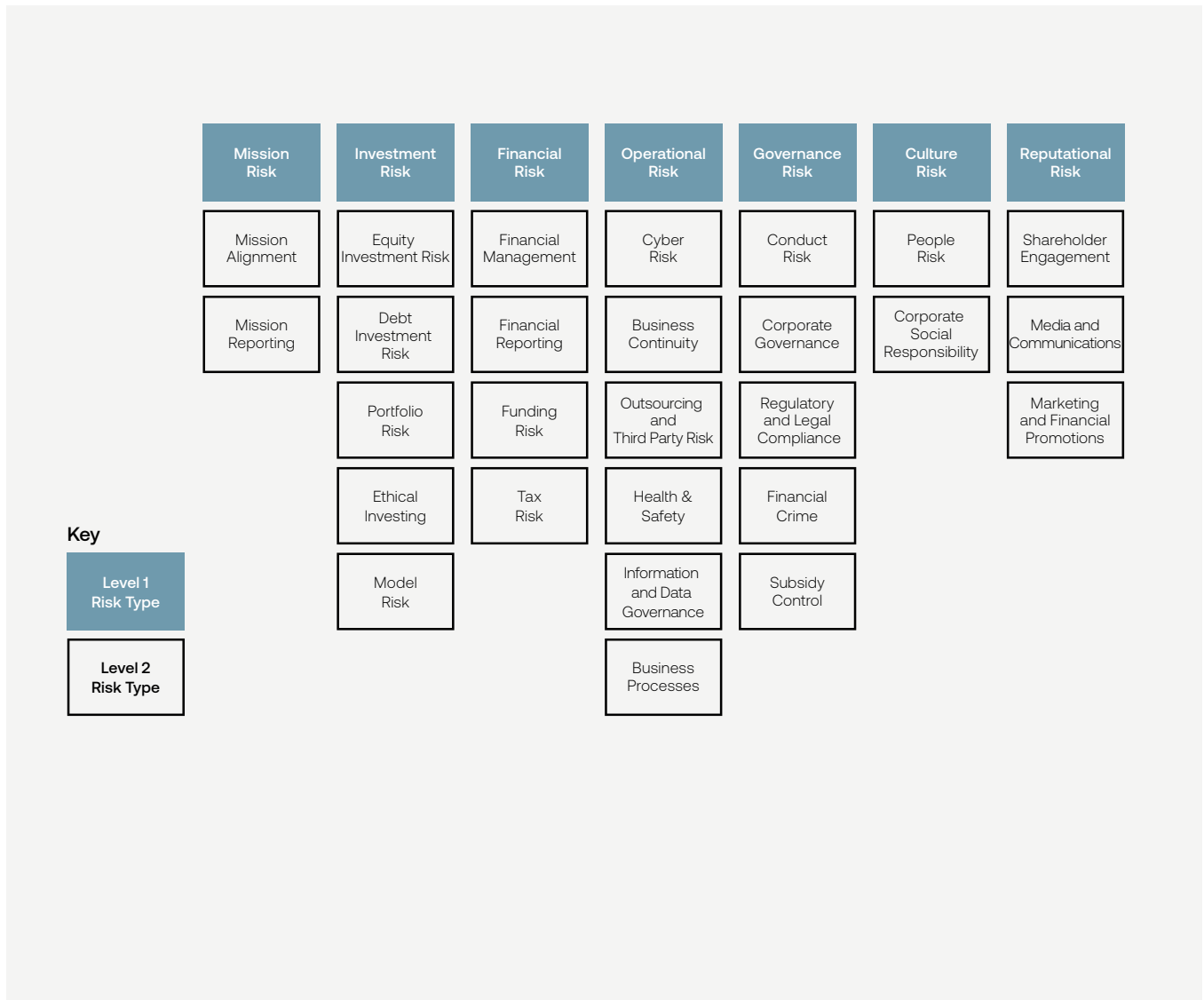
Table 1: Level 1 Risk Categories

| Risk | Definition |
|-------------------------|---|
| Mission Risk | The risk that investments made by the Bank are not sufficiently aligned to a mission or fail to deliver the desired benefits. |
| Investment Risk | The risk of losses due to failed investments or inadequate portfolio management creating volatility that could result in losses. |
| Financial Risk | The risk of unstable capital or liquidity arising from fluctuations in funding streams, investment returns, financial performance or external factors. |
| Operational Risk | The risk of direct or indirect losses resulting from inadequate or failed internal processes, people and systems or from external events. |
| Governance Risk | The risk that the Bank's frameworks and processes for decision making are ineffective or are not supported by the Bank's culture and high standards of conduct. |
| Culture Risk | The risk that the Bank's culture fails to encourage respect, collaboration, collective and personal responsibility. |
| Reputation Risk | The risk that stakeholders form a negative view of the Bank due to actions by its employees, partners, third parties or invested companies. |



Each Level 1 risk type is further sub-classified to Level 2 risk types, to further aid effective risk identification and assessment. The Bank’s Level 1 risks and the corresponding Level 2 key sub-risks are detailed below (see Figure 2).

Figure 2: Level 2 Risk Types





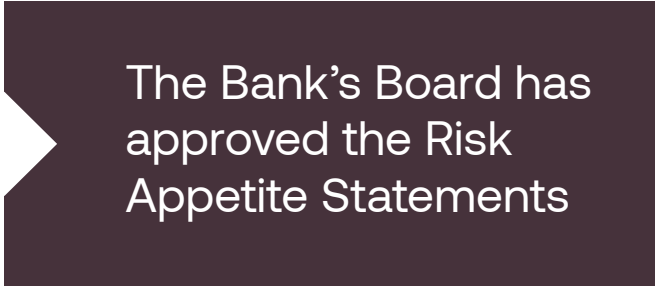
Ownership and Governance

The Board has overall accountability for approving, owning and monitoring the Bank's risk appetite, and delegates its implementation responsibility to the Board's Risk Management and Conflicts Committee. The Head of Investment Risk and General Counsel are jointly responsible for ensuring a robust approach is in place for setting, approving and monitoring risk appetite on an ongoing basis, and for responding to breaches in a timely and effective manner. The Head of Investment Risk and General Counsel work closely with other members of the executive team in clearly defining roles and responsibilities in relation to risk appetite.

