United Lincolnshire Hospitals NHS Trust

Risk Management Policy

Version:	2.0
New or Replacement:	Replacement
Policy number:	ULHT-MD-GOV-RM-PMIMSI
Document author(s):	Paul White, Risk Manager
Contributor(s):	Members of the Trust Board & Senior Leadership Team
Approved by:	Trust Board
Date approved:	August 2018 (tbc)
Document status (RAG):	Green
Review date:	July 2021

Policy is:	**Trust-wide**

Version History Log

Version	Date Published	Details of key changes
2.0	July 2018 (tbc)	Complete revision to incorporate principles of the international standard for risk management (ISO 31000); separation of incident management into its own policy.
1.0	October 2014	New document bringing all aspects of risk management under one cover.

United Lincolnshire Hospitals NHS Trust

Contents

Summary

This Risk Management Policy defines the basic principles and techniques of risk management that United Lincolnshire Hospitals NHS Trust has decided to adopt and as such forms the basis of risk-based decision making within all areas of the organisation.

It defines key roles and responsibilities with regard to risk management at corporate and operational levels as well as essential requirements for the maintenance of the Trust's risk registers.

1. Purpose

1.1 The purpose of this Risk Management Policy is to define and communicate essential requirements for consistent application of agreed risk management principles and techniques throughout United Lincolnshire Hospitals NHS Trust (The Trust).

2. Context

2.1 The Trust Board recognises that an effective approach to risk management is a key component of its corporate governance arrangements and system of internal control.

2.2 An effective Risk Management Policy enables the Board to set clear criteria for the assessment and management of risks to its objectives that will enable management to determine the extent of risk the Trust is exposed to at any given time.

2.3 Risk responses can then be agreed and appropriate resources assigned in a way that is proportionate to the level of risk.

3. Objectives

3.1 The primary objective of this policy is to establish foundations that will enable consistent and effective risk management to become embedded within routine management activity throughout the Trust.

3.2 This policy sets out clear definitions, responsibilities, and essential management requirements that will enable risks to be managed in a consistent manner throughout the organisation to support the delivery of safer, more efficient, more effective and more resilient services.

3.3 It also to support the Trust in complying with its corporate governance requirements for maintaining an effective internal control environment.

3.4 Regular review and routine monitoring of the application of this policy will also inform the content of the Trust's Annual Governance Statement (AGS).

4. Scope

4.1 The specific requirements defined in this policy are applicable to the use of risk management in a formal, organisational context. Typically, this involves the use of risk registers.

4.2 Additional requirements relating to specialist areas of risk management (such as health & safety; safeguarding; security; information governance; business continuity; and project management) will be defined in policies and procedures specific to those areas.

5. Compliance

5.1 NHS Trusts are not required to comply with the United Kingdom Corporate Governance Code. Requirements for the Trust's Annual Governance Statement (AGS) are set by NHS Improvement.

5.2 The AGS forms part of the Trust's annual report requirements as set out in chapter 2 of the Department of Health's Group Accounting Manual (paragraph 2.30).

5.3 Amongst the key elements to be covered by the AGS are a description of the risk and control framework and a summary of major and newly identified risks. Consistent application of this policy will support the Trust in meeting these requirements.

6. Roles and Responsibilities

6.1 The **Chief Executive**, as the *Accountable Officer (AO)* for the Trust is responsible for:

- The establishment and maintenance of effective corporate governance and internal control arrangements
- Being open and communicating effectively about the Trust's management of risks, both internally and externally

6.2 **Executive and non-executive members of the Trust Board** are responsible for:

- Maintaining oversight of the effectiveness of risk management within their areas of accountability
- Supporting and promoting the consistent application of this Policy through the Trust's governance arrangements

6.3 The **Medical Director**, as the executive lead for risk management is responsible for:

- Monitoring the consistent application of this Risk Management Policy throughout the Trust
- Retaining a suitable level of professional risk management expertise to support the effective implementation of this Policy

6.4 Corporate service **deputy or associate directors and clinical directorate triumvirates** (clinical directors; heads of nursing and general managers) are responsible for:

- The consistent application of this Policy within their areas of accountability
- The management of specific risks that have been assigned to them and are recorded in the risk register, in accordance with the criteria set out in this policy
- Reporting on risk management matters as and when required to ensure that risk management performance can be monitored, assurance provided and risks escalated to a more senior level of management where appropriate

6.5 All **members of staff** are responsible for:

- Applying this policy to any relevant risk management activity undertaken in the course of their duties
- The completion of any risk management-related mandatory Core Learning

