Outstanding Care,
Compassionate People,
Healthier Communities

NHS
Sherwood Forest Hospitals
NHS Foundation Trust

RISK MANAGEMENT AND ASSURANCE POLICY

POLICY

Reference	G/RMP		
Approving Body	Risk Committee		
Date Approved	9th February 2026		
For publication to external SFH website	**Positive confirmation received from the approving body that the content does not risk the safety of patients or the public:**		
	YES	**NO**	**N/A**
	✓		
Issue Date	February 2026		
Version	14		
Summary of Changes from Previous Version	• Section 4 – update in frequency of Board Assurance Framework reporting • Sections 4 and 6 – update on risk score increase approvals • Appendix 1 – Risk Scoring Matrix – to include values on consequence scores for Finances		
Supersedes	13		
Document Category	Governance		
Consultation Undertaken	Risk Committee		
Date of Completion of Equality Impact Assessment	January 2026		
Date of Environmental Impact Assessment (if applicable)	N/A		
Legal and/or Accreditation Implications	None		
Target Audience	All Trust staff groups		
Review Date	February 2027		
Sponsor (Position)	Director of Corporate Affairs		
Author (Position & Name)	Risk and Assurance Manager		
Lead Division/Directorate	Corporate		
Lead Specialty/Service/Department	Risk Management		
Position of Person able to provide Further Guidance/Information	Risk and Assurance Manager		

Associated Documents/ Information	**Date Associated Documents/Information was reviewed**
Risk Management Strategy	*May 2023*

CONTENTS

APPENDICIES

1.0 INTRODUCTION

Risk management is both a statutory requirement and an indispensable element of good management. It is a fundamental part of the total approach to quality, corporate and clinical governance and is essential to the Trust's ability to discharge its functions as a partner in the local health and social care community, as a provider of health services to the public and as an employer of staff.

The activities associated with caring for patients, employing staff, providing facilities and services and managing finances are all, by their nature, activities that involve risk. These risks are present on a day-to-day basis throughout the organisation and whilst it may not always be possible to eliminate these risks, they can be managed to an acceptable level.

Good risk management is integral to the effectiveness of all the Trust's activities and as such must be integrated into all functions' day-to-day practice and embedded within the culture of the organisation so that appropriate risk-based decisions are regularly made by managers and staff at all levels.

An effective Risk Management policy enables the Board of Directors to determine the extent of risk exposure it currently faces with regard to the achievement of its objectives. As a key component of the internal control framework, regular review and routine monitoring of this policy will also inform the Trust's Annual Governance Statement.

This policy is issued and maintained by the Director of Corporate Affairs (the sponsor) on behalf of the Trust, at the issue defined on the front sheet, which supersedes and replaces all previous versions.

2.0 POLICY STATEMENT

The purpose of this Risk Management and Assurance Policy is to define the approach taken by Sherwood Forest Hospitals NHS Foundation Trust (The Trust) in applying risk management to its decision making at all levels.

The main objective of this policy is to establish the foundations for a culture of effective risk management throughout the organisation. It sets out clear definitions, responsibilities, and process requirements to enable the principles and techniques of risk management to be applied consistently throughout the organisation.

It is the policy of the Trust that risk management is everyone's responsibility and that the principles of effective risk management should form an integral component of decision making at all levels.

The principles and techniques of risk management as defined in this policy should be fully integrated within the formal governance arrangements and decision-making processes of the organisation.

All Trust staff are responsible for making sure that they are aware of the organisation's objectives and are empowered to make decisions to manage risks to the achievement of those objectives so long as those decisions are within the scope of their role and level of authority.

Where a risk is identified but cannot be managed without some significant change to the way the organisation operates, it must be escalated through the relevant line management structure.

The Risk Management and Assurance Policy applies to all areas of the Trust and at all levels. It defines the basic principles and techniques of risk management that the organisation has decided to adopt and forms the basis of all risk-based decision making.

It is expected that all risk management activities in the Trust will follow the process described within this document to ensure a common and robust approach to risk management.

3.0 DEFINITIONS AND ABBREVIATIONS

The following terms are used in this Policy:

Accept - taking no action in response to a risk, acknowledging that it may occur with full affect.

Adverse event is any event or harm or circumstance leading to unintentional harm or suffering i.e. the occurrence by which a risk materialises (i.e. becomes an incident).

Assurance - evidence that shows we are reasonably managing our risks and that our objectives are being delivered. Sources of assurance incorporate the three lines of defence: (1) **Management** (those responsible for the area reported on); (2) **Risk and compliance** functions (internal but independent of the area reported on); and (3) **Independent assurance** (internal audit and other external assurance providers).

Avoid - removing a risk entirely, by ceasing the activity that makes it possible.

Board Assurance Framework (BAF) - provides the Trust with a simple but comprehensive method for the effective and focused management of the principal risks to meeting their objectives. It is reported regularly to the Board of Directors and provides a structure for the evidence to support the Chief Executive Officer's Annual Governance Statement.

Cause - the factor(s) which make a risk possible (such as a hazard or vulnerability).