2.2 Risk Appetite Statements

The Bank has developed and maintains Risk Appetite Statements that set out the types and levels of risk that the Bank is willing to accept, or pro-actively avoid or limit, in pursuit of the missions, Business Plan and Investment Strategy.

Qualitative statements of risk appetite cover all of the Bank's Level 1 and Level 2 risk types, and are complemented by a comprehensive set of quantitative measures that are regularly monitored to assess adherence to the Bank's overall risk appetite.



The Bank's Board has approved the Risk Appetite Statements



3. Risk Culture

Developing an appropriate risk management culture is key to supporting the effective operation of the Risk Management Framework to enable informed risk-based decision-making in the Bank. The Bank encourages risk taking within controlled boundaries where the expected rewards exceed the expected cost of that risk to achieve the Bank's objectives.

The Bank believes that a positive risk management culture exists when everyone understands the organisation's approach to risk, takes personal responsibility to manage risk in everything they do, and encourages others to follow their example.

The Bank aims to develop a risk culture by designing and embedding risk policies through communication and staff training regarding the Bank's activities, strategy and risk profile. The Bank's objective in relation to risk management culture is that management and all employees understand and champion the basis for risk measures and risk management programmes.

4. Risk Governance

Risk governance collectively refers to the role and responsibilities of the Board, the Bank-wide risk management resources, and the independent assessment of the Bank's risk governance structure. The Bank's approach to risk governance ensures that risk management is directed and controlled by the Bank's Board and utilises hierarchical management control structures and management information (MI).