7. Definitions

7.1 The following terms are used in this Policy:

The Trust	United Lincolnshire Hospitals NHS Trust
Staff	All employees of the Trust, including those managed by a third party organisation on behalf of the Trust
Governance	The arrangements by which the organisation is directed and controlled in order to achieve its objectives
AGS	Annual Governance Statement
AO	Accountable Officer
A risk	An uncertain event which, if it occurred would have an effect on the achievement of objectives
Risk management	The process of identifying and assessing risks, then planning and implementing responses
Risk register	A corporate document used to formally record information about specific risks
BAF	The Board Assurance Framework, a corporate document used by the Trust Board to maintain a focus on the management of significant risks to the strategic objectives of the organisation

Datix	The Datix Risk Management System (also known as Datix Web), is the software application which hosts the Trust risk register
Likelihood	A measure of the probability that a risk event will occur
Severity	A measure of consequence if a risk were to materialise
Risk appetite	The tendency of an individual or group to accept risk in a given situation
Risk control	A system, process or activity that is designed and implemented in order to reduce the level of uncertainty or mitigate the scale of impact associated with a risk
Inherent risk	The extent of risk exposure before any control measures are taken into account
Residual risk	The extent of risk exposure that remains after current controls are taken into account
Acceptable risk	The extent of risk exposure that could be tolerated
Corporate risk	A risk that is wider than a single directorate in its scope and substantial in terms of its potential severity
Strategic risk	A corporate risk that is considered by the Trust Board to be of strategic significance and is therefore recorded on the BAF
Operational risk	A risk within a single directorate that is significant in terms of its severity
Programme risk	A risk to the overall delivery of an established improvement programme (impacting on the timeliness, cost or quality of the programme)
Project risk	A risk to the delivery of an established project (impacting on the timeliness, cost or quality of the project)
KRI	Key Risk Indicator, a statistical measure that informs the assessment of a risk

8. Associated documentation

8.1 This policy defines the essential principles and techniques of risk management that are applicable throughout the Trust.

8.2 There are also a number of specialist areas of risk management that have their own policy and procedural requirements which should be applied in ways that are consistent with this policy. This includes policies and guidance within the following areas:

- Corporate, directorate and specialty governance
- Patient safety
- Health & safety
- Fire safety
- Site security
- Information governance & security
- Data quality
- Emergency planning
- Business continuity
- Financial management
- Communication & engagement
- Training & development
- Estates & facilities management
- Supply chain management
- Diversity & inclusivity
- Programme & project management

9. Risk management policy

9.1 The aim of this Policy to provide clarity regarding the essential elements of the risk management process and how they are to be applied within the Trust. This specifically refers to those corporate and operational risks which are managed in accordance with the Risk Management Strategy and are recorded on the Trust's risk register (held on the Datix Risk Management System).

Risk identification & response

9.2 In accordance with the Risk Management Strategy, risks that are recorded within the Trust's risk registers will be defined centrally and to a corporate standard, covering the full range of the organisation's objectives. Any risks that are identified as falling outside of the existing risk framework must be formally assessed with support from the Risk Manager before being added to the risk register as a new risk.

9.3 Key to the effective management of risk is a clear and unambiguous description of the risk itself. To ensure that all risks recorded within the Trust's risk registers are clearly and appropriately described, detailing the potential cause, event and effect of the risk, the following structure will be used for all risk descriptions:

If [event X] were to happen;

Caused by [issue Y];

It could result in [outcome Z].

9.4 With comprehensive risk registers in place the role of management is to review those risks in light of available evidence and identify any factors which increase the likelihood of the risk occurring. Specifically, this involves giving due consideration to the effectiveness of existing risk control measures and any identifying any significant gaps or weaknesses that could be exploited in the future by known or potential threats.

9.5 Wherever gaps or weaknesses in the control framework are identified they must be recorded on the relevant risk register, along with details of a mitigating action plan to address them.

9.6 Every risk entered on the Trust's risk register requires a named individual who is responsible for its management. This should be the person best placed to manage the risk with sufficient authority to make any decisions that are required, which will usually be the clinical or associate director.

9.7 The responsible manager will decide on an appropriate risk treatment strategy to be applied to each risk assigned to them, from the following options:

- **Reduce** the risk – take decisive action to affect the likelihood of the risk occurring, or mitigate the potential impact through the preparation of contingency plans
- **Accept** the risk – take no action, in the knowledge that the risk may occur with full effect

9.8 There are two further potential options available when deciding on a risk treatment strategy, although in practice these are rarely used as they require a fundamental change to the way in which a service is delivered. Those options are:

- **Avoid** the risk – take decisive action to cease the activity that makes the risk possible
- **Transfer** the risk – take decisive action to pass responsibility for the risk, either wholly or in part, to a third party by means of a formal arrangement such as a contract or insurance policy

Risk assessment

9.9 There are two quantifiable components to any risk assessment:

- Likelihood (sometimes referred to as probability); and
- Severity (sometimes referred to as impact or consequence)

9.10 Both of these components need to be evaluated according to clearly defined criteria that are applied consistently throughout the organisation, to enable meaningful prioritisation of risks and for proportionate responses to be decided upon, planned and implemented.

