1 Introduction

1.1 Risk Management is central to Foundation Scotland's [FS's] planning and governance. It is the process by which we methodically address the risks attaching to our activities with the aim of improving the likelihood that we will deliver our objectives.

2 Scope

2.1 This policy applies to all FS employees, Board, and Committee members. The objective of the policy is to ensure that FS has a clear and consistent basis for identifying, measuring, controlling, monitoring, and reporting risk at all levels and in all parts of the organisation.

3 Abbreviations and Definitions

Abbreviations

- CFOO – Chief Finance and Operations Officer
- CEO – Chief Executive Officer
- LT – Leadership Team
- RM – Risk Management
- RiskMate – Risk Management System. The system also handles Incidents, Complaints, Whistleblowing, and Policy Management.

Definitions[1]

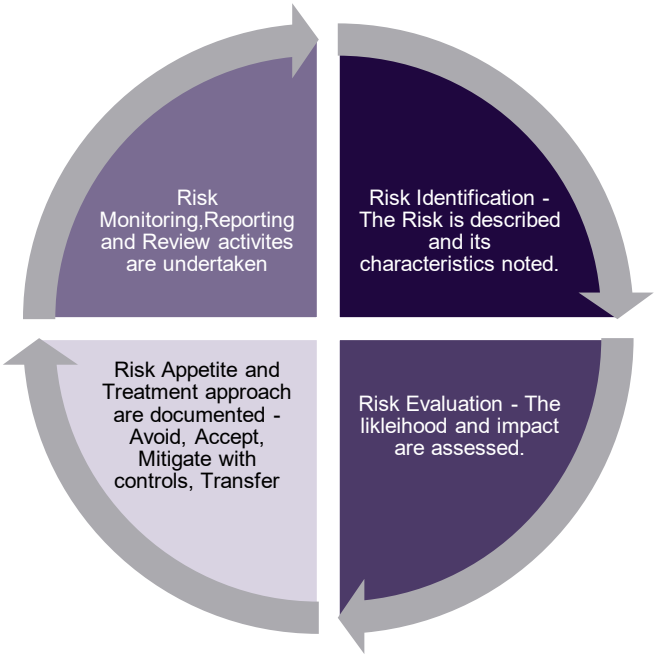
- Risk – is the effect of uncertainty on objectives. It is the combination of the likelihood of an event and its impact. (Likelihood X Impact).
- Inherent Risk - is a pure risk, as if there were no controls in place to manage it.
- Residual Risk - is the current level of risk given the effect of the controls already in place.
- Risk Appetite - is the level of risk the organisation is prepared to tolerate or accept in the pursuit of its objectives.
- Risk Management [RM] - is any activity undertaken to identify and then control the level of risk which objectives face.
- Control – is a specific action which will reduce the likelihood of a risk occurring.

[1] Adapted from ISO 31000:2018 Risk management – Guidelines and the Institute of Risk Management

4 Policy

Risk Management Process

4.1 RM is an on-going process carried out at all levels and all parts of the organisation. We recognise that new risks may emerge, and risks already identified may become more or less likely to occur. The diagram below illustrates the process we follow.



Risk Identification and Categorisation

4.2 Risks may be identified at any point of a project or as part of routine operations.

4.3 As risks are identified they should be discussed by teams and then added to RiskMate. The CFOO, working with Risk Owners, is responsible for reviewing the status of existing risks, risk actions and any controls being used to mitigate them.

4.4 To aid understanding and management, we categorise risks using the following characteristics:

Characteristics	
Risk Owner	The person responsible for managing the risk
Department	The team which the owner works in
Category	The source of the risk/ classification
Corporate Objective	Which of the ambitions the risk impacts
Committee	Which Committee or Board is reviewing the Risks. Risks may also be held at staff level.

Risk Evaluation

4.5 To assist in ranking the significance of Risks they are scored using a combination of the Impact and Likelihood to give a total score.