Clinical risk is the chance of something happening to a patient during NHS care that could have or did lead to unintended or unexpected harm, loss or damage. This is a broad definition that may range from dissatisfaction on the part of patients at having to wait so long for treatment or at lack of communication, to undergoing the wrong operation, or suffering permanent disability or death.

Consequence (Impact/Severity) is the level of harm or disruption that has, or may be, suffered, and is measured at the Trust on a scale of 1 to 5. *(Please refer to Appendix 1 for additional guidance.)*

Controls are arrangements and systems that are intended to minimise the likelihood or severity of a risk. An effective control will always reduce the probability of a risk occurring. If this is not the case, then the control is ineffective and needs to be reconsidered. Controls are intended to improve resilience.

Current risk is the risk remaining with the current controls in place.

Datix - the software application that hosts the Trust risk register.

Gap in assurance is deemed to exist where there is a failure to gain evidence that the controls are effective.

Gap in control is deemed to exist where adequate controls are not in place or where collectively they are not sufficiently effective. A negative assurance, for example an Internal Audit report issued with limited assurance, that highlights gaps in control.

Governance - the ways in which the organisation is directed and controlled in order to achieve its objectives.

Hazard is something which has the potential to cause harm, e.g. substances, equipment, methods of work, and other aspects of work organisation.

Inherent risk is the risk linked to the activity itself without the application of controls.

Inherent clinical risk is the permanent or currently unavoidable clinical risk that is associated with a particular clinical investigation or treatment. It is the risk from undergoing a particular procedure in ideal conditions and performed by competent staff using the most up-to-date research, equipment and techniques. It can be considered permanent or currently unavoidable when used for the purpose of risk assessment. The risk that should be targeted by clinical risk assessment is the risk that is added to the inherent risk and results from, for example, a poor safety culture, poor communication and teamwork, inadequate supervision of inexperienced staff, unreliable equipment or an unsuitable environment.

Internal control is the process effected by the Board of Directors designed to provide reasonable assurance that the Trust's objectives will be met with regards to: (1) Effectiveness and efficiency of operations; (2) Reliability of financial reporting; (3) Compliance with applicable laws and regulations.

Likelihood is measured by the frequency of exposure to the hazard or the probability of an event occurring on a scale of 1 to 5. *(Please refer to Appendix 1 for additional guidance.)*

Modify - taking action to influence the likelihood of a risk event materialising, or plan a contingency.

Opportunity - a risk with a positive impact on objectives.

Patient safety incident is any unintended or unexpected incident which could have or did lead to harm for one or more patients receiving healthcare. It is a specific type of adverse event.

Principal Risk is a risk that can adversely affect the achievement of the Trust's corporate objectives and is identified, assessed and monitored by the Board Assurance Framework.

Probability is the chance that something will happen, calculated statistically.

Residual risk is ‘the mitigated risk remaining after all reasonable controls have been applied to associated hazards that have been identified, quantified, analysed, communicated to the appropriate level of management and accepted after proper evaluation’.

Risk - an uncertain event which, if it occurred would have an effect on the achievement of objectives. The level of risk is calculated by considering the likelihood (probability) that an event will occur in a specific time period, or as a result of a specific situation and the impact of the consequence should it occur.

Risk appetite - amount and type of risk that an organisation is willing to pursue or retain.

Risk assessment is the process by which risks are prioritised and then categorised through the application of a 5 by 5 calculation to produce a composite score out of a maximum of 25 (25 being the most severe). The risk assessment is based on the probability (likelihood) of an event occurring on a 1 to 5 scale, multiplied by its likely consequence or impact (severity) which is measured on a similar 1 to 5 scale. An account of the criteria for obtaining accurate measures of risk and severity of consequence or impact can be found in Appendix 1.

Risk management is the systematic identification, assessment, treatment, monitoring and communication of risks. This process is followed by the application of current or planned resources to effectively control, monitor and minimise the overall likelihood (and in some instances, impact) of the identified risk.

Risk lead - the individual who has been assigned to oversee and co-ordinate the review and co-ordination of any actions (or risk treatments) to effectively manage the risk.

Risk register - is a management tool that allows the Trust to understand its comprehensive risk profile. It is simply a repository of risk information linking risks and controls for the whole organisation.

Risk tolerance - organisation’s or stakeholder’s readiness to bear the risk after risk treatment in order to achieve its objectives.

Risk treatment - the approach taken by the risk lead in response to an unacceptable risk.

Seek - actively pursue a risk, on the basis that it would be beneficial to do so.

Target risk is the remaining risk when **all** reasonable controls have been applied – when the additional controls to mitigate the residual risk have been applied and are effective.

The Trust - Sherwood Forest Hospitals NHS Foundation Trust.

Threat - a risk with a negative potential impact on objectives.

Transfer - passing responsibility for a risk, either wholly or in part, to a third party by means of a formal arrangement (such as a contract or insurance policy).

4.0 ROLES AND RESPONSIBILITIES

This section details those groups and individuals within the Trust that have specific responsibilities with regard to the Risk Management and Assurance Policy.

