Risk Management Policy

Title: Risk Management Policy			
Date effective from:	31/10/2024	**Review date:**	05/02/2026
Approved by:	NHS Lothian Board		
Approval Date:	07/11/2024		
Author/s:	Quality & Safety Assurance Lead		
Policy Owner:	Associate Director for Quality Improvement & Safety		
Executive Lead:	NHS Lothian Medical Director		
Target Audience:	Managers/All NHSL Staff		
Supersedes:	Risk Management Policy v3.0 (April 2023)		
Keywords (min. 5):	Risk, Risk Management, Residual Risk, Governance, Register		

Version Control

Date	Author	Version/Page	Reason for change
June 2012	Quality & Safety Assurance Lead	1.0	
May 2018	Quality & Safety Assurance Lead	1.1	Under review
June 2018	Quality & Safety Assurance Lead	2.0	Review Approved
Dec 2022	Quality & Safety Assurance Lead	2.6	Under review
April 2023	Quality & Safety Assurance Lead	3.0	Review Approved
Oct 2024	Quality & Safety Assurance Lead	3.1	Technical Update

RISK MANAGEMENT POLICY

1 EXECUTIVE SUMMARY

1.1 Key Messages

There will always be a degree of risk in whatever an organisation is trying to achieve. For NHS Lothian, that is the provision of safe and effective healthcare care services in secondary, community and primary care settings. The range of associated activities include caring for people using our services, employing staff and managing finance and premises, all of which, by their very nature carry inherent risk.

Risk creates uncertainty, and if we do not actively manage risk, this may impact on our ability to achieve our goals and objectives.
To increase our chances of success in achieving our purpose, we should:

- Be very clear what we are trying to achieve, and purposely set out the objectives
- Identify the risks to those objectives. Risks should always be related to objectives, as this allows us to properly assess them and consider how important they are in terms of their threat to success
- Put in place measures and take appropriate action to manage the risks.

This Risk Management Policy has been produced to embed a consistent approach to risk management across NHS Lothian as an integral part of everything we do.

1.2 Implementation

The Board shall have a record of its risks and the Corporate Management Team is responsible for directing this policy through operational management structures. All senior management teams must ensure that:

- There is a process in place to systematically consider the relevance and management of existing and new risks in their area of responsibility
- All departments within their area effectively implement this policy
- All employees are clear of their roles and responsibilities in implementing this policy.

2 Why do we have this policy?

2.1 Lothian NHS Board (the "Board") exists to carry out NHS functions and services as directed by the Scottish Government. The Board will develop strategies and set objectives to deliver its purposes and intended outcomes.

The purpose of this document is to provide a consistent and systematic process for the identification, quantification, recording and reporting of risks which could threaten achievement of NHS Lothian's objectives.

2.2 Whatever you may be trying to achieve there will always be some risk. Risk creates uncertainty and, if we do not actively manage risk, could lead to us not achieving our goals and objectives, including safe and effective care.