4.6 When deciding on the impact score the following criteria are used.

Impact Area	1	2	3	4	5
	Insignificant	Minor	Moderate	Major	Critical
Finance – Unrestricted Operational Income	<£20k	£20k-£100k	£101k-£500k	£501k-£1m	>£1m
Finance – Restricted Distribution	<£50k	£50k-£100k	£101k-£1m	£1m+-£4.999m	>£5m
Reputational [illustrative]	Letter to local sector press.	Series of articles in local press.	Extended negative local/sector media coverage.	Short term negative national media coverage.	Extensive, sustained negative national media coverage.
	Stakeholder dissatisfaction, but quickly resolved.	Stakeholder dissatisfaction, escalated, but managed and no long-term impact.	Stakeholder dissatisfaction, escalated and drawn out; resolved, but through fund closure.	Stakeholder dissatisfaction poorly managed leading to loss of donor and fund, but also negative effect on another stakeholder (word of mouth).	Stakeholder dissatisfaction leading to donor contagion by word of mouth and emails; loss of many donors.
Regulatory	Minor breaches by individual staff members.	No fine or disruption to activities.	Fine but no disruption to activities.	Fine and disruption to activities.	Significant disruption to activities over an extended period. Loss of charitable status.

Impact Area	1	2	3	4	5
	Insignificant	Minor	Moderate	Major	Critical
Health and Safety	Incident contained quickly.	Incident contained with internal assistance.	Incident contained with assistance.	Prolonged or major incident with serious casualties.	Major incident with fatalities.
Human Resources	Single complaint (one-ff, not systemic)	Multiple staff complaints or one complaint that appears systemic.	Evidence of discontent across departments (raised as multiple individual complaints or collectively expressed).	Significant discontent evident in all departments requiring LT action.	Significant discontent evident in all departments requiring Board action.
Operations	Very small interference in operations.	Small interference in operations.	Slowing down of operations. Internal deadlines missed.	Noticeable slowing down of operations and a loss of efficacy. External deadlines missed.	Activities suspended.

Impact Area	1	2	3	4	5
	Insignificant	Minor	Moderate	Major	Critical
Strategic	Minimal or no effect on delivery of Foundation Scotland's long-term mission or strategic objectives. Any deviation from strategy is easily corrected without requiring additional resources. No impact on sector positioning or partnerships.	Small misalignment with strategic goals, but manageable within existing plans. Requires limited adjustment of priorities or resources, with no long-term consequence. Minimal impact on reputation with key stakeholders or sector influence.	Noticeable delay or compromise in achieving one or more strategic objectives. Requires reprioritisation of resources or additional management oversight. Potential to weaken credibility with funders, partners, or policymakers if not addressed promptly	Significant hindrance to the achievement of multiple strategic objectives. Requires Board intervention, major reallocation of resources, or a revision of the strategy. Material impact on external positioning, leading to reduced influence, lost opportunities, or weakened partnerships.	Fundamental failure of strategic direction; mission-critical objectives cannot be delivered. Long-term damage to positioning, with severe loss of trust from funders, partners, and stakeholders. Requires wholesale review of strategy and its operating model.

4.7 When deciding the likelihood of a risk occurring the following categories are applied:

Description	Chance		Score
Event may occur in some circumstances - once a month.	>90%	Almost certain	5
Event may occur in some circumstances - once a year.	50-90%	Likely	4
Event should occur at some point - once in 5 years.	30-49%	Possible	3
Event could occur at some point - once in 15 years.	10-29%	Unlikely	2
Event may occur only in exceptional circumstances - once in 50 years.	<10%	Rare	1

Risk Appetite2 and our approach to risk treatment

4.8 We understand that we will not be able to achieve our objectives without taking risk. The Board has considered the main activities we undertake, against the backdrop of the maturity of our internal controls and our desire to grow and improve what we do and has agreed the following framework.

Activity	2-6	7-12	13-30
Compliance	✓		
Governance and Ethics	✓		
Human Resources	✓		
Investment Performance against agreed benchmarks	✓		
Finance		✓	
IT		✓	
Operations		✓	
Fund Distribution including Social Investment			✓

4.9 We place importance on compliance and have no tolerance for breaches in statute. We wish to maintain and attain accreditations and have a low appetite for risk relating to actions which may jeopardise these.

4.10 We have earned the trust of our donors, grantees and community panels and therefore have a low appetite for any risks which would impact negatively on our reputation, brand, or ethical standing.

4.11 We have a low appetite for compromising the safety of staff, their welfare. Training, support, and performance management are being strengthened as our appetite for poor staff performance is low.

[2] Risk Appetite and Tolerance – Institute of Risk Management

4.12 We aim to maintain our long-term financial sustainability and comply with our Reserves Policy. We take balanced risks with the Investments entrusted to us.