9.11 The Trust's criteria for assessing the likelihood and severity of any risk recorded on the risk register are set out in **Appendix I – Risk scoring guide**. Should risk scoring criteria be required for a purpose other than the use of a risk register (such as for a corporate project or personal risk assessment) then an appropriate guide must be developed based on the principles described in this policy.

9.12 Any risk assessment should aim to be as objective as possible, making use of available evidence and engaging with all relevant stakeholders so that different perspectives are taken into account and understanding of the risk is optimised.

9.13 By making clear from the initial assessment precisely how a risk has been assessed (what evidence and perspectives have been used), it will be possible over time to evaluate the effectiveness of the risk response.

9.14 It is essential for effective risk-based decision making that whoever is making the decision does so with an awareness of the reliability of any evidence used to inform the risk assessment. If an assessment is based on subjective or anecdotal evidence alone, rather than verifiable data, this should be recorded in the risk register.

9.15 Organisational learning to inform risk management decisions can come from many different sources, including:

- Root cause analysis from incident investigations
- Data analysis and forecasting of Key Risk Indicators (KRIs)
- Consultation & engagement exercises
- Patient experience reports
- Mortality reviews
- Coroner's inquests
- De-briefs from major incidents
- Audit and inspection reports

Reviewing risks

9.16 All risks that are currently active on the Trust risk register should be reviewed regularly by the manager responsible. Reviewing a risk should include as a minimum requirement:

- Consideration of the current (residual) risk rating
- Updates to any outstanding actions that have been planned to address gaps or weaknesses in control

- Recording on the risk register (Datix) the next date the risk is due for review

9.17 The minimum frequency required for formal review of corporate and operational risks within the Trust risk register is quarterly.

9.18 This requirement relates to the process of formal review and updating of the risk register on Datix. More frequent reviews can take place at the discretion of the responsible manager, as and when material changes in particular risks are identified.

9.19 It is good practice to routinely monitor evidence in relation to all risks within a risk register as an established element of regular governance arrangements. This will enable emerging areas of risk to be identified at an early stage and appropriate action instigated promptly where possible.

9.20 The method of review can be determined by the responsible manager. It does not need to take place at a formal meeting, but should involve key stakeholders (those who have a direct interest in the management of the risk).

9.21 The task of maintaining the risk register may be assigned to any suitably skilled member of the team provided they have the necessary access to Datix. It does not have to be the responsible manager.

9.22 Following each formal review the risk record must be updated to show that a review has taken place, even if no changes have been made, and a new review date set as the last day of the month, 3 months from the date of most recent review.

9.23 Risks that form part of the corporate risk framework cannot be closed at directorate level; they can only be closed if the Trust Board decides that the risk in question no longer needs to be recorded. Any additional risks that have been added following formal assessment with the Risk Manager may be closed when the level of residual risk is agreed as acceptable by the responsible manager. An explanation of the reason for closing any risk must always be recorded on Datix.

Risk management performance reporting

9.24 Every directorate within the Trust is expected to make active use of the Datix risk register to support their management of risks.

9.25 All clinical directorates will be expected to provide a regular report on the content of their risk registers as part of the Trust's performance management arrangements.

9.26 Every executive-led management committee that has oversight of elements of risk management will receive regular reports that highlight high risks and provide assurance regarding risks that are being managed effectively.

9.27 Every assurance committee of the Trust Board will receive a regular report from the Risk Manager detailing those elements of the Corporate Risk Register that fall within its remit as well as any high and emerging operational risks, in order to inform their regular review of relevant sections of the Board Assurance Framework (BAF).

9,28 The Audit Committee of the Trust Board will receive a regular report from the Risk Manager providing evidence of the effectiveness of risk management arrangements, including data and analysis in relation to each of the Key Performance Indictors (KPIs) detailed in this Policy.

9.29 The Trust Board will receive a regular report from the Risk Manager detailing the Corporate Risk Register and any high and emerging operational risks, in order to inform its regular review of the BAF.

10. Implementation, Monitoring and Review

10.1 This policy will be published on the Trust website and on the intranet, where it will be accessible to all staff.

10.2 Training in risk management and the use of risk registers on Datix will be incorporated within the Trust's Leadership Programme as a Core Management Skill (M3 – Improving Services). This will include the provision of classroom based training sessions and e-learning that is made available through the Trust intranet.

10.3 Additional training and support will be made available on request from the Risk Management team.

10.4 A range of guidance documents will also be published on the intranet to support the implementation of this policy and the use of the Datix system.