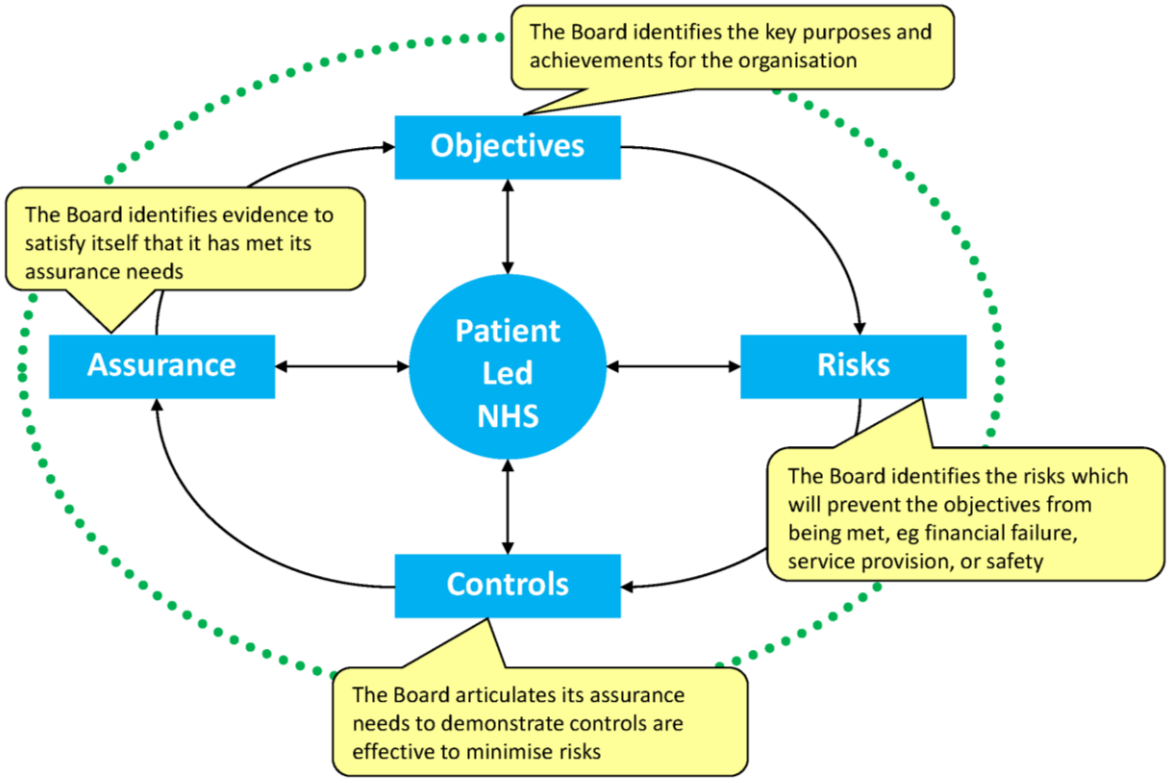
To increase our chances of achieving our goal and objectives, we should:

- Be very clear what we are trying to achieve, and purposely set out the objectives.
- Identify the risks to those objectives. Risks should always be related to objectives, as this allows us to properly assess them and consider how important they are in terms of their threat to success.
- Put in place measures and take appropriate action to manage the risks.

This Risk Management Policy has been produced to embed a consistent approach to risk management across the NHS Lothian.

2.3 Figure 1 below illustrates the general concept. This is taken from the guidance on Corporate Governance and Assurance. Levels of assurance have been adapted to be specific to the management of risks and can be found here.

Figure 1



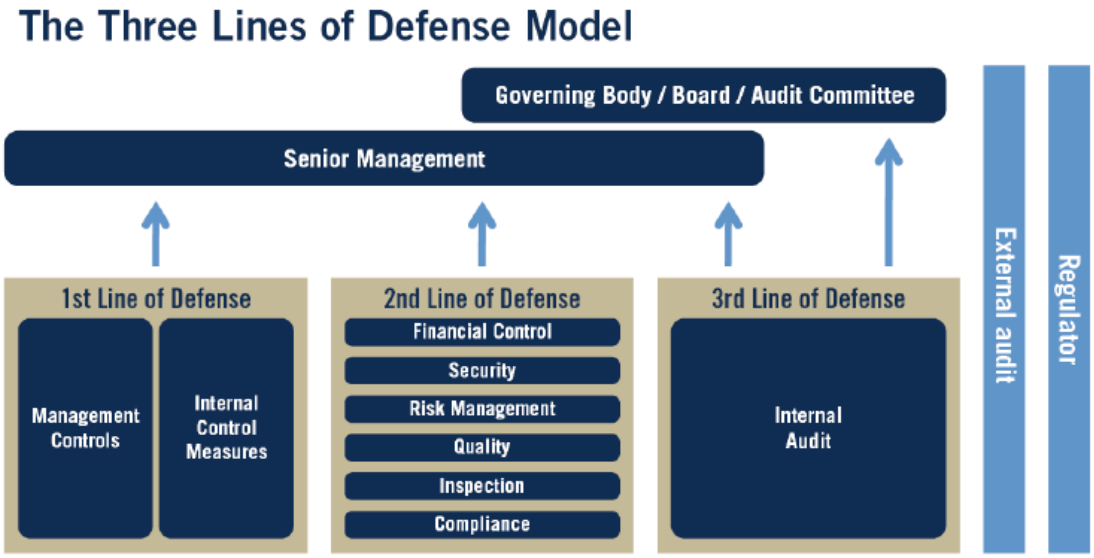
Source: adapted by NHS Lothian from Health Care Standards Unit, as referred to in the Oxford University Hospitals Foundation NHS Trust Assurance Strategy (September 2015)