4.13 We have a low appetite for IT security risks however our IT Governance Strategy and trusted external IT support are enabling us to take greater risks regarding the adoption of new technologies.

4.14 We see the importance of continuous improvement and therefore have a medium appetite for making improvements to systems and service delivery.

4.15 While exercising a high degree of due diligence to check credentials, we wish to be innovative and agile regarding our grant giving and distribution decision making. We distribute funds to groups that are non-constituted and to individuals. Our corresponding appetite is high.

4.16 Depending on our risk appetite compared to the total inherent risk score we adopt one of four approaches to the Risk.

- Accept the level of risk and take no further action
- Avoid the risk by stopping the activity
- Manage the risk by applying controls
- Transfer the risk to another party – e.g. by outsourcing or insuring

Monitoring and Review

4.17 The CFOO is responsible for ensuring that the risks and controls are regularly reviewed and RiskMate updated by Risk and Action Owners. The Risk Committee and the Board also monitor and review the risks, actions and controls as detailed in section 5.

Communication and Consultation

4.18 All identified risks, regardless of their total score, will be included in RiskMate. Serious specific risks will be communicated out more widely so that there is a wider organisational understanding of the risks identified and how they are being managed.

4.19 As part of good practice and as required by the regulator, a risk management report will be included in the Annual Report and Accounts.

5 Roles and Responsibilities

Staff

- Understand, accept, and implement RM processes.
- Report inefficient, unnecessary, or unworkable controls.
- Report incidents and assist in identifying risks.

Team Heads

- Build a RM culture in the team.
- Ensure controls and actions within their remit are carried out.
- Update RiskMate Risks, Actions, and Incidents under their control

CFOO

- Develop the RM Policy and keep it up to date.
- Ensure training on RM is available.
- Maintain the RiskMate Handbook/Wiki.
- Review new Risks, Incidents, Complaints, and related Actions in RiskMate.
- Co-ordinate the development of specialist contingency and recovery plans.
- Meet with Risk Owners following the quarterly LT Risk Review meeting to monitor risk actions and mitigations.
- Compile risk information and prepare any analysis and reports required for the CEO, Audit and Assurance Committee, and the Board.

CEO

- Understand the most significant risks.
- Facilitate a Risk Review session at LT meetings [Quarterly].
- Manage the organisation in a crisis.

People and Governance Committee, Social Investment Committee

- Review the Risks under their purview.

Audit and Assurance Committee

- Review the Risks under their purview.
- Review the RM Policy and make recommendations for changes to the Board [Annually]
- Review the RM systems and processes [Annually]
- Review the Risk Statements in the Annual Report and Accounts [Annually]
- Review the Risks and Actions in RiskMate actions [Bi-Annually]

Board

- Review reports from the Audit and Assurance Committee [Bi-Annually]
- Approve the Risk Statements in the Annual Report and Accounts [Annually]
- Approve changes to the Risk Management Policy [When changes occur]
- Undertake a Strategic Risk Discussion [Annually]

6 Training

6.1 The following [free] e-learning courses provide a useful introduction to the topic of Risk Management

- IRM –Risk Management for Charities – Getting Started
  https://www.youtube.com/watch?v=4iC4Vg4h4CY

- IRM – Risk Management for Charities – The Risk Management Framework https://www.youtube.com/watch?v=RQz9ebWKk_8
- IRM – Risk Management for Charities – Risk treatment, monitoring and reviewing https://www.youtube.com/watch?v=flFzdcEOsWE
- IRM – Risk Management for Charities – Risk Communication https://www.youtube.com/watch?v=tG6FR106SvU

7 References

- Risk Appetite and Tolerance – Institute of Risk Management

8 Review

8.1 This policy is reviewed, approved, and endorsed by the Board. It is updated when required by legislation, to ensure that it reflects statutory responsibilities, government guidance and best practice for FS or every 36 months whichever is the soonest.

9 Document Properties

Title	Risk Management Policy		
Type	Policy	Classification	Operations
Reference Number	2	Version - auto-generated	2.27
Status	Approved	Approval Date	15/05/2024
Author	CFOO	Approver	FS Board
Last Reviewed regardless of whether changed	15/05/2024	Next Review Date	29/04/2027