Humber Teaching
NHS Foundation Trust

Risk Management Policy
(N-064)

Version Number:	4.3
Author (name & job title)	Oliver Sims – Corporate Risk and Incident Manager
Executive Lead (name & job title):	Hilary Gledhill, Executive Director of Nursing, Allied Health and Social Care Professionals
Name of approving body:	EMT
Date full policy approved:	23 May 2024
Date Ratified at Trust Board:	29 May 2024
Next Full Review date:	May 2027

Minor amendments made prior to full review date above (see appended document control sheet for details)	
Date approved by Lead Director:	
Date EMT as approving body notified for information:	

Policies should be accessed via the Trust intranet to ensure the current version is used

Contents

1. Introduction

The management of risk is a key factor in achieving the provision of the highest quality care, requiring the identification, management and minimising of activities or events which could result in unnecessary risks to service users, staff and visitors/members of the public.

Risk is the possibility of loss, damage, missed opportunity, injury or failure to achieve objectives or deliver our plans as a result of an uncertain action or event. Risk management is the continuous and critical process that enables the Trust to manage uncertainty (positive or negative) or our exposure to risk.

We achieve this by the identification, assessment, and systematic reduction and effective control of risks that threaten the delivery of safe and effective services. This includes the protection of:

- **People** – including patients, carers, staff, contractors, visitors, and the general public.
- **Finances** – through value for money, reduction of losses and improved financial stability.
- **Reputation** – internally and externally to commissioners, general public, media and the wider NHS.

Risks must be assessed in respect of the combination of the probability of an event happening and the severity of the impact which occurs.

At its simplest risk management is good management practice and should not be seen as an end in itself, but as part of an overall management approach. This policy supports the implementation of the Risk Management Strategy (2021-2024) which provides the overarching framework within which risk is managed by the organization.

2. Policy Statement

The Risk Management Policy outlines the Trusts processes for managing risk and for the provision of assurance in areas of risk. It underpins the Risk Management Strategy through defining how the strategy will be delivered and is supported by procedural guidance on the use of risk registers and the Board Assurance Framework.

3. Purpose

The Trust acknowledges that healthcare provision and the activities associated with caring for patients, employing staff, providing facilities, 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. Most cannot be avoided, but they can in most instances be managed to an acceptable level, enabling the Trust to deliver high quality, safe and effective services.

This policy defines the Trusts approach to risk management and the processes to be followed to ensure risks are identified, captured, the impact understood and managed, and reported to the Trust Board.

4. Scope

This policy does not apply to the process of clinical risk assessment and instead outlines the Trust processes for the management and review of its risk registers.
This policy is a Trust-wide document and applies to all members of staff, either permanent or temporary and to those working within, or for Humber Teaching NHS Foundation Trust. This includes staff on honorary contracts, students and volunteers.

Risk identification is the responsibility of all staff and stakeholders, and staff will be supported in this responsibility with training and guidance provided by the Trust.

5. Risk Management Objectives

This policy supports the delivery of the Trust's Risk Management Strategy and the identified risk management objectives which have been determined from the good practice and development identified from the Trust Risk Management Maturity Assessment. This assessment was undertaken by the Trust Board using the 'Alarm National Model for Risk Management' which centers around seven areas:

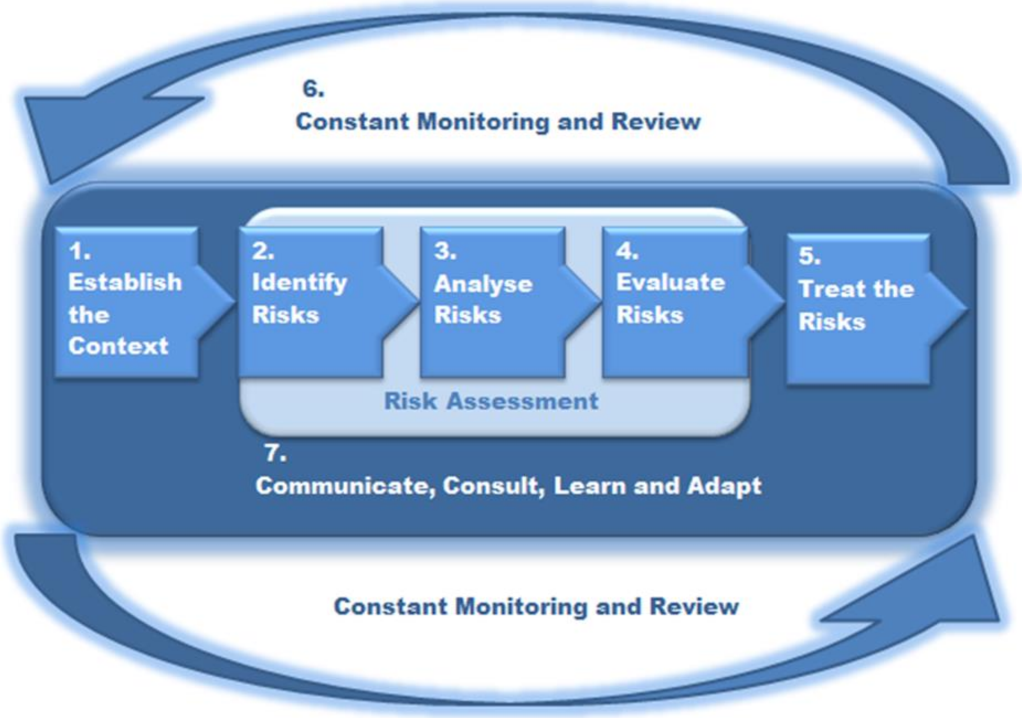
Area	Objective
Risk Leadership	• To demonstrate clear leadership and commitment to risk management, ensuring risk is 'owned' and operating effectively at all levels of the organisation from ward to Board. • Develop and expand the use of risk information to inform decision making and strategy and policy development. • Develop a culture of managed risk-taking.
Strategy and Policy	• Ensure that the risk management strategy and framework reflect the Trust's ambitions for the management of risk, providing structure, direction and guidance, covering the full range of Trust activities.
People	• Ensure appropriate training is delivered at all levels of the organisation to build skills and knowledge to manage risk effectively and implement the risk management framework.
Partnerships, Shared risks and Resources	• Ensure sound governance arrangements are in place with partners, and that risk is well managed across organisational boundaries.
Processes and Tools	• Ensure that a consistent and integrated approach to risk management is embedded in the day-to-day working practices of the organisation at all levels, embracing clinical, non-clinical and corporate risks. • Ensure Committee, groups and teams understand their collective role in identifying, recording, managing, reviewing, escalating and closing risks.
Risk Handling and assurance	• Ensure that the Board and senior management are provided with adequate assurance that risks are being appropriately identified, assessed, and mitigated from ward to Board.
Outcomes and delivery	• Ensure we learn from risk management processes and actions taken across the organisation. • Ensure we identify and utilise performance measures that can demonstrate successful management of risk.

6. Risk Management Process

6.1. Overview

Risk management activities undertaken within the Trust operate at a number of levels: for example, a health or social care professional creating a risk management plan for a service user; corporate planning around the organisational response to a major incident; risk assessment and mitigation for business expansion and development. This strategy and its related procedures serve to set these various risk management activities within a broader corporate framework and to identify consistent processes for risk management across the Trust.

The overall risk management process is shown pictorially below, there being 7 major elements in the process.



Step 1: Establish the context: When we are considering risk we determine the facts, understand the situation and environment, considering both external and internal factors.

Step 2: Identify risk: Identify what, why and how things can arise as the basis for further analysis. Risk can be identified from many sources of information. These are grouped as reactive (e.g. incidents) or proactive (risk assessments), as well as internal (staff consultations) or external (inspections).

Steps 3 through 5: Risk Assessment: these three steps are brought together under the heading of risk assessment as they are undertaken collectively, revisiting steps as required.

Step 3: Analyse risk: Determining the relative importance of individual risks is a key element of the risk management process, enabling risk control priorities to be identified and appropriate action to be taken in response. This is achieved by:

- Assigning a level of '**likelihood**' of a risk event occurring using the likelihood matrix.
- Assigning a level of or '**impact**' or '**consequence**' to the risk event using the consequences matrix.

Step 4: Evaluate risks: Review 'residual' risk level against policy requirements and risk appetite and determine whether treatment is required. Compare estimated levels of 'residual' risk. This enables risks to be ranked so as to identify management priorities.

Step 5: Treatment of risks: Risk treatment involves identifying the range of options for controlling or treating risk, assessing those options, preparing risk treatment plans and implementing them.

Step 6: Constant monitoring and review: Of risks, their controls, assurances, and actions, and of the Risk Management System.

Step 7: Communicate, consult, learn and adapt: Communicate and consult widely, including with external stakeholders as appropriate, at each stage of the risk management process.

6.2. Identifying and Describing Risks

Identification of Risks

The Trust cannot manage its risks effectively unless we know what the risks are. Risk identification is therefore vital to the organisational success of the Trust's risk management process.

Risk is the possibility of loss, damage, missed opportunity, injury or failure to achieve objectives or deliver our plans as a result of an uncertain action or event.

All staff within the Trust can identify risks through the course of their work and their interaction with patients, the public, partner organisations and other key stakeholders.

Risk identification should take place on a continual basis, but particularly where new activities are planned, new legislation or NHS policy requirements are identified, new strategies and plans are developed, or where incidents or near misses have taken place.

The following table indicates where risks may be identified.