The **Board of Directors** is responsible for providing strategic leadership to risk management throughout the organisation, which includes:

- Maintaining oversight of strategic risks through the Board Assurance Framework (BAF)
- Leading by example in creating a culture of risk awareness

The **Chief Executive Officer** as the *Accountable Officer* is responsible for ensuring an effective system of internal control is maintained to support the achievement of the Trust's strategic objectives. This includes:

- The establishment and maintenance of effective corporate governance arrangements
- Ensuring that this Risk Management and Assurance Policy is applied consistently and effectively throughout the Trust
- Ensuring that the Trust is open and communicates effectively about its risks, both internally and externally
- Retaining sufficient professional risk management expertise to support the effective implementation of this Policy

The **Director of Corporate Affairs** is accountable to the Board of Directors and Chief Executive Officer for the Trust's governance and risk management activities. With Executive responsibility for corporate governance and risk management the Director of Corporate Affairs (with support from the **Risk and Assurance Manager**) provides a clear focus for the management of organisational risks and for coordinating and integrating all the Trust's risk management arrangements on behalf of the Board of Directors.

Members of the **executive**, **divisional** and **directorate senior management teams** are responsible for the consistent application of this Policy within their areas of accountability, which includes:

- Maintaining an awareness of the overall level of risk within the organisation
- The management of specific risks that have been assigned to them, in accordance with the criteria set out in this Policy
- Promoting a risk aware culture within their teams and in the course of their duties

Heads of service are responsible for the consistent application of this Policy within their areas of accountability, which includes:

- Making active use of the Trust risk register and the processes described in this Policy to support the management of their service
- The management of specific risks that have been assigned to them in accordance with the criteria set out in this Policy
- Promoting a risk-aware culture within their teams and in the course of their duties
- Ensuring that as far as possible risk assessments carried out within their service are based on reliable evidence

Risk leads are responsible for managing risks to which they are assigned and ensuring that the risk register is kept up to date

Every member of staff is responsible for identifying and managing risks within their day-to-day work, which includes:

- Maintaining an awareness of the primary risks within their service
- The identification, and as far as possible, the management of risks that they identify in the course of their duties
- Bringing to the attention of their line manager any risks that are beyond their ability or authority to manage

Board and Committee Responsibilities

The Trust strives to ensure effective risk awareness and management is integrated throughout the Trust and therefore it is expected that discussions of risk will take place within all appropriate forums, and this is reflected within sub-committees' and groups' Terms of Reference. However, the following committees have specific roles and responsibilities assigned to them.

The **Board of Directors** is responsible for assuring that appropriate risk management systems are in place to enable the organisation to deliver its objectives.

The Board of Directors is also responsible for identifying and controlling the organisation's Principal (strategic) Risks and Assurance Framework and will receive the Board Assurance Framework at least 3 times per year.

The **Quality, Finance, People, Partnerships & Communities and Risk** Committees have responsibility for maintaining effective oversight of strategic risks assigned to them by the Board, providing a process of regular formal review at committee meetings, at least 3 times per year, in light of assurances received and agreeing any necessary changes to enable the BAF to be updated before it is next reviewed by the Board.

Risk Committee receives the full BAF 4-monthly. If any additional changes to principal risks are discussed in Risk Committee meetings, the Lead Director will be requested to propose these at the respective Lead Committee meetings.

The **Risk Committee** is responsible for the regular review and maintenance of this Policy, and for making recommendations to the Executive if any material changes are required. The Risk Committee's responsibilities are outlined within its Terms of Reference but include:

- Defining the Risk Management and Assurance Policy
- Receiving regular internal reports on the application and effectiveness of this Policy, including the review of significant risks
- Commissioning independent audits of the Trust's risk management arrangements
- Bringing to the attention of the relevant Executive Director any risk management issues highlighted through internal reporting or independent audit
- Overseeing a continuous programme of risk management training and communication
- Maintaining effective oversight of strategic risks assigned from the BAF by the Board
- Maintaining a holistic view of risk management across the organisation, ensuring consistency between operational and strategic risk assessments and escalation of significant risks or risks that may impact upon strategic priorities

Specialty and **Divisional Governance meetings** will include the review of risks specific to the Specialty or Division in accordance with the risk escalation and reporting procedures described in the ‘ Report on the risk’ section below.

Each new risk added to the Datix system, or increase in the score of an existing risk, must be reviewed and approved as set out in the ‘Report on the risk’ section on page 13 below

Additionally, the Audit and Assurance Committee provides assurance on the robustness of risk management processes to the Board of Directors.

5.0 APPROVAL

This Policy is approved by the Risk Committee.

6.0 DOCUMENT REQUIREMENTS

Risk management approach

The basic principle at the heart of the Trust’s risk management approach is that an awareness and understanding of risk should be used to inform decision making at all levels.

This requires not only the active engagement of all staff with risk management activity in practice, but also the integration of risk management principles and techniques within the formal governance arrangements of the organisation.

