Risk Management Framework

The Scottish National Investment Bank

2022

The Bank's Board and Management Team believe that effective risk management is intrinsic to successful achievement of strategic objectives and the creation and protection of shareholder value.

Contents

1. Introduction

The Bank's Board and Management Team believe that effective risk management is intrinsic to successful achievement of strategic objectives and the creation and protection of shareholder value.

To this end, the Bank operates a *risk management framework* ('the Framework', 'RMF'). The Framework is the collection of principles, policies, processes and decision-making structures that contribute to the effective management of risk at the Bank.

The goal of the Framework is not to eliminate risk, but to support decision-making that manages it to a level that is aligned to Stakeholder expectations.

The Framework is underpinned by a risk-aware culture at the Bank, and the positive risk behaviours associated with this.

1.1. Definitions and scope

The Framework uses the ISO definition of risk, namely the "effect of uncertainty on objectives". Note that this definition implies both positive and negative effects, as well as objectives at all levels of the business planning hierarchy (strategic, project, operational, etc).

The Framework covers all business activities and types of risk. The standards outlined in the Framework apply to all employees and third-party contractors operating on behalf of the Bank.

1.2. Ownership and governance

While the Board are ultimately responsible for risk management at the Bank, this Framework is owned on behalf of the Bank's management by the General Counsel. The design and implementation of the Framework is overseen by the Risk Management and Conflicts Committee, who are required to review and approve the document on at least an annual basis.

The document should be reviewed more frequently in the event of a significant change in any of the Bank's business model, strategy or operating environment.

1.3. Related documents

The Framework is the senior policy relating to risk management and so is deliberately high-level in nature. However, there are other supporting internal policies, procedures and other key reference documents that provide further detail to support implementation of the Framework.

These are detailed in Appendix 1.

1.4. Reference Frameworks

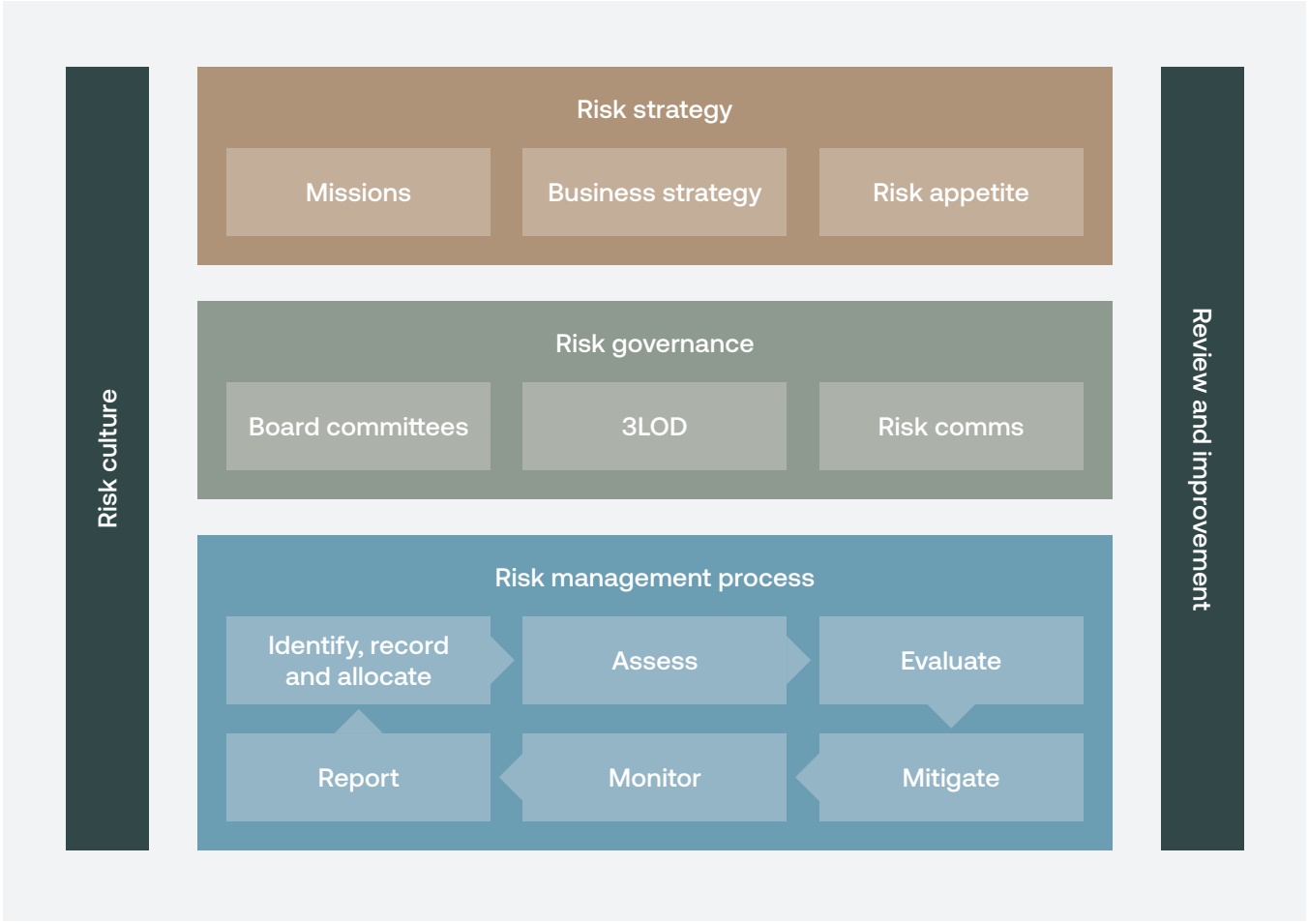
The Bank's Board have taken into account a range of stakeholder requirements in designing the Framework, including the Risk Management chapter in the Scottish Public Finance Manual and the guidance contained within the FCA Handbook (SYSC sourcebook, in particular).