External Scrutiny and Inspection	Occurrences	Internal Assessments
External audit reports	Never Events/ Serious Incidents/ Significant Events	Board Assurance Framework
CQC reports/ visits	Incident and near miss reporting	Performance management
Reports from professional bodies	Complaints	Internal audit reports
Health and Safety Executive	Legal claims	Clinical audit programmes
Environmental Health reports	Patient satisfaction measures	Risk Assessments
Monitor reports	Employee satisfaction measures	Networking – use of media reports and information from other Trusts
Coroner's reports.	Sickness and absence records	Fraud & Corruption
NICE Guidance/Guidelines.	Staff turnover	Other self-assessment tools (including self-assessment against CQC standards)
Commissioner feedback	Levels of agency utilisation	Inspections
NHS Improvement oversight	Whistleblowing	Equality Analysis
Healthwatch	Inquests	

(Note – this list is by no means exhaustive)

Proactive risk identification should be carried out throughout the Trust at all levels, for example:

- Strategic objectives are cascaded into Operational Division and Directorate led strategies and service plans, and risks to the achievement of these identified and assessed.
- Multidisciplinary teams delivering clinical services carry out risk identification and assessment of clinical activities as well as identifying and reporting risks, act upon local risk assessments and consider any risks for the Risk Register.
- Risk management specialists e.g. health and safety, security, fire, counter fraud, clinical safety, carry out risk identification specific to their area of expertise.
- Service/department teams identify and assess risks to patients, staff or visitors within the service/department environment.
- Clinical risk assessments are carried out with individual clients/patients using clinical risk assessment tools and plans of care are developed accordingly.
- Project management teams carry out risk assessments throughout projects, maintain project risk registers, and assess at the end of the project any remaining risks as to their suitability for transferring to the relevant Risk Register.

Incident and near miss reporting, whistle blowing, complaints, claims, PALS contacts and the outcomes of external reviews are sources of reactive risk identification.

Defining and Describing Risk

How a risk is defined is an important factor, both to ensure a shared understanding of the risk, and to aid the identification of controls, assurances, and subsequent treatment of the risk.

When describing risks, the Trust defines the:

- Cause of the risk, the current position, issues and underlying causes behind the risk,
- Risk event that could occur; the ‘something uncertain’,
- Impact and consequences to the Trust if the event occurs, and,
- Probability of the risk occurring.

We describe risks in the following ways.

‘As a result of 'an existing condition', 'something uncertain' may occur, which would lead to ‘effect on objectives/impact'.’ or;

There is a risk that….. This is caused by….. And would result in…… leading to an impact upon…….. ‘

6.3. Risk Assessment

Risk Analysis: Determining the relative importance of individual risks is a key element of the risk management process, enabling risk control priorities to be identified and appropriate action to be taken in response. This is achieved by:

- Assigning a level of ‘**likelihood**’ of a risk event occurring using the likelihood matrix.
- Assigning a level of or ‘**impact**’ or ‘**consequence**’ to the risk event using the consequences matrix.
- The assessment is completed using a likelihood matrix (Table 1) and consequence matrix (Table 2). While the likelihood matrix offers an option of frequency or probability, the likelihood matrix offers options based on the type of consequence (impact) that will arise if the risk should occur

Table 1 – Likelihood Table

Likelihood Score	**1**	**2**	**3**	**4**	**5**
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost certain**
Frequency How often might it/does it happen	This will probably never happen/recur Not expected to happen for years	Do not expect it to happen/recur but it is possible it may do so Expected to occur at least annually	Might happen or recur occasionally Expected to occur at least monthly	Will probably happen/recur but it is not a persisting issue Expected to occur at least weekly	Will undoubtedly happen/recur, possibly frequently Expected to occur at least daily
Probability	<1% Unlikely to occur	1-5% Unlikely to occur	6-20% Reasonable chance of occurring	21-50% Likely to occur	>50% More likely to occur than not