This will ensure that major strategic, policy and investment decisions are made with a full and reliable appreciation of the risks associated with them as well as any existing risks that those decisions may serve to mitigate.

Risk management process

All formal risk management activity carried out within the Trust should follow the same 7 basic steps that form a continuous cycle:

1. Determine priorities
2. Identify the risk
3. Assess the risk
4. Respond to the risk
5. Report on the risk
6. Review the risk
7. Learn and adapt

This risk management process is described in more detail below.

Determine priorities

The risks that require management are those that would have consequences for the organisation and its ability to achieve its objectives, which first requires a clear understanding of what those objectives and current priorities are. This enables the identification and treatment of risks to be targeted and relevant.

Risk Identification

New risks and factors that increase a known risk may be identified at any time and by anyone within the organisation and can take many different forms.

Some risks can be managed effectively by the person identifying them, by taking appropriate action themselves or within their immediate team. This is particularly true with types of safety risk, where identification and removal of the hazard will often be sufficient to manage the risk.

Staff should initially consider what their main areas of work are and how these relate to their local objectives, and the objectives of the Trust. Every work activity that has a significant hazard should be assessed for risk. Identification using a systematic approach is critical because a potential risk not identified at this stage will be excluded from further analysis.

All risks, whether under the control of the Trust or not, should be included at this stage. The aim is to generate an informed list of events that might occur. Key sources that will inform this exercise include:

- Root cause analysis of incidents, inquiries, complaints or claims
- Care pathway analysis
- Recommendations from recent internal or external audit reports Performance data
- Evaluation reports
- Trend and forecasting analysis
- Compliance requirements with regulators and stakeholders such as the CQC, the Integrated Care System (ICS) and NHS England
- Partnerships and collaborative working arrangements, including ICS risks
- Risks associated with the achievement of corporate objectives
- Other methods of horizon scanning

Assess the risk

There are two quantitative components to any risk assessment: **likelihood** (sometimes referred to as probability) and **consequence** (sometimes referred to as impact or severity).

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 actions and for proportionate responses to be decided upon, planned and implemented. The Trust's criteria for assessing the likelihood and consequence of a risk occurring are set out in Appendix1.

When assessing the level of risk, three ratings should be calculated:

1. **Inherent (unmitigated) risk rating** – the consequence x likelihood without any controls in place. This becomes important when reviewing and considering the level of assurance required; the greater the difference between the initial risk rating and the current risk rating the greater the reliance on the control measures in place.

2. **Current risk rating** – the consequence x likelihood with controls in place at the time of assessment or review.

3. **Target risk rating** – the consequence x likelihood with all controls in place and all controls being fully implemented and working effectively. The target risk rating should always be at least as low as the Board of Directors' defined tolerance level.

A Risk Assessment template has been provided to support this process (see Appendix 2). This template should also be used when considering risks associated with new processes, equipment or business cases.

Respond to the risk

The response to the risk should be in proportion to the level of risk identified and in accordance with the risk appetite and tolerance levels set by the Board of Directors.

Given the nature of the organisation as a provider of healthcare services, the Trust generally has a **'minimal'** appetite for risks to the safety and care of patients. This also applies to any risks to the safety and wellbeing of staff and visitors.

When any risk to safety is identified the objective should always be to reduce the risk to as low a level (tolerance) as is practicable before it is accepted, or to avoid it altogether where that is an option.
It is unlikely that the Trust would make any decision that may result in a significant risk to the safety of its patients or staff, unless the only alternative options represented an even greater risk.

The appetite of the Trust where risks to its finances, reputation or the continuity of its services are concerned is described as '**cautious'**, which means that safe options are preferred. The aim should still be to reduce the risk as far as is practicable, but it is possible that a moderate level of risk may be tolerated when all circumstances are taken into account.

This is particularly relevant when balancing these types of organisational risks with safety risks as part of the same decision.

Appetite categories of '**averse'** (aim to avoid the risk entirely) and '**open'** (prepared to accept a higher level of residual risk than usual, in pursuit of potential benefits) are also available, but are not currently applied to any risk types.

The Trust's current statement of risk appetite and target by risk type is summarised on the following table:

Risk type	**Risk appetite**	**Target risk** (maximum)
Patient harm	Minimal	Low
Public harm	Minimal	Low
Staff harm	Minimal	Low
Services	Cautious	Medium
Reputation / regulatory action	Cautious	Medium
Finances	Cautious	Medium

The options for managing identified risks need to be assessed based on cost and benefits derived. Options can be taken in combination or separately. In general, the cost of managing risks needs to be commensurate with the benefits obtained. However, decisions should take account of the need to carefully consider rare but severe risks, which may warrant risk reduction measures that are not justifiable on strictly economic grounds.