The Framework design also references the standards outlined in the International Organisation for Standardisation's ('ISO') standard on Risk Management (ISO 31000).

However, care has been taken in the design of the Framework to ensure proportionality to the Bank's size and complexity, as well as alignment to the Bank's approach to delivery against strategic objectives.

1. Introduction continued

1.5. Risk Framework summary



2. Risk strategy

The Bank's strategic approach to risk management is intrinsically linked to the Bank's overall strategy. Therefore, there are elements of the risk strategy that are fixed and those that are more dynamic.

2.1. Missions

The Missions are a set of concrete challenges that the Scottish Government consider to be of high societal importance. A mission-oriented approach encourages transformative solutions that are sector and technology neutral. As such, the Missions do not specify the solutions, nor the types of businesses or sectors in which the Bank should invest. The Missions are considered to be a collective endeavour involving the Bank, the Scottish Government, and other partners – all of which use the levers under their control to tackle these challenges faced by Scotland.

The Missions are intended to be in place long enough for the Bank's activities to have a measurable impact. However, the Scottish Ministers may choose to modify the missions, either driven by an emerging challenge or following the request of the Bank's Board.

2.2. Business strategy

The vision of the Bank is supported by a desire to increase the supply and diversity of debt and equity capital available to Scottish businesses and projects. The Bank will invest on commercial terms. The Bank will develop its own investment pipeline and will invest through a variety of instruments including debt, equity and mezzanine finance.

2.3. Risk strategy

The Bank's approach to risk management supports and complements the above strategy, but also seeks to add value through challenge and independent oversight of business activities.

Through this Framework, the Bank aims to deliver the following strategic risk objectives:

- Clear articulation of the level of risk the Bank is willing to take in pursuit of its business objectives and missions;
- Risk management activities are proportionate to the nature, scale and complexity of the Bank as it changes over time;
- A positive risk management culture exists at the Bank – where each employee understands their personal responsibilities and leads by example in delivering these;
- Risk is taken into account in every decision, from day-today operations to strategic resource allocation;
- There is a culture of compliance where regulatory requirements are followed in spirit and in letter;
- Operational incidents and failures of internal control are seen as a source of risk intelligence and an opportunity to learn and improve;
- Ensure that climate related risks and opportunities, both physical and transition, are appropriately identified, reported and managed; and
- The principles of risk management applied to the Bank are extended to the wider enterprise, including key third party suppliers.