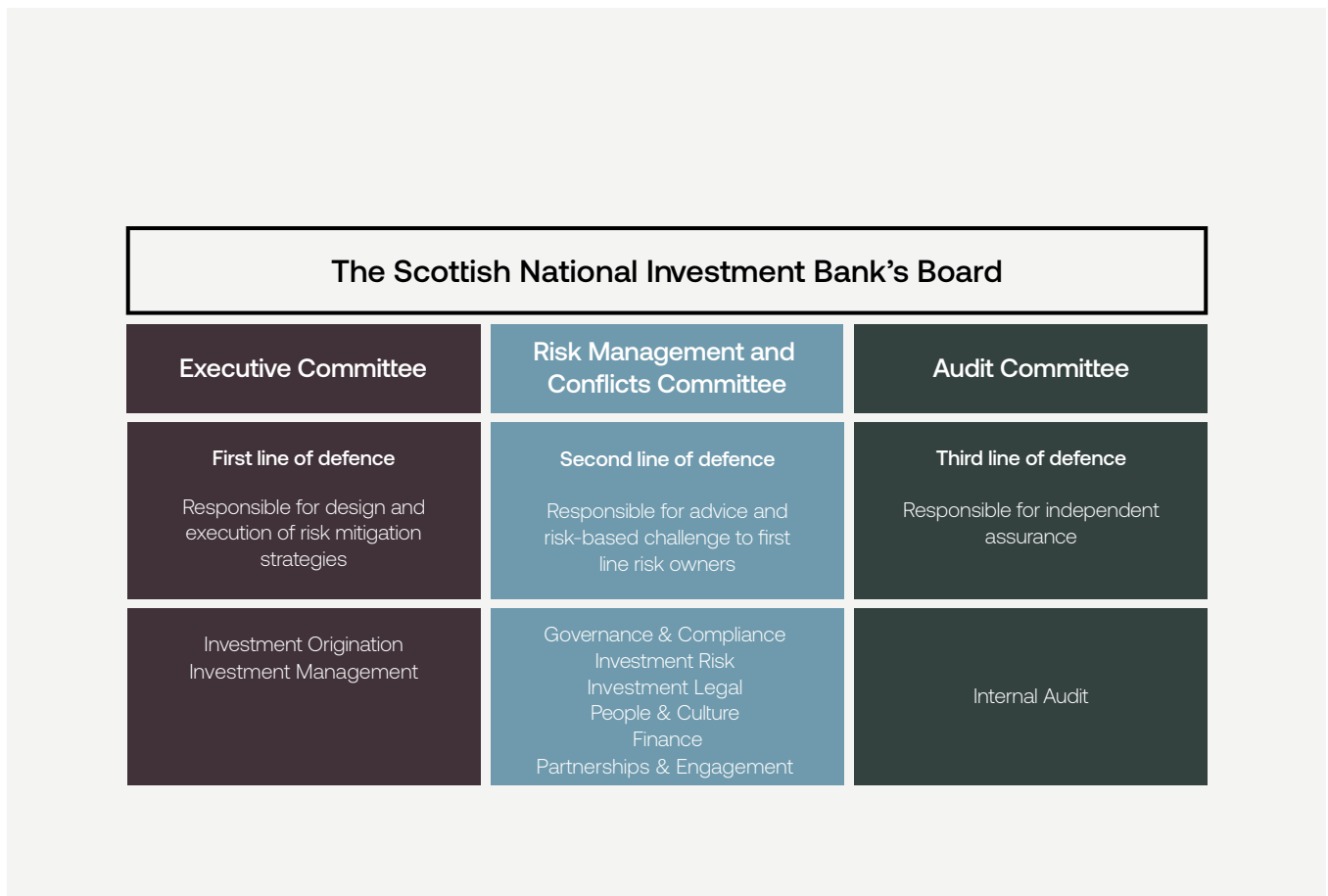


4.1 Three Lines of Defence

For any RMF to function effectively it is important that the roles and responsibilities for the management of risk are clearly defined, communicated and widely understood. The Bank’s approach to assigning these responsibilities is based upon the three lines of defence risk governance model, common to most investment organisations (see Figure 3).

- ◆ The first line of defence is responsible for the day-to-day identification, reporting and management of risks.
- ◆ The second line of defence is responsible for the design of risk policies, methodologies, identifying risks (in collaboration with first line), monitoring performance and compliance, risk reporting and providing objective independent review, monitoring, and appropriate challenge to the first line of defence.
- ◆ The third line of defence provides independent assurance of the overall system of internal control including assessment of the risk governance framework.

