Risk Management Framework

The Scottish National Investment Bank

The Risk Management Framework contains the principles, policies, processes and decision-making structures that contribute to the effective management of risk at the Bank.

Contents

1. Introduction

This document contains the Scottish National Investment Bank Plc's ("The Bank's") Risk Management Framework. The Risk Management Framework ("RMF") contains the principles, policies, processes and decision-making structures that contribute to the effective management of risk at the Bank.

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

1.1. Definitions and scope

For the purposes of this document, the Bank comprises of Scottish National Investment Bank PLC, Scottish Investments Limited ("SIL") and Scottish Investments Services Limited ("SISL"). This RMF is approved annually by the Bank and SIL and is applicable to all entities.

The RMF uses the ISO definition of risk, namely the *"effect of uncertainty on objectives"*. 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 RMF 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

The Board is responsible for the effective management of risk in the Bank. The design and implementation of the RMF is overseen by the Risk Management and Conflicts Committee, who are required to review and approve the document on at least an annual basis. This Committee reports to the Board on its review and approval. The RMF is owned and operationalised on behalf of the Bank's management by the Chief Risk Officer and General Counsel.

The Internal Audit function reviews the RMF and the Bank's approach to risk management on a periodic basis in line with its rolling risk-based plan.

1.3. Related documents

The RMF is the senior policy relating to risk management and is deliberately high-level in nature. The RMF is supported by policies and other key reference documents that provide further detail to support implementation. These Risk Policies, shown in Appendix 2, and the associated training:

- Provide clear requirements to be followed to ensure that the Bank's activities are conducted in compliance with the applicable law and regulations;
- 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;
- Set out principles on, and provide examples of, acceptable and unacceptable behaviours linked, in particular to, financial misreporting and misconduct, 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.

The Governance, Legal, Risk & Compliance 'GLRC' function is responsible for developing, documenting and maintaining the Risk Policies and for overseeing their approval. The Chief Risk Officer and General Counsel is accountable for delivery, maintenance and monitoring of compliance for all the Risk Policies.

Compliance with Risk Policies is monitored by GLRC on a regular basis and policy breaches are escalated to the appropriate level within a set timeframe. The GLRC function is responsible for managing the remediation of exceptions and the formal review of all Risk Policies in Appendix 2.