3 Policy Statement

3.1 The Board will have a systematic approach to the management of risk in all of its functions and services. As part of this approach, the Board expects employees to give greater priority to managing and reducing risks associated with the safety of people, the experience of people who receive care, and the delivery of effective care.

3.2 Our assurance system has been designed to replicate the 'Three lines of defence' model as illustrated in Figure 2 below.

Figure 2



Graphic taken from The IIA Position Paper The Three Lines of Defense in Effective Risk Management and Control *published in 2013, adapted from ECIIA/FERMA Guidance on the 8th EU Company Law Directive, article 41*

3.3 The Audit & Risk Committee shall seek assurance that:

- There is a comprehensive risk management system in place to identify, assess, manage and monitor risk at all levels of the organisation

- There is appropriate ownership of risk in the organisation, and that there is an effective culture of risk management.

In order to discharge its advisory role to the Board and Accountable Officer, and to inform its assessment on the state of corporate governance, internal control and risk management, the Committee shall:

- Review regular reports summarising any significant changes to the Board's corporate risk register, and what plans are in place to manage them.

- Review the updated position for each risk, including assurance agreed by the relevant committee

- Assess whether the Corporate Risk Register is an appropriate reflection of the key risks to the Board and advise the Board accordingly

- The Committee may also elect to occasionally receive information on significant risks held on other risk registers held in the organisation.

- Consider the impact of changes to the risk register on the assurance needs of the Board and the Accountable Officer, and communicate any issues when required

- Receive an annual report on risk management, confirming whether there have been adequate and effective risk management arrangements throughout the year, and highlighting any material areas of risk

- Use this information to inform internal audit priorities.

3.4 Whilst the Audit and Risk Committee shall seek assurance on the overall system of risk management and have an oversight of all risks on the corporate risk register, each risk will be assigned to a relevant committee of the Board for assurance, in line with the committees' terms of reference.

3.5 All of the committees shall use the standard levels of assurance for risk management (significant, moderate, limited, none) in the course of discharging its remit.

4 DEFINITIONS

4.1 **Risk** is uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. It is the combination of the likelihood and impact of the risk materialising.

4.2 **Risk should always be related to some objective or purpose. A statement of risk should always contain:**

1. The cause of the impact on the objective, AND
2. The impact on the objective (i.e. the consequence of the risk)

4.3 **Risk Management** is a process which helps the whole organisation to identify areas that require attention and remedial action. It can be defined as the processes involved in managing those risks, including:

- identifying risks
- assessing and judging risks
- assigning ownership for the management of the risk
- taking actions to mitigate or anticipate risks
- monitoring and reviewing progress

4.4 The **risk register** is a record of the risks identified, the assessment of them, existing controls in place to mitigate the risk and any additional plans to improve controls. Risk registers are held at all levels of the organisation.

4.5 An **internal control** is a measure put in place with the aim to mitigate risk. Internal controls will constrain risks but are unlikely to eliminate them entirely and every control will come at some type of cost.

4.6 When designing systems of control, the investment in controls should be in proportion to the risk, e.g., when trying to avoid the most extreme of undesirable outcomes, such as the loss of human life, the associated systems of control have to be forensically designed and effectively implemented. One should expect to undertake a higher degree of effort to reach a "significant" level of assurance for these areas. An active process utilising the agreed levels of assurance for **risk appetite** and **tolerance** is in place.