Figure 3: Three Lines of Defence Risk Governance Model





The key principles of the Bank's three lines of defence model are as follows:

- ◆ The Board has overall accountability and responsibility for the management of risk within the Bank.
- ◆ The Board delegates specific risk management roles and responsibilities to the Board Risk Management and Conflicts Committee, the Audit Committee and Chief Executive Officer (CEO) and General Counsel.
- ◆ The CEO is supported in delivery of these responsibilities through direct reports in the Executive Committee.
- ◆ The Head of Investment Risk and General Counsel have direct access to the Board Risk Management and Conflicts Committee and Audit Committee respectively to escalate risks and issues. However, they also have a reporting line into CEO for day-to-day operations of the business.
- ◆ The risk functions work collaboratively with the other central control functions (Compliance, Legal and Internal Audit).
- ◆ The roles of General Counsel and Head of Investment Risk are defined and overseen by the Audit Committee of the Board and are set out in the Bank's Internal Audit Charter.

4.2 Risk Management Skills & Resources

- ◆ All employees play a role in effective management of risk. This may involve the management of specific risks and controls delegated to them as part of their role or the general wider responsibility of all employees relating to relevant legislation.
- ◆ All employees have a duty to openly share and escalate risk and control information with their respective managers. This includes identifying changes in existing risks, breaches of risk appetite, new or emerging risks and the inadequacy or failure of controls.
- ◆ The Bank has in place communications, training, performance management and reward structures which support effective operation of the RMF, which are kept under review.



5. Risk Policies

The Bank's risk management policies outline the expected requirements to identify, assess, control and monitor specific risks. Compliance with the Bank's risk policies supports the achievement of the business and risk objectives and balances the needs of all stakeholders.

The Bank's risk policies and the associated procedures demonstrate how the requirements of these policies are met. These policies:

- ◆ Clarify that in addition to complying with legal and regulatory requirements and internal policies, employees are expected to conduct themselves with honesty and integrity and perform their duties with due skill, care and diligence; promote risk awareness through a strong risk culture, conveying management's expectation that activities will not go beyond the defined risk appetite and limits set by the Bank, and the respective responsibilities of employees.
- ◆ Set out principles on, and provide examples of, acceptable and unacceptable behaviours linked in particular to financial misreporting and misconduct, and economic and financial crime.
- ◆ Ensure that employees are aware of the potential internal and external disciplinary actions and legal actions that may follow misconduct and unacceptable behaviours.