1. Introduction continued

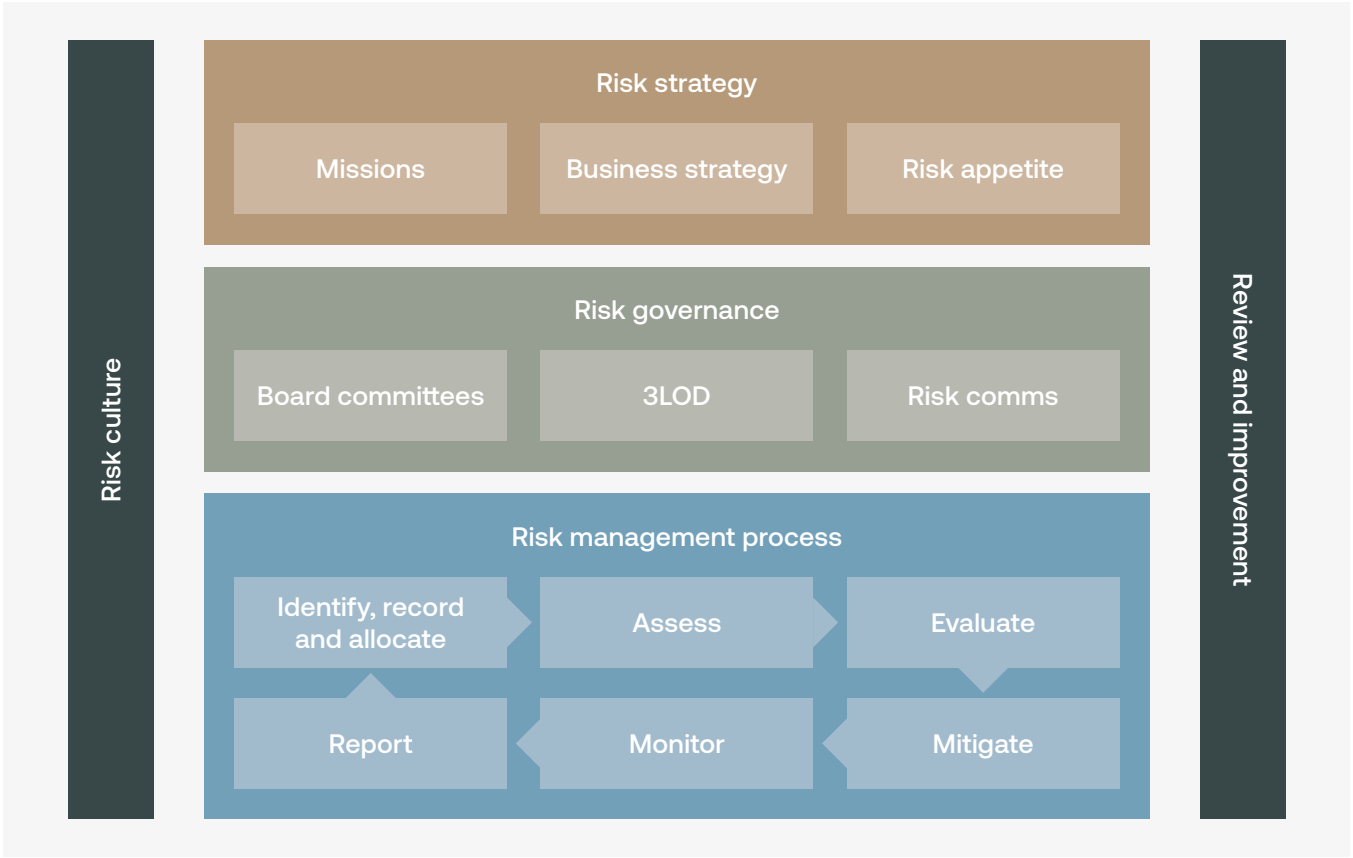
1.4. Reference frameworks

The Bank's Board have taken into account stakeholder requirements in designing the RMF, including the Risk Management chapter in the Scottish Public Finance Manual; guidance in the FCA Handbook (SYSC sourcebook); and the International Organisation for Standardisation's ('ISO') standard on Risk Management (ISO 31000).

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

1.5. Risk Management Framework summary

The RMF is summarised below.



Embedding an appropriate risk management culture is key in supporting the effective operation of the RMF across all framework elements. An appropriate risk management culture enables 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 aims to further develop the risk culture through reviewing and embedding appropriate policies, communication and training regarding its activities, strategy and risk profile. The Bank's objective in relation to risk management culture is that management understands and champions the basis for risk measures and risk management programmes.

Further detail on each framework element can be found in the sections below.

2. Risk strategy

The risk strategy is to embed a risk management framework which enables the Bank to achieve its missions and business strategy in a well-controlled manner.

2.1. Risk strategy

The Bank's approach to risk management supports and complements the business strategy. Through this RMF, 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 objectives and missions;
- Risk management activities are proportionate to the nature, scale and complexity of the Bank;
- A positive and proactive 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 investment decision and all strategic decisions;
- There is a culture of compliance where regulatory requirements are followed in spirit and in letter;
- Operational risk events and failures of internal controls are seen as a source of risk intelligence and an opportunity to learn and improve;
- The principles of risk management applied to the Bank are extended to the wider enterprise, including outsourcers.

2.2. Risk classification

The Bank classifies its risk universe into 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.

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 "Level 1" risk types have been identified, as shown below:

Risk	Definition
Mission Risk	The risk that the type, kind, or number of investments originated or held by the Bank are not sufficiently aligned to a mission or fail to deliver the impact ambitions.
Investment Risk	The risk of losses or write-downs due to failed loans, poorly performing investments or inadequate portfolio management.
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 fails to protect the environment, enable strong social outcomes and embed strong corporate governance practices, including compliance with laws and regulations.
Culture Risk	The risk that the Bank's culture does not align to the desired values, impeding the achievement of business objectives.
Stakeholder Risk	The risk that the Bank fails to meet stakeholder expectations due to actions by its staff, partners, third parties or invested companies.