2. Risk strategy continued

2.4. Risk appetite

A key pillar of the risk strategy at the Bank is the concept of risk appetite and its application to strategic and day-to-day decision-making processes. Risk appetite is defined as the level of risk that the Bank is prepared to accept in pursuit of its objectives, before action is deemed necessary to reduce the risk. The Board considers and approves the types and levels of risk it is willing to accept, or seeks to avoid or limit, in pursuit of the Bank's business strategy and objects. This is articulated to the business through a series of risk appetite statements. Management then seeks to embed these into all business activities through effective process design and appropriate risk governance.

The qualitative risk appetite statements are applied to the risk management process in a number of ways, influencing mitigation strategies and monitoring through key risk indicator thresholds. See Section 5 below for more detail.

The Board Risk Management and Conflicts Committee undertakes a full review of the risk appetite statements on an annual basis or more frequently in the event of material changes within the Bank or in the external environment.

The Internal Audit function reviews the Bank's approach to Risk Appetite on a periodic basis in line with its rolling three-year risk-based plan.

3. Risk culture and governance

3.1. Corporate culture and values

Effective risk management is an intrinsic part of the Bank's culture, as manifested through the three core values:

- Our **missions at the heart** of everything we do;
- We are **passionate and progressive**; and
- **Working in partnership** towards a fairer, sustainable, more innovative Scotland.

Risk awareness and management are not add-ons to the desired culture at the Bank, but central to it. Management are empowered to take the right amount of risk, to learn lessons from successes and failures and to maintain an openness and transparency that facilitates constructive challenge from colleagues and stakeholders.

3.2. Risk culture

An appropriate risk management culture is key in supporting the effective operation of the RMF and 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.

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 further develop the risk culture through reviewing and embedding appropriate risk policies, communication and training regarding its activities, strategy and risk profile. The Bank's objective in relation to risk management culture is that the management understands and champions the basis for risk measures and risk management programmes.

3.3. Risk communication

It is the responsibility of the Executive Committee to ensure that the strategy and culture for risk and compliance management are cascaded and embedded throughout the Bank. This is to ensure that all employees are aware of the approach to risk management and their individual responsibilities when executing their day-to-day duties. Each policy owner is responsible for ensuring that the respective risk management policy is cascaded and embedded to all relevant employees within the Bank.

The Bank embeds its risk management culture through a number of perspectives as summarised below:

- **Tone from the top**

  The Bank's management, including key function holders contributes to the internal communication of core values and expectations to staff. The Board and Executive team will promote, monitor and assess the risk culture of the Bank; consider the impact of the risk culture on the financial stability, risk profile and robust governance of the institution; and make changes where necessary.

- **Accountability**

  Employees at all levels are expected to know and understand the core values (including the Vision, Business Objects, Missions, Business Strategy and Risk Strategy) of the Bank and, to the extent necessary for their role, its risk appetite. All employees are aware that they are held accountable for their actions in relation to the Bank's risk-taking behaviour.

- **Effective communication and challenge**

  Promote an environment of open communication and effective challenge in which the decision-making processes encourages a broad range of views, allows for testing of current practices, stimulates a constructive critical attitude amongst the employees, and promotes an environment of open and constructive engagement throughout the Bank.

3. Risk culture and governance continued

- **Incentives**

  Appropriate incentives play a key role in aligning the risk-taking behaviour with the Bank's risk profile and long-term interest. The Board and the Executive team seek to reward and encourage all employees to demonstrate the right behaviours and culture as reflected in the Remuneration Policy.

- **Collaboration**

  The 1st line of defence and the 2nd line of defence (LOD) actively work in synchronisation in managing the Bank's risk profile. The 2nd LOD must ensure that it maintains operational independence at all times from the 1st LOD.

- **Active Discussion**

  Risk and compliance matters are actively discussed as part of daily/weekly/monthly team meetings and committees. A holistic view of the Bank's risk and compliance issues are reviewed and discussed at the Board's Risk Management and Conflicts Committee and Valuations Committee.

3.4. Policies

Risk management policies support the Framework and outline the minimum requirements that must be achieved by the Bank 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 GLRC function documents risk policies and procedures for how the risk and compliance requirements are met. These policies, and the promulgation of them:

- Remind employees that the Bank's activities are to be conducted in compliance with the applicable law and regulations and with the Bank's risk strategy;
- Promote risk awareness and a strong risk culture, conveying management's expectation that activities will not go beyond the defined risk appetite and limits defined 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, economic and financial crime;
- 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; and
- Ensure that employees are aware of the potential internal and external disciplinary actions and legal actions that may follow misconduct and unacceptable behaviours.