Table 2 – Consequence Score

	Consequence score (severity levels) and examples of descriptors				
	1	2	3	4	5
Consequence Type	**Negligible**	**Minor**	**Moderate**	**Severe**	**Catastrophic**
Impact on the safety of patients, staff or public (physical/ psychological harm)	Minimal injury requiring no/minimal intervention or treatment. No time off work	Minor injury or illness, requiring minor intervention Requiring time off work for >3 days Increase in length of hospital stay by 1-3 days	Moderate injury requiring professional intervention Requiring time off work for 4-14 days Increase in length of hospital stay by 4-15 days RIDDOR/agency reportable incident An event which impacts on a small number of patients	Major injury leading to long-term incapacity/disability Requiring time off work for >14 days Increase in length of hospital stay by >15 days Mismanagement of patient care with long-term effects	Incident leading to death Multiple permanent injuries or irreversible health effects An event which impacts on a large number of patients
Quality/ complaints/ audit	Peripheral element of treatment or service suboptimal Informal complaint/inquiry Service delivery is not materially affected.	Overall treatment or service suboptimal Formal complaint (stage 1) / Local resolution Single failure to meet internal standards Minor implications for patient safety if unresolved / Reduced performance rating if unresolved Some inconvenience/ difficulty in operational performance of a particular service area	Treatment or service has significantly reduced effectiveness Formal complaint (stage 2) complaint Local resolution (with potential to go to independent review) Repeated failure to meet internal standards Major patient safety implications if findings are not acted on Operational performance of a particular service area is affected to the extent that revised planning is required to overcome difficulties.	Non-compliance with national standards with significant risk to patients if unresolved Multiple complaints/ independent review Low performance rating Critical report Operational performance of a particular service area is severely affected.	Totally unacceptable level or quality of treatment/service Gross failure of patient safety if findings not acted on Inquest/ombudsman inquiry Gross failure to meet national standards Operational performance is compromised to the extent that the organisation is unable to meet its obligations in core activity areas.
Human resources/ organisational development/ staffing/ competence	Short-term low staffing level that temporarily reduces service quality (< 1 day)	Low staffing level that reduces the service quality	Late delivery of key objective/ service due to lack of staff Unsafe staffing level or competence (>1 day) Low staff morale Poor staff attendance for mandatory/key training	Uncertain delivery of key objective/service due to lack of staff Unsafe staffing level or competence (>5 days) Loss of key staff Very low staff morale No staff attending mandatory/ key training	Non-delivery of key objective/service due to lack of staff Ongoing unsafe staffing levels or competence Loss of several key staff No staff attending mandatory training / key training on an ongoing basis
Statutory duty/ inspections	No or minimal impact or breech of guidance/ statutory duty	Breech of statutory legislation Reduced performance rating if unresolved	Single breech in statutory duty Challenging external recommendations/ improvement notice	Enforcement action Multiple breeches in statutory duty Improvement notices Low performance rating Critical report	Multiple breeches in statutory duty Prosecution Complete systems change required Zero performance rating Severely critical report
Adverse publicity/ reputation	Rumours Potential for public concern	Local media coverage – short-term reduction in public confidence Elements of public expectation not being met	Local media coverage – long-term reduction in public confidence	National media coverage with <3 days service well below reasonable public expectation	National media coverage with >3 days service well below reasonable public expectation. MP concerned (questions in the House) Total loss of public confidence
Business objectives/ projects	Insignificant cost increase/ schedule slippage	<5 per cent over project budget Schedule slippage	5–10 per cent over project budget Schedule slippage late delivery of key target.	Non-compliance with national 10–25 per cent over project budget Schedule slippage Key objectives not met Partial delivery of key targets	Incident leading >25 per cent over project budget Schedule slippage Key objectives not met Non-delivery of key targets.
Finance including claims	Small loss (less that 0.1% of budget) Risk of claim remote	Loss of 0.1–0.25 per cent of budget Claim less than £10,000	Loss of 0.25–0.5 per cent of budget Claim(s) between £10,000 and £100,000	Uncertain delivery of key objective/Loss of 0.5–1.0 per cent of budget Claim(s) between £100,000 and £1 million Purchasers failing to pay on time	Non-delivery of key objective/ Loss of >1 per cent of budget Failure to meet specification/ slippage Loss of contract / payment by results Claim(s) >£1 million
Service/business interruption Environmental impact	Loss/interruption of >1 hour No impact on ability to meet internal and external reporting requirements even though a particular service area is affected. Minimal or no impact on the environment	Loss/interruption of >8 hours Inability to meet a specific reporting requirement. Minor impact on environment	Loss/interruption of >1 day Difficulty in complying with key reporting requirements. Moderate impact on environment	Loss/interruption of >1 week Unable to comply with the majority of reporting requirements. Major impact on environment	Permanent loss of service or facility Unable to access any service user or corporate information. Catastrophic impact on environment

The two numerical assessment scores are then multiplied to give a risk rating and level of risk as shown in table 3.

Table 3 – Risk Scoring and Levels
The Trust's risk assessment matrix is therefore as follows:

			Severity of Impact/ Consequence				
			1	2	3	4	5
			Negligible	Minor	Moderate	Severe	Catastrophic
Likelihood	5	Almost certain	5 Moderate	10 High	15 Significant	20 Significant	25 Significant
	4	Likely	4 Moderate	8 High	12 High	16 Significant	20 Significant
	3	Possible	3 Low	6 Moderate	9 High	12 High	15 Significant
	2	Unlikely	2 Low	4 Moderate	6 Moderate	8 High	10 High
	1	Rare	1 Low	2 Low	3 Low	4 Moderate	5 Moderate

We undertake assessment of risk at three stages:

- **Initial risk** (inherent or gross risk) is an assessment of the risk prior to considering any controls in place.
- **Residual risk** (current risk) is an assessment of the risk after identification of controls, assurances, and gaps in control or assurance, hence reflecting how these controls reduce either the likelihood or impact of the risk.
- **Target risk** is an assessment of the anticipated risk score following the successful implementation of identified actions to create additional controls. This is undertaken where the residual risk score reflects that further controls are needed, and these are identified in the form of actions. The target risk score enables managers to fully understand the impact of the actions to be taken, as well as whether these actions alone will reduce (mitigate) the risk to an acceptable level.