2. Risk strategy 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 risk taxonomy, including both the Level 1 and Level 2 risks, is shown 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	Regulatory and Legal Compliance	Corporate Social Responsibility	Media, Marketing and Communications
	Portfolio Risk	Funding Risk	Outsourcing and Third-Party Risk	Financial Crime	Equality, Diversity, and Inclusion	
	Ethical Investment Risk	Tax Risk	Employment Practice and Workplace Safety	Climate Related Risk		
	Model Risk		Information and Data Governance			Key: Level 1 Risk Type
	Subsidy Control		Execution Delivery and Process Management			Level 2 Risk Type

The classification of risk is formally reviewed on an annual basis, in line with the review of this RMF, or sooner if required to reflect new threats and opportunities that could impact the Bank’s risk profile. In this case, any proposed changes to the taxonomy must be approved by the Risk Management and Conflicts Committee, which meets quarterly.

2. Risk strategy continued

2.3. Risk appetite

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 Risk Appetite outlines the types and levels of risk it is willing to accept in pursuit of the Bank's missions and business strategy. Risk appetite statements are in place for each of the Bank's Level 1 risks, shown below.

Risk	Risk Appetite Statement
Mission Risk	The Bank has a low appetite for failing to deliver the expected mission impact ambitions.
Investment Risk	As a development Bank, the Bank will seek out underinvested risk which by its nature will be high risk. The Bank therefore has a high appetite for investment risk. There is a low appetite for losses due to inadequate controls over the investment process or inadequate portfolio management.
Financial Risk	The Bank accepts the funding risk associated with relying solely on the Scottish Government for its funding. The Bank has a low risk appetite for not having the ability to recycle capital, recognising it is the ambition of both the Bank and Scottish Government for the Bank to be a perpetual institution. The Bank has a low appetite for inaccurate and untimely financial reporting.
Operational Risk	The Bank has a low appetite for operational risk.
Environmental, Social and Governance Risk	The Bank has a low appetite for risks arising from a failure to establish, maintain and develop frameworks for the management of ESG risk, including a low appetite for compliance errors and breaches.
Culture Risk	The Bank has a low appetite for any behaviour that goes against the Bank's values.
Stakeholder Risk	The Bank has a low appetite for reputational risk due to actions by its staff, partners, third parties or invested companies or from failing to proactively manage reputation.

Key Risk Indicators are in place against each of the Level 1 risks. These are monitored on a quarterly basis to ensure that the Bank is operating within its stated appetite. Breaches are reported to the Board.