The GLRC function is responsible for developing, documenting and maintaining risk management policies and for overseeing their approval.

The following roles are nominated for each risk management policy to ensure that the policies are managed in a consistent manner across the Bank:

- There is a risk policy owner for each Level 1 risk at a minimum, who defines the policy requirements;
- Each risk type is reported on a regular basis to the Board Risk Management and Conflicts Committee or the Board; and
- The General Counsel is accountable for delivery, maintenance and monitoring of compliance for all the risk policies.

Policies are drafted using a standard template to ensure consistency and familiarity.

Compliance with policies is monitored by the risk functions on a regular basis and policy breaches are escalated to the appropriate level within a set timeframe. The GLRC and Investment Risk functions are responsible for managing the remediation of exceptions and the formal review of all risk policies.

3. Risk culture and governance continued

3.5. 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 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).

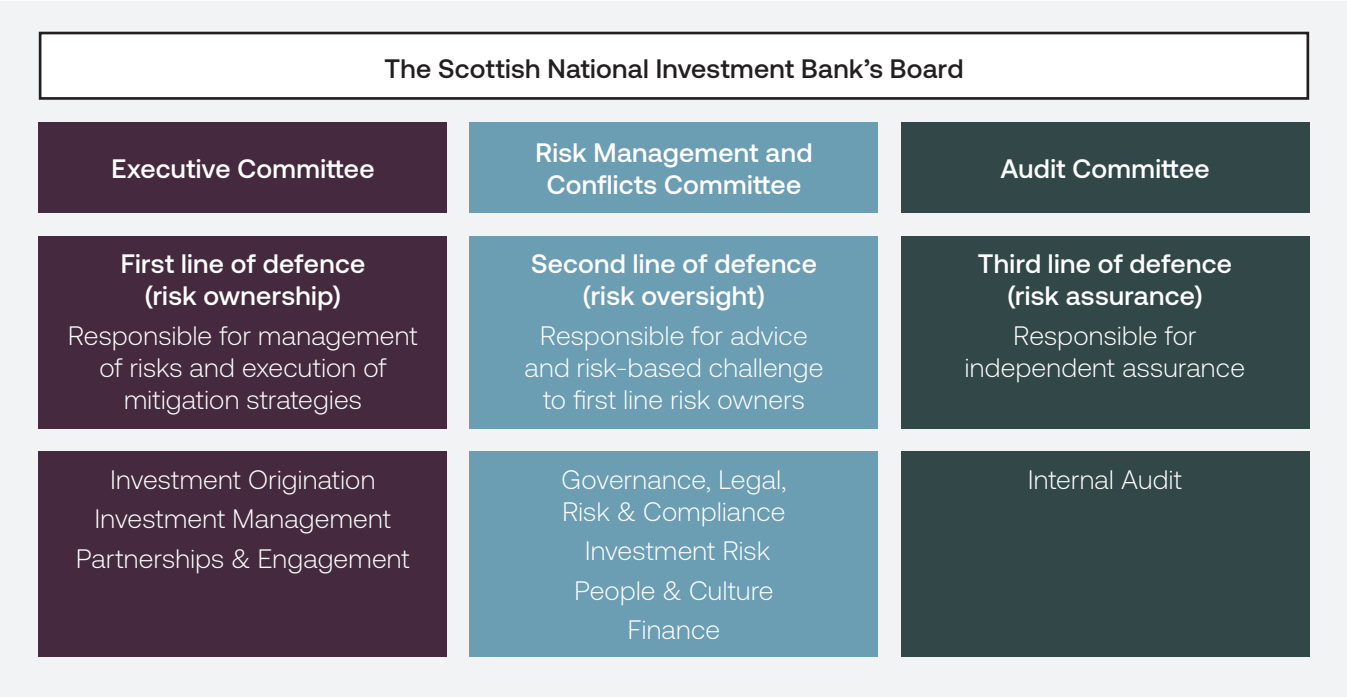
The key principles of the Bank's risk governance model are as follows:

- The Board has overall accountability and responsibility for the management of risk within the Bank via delegated authority from the Scottish Government;
- The Board delegates specific risk management roles and responsibilities to its sub-Committees (primarily Risk Management and Conflicts Committee and Audit Committee, but also the Nominations and Remuneration and Valuations Committees);
- The Board delegates the day-to-day management of risk to the Executive Committee (and to the CEO, in particular as Accountable Officer);
- The General Counsel has direct access to the Board Risk Management and Conflicts Committee and Audit Committee for the escalation of risks and issues. However, they also have a reporting line into the CEO for day–to-day operations of the business; and
- The role of Internal Audit is defined and overseen by the Board Audit Committee and is set out in the Bank's Internal Audit Charter.