Risk treatment strategies include:

- **Accept** – take no further action to improve control of the risk (can be used when the risk level is below the established risk tolerance level and in line with the risk appetite of the organisation)
- **Modify** – take action to improve control of the risk
- **Transfer** – pass the risk to a third party by contract or insurance
- **Avoid** – take action to prevent the risk from materialising
- **Seek** – take action to make the risk materialise (used for positive risks which are in line with the organisation's risk appetite and where the activity presents an opportunity)

Where further action is required, additional controls must be identified, and an action plan developed to ensure the controls are both implemented and effective. Controls fall into three main categories:

- **Prevention / Promotion** – these controls prevent a hazard or problem from occurring or promote a particular positive action (for example Policies, Procedures, Guidelines, Techniques, Processes, Training, Use of Equipment, Checklists, Computer Systems, Protective Clothing, etc.)
- **Detection** – these controls provide an early warning of control failure (for example Audit, Inspection, Monitoring, Incident Reporting, Smoke detectors, Complaints, Surveys, Tests, etc.)
- **Contingency** – these controls provide effective reaction in response to a significant control failure or overwhelming event and are designed to mitigate harm and improve resilience (for example Evacuation Plan, Escalation Procedure, Continuity Plan, Back-up Generator, Locum/Agency cover, Insurance, etc.)

Ward, departmental, corporate and divisional managers must ensure actions are taken to address identified gaps in control.

Actions identified to meet compliance requirements with regulators and stakeholders, and to address recommendations from internal or external auditors, should be captured in a specific, measurable, achievable, relevant and time-assigned (SMART) format within relevant risks, and have appropriate completion timescales.

There is an expectation that managers will ensure that action plans are delivered by the required date.

Report on the risk

The Datix system hosts the Trust's risk register. If a paper risk assessment has been completed, this should be transferred to the electronic risk register.

Every clinical specialty, corporate service, division and directorate within the Trust is expected to make active use of the Datix risk register to support their management of risks.

The key to understanding the true meaning of a risk is ensuring that the risk has a clear description. As a rule, always ensure the risk is fully visible by stating the risk failure followed by the cause of the risk, and impact (consequence) of the risk. For example:

A failure to…
Caused by…
May result in…

Gaps in control/assurance or other specific issues should also be clearly described.

Every risk entered on the risk register requires a named individual who is responsible for co-ordinating an effective response i.e. the **Risk Lead**. Risks can be specific to one division (Service level risk) or may apply to a number of divisions or Trust-wide (Corporate level risk). All divisions must co-operate fully with a risk lead co-ordinating the risk management response to a Corporate level risk.
Unless specifically delegated, all Service level operational risks will be, by default, assigned to the relevant head of service and Corporate risks to the specialist lead.

Each new risk added to the Datix system must be reviewed and approved by:

- Clinical Division - a member of the divisional triumvirate or agreed at the Divisional Clinical Governance meeting
- Corporate Services – the relevant officer below for risks within their portfolio:
    - Executive Director
    - Deputy to Executive Director
    - Chief or Deputy Chief Digital Information Officer
    - Acting/Deputy Director of Strategy and Partnerships
    - Associate Director of Transformation
    - Associate Director of Strategy and Partnerships
    - Director of Midwifery
    - Director of Nursing Quality & Governance

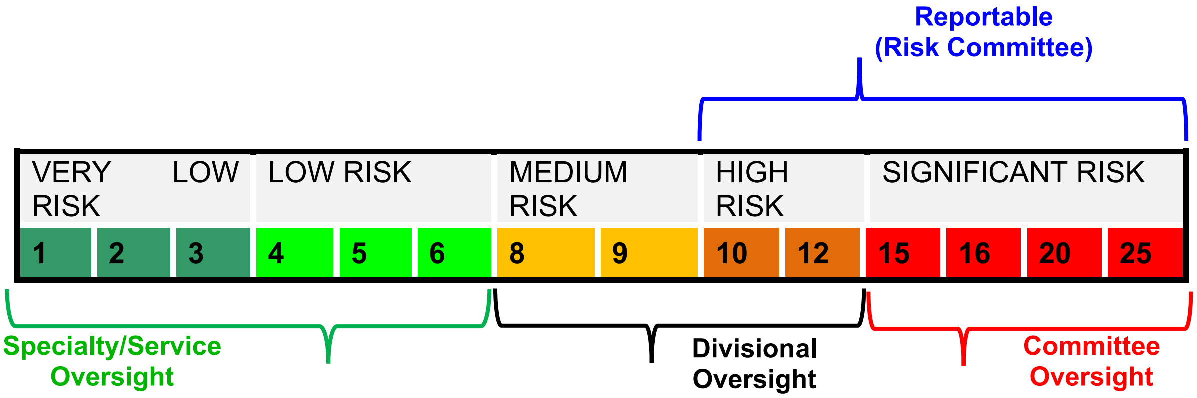
Increases in risk scores for clinical divisions should be agreed at a Divisional Clinical Governance meeting, and ones that increase to 'significant' agreed by the divisional triumvirate. For Corporate services the approval is by the relevant officer above.

Any risks that are being **modified** or **avoided** require an action plan, which must be added to and kept up to date on the risk register.

Risks that have been successfully avoided and therefore no longer present a risk should be closed on the risk register. All other risks should remain on the risk register for as long as they remain relevant, with sufficient monitoring arrangements in place to enable any changes to be detected at an early stage.