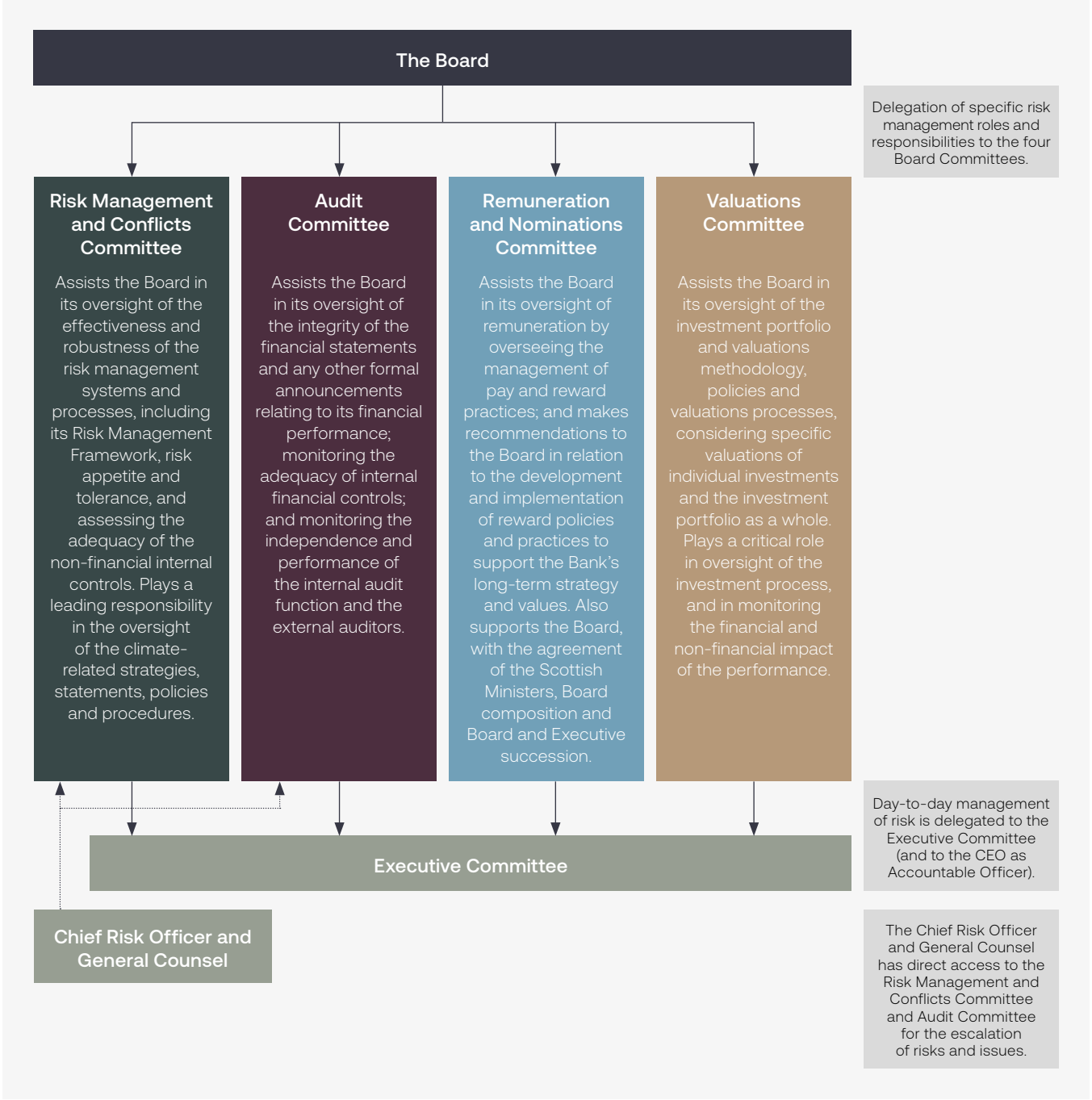
The Risk Management and Conflicts Committee undertakes a full review of the risk appetite statements on an annual basis or more frequently in the event of material changes within the Bank or in the external environment.

3. Risk governance

3.1. Governance

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

The Bank Board has overall accountability and responsibility for the management of risk within the Bank via delegated authority from the Scottish Government. The governance model is outlined below:



3. Risk culture and governance continued

The role of Accountable Officer is held by the CEO. It is incumbent on the Accountable Officer to ensure the propriety and regularity of the Bank's finances and to ensure that there are sound and effective arrangements for internal control and risk management.

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.

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.

3.2. Three lines of defence model

The Bank operates a three lines of defence model which assigns clear roles and responsibility for the management of risk.

First Line of Defence (Risk Ownership)	Second Line of Defence (Risk Oversight)	Third Line of Defence (Independent Assurance)
Identify, assess, own and manage risks and maintain effective internal controls. Execution of mitigation strategies.	Define frameworks, standards and policies. Oversee and challenge first line compliance with requirements.	Independent assurance of risk management and controls.
Investments Partnerships & Engagement People & Culture Finance & Operations	Governance, Legal, Risk & Compliance	Internal Audit

The key requirements of this model are outlined below:

- **The first line of defence:** Responsible for the ongoing management of risk and control. Risk and controls are owned by each respective first line 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:** Responsible for facilitating the risk management process (including provision of frameworks and policies) and for the oversight and challenge of the first line of defence.
- **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. Internal Audit reviews the RMF on a periodic basis in line with its rolling risk-based plan, which also includes detailed audits of key focus areas.

3. Risk culture and governance continued

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. The Bank embeds and communicates its risk management culture in a number of ways as summarised below:

- **Tone from the top:** The Bank's management contributes to the communication of core values and expectations to staff. This includes the promotion of an environment of open communication and effective challenge. The Board and Executive team promote, monitor and assess the risk culture of the Bank.
- **Accountability:** There is clear ownership of risks and controls across the Bank. Employees at all levels are expected to know and understand the core values of the Bank and their role in managing risk.
- **Incentives:** 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.

4. 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 Policy.

4.1. Risk identification and recording

Each Business Area in the Bank must undertake a Risk and Control Self-Assessment (RCSA) process on a minimum six-monthly basis. This process enables business areas to identify and record the key risks to their objectives. These risks are stored on a central risk register.