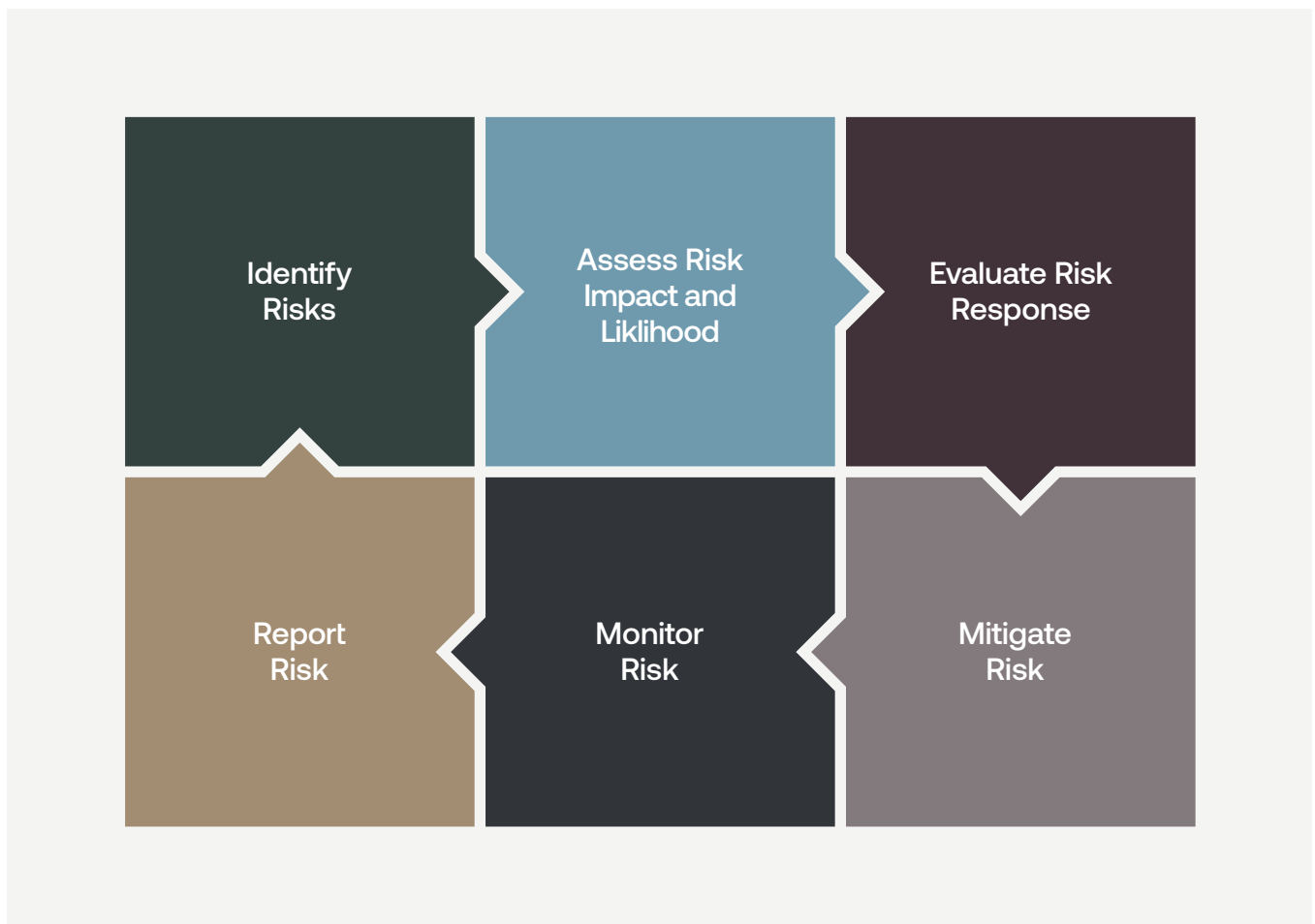
6. Risk Management Methodology

The Bank's primary processes for managing the risks inherent in its business model are defined in its risk management methodology. The risk management methodology is consistently applied by all its employees and delivery partners to control and manage risk. The Bank's risk management approach is grouped into six inter-dependent risk management methodology categories, which are set out in the 'Risk Management Cycle' below (see Figure 4).

Within each of the risk management methodology categories the Bank has documented clear guidelines. Collectively these guidelines constitute the Bank's risk management approach. The guidelines for each risk management methodology category are described below.

The Bank follows this risk management methodology when making investment decisions. A more detailed risk management methodology relating to the investment activity is documented in the Investment Risk Policy.

Figure 4: Risk Management Cycle





6.1 Risk Identification

Each year the Bank identifies the main risks to the business, and to achieving the business plan.

To ensure appropriate identification of the risk types, the Bank uses a 'Material Risk Identification Process' (MRIP). The aim of the MRIP is to provide adequate transparency and understanding of the existing and emerging risks across the Bank. The MRIP is a risk evaluation process carried out with the aim of obtaining a comprehensive view of the Bank's risk exposure and to provide the management with an updated view of the Bank's risk profile.

The MRIP leverages intelligence across organisational levels and utilises existing information whenever possible. As part of this process the business (first line of defence) and risk functions (second line of defence) work closely to leverage insights and to strengthen the downstream capabilities, such as strategic planning and scenario design for stress testing. Following the completion of the MRIP a risk inventory is updated across all the risk types.

6.2 Risk Assessment

Once all potential risks have been identified, the Bank's Enterprise Risk team assesses them by taking into consideration the impact and likelihood of each identified risk on the business and the effectiveness of the corresponding control environment. This Risk Assessment is undertaken annually and is led by the Head of Enterprise Risk.

