NHS Lothian Charity

Risk Management Policy

December 2024

Policy Reference Information

Status	APPROVED
Author	Jane Ferguson
Approval	Trustees
Date of Last Review	December 2024
Date of Next Formal Review	December 2026

Related Policies

Policy Title
Charter Charitable Funds Committee TOR The Charities SORP (FRS102) Whistleblowing Statement

NHS Lothian Charity

1. Background

1.1 The purpose of risk management is the creation and protection of value for the charity. It supports the achievement of objectives, helps protect funds, assets and reputation, and maintains stakeholder confidence.

1.2 The aim of NHS Lothian Charity ("the Charity") is to adopt best practice in the identification, evaluation and effective control of risks, to ensure that they are either eliminated or reduced to an acceptable level.

1.3 Risk is a factor of every-day life and can never be eliminated completely. All employees must understand the nature of risk and accept responsibility for risks associated with their area of authority. The necessary support, assistance and commitment of senior management will be provided.

2. Definitions

Risk: is something uncertain, that might or might not happen but, if it does, could effect the charity achieving its objectives. It can be defined as the combination of the probability of an event and its consequences;

Risk Management: is any activity undertaken to identify and then control the level of risk which objectives face.

Issue: is an unplanned event which has already happened and needs action to manage it.

Control: a specific action that will reduce the likelihood of a risk occurring;

Mitigation: to mitigate a risk is to make the impact of it less severe.

3. Policy Statement

3.1 To support our vision of *making healthcare better, **together*** we proactively work to manage and reduce risks which would impact our ability to invest in enhanced experience and care for patients in hospitals and their communities, having a positive impact on health in Lothians.

3.2 The Charity Trustees acknowledge that efficient and effective management of risk is important in achieving its business objectives. This policy reflects its commitment to sound risk management policies and practices.

4. Risk Management

4.1 NHS Lothian Charity assesses the risks it faces through identification, analysis and evaluation:

- Using the primary objectives articulated within our strategy as a starting point, we matrix four categories of risk identification: Governance and Management, Operational and External, Economic and Financial, and Compliance and Regulatory; we consult colleagues and stakeholders to populate a Corporate Risk Register.
- We consider risk causes and effects.
- Assessing risk considering control strength and assurance levels we use a 5x5 Impact x Likelihood scoring matrix, recording RAG risk scores NET after controls (explained at 7.2 and 7.3 below).
- Considering project and operational risk using similar methodologies, and ensuring the management of operational and corporate risk registers is integrated.

4.2 We manage risk by considering appropriate actions to take, including any additional mitigating controls, and who will own each action. We may also decide to tolerate a risk, or to stop a risky activity.

4.3 We continually monitor and review risks, by considering external factors, checking existing controls are still effective, considering additional actions necessary to increase assurance and reduce the NET risk scores, and updating the risk register accordingly to keep it 'live'.

4.4 We communicate and report on risk, engaging with colleagues and stakeholders, producing a regular risk report which is assessed quarterly by SMT and CFC, including a risk statement in our annual report, considering training in risk where a need is identified, and encouraging people to speak up about their concerns.

4.5 The Risk Management Statement in the Annual Report confirms that the trustees have given consideration to the major risks to which the Charity is exposed and satisfied themselves that systems of procedures are established in order to manage those

risks. The statement should include:

- an acknowledgement of the Trustee's responsibility
- an overview of the risk identification process
- an indication that major risks identified have been reviewed or assessed
- confirmation that control systems have been established to manage those risks
- a description of the current key strategic risks faced
- how each risk is managed or mitigated
- that these risks and other identified risks relating to the Charity are analysed in a formal risk register which includes controls and actions to mitigate the risks.

4.6 Operational risks are assigned to the SMT (finance, programme delivery, engagement respectively), and receive a quarterly review alongside corporate risk controls and their effect, risk scores and additional actions.

5. Risk Roles and Responsibilities

Everyone involved in the charity's activities has a part to play in risk management, but to ensure this is co-ordinated effectively this section outlines the framework for risk management: who is responsible for risk management at every level within the charity

5.1 Trustees

5.1.1 The Trustees will set the culture of risk management within the Charity. The Trustees have ultimate responsibility for risk management including major decisions affecting the risk profile or exposure, and are expected to regularly review and assess the risks faced by the charity in all areas of its work and plan for the management of those risks. The Charities SORP (FRS102) requires of trustees a statement of the principal risks and uncertainties facing the charity, as identified by the trustees, together with a summary of their plans and strategies for managing those risks within the Annual Report and Accounts. For this reason, the Risk Management policy is a matter reserved for Trustees.