Key risks may also be identified on an ad-hoc basis and all employees are encouraged to pro-actively identify risks in their area and to discuss these with their line manager and / or a member of the GLRC function.

4. Risk management process continued

4.2. Risk assessment and evaluation

The potential impact and the likelihood of each key risk is assessed against the Bank's risk matrix in Appendix 1. 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.

Key controls are required to be implemented for all risks rated inherently High or above. It must be ensured that the key controls cover the causes of each risk. All key controls must be assessed for both design adequacy and operating effectiveness during each RCSA cycle. In assessing the residual risk, the control assessments must be explicitly taken into account. Only controls which are both adequately designed and operating effectively can reduce the residual risk position.

Having assessed the residual risk level, risk owners must then make a decision as to how best 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) **accept** the risk;

(ii) **treat** the risk by implementing additional internal controls or improve existing controls;

(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.

4.3. Risk mitigation

Where the risk exposure is above the tolerable level, and is not being accepted, management are expected to implement controls to manage the risk.

Where existing controls are insufficient to manage the risk, a mitigation plan will be required. Actions in the mitigation plan may include, but are not limited to, implementing new controls where gaps exist and remediating ineffective controls.

4.4. 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 Bank's colleagues are required to self-identify and record the issues in their area's control environment which may cause problems for the Bank. Instances requiring an issue and action to be raised include to address residual risks which are outside of appetite, fill control gaps or remediate controls which have been assessed as being inadequately designed or operating ineffectively.

Any significant changes in risk profile should be immediately escalated to Executive Committee and Operational Risk via the risk owner. Escalation to the Board or to Risk Management and Conflicts Committee is required when the Bank's risk appetite has been, or is likely to be, breached. Formal risk reporting is provided to the Executive Committee and to the Risk Management and Conflicts Committee on at least a quarterly basis.

The business is also required to identify and record risk events in a timely manner. These risk events must be rated using the impact section of the Bank's risk matrix.

5. Version Control

Version	Date	Description	Author
1.0	05/11/2019	First draft created	Fraser Walker
2.0	25/08/2020	Updated version following ExCo approval	Neil Hutchison
3.0	20/05/2022	Refreshed and approved	Aidan O'Brien
4.0	23/11/2023	Streamlined document and updated requirements for RCSA, Issues and Actions, updated risk appetite statements and introduction of 5x5 risk assessment grid.	Sean Carson
5.0	21/02/2024	Requirements added for self-identification of issues and enhanced wording on control requirements in RCSAs.	Sean Carson