The assessment of risk combines both quantitative and qualitative measures in order to assess and mitigate, in a comprehensive way, the key impacts of the identified risks to the Bank.

6.3 Risk Evaluation

Following the completion of the MRIP and mitigation process the Bank's Enterprise Risk team presents a report to the Board Risk Management and Conflicts Committee summarising all the risk types that the Bank is exposed to along with the options for the development or enhancement of controls. On the basis of this report, the Board Risk Management and Conflicts Committee agrees on Level 1 and Level 2 risk types for the Bank which then feeds into the Risk Appetite Statement (RAS).



6.4 Risk Mitigation

If the Bank's Executive Committee decides, based on the risk evaluation, that further mitigation is required, control tools are designed and implemented to enable us to mitigate those risks. These 'key risk controls' are set out below.

Key Risk Controls

Policies: Policies establish clear and prescriptive rules and requirements for the execution of relevant business activities. The Bank's policy standards are mandatory requirements that are adhered to in all but exceptional circumstances. Policy provisions outline the criteria for managing the risk profile in line with the Board approved RAS by defining explicit control objectives and requirements.

Operating Procedures: The Bank's operating procedures describe in detail the specific process that is followed to operationalise a policy, or a specific element of a policy. Operating Procedures are typically narrower in scope than policies as they relate to a specific control process. Taken as a whole, the Bank's Operating Procedures are sufficiently broad in coverage to ensure that all elements of the policies can be operationalised and controls performed. Operating procedures are designed to assure the control objectives of the policies. Operating procedures are owned and executed by relevant teams.

Effectiveness of control assessment: To complete risk evaluation the Bank conducts an assessment of the effectiveness of the control environment related to all the identified risk types across all the risk categories (i.e. high impact, medium impact, low impact, high likelihood, medium likelihood and low likelihood).

6.5 Risk Monitoring

The Bank monitors the results provided by the control tools in order to assess the risk profile of the Bank on a continuous basis. Monitoring risk exposures and underlying environmental conditions is an ongoing activity, recognising that these could change regularly.

Risks are monitored by the first line of defence, which has a key role in ensuring robust risk management is practiced within the Bank in line with the RMF. Risk controls are tested by second line of defence to ensure their effectiveness. The assessment of control effectiveness forms part of risk reporting and monitoring. Control monitoring is how members of the Bank's Executive Committee obtain positive confirmation that controls are working as intended.

6.6 Risk Reporting

Reporting of risk is how the Bank ensures that it is effectively prepared to respond to risk events as they arise. Reporting is also critical in ensuring that the Bank maintains proper disclosure and communication with key internal and external stakeholders.

It is the responsibility of everyone in the Bank to be properly informed of the risks they run, and to ensure these are properly reported to the appropriate governance committee.

Having timely, accurate and insightful MI to monitor risk levels is critical, and appropriate risk reporting and monitoring information is regularly provided to the Bank's Executive Committee and Board Risk Management and Conflicts Committee.



7. Validations and Assurance

The Bank use validation to confirm that the Bank's RMF is performing as expected, in line with its objectives. The RMF is regularly monitored, reviewed and tested by the Head of Enterprise Risk. Internal Audit and the external Auditor provide independent assurance to the Board about the validity of the framework. Validation processes ensure that all the key components of the framework are embedded across the Bank, and interact to align to the risk strategy and the overall business plan.

8. Risk Data & IT Systems

The Bank recognises the importance of making available timely, complete and accurate information that underpins the quality of the risk management decisions made on a day-to-day basis. The Bank's risk data and IT systems have been designed to supply risk management processes with the information needed to operate effectively and produce the output required to deliver the risk strategy.

8.1 Risk Data

The Bank's External Reporting Policy and Financial Reporting Policy set out the standards for ensuring consistency of risk reporting practices. The Data Policy outlines the end-to-end process of defining, gathering and processing of risk data to meet all the risk reporting requirements.

8.2 Risk IT Systems

The Bank maintains physical and systems infrastructure to ensure it is reliable and fit for purpose. The Bank is ensuring that its infrastructure and processes are sufficiently scalable to accommodate anticipated growth.