The assessment undertaken is the same at each stage, enabling consistency and demonstration as to how well risks are being managed by current controls.

Within the Trust we undertake this analysis two to three times depending on the risk evaluation results.

Risk Evaluation: Review 'residual' risk level against policy requirements and risk appetite and determine whether treatment is required. Compare estimated levels of 'residual' risk. This enables risks to be ranked so as to identify management priorities.

All risks with a residual score that results in a classification of 'High' or 'Significant' require a supporting action plan that describes the activities and actions being taken to further mitigate the level of risk in an effort to achieve the defined target risk rating or the level of risk that can be tolerated allowing for the risk to be closed.

Residual risks with a level of moderate may be required to have action plans in place to further mitigate the risk. Low residual risks do not usually need any further action and are recorded for the purposes of monitoring but should be reviewed on a monthly basis and escalated where required should the level of risk increase. Should a risk be escalated to a higher current rating, consideration should be given to what further controls are required to mitigate the level of risk, and an associated action plan should be developed.

Although actions should always be taken to reduce risks where this involves measures that are clearly proportionate in relation to the risk, actions should not always be taken just because there is a level of risk. Applying this often requires the use of common sense and judgment, rather than a formal cost-benefit analysis. However, some risks will remain above the minimal level even after being mitigated in this way. Such risks may be deemed acceptable provided:

- The risk is maintained at a level which is both 'as low as reasonably practicable' and acceptably low in absolute terms,
- The risk and the control measures are communicated to staff / management /service users,
- The risk, and control mechanisms, are reviewed regularly,
- It does not exceed the Trust's risk appetite,
- It does not lead the Trust to breach its terms of authorisation.

If a risk requires further mitigation, the scale and urgency of the risk treatment is determined based on the level and immediacy of the risk.

The level of risk the controls are managing is important in considering the type and frequency of assurances required to be fully assured that the systems and process continue to work effectively to mitigate the risk. The Trust will use this information to inform the internal audit and clinical audit plans, as well as management reviews.

6.4. Authority for Managing Risk/ Risk Escalation

Authority for Managing Risk

The responsibility for managing an identified risk rests with the individual who has identified it unless, and until, that risk is accepted by another.

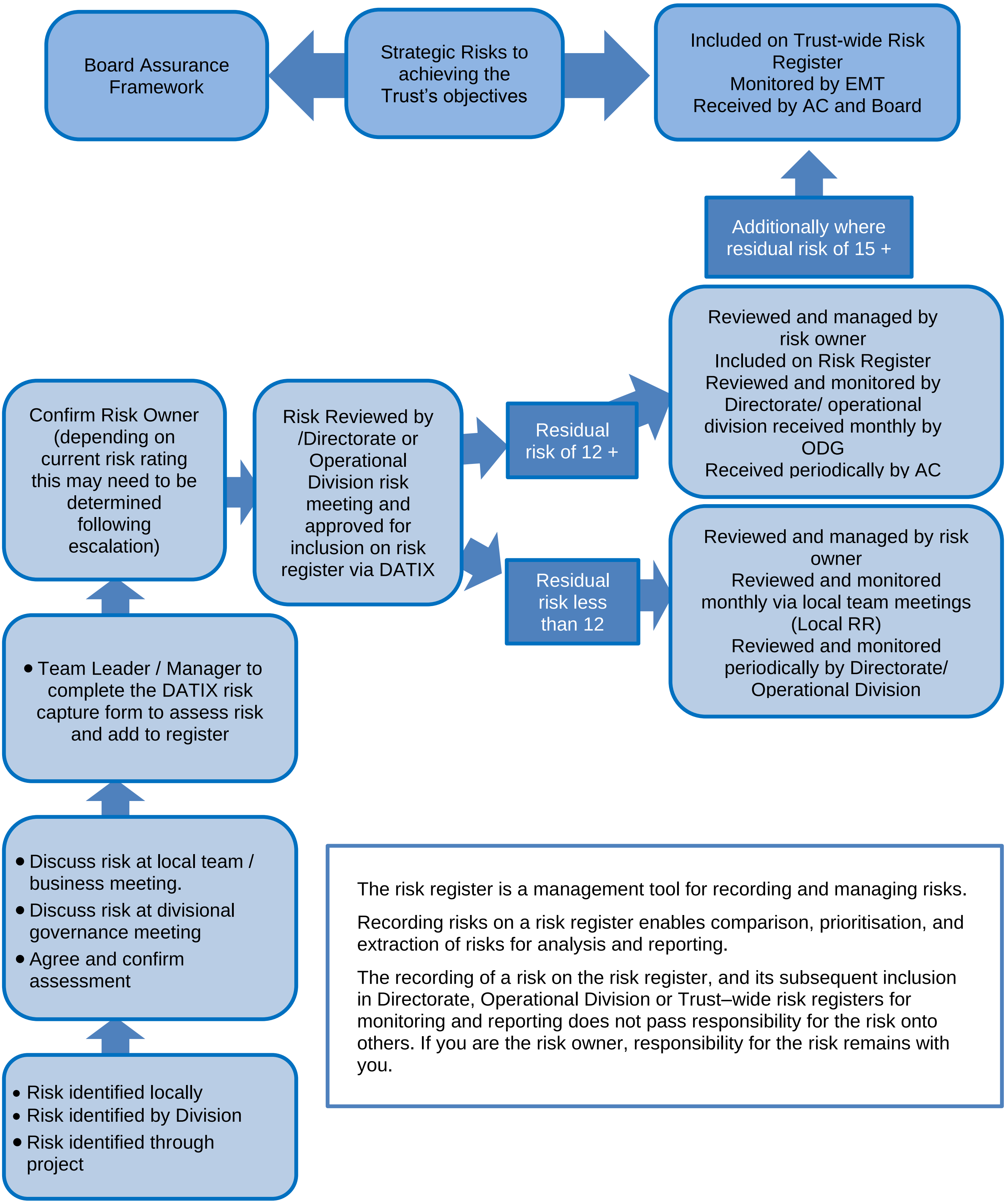
Although a named individual may be responsible for the risk and the implementation of actions to further mitigate the risk, the current controls (mitigations) in place to manage the risk may be the responsibility of all staff involved in the process. For example, a building/ fixtures risk relating to safety may be the responsibility of a member of the estates personnel in terms of taking forward plans for repair; however, processes/procedures put in place to manage and maintain the safety of staff, patients, and visitors within the vicinity, are the responsibility of all staff within the unit.