Appendix 1 – The Bank's risk matrix

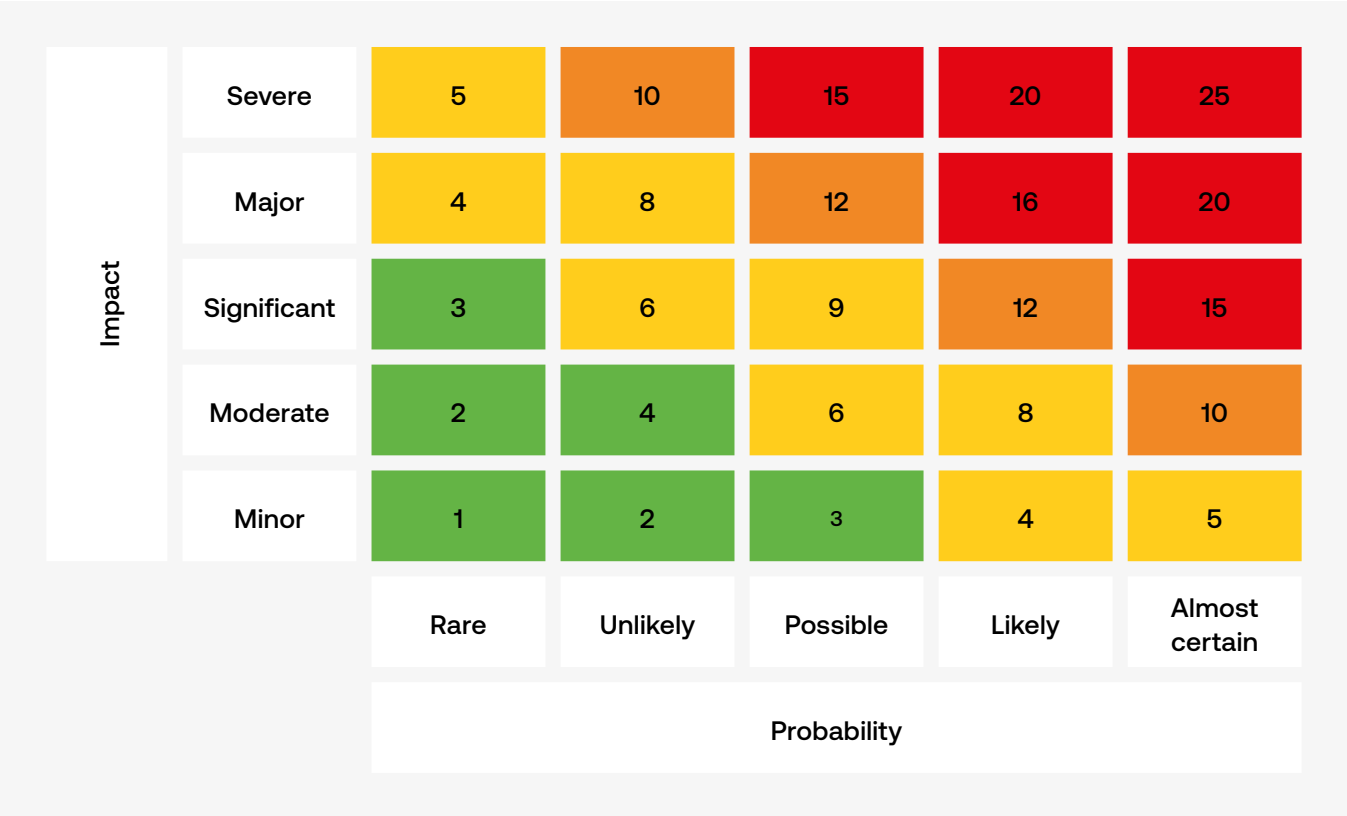
Impact assessment	Financial	MI and Reporting	Regulatory / Legal	Investees	Operational Resilience	Reputational
Severe	Severe financial impact requiring shareholder action.	Severe reporting error which has a material detrimental impact in key internal decisions (e.g. strategy/ investment decisions). Material external reporting error which requires to be restated and may impact the annual report going concern basis.	Severe systemic regulatory breach requiring disclosure to regulator, or successful legal action. Impacts could include restriction in permissions and public censure/ material fines/ damages.	Severe impact to one or more Bank investees, leading to a material breach of debt, performance or mission covenants. Has the potential to have a substantial negative impact on the value of the Bank's portfolio (>10% write-down).	Severe operational disruption with material impact on delivery of strategy/ missions. E.g. >3 day disruption to business critical system, >10 working day disruption of non-business critical system. Severe impact on key business processes which risks the achievement of business plan/ missions. Material data loss.	Severe impact on the Bank's reputation and trust in the Bank. Sustained adverse coverage (>1 week) across multiple mainstream outlets and platforms. Multiple negative comments from First Minister/ Cabinet. Restriction/loss of shareholder support.
Major	Event results in material impact on financial performance /stability.	Reporting error in MI provided to an internal meeting /committee which has the potential to negatively impact key decisions. Material external reporting error which requires restatement.	Systemic regulatory breach requiring disclosure to regulator, or successful legal action. Impacts could include public censure/ fines/damages.	Major impact to one or more Bank investees, leading to a breach of debt, performance or mission covenants. Has the potential to have a negative impact on the value of the Bank's portfolio (5-10% write-down).	Major operational disruption with impact on delivery of strategy/ missions. E.g. 1-3 day disruption to business critical system, 4-9 day disruption of non-business critical system. Delays key business deals and or processes (e.g. payroll). Material data loss.	Major impact on the Bank's reputation and trust in the Bank. Adverse coverage in multiple mainstream outlets for over 1 week. Isolated negative comments from First Minister /Cabinet. Restriction/loss of support from other political stakeholders.
Significant	Some financial impact (e.g. cost or loss of revenue) that can be absorbed into annual budgets.	Reporting error in MI provided to an internal meeting/ committee which may influence key decisions. External reporting error which may require restatement due to its nature, e.g. regulatory fines requiring disclosure etc.	Significant isolated regulatory breach. Breach requires notification to the regulator and may lead to enhanced regulatory oversight and /or litigation.	Major impact to one or more of the Bank's investees, which may lead to a covenant breach. Has the potential to have a negative impact on the value of the Bank's portfolio (0-5% write-down).	Significant operational disruption with impact on delivery of strategy/ missions. E.g. 4-8 hour disruption to business critical system, 1-3 day disruption of non-business critical system. Delay to processing deal/payment but payment made in sufficiently timely manner to not detriment recipients/the Bank. Data loss requiring supplier support to resolve/recover.	Significant impact on the Bank's reputation. Adverse coverage in two or more mainstream outlets for up to one week. Sustained negative comments from opposition parties.