Risk escalation and reporting

The purpose of establishing a process for the escalation of risks between different levels of authority within the organisation is to ensure that there is a level of oversight to the management of risks that is appropriate to the extent of risk exposure at any given time.
The hierarchy for oversight and reporting on risks is based on its current risk rating and is summarised on the following diagram:



The definition of oversight within this process refers to the management level within the Trust's governance structure that is responsible for the routine review of those risks. In addition, all risks rated High or Significant are also reportable to the Risk Committee in accordance with an established annual schedule.

This process is designed to ensure that the presence of significant risks is brought to the attention of the appropriate senior managers and executives in a timely manner so that appropriate decisions can be made regarding how they should be managed.

Review the risk

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

- A review of all outstanding actions to address gaps in control
- A review of the current risk rating
- Sources of assurance available that provide confidence the risk is being adequately managed

The minimum required frequency of formal review is determined by the current risk rating, as follows:

Risk rating	Very low	Low	Medium	High	Significant
Frequency	Annually		Quarterly		Monthly

This requirement relates to the process of formal review and updating of the risk register. More frequent reviews can take place at the discretion of the Risk Lead. It is good practice to routinely monitor all risks within a risk register as an established element of regular governance arrangements.

Significant Incidents should always result in the review of the risk register to ensure that any risks are recorded but also that any additional control measures identified through the investigation process are recorded and monitored.

The method of review can be determined by the Risk Lead. 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).

The task of maintaining the risk register may be assigned to any suitably skilled member of the divisional team provided they have the necessary access to Datix. It does not have to be the Risk Lead, although the Risk Lead is responsible for ensuring that the risk register is kept up to date.

Following each formal review, the risk record must be updated to show that a review has taken place (Date of last review), even if no changes have been made, and a new review date set in accordance with the frequency requirements detailed above.

The Risk Committee will receive a regular report from the Risk and Assurance Manager detailing current Significant risks (those rated 15 or more). The Risk Committee will then determine which of these risks should be escalated to the Trust Executive.

In addition, divisions and directorates will be expected to report to the Risk Committee on their High and Significant risks (scoring 10 or more) twice yearly according to the Risk Committee's agreed Work Programme. This process is designed to enable the Risk Committee to take assurance as to the effectiveness of risk management within the Trust and to intervene to support the management of specific risks where necessary.

Division and directorate management teams should ensure that they maintain oversight of all risks rated Medium or above (scoring 8 or more) within their areas of responsibility and seek assurances that controls are effective. These assurances are obtained from a variety of sources, such as:

- Management reports
- Internal and external audit
- Other external assessors such as the Care Quality Commission and the NHSLA

Both positive and negative assurances must be explained, which means that a clear description of what would be seen, known, understood if the controls were effective or not effective in mitigating the risk.

Ward, departmental, corporate and divisional managers must ensure that any gaps in the assurances are clearly identified, and that appropriate actions are taken to identify any gaps in the assurance processes. There is an expectation that managers will ensure that actions to control assurance gaps are delivered within the same timescale as closing gaps in control.

Learn and adapt

Effective risk management in a large and complex organisation is about much more than dealing with individual risks as they are identified. It is essential that the Trust routinely learns lessons from its risk management activities and adapts its systems and processes where necessary.

This stage in the process involves analysing trends, capturing organisational learning and making changes to improve resilience and enhance the future management of risk.

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

- Root cause analysis from reported incident investigations
- Coroner inquests
- De-briefs from major incidents
- Clinical audit results
- Internal audit results
- Data analysis and forecasting
- Patient experience reports
- Policy reviews
- Consultation and engagement exercises

The Risk Committee is central to ensuring that learning is disseminated, and policies, processes and procedures are adapted to mitigate risks. This is achieved by:

- Overseeing a continuous programme of risk reporting and management
- Identifying additional controls and assigning associated actions required to mitigate risks
- Escalating to the Executive Team any risks that require additional support to implement mitigating actions

Maintaining a holistic view of risk management across the organisation, ensuring consistency between operational and strategic risk assessments and escalation of significant risks or risks that may impact upon strategic priorities.

7.0 MONITORING COMPLIANCE AND EFFECTIVENESS

The following are received by the Risk Committee to ensure oversight of significant and high risks, and to monitor performance of risk management and the timely completion of associated actions.