4.7 **Risk Appetite Statement**

NHS Lothian operates within a low overall risk appetite. The Board and the relevant Board committees will not accept risks with an assurance level of less than moderate (No appetite for none or limited assurance). A higher level of scrutiny will be applied to risks and associated mitigation plans where the level of assurance is none or limited, until a minimum of moderate assurance is agreed. (Tolerate moderate assurance).

4.8 **Inherent risk** can be defined as the exposure arising from a specific risk before any action is taken to manage it i.e. there are no controls in place.

4.9 **Residual risk** - the exposure arising from a specific risk after action has been taken to manage it and making the assumption that the action is effective i.e., controls are in place and are operated as intended

4.10 **Risk escalation** is the process of communicating a risk across up, down or across the organisation to ensure that is managed effectively

4.11 **Risk tolerance** – the boundaries of risks judged to be justifiable and which the Board is prepared to accept or be exposed to at any point in time. This will typically be expressed in quantifiable measures that will be monitored.

5 IMPLEMENTATION AND ROLES AND RESPONSIBILITIES

5.1 Chief Executive

5.1.1 The Chief Executive is the Accountable Officer for NHS Lothian, and as such is legally responsible for ensuring that risks are identified, that their significance is assessed and that systems appropriate to the risks are in place in all relevant areas to manage them.

5.1.2 For the purpose of the role of Accountable Officer, the Chief Executive shall require assurance from the executive directors that risks are being managed. The Chief Executive shall also take independent assurance from the Audit and Risk Committee as to the robustness of the risk management arrangements throughout the Board.

5.2 **Medical Director**

5.2.1 The Medical Director is the lead executive director for the Board's risk management arrangements and has delegated responsibility for leading on their development and implementation.

5.3 **Associate Director for Quality Improvement & Safety**

5.3.1 The Associate Director for Quality Improvement & Safety (as NHS Lothian designated chief risk officer) promotes arrangements for risk management, including maintenance of materials to support the process, and support for operational management teams including training. This includes preparation of an annual report on risk management and periodic reporting to the Board and others as required, in accordance with the agreed corporate risk register process.

5.4 **Managers of Functions and Services**

Managers must ensure that within their area of responsibility:

- risk is effectively identified and managed, including, but not limited to, ensuring that this policy and other arrangements put in place are followed
- they ensure all local efforts taken to mitigate the risk have been exhausted prior to escalation.

5.5 **All Staff**

All staff are responsible for:

- continually considering the potential risks
- identifying risks
- taking quick and appropriate action to escalate any risk they have identified

6 Associated Procedures & Guidelines

7 Implementation of this policy is predominantly achieved by recording the risk management information in the risk register module on DATIX. Following NHS Lothian policies, procedures, guidance and systems on all matters is in itself a 'key' to controlling risk. All NHS Lothian policies, procedures, guidance and systems are designed to achieve the aims and objectives of the subject matter. This Risk Management Policy and its associated procedures should assist in managing the risks that arise from these activities. Details of the processes are set out in the Risk Management Procedure and supporting guidance documents

7.1 The principles of this policy and its associated procedure are based upon recognised good practice in risk management, as set out in the following publications:

Blueprint for Good Governance in NHS Scotland *second edition, published in December 2022*
The Orange Book *Management of Risk - Principles and Concepts published by HM Treasury 2020. The Orange Book (publishing.service.gov.uk)*
Institute of Risk Management – *Risk management standard 2002 IRM's risk management standard (theirm.org)*

https://www.gov.scot/publications/scottish-public-finance-manual/accountability/annex-1-memorandum-to-accountable-officers-scottish-administration/

Scottish Government's Audit & Assurance Handbook (April 18)

8 REVIEW OF THIS POLICY

8.1 The Responsible Officer will continually keep this policy under review with a formal review every 3 years.