Risk Escalation

The risks held on the Trust's risk registers are linked to a Directorate or Operational Division, except for the Trusts risks to Strategic Aims.

All risks are escalated/ reviewed based on their residual (current) risk score. All risks within a Operational Division or Directorate form part of the Operational Division or Directorate risk register, and risks will be regularly reviewed at the Operational Division or Directorate Business Meeting, as well being managed and reviewed locally within the Service or Department. All risks with a current rating of 'High' held on the risk registers are also reviewed monthly by the Operational Delivery Group for further assurance regarding the management of these risks.

Adding Risks to the Risk Register & the Risk Escalation Process



Board Assurance Framework

Strategic Risks to achieving the Trust’s objectives

Included on Trust-wide Risk Register
Monitored by EMT
Received by AC and Board

Additionally where residual risk of 15 +

Reviewed and managed by risk owner
Included on Risk Register
Reviewed and monitored by Directorate/ operational division received monthly by ODG
Received periodically by AC

Confirm Risk Owner (depending on current risk rating this may need to be determined following escalation)

Risk Reviewed by /Directorate or Operational Division risk meeting and approved for inclusion on risk register via DATIX

Residual risk of 12 +

Residual risk less than 12

Reviewed and managed by risk owner
Reviewed and monitored monthly via local team meetings (Local RR)
Reviewed and monitored periodically by Directorate/ Operational Division

- Team Leader / Manager to complete the DATIX risk capture form to assess risk and add to register

- Discuss risk at local team / business meeting.
- Discuss risk at divisional governance meeting
- Agree and confirm assessment

- Risk identified locally
- Risk identified by Division
- Risk identified through project

The risk register is a management tool for recording and managing risks.

Recording risks on a risk register enables comparison, prioritisation, and extraction of risks for analysis and reporting.

The recording of a risk on the risk register, and its subsequent inclusion in Directorate, Operational Division or Trust–wide risk registers for monitoring and reporting does not pass responsibility for the risk onto others. If you are the risk owner, responsibility for the risk remains with you.

Find further information on the levels of risk register at section 6.6 Monitoring and Review.

Whenever a risk requires actions that need approval at a senior level, or requires a response that is coordinated with other Operational Division or Directorates, the owner should raise it with their manager, regardless of risk score. Such risks should be escalated to the Operational Division/Directorate business meetings where they can then be reviewed for to agree actions needed.