Minimum Requirement to be Monitored **(WHAT – element of compliance or effectiveness within the document will be monitored)**	**Responsible Individual** **(WHO – is going to monitor this element)**	**Process for Monitoring e.g. Audit** **(HOW – will this element be monitored (method used))**	**Frequency of Monitoring** **(WHEN – will this element be monitored (frequency/ how often))**	**Responsible Individual or Committee/Group for Review of Results** **(WHERE – Which individual/ committee or group will this be reported to, in what format (e.g. verbal, formal report etc.) and by who)**
Significant risks (scoring 15+)	Risk and Assurance Manager	Extract from Datix, included in the Significant Risks Report	Monthly	Risk Committee Risk and Assurance Manager
Reportable risks (scoring 10+)	Divisional General Manager / Corporate Head of Service	Extract from Datix, included in Divisional/Corporate Risk Report	Twice per year	Risk Committee Divisional General Manager / Executive Director
Actions overdue for completion	Risk and Assurance Manager	Extract from Datix, included in the Significant Risks Report	Monthly	Risk Committee Risk and Assurance Manager
Risks overdue for review	Risk and Assurance Manager	Extract from Datix, included in the Significant Risks Report	Monthly	Risk Committee Risk and Assurance Manager
New risks added	Risk and Assurance Manager	Extract from Datix, included in the Significant Risks Report	Monthly	Risk Committee Risk and Assurance Manager
Risks closed	Risk and Assurance Manager	Extract from Datix, included in the Significant Risks Report	Monthly	Risk Committee Risk and Assurance Manager

8.0 TRAINING AND IMPLEMENTATION

Training

In order to ensure that staff possess sufficient awareness of risk management and are competent to identify, assess and manage risk within their working environment, face-to-face Risk Management training is provided to relevant staff as part of a schedule of non-mandatory training sessions.

An e-learning risk management package is also available and face-to-face training is provided on request.

To ensure that this Policy is made available to all staff it is published with its appendices on the Trust intranet alongside other Governance Policies.

The Trust will also maintain a dedicated Risk Management section of its intranet.

This section will be used to provide advice and guidance on risk management, as well as for communicating current messages of corporate importance such as significant areas of risk and successful risk management initiatives.

Important information regarding organisational learning and risk management issues will be communicated whenever appropriate using the Trust's existing internal communication channels.

9.0 IMPACT ASSESSMENTS

Equality Impact Assessment

An Equality Impact Assessment has been undertaken on this Policy and has not indicated that any additional considerations are necessary with regard to differential impacts on those with protected characteristics.

Environmental Impact Assessment

An Environmental Impact Assessment is not required for this Policy as it concerns management activity only.

10.0 EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED SFHFT DOCUMENTS

Evidence Base:
The following sources informed the development of this policy:

- International Framework: Good Governance in the Public Sector *IFAC / CIPFA*
- NHS Foundation Trust Code of Governance (2014) *Monitor*
- Risk Management Standards for NHS Trusts (2013) *NHSLA*
- International Standard for Risk Management: ISO 31000 *International Organization for Standardization*
- A Risk Matrix for Risk Managers (2008) *NPSA*
- BSI Risk Management Code of Practice – BS 31100 *British Standards Institution*
- The Orange Book: Management of Risk – Principles & Concepts *HM Treasury*

There are a number of specialist policy areas within the Trust which involve significant aspects of risk management, and which therefore need to be applied in a way that is consistent with this Policy; these risk specialisms include:

- Patient safety
- Infection prevention & control
- Health & safety
- Fire safety & security
- Information governance
- Digital & information services
- Data quality
- Claims management
- Financial management
- Procurement
- Business continuity management
- Estates management
- Medical device & equipment management
- Programme and project management

Related SFHFT Documents:

- Standing Orders
- Scheme of Delegation

11.0 APPENDICES

Appendix 1	Risk Assessment Matrix
Appendix 2	Risk Assessment Form
Appendix 3	Equality Impact Assessment

Appendix 1 – Risk Scoring Matrix

	Consequence score and descriptor with examples				
Risk type	**1. Very low**	**2. Low**	**3. Moderate**	**4. High**	**5. Very high**
a. Patient harm or **b. Staff harm** or **c. Public harm**	Minimal physical or psychological harm, not requiring any clinical intervention. e.g.: Discomfort.	Minor, short-term injury or illness, requiring non-urgent clinical intervention (e.g. extra observations, minor treatment or first aid). e.g.: Bruise, graze, small laceration, sprain. Grade 1 pressure ulcer. Temporary stress / anxiety. Intolerance to medication.	Significant but not permanent injury or illness, requiring urgent or on-going clinical intervention. e.g.: Substantial laceration / severe sprain / fracture / dislocation / concussion. Sustained stress / anxiety / depression. Grade 2 or 3 pressure ulcer. Healthcare associated infection (HCAI). Noticeable adverse reaction to medication. RIDDOR reportable incident.	Significant long-term or permanent harm, requiring urgent and on-going clinical intervention, or the death of an individual. e.g.: Loss of a limb Permanent disability. Severe, long-term mental illness; Grade 4 pressure ulcer; Long-term HCAI. Retained instruments after surgery. Severe allergic reaction to medication.	Multiple fatal injuries or terminal illnesses. e.g.: Major incident casualties. Multiple missed cancer diagnoses. Outbreak of serious infectious disease.
d. Services	Disruption to peripheral aspects of service affecting one or more services.	Disruption to essential aspects of service affecting one or more services.	Temporary service closure affecting one or more services or disruption to services across multiple divisions.	Extended service closure affecting one or more services or prolonged disruption to services across multiple divisions.	Hospital or site closure.
e. Reputation / regulatory action	Minimal reduction in public, commissioner and regulator confidence. e.g.: Concerns expressed / small number of complaints received.	Minor, short-term reduction in public, commissioner and regulator confidence. e.g.: Recommendations for improvement. Multiple complaints received.	Significant, medium-term reduction in public, commissioner and regulator confidence. e.g.: Improvement / warning notice; Prevention of future death report; Independent review. Adverse local media coverage.	Widespread reduction in public, commissioner and regulator confidence. e.g.: Prohibition notice. HSE/CQC prosecution. Sustained adverse national / social media coverage.	Widespread loss of public, commissioner and regulator confidence. e.g.: Special Administration. Suspension of CQC Registration. Parliamentary intervention. Prosecution – e.g. corporate manslaughter.
f. Finances	Adverse financial impact but not sufficient to affect the achievement annual budgets for any service / department.	Adverse financial impact affecting the ability of one or more services / departments to operate within their budget in the current year.	Adverse financial impact affecting the ability of one or more divisions to achieve their financial control total in the current year. e.g. up to 0.5% of Trust turnover	Adverse financial impact affecting the ability of the organisation to achieve its financial control total in the current year. e.g. over 0.5% up to 1% of Trust turnover	Adverse financial impact affecting the long-term financial sustainability of the organisation. e.g. over 1% of Trust turnover