For the Framework 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 a "three lines of defence" model.

3.6. Three lines of defence model

The effective execution of risk management roles and responsibilities is enabled through the adoption of the three lines of defence risk governance model.



3. Risk culture and governance continued

The first line of defence is responsible for day-to-day management of risk and control. Function heads have primary accountability for the performance, operation, compliance and effective control of risks affecting their business area. The Executive Committee monitors the overall risk profile and ensures that the RMF is implemented and embedded in business operations.

The second line of defence consists of an independent risk management capability that provides objective independent review, monitoring, and appropriate challenge of the operation of the first line. This includes oversight of the effectiveness of functions in managing risk, and the controls in place to mitigate any risks. The Head of Investment Risk and Head of Operational Risk exercise objective scrutiny of all risk-based decisions and provide reporting to the Board Risk Management and Conflicts Committee.

The third line of defence provides independent assurance to the Board via the Audit Committee. It is independent of both management and the risk functions. The primary source of third line assurance is Internal Audit, which is provided through a programme of risk-based Audits. The annual planning process for risk-based Audits takes into account the risk management information generated from the application of the Risk Management Process. The findings of these Audits are reported to management and the Audit Committee.

Although External Audit and Audit Scotland are not part of the Bank's internal risk governance model, each plays an important role in providing feedback to the Board in terms of risk management effectiveness.

The Scottish Government (as the Bank's sole shareholder) does not have a role in the Bank's internal governance or the operational decisions made by the Board. As set out in the Shareholder Relationship Framework Document, the Scottish Government gives the Board "delegated authorities" which define the parameters under which the Bank is permitted to operate. The Board escalates matters to the Scottish Ministers where there are decisions to be made which fall outside the delegated authorities. In addition, the Bank will formally escalate any significant risks or issues through the Scottish Government team to ensure the team are aware of them as appropriate.

4. Risk classification

The Bank is exposed to a wide range of uncertainties, arising from within the Bank and in the external environment. To aid with the understanding and management of these, the Bank classifies its risk universe into several risk types. This supports the clear allocation of ownership of risk, the documentation of root causes and impacts, the design of mitigation strategies and provides structure to risk reporting to interested stakeholders.

It should be noted that these risk types may not always be mutually exclusive, with boundary risks and contagion between risk types possible.

4.1. Risk taxonomy

The main tool of risk classification is the Bank's risk taxonomy. The taxonomy seeks to define (at a high level) the main types of risk that the Bank is exposed to. Seven of these "Level 1" risk types have been identified, as shown below:

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.
Environmental, Social and 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, or that decisions are made, or actions undertaken that do not take account of the environmental and/or social implications therein.
Culture Risk	The risk that the Bank's culture fails to encourage respect, collaboration, collective and personal responsibility.
Stakeholder Risk	The risk that stakeholders form a negative view of the Bank due to actions by its employees, partners, third parties or invested companies.

4. Risk classification continued

Each Level 1 risk type is further sub-classified into "Level 2" risk types, which is the level at which the risk management methodology (ownership, analysis, mitigation, reporting, etc) is applied.

The Bank's Level 1 risks and the corresponding Level 2 key sub-risks are detailed below.