Appendix 1 – The Bank's risk matrix continued

Impact assessment	Financial	MI and Reporting	Regulatory / Legal	Investees	Operational Resilience	Reputational
Moderate	Negligible financial impact.	Reporting error in MI provided to an internal meeting/ committee but which does not impact key decisions. External reporting error below the level of materiality.	Isolated regulatory breach not requiring disclosure to regulator. Corrective action likely to exceed 24 hours and requires management oversight.	Moderate impact to one of the Bank's investees. Requires the Bank's oversight to resolve. Does not impact the Bank's investment and does not lead to a covenant breach.	Moderate operational disruption with limited impact on delivery of strategy/ missions. E.g. 1-4 hour disruption to business critical system, 4-8 hour disruption of non-business critical system. E.g. slight delay to processing deal/payment but payment made same day. Data loss requiring corrective action likely to exceed 24 hours and requires management oversight.	Moderate impact on the Bank's reputation and trust in the Bank. Adverse coverage in one mainstream outlet for up to one week. Isolated negative comments from opposition parties.
Minor	No financial impact.	Immaterial reporting error which does not have an impact on decision making/external reporting.	Isolated minor regulatory breach not requiring disclosure to regulator. Can be resolved locally within 24 hours.	Minor impact to one of the Bank's investees. Can be resolved within 24 hours. Does not impact the Bank's investment and does not lead to a covenant breach.	Minor operational disruption with no impact on delivery of strategy/ missions. E.g. <1 hour disruption to business critical system, <4 hour disruption of non-business critical system. Data loss which be can be resolved locally within 24 hours.	Minor impact on the Bank's reputation and trust in the Bank. Limited adverse coverage in one non-mainstream outlet. Isolated negative comments from single political stakeholders.

Likelihood Rating	Description	Probability in next 12 months
Almost Certain	An event is very likely to occur in the next 12 months.	>80%
Likely	An event is more likely than not to occur in the next 12 months.	60%-80%
Possible	An event is just as likely as not to occur in the next 12 months.	40-60%
Unlikely	An event is less likely to occur than it is to occur in the next 12 months.	20-40%
Rare	An event is very unlikely to occur in the next 12 months.	<20%

Appendix 1 – The Bank's risk matrix continued



Risk Rating	Description
Very High	The Bank is likely to be operating outside its risk appetite. Control improvements are required and should be prioritised unless the risk is accepted.
High	The Bank is approaching its risk appetite. Control improvements are highly desirable and should be implemented in a timely manner.
Medium	The risk is within the Bank's risk appetite. The risk should be monitored and improvements to controls considered where appropriate.
Low	The risk is well within the Bank's appetite. Improvements to controls are not required.

Appendix 2 – Risk Policies

The list below outlines the risk management policies that support the RMF, referred to as the 'Risk Policies':

- Operational Risk Policy
- Business Continuity Policy
- Information Security Policy
- Information Governance Policy
- IT Policy
- Whistleblowing Policy
- Compliance Breach Policy
- Procurement & Outsourcing Policy
- Investment Risk Policy
- Financial Crime Policy
- Complaints Policy
- Conflicts of Interest and Gifts and Hospitality Policy
- Market Abuse & Personal Account 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.

The Scottish National Investment Bank

Scottish National
Investment Bank plc
Waverley Gate,
2-4 Waterloo Place,
Edinburgh,
United Kingdom
EH1 3EG

www.thebank.scot
enquiries@thebank.scot

Scottish National Investment Bank plc is wholly owned by Scottish Ministers
Registered in Scotland with Company number SC677431

SNIB065.0224