10.5 The Trust uses the Risk module within the Datix Risk Management System as its risk register. This carries an annual licence and support cost which will be included within the Risk Management budget.

10.6 A number of Key Performance Indicators (KPIs) which will be used to monitor the effectiveness of this policy are defined in the table below. These will be reported routinely to the Audit Committee of the Trust Board along with the results of regular internal audits of risk management.

Monitoring Compliance

Minimum requirement to be monitored –monitoring against standards set out in policy	Process for monitoring e.g. audit	Responsible individuals/ group/ committee	Frequency of monitoring/ audit/ reporting	Responsible individuals/ group/ committee for review of results and determining actions required
Number of risks overdue their required review date (by risk lead)	Data extract (Datix)	Risk Manager	Quarterly	Audit Committee
Number of new risks added to the risk register (by risk register type, corporate or operational)	Data extract (Datix)	Risk Manager	Quarterly	Audit Committee
Number of risks closed on the risk register (by risk register type, corporate or operational)	Data extract (Datix)	Risk Manager	Quarterly	Audit Committee
Risk management training completion rates	Data extract (ESR)	Risk Manager	Quarterly	Audit Committee
Independent review of risk management	Audit	Internal audit	Annual	Audit Committee

Appendices

Appendix I – Risk scoring guide

Appendix II – Generic risk assessment form

United Lincolnshire Hospitals NHS Trust

Equality Analysis: Initial Assessment Form

Title: *of the function to which the Equality Analysis Initial Assessment applies*
Risk Management Policy

Describe the function to which the Equality Analysis Initial Assessment applies:		
☐ Service delivery	☐ Service improvement	☐ Service change
☒ Policy	☐ Strategy	☐ Procedure/Guidance
☐ Board paper	☐ Committee / Forum paper	☐ Business case
☐ Other (please specify) ……		

Is this assessment for a new or existing function?	**Existing**
Name and designation of function Lead professional:	**Paul White, Risk Manager**
Business Unit / Clinical Directorate:	**Corporate / Risk Management**

What are the intended outcomes of this function? (*Please include outline of function objectives and aims):* To establish clear requirements for staff carrying out risk management activities in a consistent manner throughout all areas of the Trust.		
Who will be affected? Please describe in what manner they will be affected?		
Patients / Service Users:	**Staff:**	**Wider Community:**
May encounter risk management information published or released by the Trust.	Will be required to follow the policy when carrying out risk management activities in the course of their employment.	May encounter risk management information published or released by the Trust.

What impact is the function expected to have on people identifying with any of the protected characteristics (below), as articulated in the Equality Act 2010? (Please tick as appropriate)

	Positive	Neutral	Negative	**Please state the reason for your response and the evidence used in your assessment.**
Disability		X		This is an internal management policy that defines requirements within the Trust's internal control framework and as such does not differentiate between individuals nor have the potential to impact on those with protected characteristics.
Sex		X		As above.
Race		X		As above.
Age		X		As above.
Gender Reassignment		X		As above.
Sexual Orientation		X		As above.
Religion or Belief		X		As above.
Pregnancy & Maternity		X		As above.
Marriage & Civil Partnership		X		As above.
Carers		X		As above.
Other groups identified (please specify)		N/A		As above.

If the answer to the above question is a predicted negative impact for one or more of the protected characteristic groups, a full Equality Analysis must be completed. (The template is located on the Intranet)

Name of person/s who carried out the Equality Analysis Initial Assessment:	**Paul White**
Date assessment completed:	**16th April 2018**
Name of function owner:	**Jeanette Hall, Interim Director of Governance**
Date assessment signed off by function owner:	**16th April 2018**
Proposed review date (please place in your diary)	**16th April 2021**

As we have a duty to publicise the results of all Equality Analyses, please forward a copy of this completed document to tim.couchman@ulh.nhs.uk.

Referenced Documents

References

AIRMIC, ALARM, IRM [2010] *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000.* https://www.theirm.org/media/886062/ISO3100_doc.pdf

IFAC / CIPFA [2015] *International Framework: Good Governance in the Public Sector*

OGC [2010] *Management of Risk (M_o_R) Guidance for Practitioners – 3rd Edition*

NPSA [2008] *A Risk Matrix for Risk Managers*

HM Treasury [2004] *The Orange Book: Management of Risk – Principles & Concepts*

United Lincolnshire Hospitals NHS Trust

Signature Sheet

Names of people consulted about this policy:

Name	Job title	Department
		All members of the Executive Team & deputies / associates
		All members of clinical directorate triumvirates
		Quality & Risk management teams
		Quality & Safety Officers
		Programme Management team
		Health & Safety management team
		Research management team
		Specialists in: security; information governance; business continuity / emergency planning; fraud

Names of committees which have approved the policy	Approved on
Trust Board	August 2018 (tbc)