Mission Risk	Investment Risk	Financial Risk	Operational Risk	Environmental, Social & Governance (ESG) Risk	Culture Risk	Stakeholder Risk
Mission Alignment	Equity Investment Risk	Financial Management	Technology and Cyber Risk	Corporate Governance	People Risk	Shareholder Engagement
Mission Reporting	Debt Investment Risk	Financial Reporting	Business Continuity	Conduct Risk	Corporate Social Responsibility	Media and Communications
	Portfolio Risk	Funding Risk	Outsourcing and Third-Party Risk	Regulatory and Legal Compliance		Marketing and Financial Promotions
	Ethical Investment Risk	Tax Risk	Employment Practice and Workplace Safety (H&S)	Financial Crime		
	Model Risk		Information and Data Governance	Climate Related Risk		
	Subsidy Control		Execution Delivery and Process Management			
			Fraud			

Key

Level 1 Risk Type

Level 2 Risk Type

The classification of risk is formally reviewed on an annual basis, in line with the review of this Framework. However, management are constantly considering whether new threats and opportunities that could impact on how the Bank thinks about risk. In this case, any proposed changes to the taxonomy would be approved by the Board Risk Management and Conflicts Committee, which meets quarterly.

5. Risk management process

To embed the risk strategy into the Bank's operating and investment models, a Risk Management Process (referencing ISO 31000) has been established and rolled-out to all staff. The Process is cyclical, consisting of six sequential process steps, described in more detail in the sections below:

This Process is applied to all risk types, with the exception of Investment Risk, which is managed on a transaction and portfolio basis, rather than through the cyclical identification and assessment of specific risks. The process for the management of Investment Risk is outlined in the separate Investment Risk Management Framework.

5. Risk management process continued

5.1. Risk identification and recording

Risks are, by their nature as uncertain future events, somewhat intangible. Therefore, management and the Board apply a range of processes and sources to identify potential threats and opportunities relating to the Bank's business model and external environment.

All employees are encouraged to pro-actively identify risks in their area of the business and to discuss these with their line manager and/or a member of the risk function. A particularly rich source of risk intelligence is the process for managing risk events, which has control improvement and learning of lessons as core objectives.

Operational Risk will, from time-to-time facilitate risk identification workshops with various groups of staff and Board members. These sessions can take place at any time, but form a key part of the annual business planning cycle in the second half of the financial year, where 2nd line challenge and testing of assumptions is applied to enhance the rigour of the planning activities.

The Bank's risk taxonomy (see section 4.1 above) articulates the main risk types inherent in the Bank's business model. This is regularly reported to the Bank's Risk Management and Conflicts Committee and is subject to a formal annual review by the Risk Co on behalf of the Board.

All Level 1 risks are allocated to a member of the Executive Committee as risk sponsor, as well as to a risk owner for day-to-day management. Responsibility for second line oversight will also be identified at this stage.

Each Level 2 risk in the taxonomy (with the exception of investment risks) is recorded in the Bank's risk register and subject to further analysis in terms of root cause and potential effects of the risk materialising.

5.2. Risk assessment and evaluation

Identified risks are assessed on the basis of both the potential impact on business objectives and the likelihood of this impact materialising. Risks are assessed on both an inherent and residual basis, i.e. before and after the effects of current mitigating activities are taken into account. Therefore, this step will require the identification and documentation of mitigating activities.

See Appendix 2 for further detail on the standard assessment criteria.

Having quantified the risk based on impact, likelihood and the current control environment, the risk owners should then make a decision as to whether and how to manage the risk going forward. This decision should take into account the Board's stated appetite for the risk in question, as well as the resources required to implement any mitigation strategies.

The options under consideration are to:

(i) **tolerate** the risk as being within appetite;

(ii) **treat** the risk by implementing additional internal controls or other mitigation;

(iii) **transfer** the risk or part of the risk to a third party (e.g. through insurance); or

(iv) **terminate** the activity that is the source of the risk.

This process of assessment and evaluation is formally applied to all Level 2 risks, but can also be used to provide objective assessment of other types of risks, such as those arising from change activity or new fund structures.

5. Risk management process continued

5.3. Risk mitigation

If the risk owner decides that the risk cannot be tolerated based on the residual risk assessment, then further action will be required. This will usually take the form of an ongoing risk mitigation plan, although it is also possible that the action will be to change the business model to prevent the risk arising in the first place.

Risk mitigation can take a number of forms, including the implementation of internal controls such as segregation of duties, independent checks or logical access restrictions. Recruitment of additional staff, or training for existing staff (perhaps via policy dissemination) could also provide further risk mitigation.

The first line risk owner is responsible for the design and implementation of the risk mitigation plan, with oversight and challenge from the second line of defence (primarily the Operational Risk function).