6.5. Treatment of Risk

Risk treatment involves identifying the range of options for controlling or treating risk, assessing those options, preparing risk treatment plans and implementing them. The options available for the treatment of risks include:

- **Tolerate (accept) the risk** - if, after controls are put in place, the remaining risk is deemed acceptable to the organisation, the risk can be retained. The process for recording and updating risks provides an option to 'accept' the risk, this reflects that although a level of risk remains, even if this is high, the risk is being managed and accepted at the current risk level. This may be the case where the risk is inherent to the service provided, and although all controls are in place to manage and mitigate the risk as it arises, the risk of reoccurrence, and resulting possible outcomes, remains. In such instances assurance should be sought on a regular basis that the key controls remain effective, incidents of occurrence reviewed, and the risk updated to reflect assurances and gaps in assurance.
- Treat the risk
  - **Reduce the likelihood of the risk occurring** – for example using; preventative maintenance, market assessment, relationship management, audit and compliance programmes, supervision, policies and procedures, testing, investment, training of staff, technical controls and quality assurance.
  - **Reduce the consequences of the risk occurring** – for example using; insurance, financial reserves, contingency planning, disaster recovery & business continuity plans, off-site back-up, public relations, emergency procedures and staff training.
- **Transfer the risk** - this involves another party bearing or sharing some part of the risk by the use of contracts, insurance, outsourcing, joint ventures or partnerships.
- **Terminate (avoid) the risk** - decide not to proceed with the activity likely to generate the risk, where this is practical.

The responsibility for managing an identified risk rests with the individual who has identified it unless, and until, that risk is accepted by another.

The accountability for managing risks identified within a directorate rests with the Executive lead, but they may delegate day to day responsibility to an appropriate manager or colleague.

6.6. Monitoring and Review

Risk Registers

The Trust uses a standardised risk register template for recording risks via the DATIX Risk Management System. Risk registers and the capture form for logging risk entries, are held on the DATIX management system which enables risks to be quantified and ranked with the aim of drawing attention to the risks that affect the organisation as a whole, as well as identifying trends and themes. Use of the system also allows for clear tracking of management of risks, allows for monitoring of risk progress and completion of associated actions to further mitigate levels of risk.

All risks entered onto the registers will have a unique identifying number, these being established when a risk is added to a register for the first time. Risk registers at all levels of the Trust should captured via DATIX to ensure a record and therefore an audit trail is maintained of all updates to the register and risks that are closed when appropriate.

Risk Registers are maintained at Directorate and Operational Division level, with local team and department risks added following assessment as department/team meetings. Local service/department risk registers can be extracted from DATIX registers to provide a local register for review at meetings. Updates should be made to all risk register entries on the DATIX system when reviews are undertaken, and this should be completed local by staff from the team / service with access to the risk register on the system.

Structure of Risk Registers

Level 1 - Trust-wide Risk Register

This register contains strategic risks and risks escalated from Directorates and Operational Divisions (Level 2) that are currently significant (15 or more).

Risks from Directorate and Operational Division risk registers (see Level 2 below) will be escalated and included within the Trust-wide risk register based on residual (current) risk level. However, each Director is responsible for identifying significant risks within their business area risk registers that should be escalated to the Trust-wide risk register where there is a requirement for wider control or action as well as assurance as to the management of the risk, regardless of the risk score. The risk is not removed from the Directorate or Operational Division risk register and remains the responsibility of the Directorate or Operational Division Director, with the exception that some actions may be agreed and become the responsibility of (or shared responsibility of) other Directors.

The owner of the Trust-wide risk register is the Chief Executive. The Trust-wide risk register will be collated by the Corporate Risk and Incident Manager and agreed by the Executive Management Team.

Level 2 - Directorate & Operational Division Risk Registers

Each Directorate and Operational Division is required to develop and maintain its own risk register, this is collated from Level 3 risk registers as well as risks identified at Directorate or Operational Division level. These are known as Directorate/ Operational Division risk registers. They will be reviewed through Directorate meetings and informed by both operational and governance related issues. The risks on the registers will be reviewed in line with individual risk and action plan requirements, with a monthly update provided for all risks with a residual rating of 8 and above. It is the responsibility of teams/services to add newly identified risks to the DATIX system and to ensure that the entries are maintained on the system.

The Corporate Risk and Incident Manager should be notified of any suggested escalation/ de-escalation to or from the Trust-wide risk register and will prepare the Trust-wide risk register with inclusions/ removals following agreement by the Executive Management Team. These registers will be scrutinised for consistency and quality and their efficacy considered as part of the work plan of the Corporate Risk and Incident Manager, being reported to the Audit Committee.

All risks held on a Directorate or Operational Division risk register should be subject to monthly review to ensure that the mitigations are appropriate and that the level of risk has not changed.

Level 3 - Local Risk Registers

All local risks are added to the Operational Division or Directorate register, however the local risks are managed and updated at a local level, i.e., service/ departmental and the Operational Division or Directorate register can be filtered, or risks extracted from the DATIX system for the team/service, to show a ‘local’ register. Risks should only be managed locally and held on local risk registers where their residual risk rating is less than 12 (High Risk). It is the responsibility of teams/services to add newly identified risks to the DATIX system and to ensure that the entries are maintained on the system.

Responsibility for managing risk and implementing action plans will in most instances remain the responsibility of the lead within the team or department. Inclusion on the Directorate or Operational Division risk register may mean that decisions relating to actions required may be made above team or department level, however this does not mean that the responsibility for the management of the risk changes.