When assessing likelihood, it is important to take into consideration the controls already in place. The likelihood score is a reflection of how likely it is that the adverse consequence described will occur.

Reference to incident reports; complaints; claims; performance indicators should be made and where possible evidence attached to the risk within the risk register. Reference cannot also be made to sources external to the Trust i.e. learning from other organisations.

Likelihood can be scored by considering:

- Frequency (how many times will the adverse consequence being assessed actually be realised)

Or

- Probability (what is the chance the adverse consequence will occur)

	Likelihood score and descriptor with examples				
	Very unlikely **1**	**Unlikely** **2**	**Possible** **3**	**Somewhat likely** **4**	**Very likely** **5**
Frequency How often might it/does it happen	This will probably never happen/recur	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally or there are a significant number of near misses/ incidents at a lower consequence level	Will probably happen/recur, but it is not necessarily a persisting issue/ circumstances	Will undoubtedly happen/recur, possibly frequently
Probability Will it happen or not?	Less than 1 chance in 1,000 (< 0.1%)	Between 1 chance in 1,000 and 1 in 100 (0.1 - 1%)	Between 1 chance in 100 and 1 in 10 (1-10%)	Between 1 chance in 10 and 1 in 2 (10 - 50%)	Greater than 1 chance in 2 (>50%)

Risk scoring matrix						
Consequence	**5**	**5**	**10**	**15**	**20**	**25**
	4	**4**	**8**	**12**	**16**	**20**
	3	**3**	**6**	**9**	**12**	**15**
	2	**2**	**4**	**6**	**8**	**10**
	1	**1**	**2**	**3**	**4**	**5**
		1	**2**	**3**	**4**	**5**
		Likelihood				

Rating	Very low (1-3)	Low (4-6)	Medium (8-9)	High (10-12)	Significant (15-25)

Appendix 2 - Risk Assessment Form – Risk Register

For advice on completing this Risk Assessment Form please contact the Risk & Assurance Manager – neil.wilkinson4@nhs.net

Please note - for Health & Safety risk assessments please use the relevant form on the Health & Safety intranet site: Health & Safety intranet

For advice contact Rob Dabbs, Head of Health & Safety: Robert.Dabbs@nhs.net – ext 4172.

What is the activity that is being risk assessed?

Completed by: Role: Date completed:

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	

APPENDIX 3 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: Risk Management and Assurance Policy			
New or existing service/policy/procedure: Existing			
Date of Assessment: 5th January 2026			
For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	**a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?**	**b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?**	**c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality**
The area of policy or its implementation being assessed:			
Race and Ethnicity	There are no known equality issues associated with implementation of this policy.	The policy describes business process requirements and as such is neutral with regard to potential inequalities.	None.
Gender	See above.	See above.	None.
Age	See above.	See above.	None.
Religion	See above.	See above.	None.
Disability	See above.	See above.	None.
Sexuality	See above.	See above.	None.
Pregnancy and Maternity	See above.	See above.	None.
Gender Reassignment	See above.	See above.	None.
Marriage and Civil Partnership	See above.	See above.	None.

Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	See above.	See above.	None.

What consultation with protected characteristic groups including patient groups have you carried out?
None. The policy concerns internal business processes and therefore consultation was only carried out with members of the Trust's management teams to whom it is applicable.

What data or information did you use in support of this EqIA?
None. There is no relevant data available in relation to this policy.

As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, comments, concerns, complaints or compliments?
No.

Level of impact

From the information provided above and following the Equality Impact Assessment Guidance Document (click here), please indicate the perceived level of impact:

Low Level of Impact.

For high or medium levels of impact, please forward a copy of this form to the HR Secretaries for inclusion at the next Diversity and Inclusivity meeting.

Name of Responsible Person undertaking this assessment: Neil Wilkinson

Signature:

Date: 5th January 2026