5.4. Risk monitoring and reporting

The first line risk owner is responsible for establishing mechanisms for ongoing monitoring of the effectiveness of internal controls and to identify any changes in the internal or external environment that would suggest a change in risk profile. The second line of defence will take an oversight role in this process, including testing of controls challenge of the adequacy of monitoring arrangements and of the outcomes of these.

Any significant changes in risk profile should be immediately escalated to Executive Committee via the risk sponsor. Operational Risk should be notified simultaneously. Further escalation to the Board or to Risk Management and Conflicts Committee may be required when the Bank's risk appetite has been, or is likely to be, breached.

There should be a formal risk report to the Executive Committee and to the Risk Management and Conflicts Committee on at least a quarterly basis. Operational Risk will collate and present this reporting on behalf of the business.

The Board escalates matters to the Scottish Ministers where there are decisions to be made which fall outside the Board's delegated authorities. In addition, the Bank will formally escalate any significant risks or issues through the Scottish Government team to ensure the team are aware of them as appropriate.

6. Framework review and improvement

The Framework is fixed in that it represents the Bank's approach to risk management at a point in time. However, it is also dynamic in that it is subject to ongoing review and continuous improvement in response to changes in the business and/or external environment and to industry best practice.

6.1. Periodic review

The Framework will be formally reviewed on at least an annual basis. The Operational Risk function will co-ordinate this exercise, with input from across the business and from the members of the Executive Committee, in particular. The updated Framework will be submitted to the Risk Management and Conflicts Committee prior to adoption and roll out to the business.

This periodic review will take into account any changes in the Bank's business strategy since the last update, as well as any new or updated regulatory or shareholder requirements. The review will also consider the effectiveness of the Framework against stated objectives and fitness for purpose in support of future strategic plans, to the extent these are known.

6.2. Internal audit

Internal audit takes a risk-based approach to audit planning and delivery. Therefore, it is essential that reliance can be placed on the Bank's systems for the management and reporting of risk. Therefore, it is expected that Internal Audit will periodically (and no less frequently than every three years) review the Bank's risk management framework, providing assurance to the Board via the Audit and Risk Management and Conflicts Committees.

Appendix 1 – References

This list of supporting policies is not exhaustive and following initial development in the first year of the Bank's existence, will be reviewed, revised and refined during the course of FY22/23.

This list focuses specifically on the risk management policies that support the framework and is the current target model for the end of FY22/23.

- Operational Risk Policy
- Business Continuity Policy
- Information Security Policy
- Procurement & Outsourcing Policy
- Investment Risk Policy
- Financial Crime Policy Governance Manual
- Complaints Policy
- Conflicts of Interest Policy
- PA Dealing Policy
- Code of Conduct

It should be noted that there are other subject matter policies covering Finance, HR and other business areas that will apply to specific areas, but are not directly linked to this Framework.

Appendix 2 – Risk assessment criteria

Impact assessment	Financial	Regulatory / Legal	Client / Reputation	Operational / Staff
Major	Severe financial impact requiring shareholder action	Substantial regulatory findings or successful legal action resulting in public censure / fines / damages	Material damage to Bank brand or significant impact to one or more Bank clients	Severe disruption to operations or material impact on the well-being of staff of the Bank's ability to recruit or retain staff
Significant	Event results in material impact on financial performance / stability	Regulatory findings / legal action with some cost but not made public	Contained impact to one or more of the Bank's clients and / or reputational damage to the Bank	Material operational impact and / or significant impact on the well-being of staff of the Bank's ability to recruit or retain staff
Moderate	Some financial impact (e.g. cost or loss of revenue) that can be absorbed into annual budgets	Breach of legal agreement / regulatory responsibility, but further action not likely	Potential for some client impact and / or reputational damage	Some disruption to operations but limited impact on staff well-being
Minor	Negligible financial impact	Little to no regulatory / legal impact	No client impact and / or minor reputational damage	Little or no impact to staff or continuity of operations

Likelihood assessment	Probability
Almost Certain	High chance of occurrence in the next twelve months
Likely	Likely to occur in the next one to two years
Possible	Event is possible but not likely – expected to occur once every two to three years
Unlikely	A rare occurrence – not expected more than once every five years

Appendix 2 – Risk assessment criteria continued