5.2 Charitable Funds Committee

5.2.1 The Charitable Funds Committee will act under delegated authority of the trustees to provide an independent and objective view of the arrangements for the management of risk. It will

- report to the Trustees on internal controls and alert them to any emerging issues.
- oversee internal and external audit, review their recommendations and advise the Trustee Board on the effectiveness of the internal control system including the system for the management of risk.
- satisfy itself that risks are appropriately owned and that risk owners are actively managing their risks with the appropriate controls in place and working effectively.
- monitor and critically review the management of important risks and the maintenance of the risk register to ensure they are fit for purpose.
- be responsible for preparing the Risk Management Statement for the Annual Report and Accounts.

5.3 Director and Senior Management Team

5.3.1 Risk management is delegated to the Charity Director and the Senior Management Team, who are responsible for supporting the Trustees and Committees in the identification and assessment of major risks. The Director will ensure that controls are implemented and provide regular reports to the Trustee and Committees on the status of the risks and the effectiveness of the controls. The Director and Senior Management Team are responsible for encouraging good risk management practices and a positive attitude towards the control of risk among all staff.

5.4 Charity Staff

5.4.1 Everyone involved in the charity's activities has a part to play in risk management. Charity Staff are responsible for controlling risk when carrying out their duties, for following policies and procedures designed to mitigate risk (both those approved by trustees and those set by NHS Lothian), and for providing such information as the Trustee or its Committees may require in fulfilling their responsibilities under this Policy. They will also often be the first to identify new and emerging risks, and staff meetings will routinely consider potential new or changing risks to the Charity.

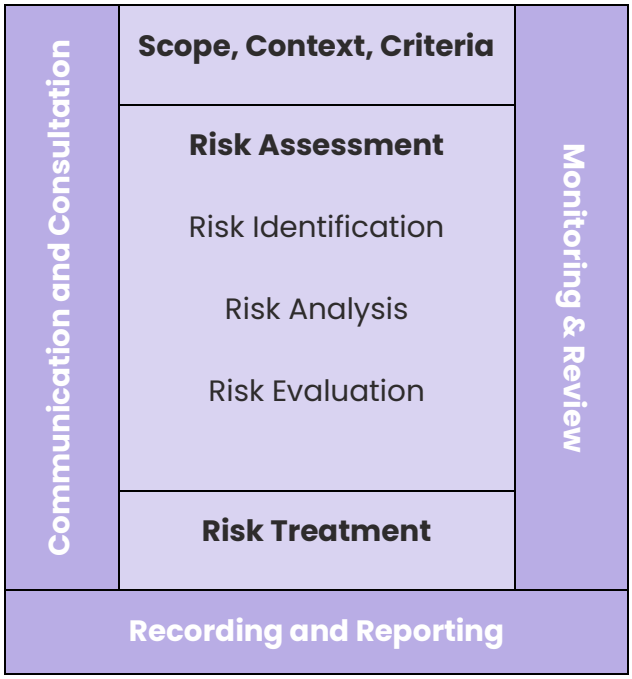
NHS Lothian Charity

6. Risk Appetite

6.1 Trustees' approach to risk appetite is to score 'target risk' as the level of risk they deem acceptable; additional controls and actions are considered and implemented in order to move the residual risk (NET after controls) to target risk, ie to within agreed appetite.

7. Risk Management Process Tools

7.1 This diagram summarises the risk management process as set out in ISO 31000:



7.2 Risk Matrix

(Y) Likelihood						
	(5) Almost certain (over 75%)	Medium 5	High 10	High 15	V High 20	V High 25
	(4) Likely (50-75%)	Medium 4	Medium 8	High 12	High 16	V High 20
	(3) Possible (25-50%)	Low 3	Medium 6	Medium 9	High 12	High 15
	(2) Unlikely (10-25%)	Low 2	Medium 4	Medium 6	Medium 8	High 10
	(1) Remote (under 10%)	Low 1	Low 2	Low 3	Medium 4	Medium 5
		(1) Insignificant	(2) Minor	(3) Moderate	(4) Major	(5) Critical
		(X) Impact				

7.3 Assurance Levels

High level of assurance	Medium level of assurance	Low level of assurance	Critical
Likelihood of risk is low or has been reduced by controls in place.Impact of risk is low or has been sufficiently reduced by controls in place. Residual Risk (RR) trend is equal to or approaching Target Risk (TR). No additional actions required	Likelihood of risk is medium or is being reduced by controls. Impact of risk is medium or is being reduced by controls. Residual Risk (RR) is static, not moving towards Target Risk (TR). Some additional actions to improve	Likelihood of risk is high or is not being reduced by controls. Impact of risk is high or is not being reduced by controls. Other internal/external factors impacting. Residual Risk (RR) is moving away from Target Risk (TR). Further controls required as priority	Likelihood of risk is very high, controls are ineffective. Impact of risk is very high, controls are ineffective. Major internal / external factors are critical. Residual Risk (RR) is very high / critical. Remedial controls essential