<table>
<thead>
<tr>
<th><strong>Title:</strong></th>
<th>Risk Management Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Date effective from:</strong></td>
<td>03/10/2018</td>
</tr>
<tr>
<td><strong>Review date:</strong></td>
<td>03/10/2021</td>
</tr>
<tr>
<td><strong>Approved by:</strong></td>
<td>NHS Lothian Board</td>
</tr>
<tr>
<td><strong>Approval Date:</strong></td>
<td>03/10/2018</td>
</tr>
<tr>
<td><strong>Author/s:</strong></td>
<td>Quality &amp; Safety Assurance Lead</td>
</tr>
<tr>
<td><strong>Policy Owner:</strong></td>
<td>Associate Director for Quality Improvement &amp; Safety</td>
</tr>
<tr>
<td><strong>Executive Lead:</strong></td>
<td>NHS Lothian Medical Director</td>
</tr>
<tr>
<td><strong>Target Audience:</strong></td>
<td>Managers / All NHSL Staff</td>
</tr>
<tr>
<td><strong>Supersedes:</strong></td>
<td>Risk Management Policy v1.0 (June 2012)</td>
</tr>
<tr>
<td><strong>Keywords (min. 5):</strong></td>
<td>Risk, Risk Management, Residual Risk, Governance, Register</td>
</tr>
</tbody>
</table>
RISK MANAGEMENT POLICY

1 EXECUTIVE SUMMARY

1.1 Key Messages

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, such as safe and effective care.

To increase our chances of success, 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.

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 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.
- That all employees are clear of their roles and responsibilities in regard to 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 in order for it to deliver its purposes and intended outcomes.

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, such as safe and effective care.

To increase our chances of success, 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 The following diagram, taken from the guidance on Corporate Governance and Assurance, illustrates the general concept:

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 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:

- At each meeting, review a report summarising any significant changes to the Board’s corporate risk register, and what plans are in place to manage them. The Committee may also elect to occasionally receive information on significant risks held on other risk registers held in the organisation.
- Assess whether the Corporate Risk Register is an appropriate reflection of the key risks to the Board, so as to advise the Board.
- 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.
- Reflect on the assurances that have been received to date, and identify whether entries on the Board’s risk management system requires to be updated.
- Receive an annual report on risk management, confirming whether or not there have been adequate and effective risk management arrangements throughout the year, and highlighting any material areas of risk.

3.3 Whilst the Committee shall seek assurance on the overall system of risk management for all risks and risks pertinent to its core functions, the Board’s Healthcare Governance Committee shall provide particular oversight to clinical risks and all matters relating to the Board’s legal duty to monitor and improve the quality
of health care which it provides (Reference: S12H of National Health Service (Scotland) Act 1978).

3.4 The Healthcare Governance Committee shall also provide oversight to the Board’s responsibilities for information governance, through the Information Governance Sub-Committee.

3.5 The Staff Governance Committee shall have particular oversight of risks relating to the Board’s legal duty in relation to the governance of staff. (Reference: S12I of National Health Service (Scotland) Act 1978).

3.6 All of the committees shall use the standard levels of assurance (Significant, Moderate, Limited, None, Not Assessed Yet) 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
- assessing and judging risks
- assigning ownership for the management of the risk
- taking actions to mitigate or anticipate them
- monitoring and review progress

4.4 The risk register is a record of the risks identified, the assessment of them, the controls in place to manage them and any additional actions planned to improve controls to manage them. There should be risk registers at all levels of the organisation.

4.5 An internal control is 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.

4.7 **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

4.8 **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

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

4.10 **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 Medical Director for Quality Improvement & Safety 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.
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**

6.1 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 **Evidence Base**

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

- Institute of Risk Management: A Risk Management Standard © IRM: 2002
- Scottish Government Memorandum to Accountable Officers for Parts of the Scottish Administration November 2010
- *The Scottish Public Finance Manual*
- *Scottish Government’s Audit & Assurance Handbook (April 18)*

8 **REVIEW OF THIS POLICY**

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