All risks held on local risk registers should be reviewed by the team / service and updated monthly to ensure that the mitigations are appropriate and that the level of risk has not changed. If upon review it is identified that the risk rating has increased to 12 or above. Then the escalation processes described above should be followed. The Corporate Risk and Incident Manager should be contacted if any assistance or guidance regarding risk escalation is required.

Project Risk Registers

Project risk registers are developed to help manage the risks associated with approved projects or initiatives. Project risk registers will have an Executive Lead and risks will be escalated to the Directorate/ Operational Division risk registers as appropriate in line with the agreed protocol. High/ Significant risks identified through the project risk management process will be identified for consideration of the Executive Management Team (EMT) to highlight any potential issues that may impact project delivery.

The Corporate Risk and Incident Manager will support with the development of the individual project risk register upon request and should be notified on any risks identified so that the appropriate escalation process can be followed.

Other Risk Register Extracts

Other risk listings may be extracted and used for reporting and monitoring across the Trust, for example, operations, mental health legislation, themes and cross-cutting trends.

Reviewing Risks

Operational Division and Directorates are to ensure that the risk register is reviewed and updated monthly and that the risk register entries held on the DATIX system are updated to reflect the current risk position.

The risk register is considered ‘live’, being under constant review and management. As such there should be regular monitoring and review of risks, their controls, assurances, and actions, by:

- Reviewing the risk description – does this reflect the current situation and potential/actual impact of the risk occurring? If the description requires significant change then the original risk should be closed and a new risk added.
- Reviewing controls – are these up to date and working effectively? Are there any additional controls to be added?
- Reviewing the assessment scoring – has the impact/ likelihood changed, are more actions required to mitigate against the risk?
- Reviewing actions – are they now complete? If not yet due for completion is their assurance that they are on track? Are further actions required?

The ‘progress’ field on the DATIX risk review form should be used to reflect changes made in the current month, such as controls added, gaps identified, assurances received, escalation or reduction in current risk score, and an update on action progress. Where actions are not due to be completed, there should be an indication as to whether the action is still on track.

Local Services and Departmental risk registers should be reviewed at team meetings during the month, to ensure agreement of the status of all risks, to enable the updates to be available to Operational Division and Directorate business meetings.

Operational Division and Directorate risk registers should be reviewed at business meetings monthly, to ensure agreement of the current status of all risks and identify any risks for escalation/ de-escalation to/from the Trust-wide risk register via Operational Delivery Group (ODG) and Executive Management Team (EMT).

It is the responsibility of teams/services to ensure that the risk register entries are maintained on the DATIX system. Compliance around the monthly review of risks is monitored through the risk management reporting arrangements to the Operational Delivery Group and is also considered as part of the annual review of risk management and supporting report delivered to the Trust's Audit Committee.

Risk Management System
Monitoring and review of the wider risk management system is required to ensure it is fit for purpose.

The Trust's arrangements for risk management were evaluated against the 'Alarm National Model for Risk Management', from which areas for development were identified and priorities determined.

Cyclical review of Operational Division and Directorate Risk Registers is be undertaken by the Corporate Risk and Incident Manager and reported to the Audit Committee and Trust Board, to ensure that appropriate risk registers are being maintained, risks are being effectively captured and assessed, scoring is appropriate and consistent, appropriate mitigating actions are being taken, and risks escalated/ de-escalated in line with Trust policy.

The Risk Management Strategy, Policy and related guidance and documentation will be reviewed and updated annually considering the assessment, as well as any changes to external and internal factors.

Review and Management of Risk Registers
Risk registers are reviewed and managed as close to the risk as possible, and as such, local department, service or unit risks are to be reviewed and managed at a local level by the team involved in local management meetings.

Some risks will be identified either at, or more appropriately managed at, a Directorate or Operational Division level, and will be reviewed in Directorate or Operation Division Business Meetings, along with local risks. This is to ensure that the Directorate or Operational Division Management team are fully conversant with risks across their directorate or Operational Division, enabling them to gain assurance that risks are being appropriately managed, as well as identifying where wider support may be required. Local governance processes will identify the arrangements in place within each Directorate or Operational Division.
Risks with significant or high residual risk scores may require wider support across Operational Divisions and Directorates, and as such can be escalated to the Executive Management Team for further action. New and revised risks with residual risk scores of 15 or more will be reviewed by the Executive Management Team.

Risks with a residual score of 15 or more (significant risks) will form part of the Trust-wide risk register and be reported to the Trust Board. The Trust-wide register is also received by the Audit Committee (AC) on a quarterly basis. Audit Committee (AC) will also receive registers from across the Trust, whether Directorate or Operational Division on quarterly basis, for review as part of a rolling programme.

6.7. Communicate and Learn

Communicate and consult widely, including with external stakeholders as appropriate, at each stage of the risk management process. Risks may emerge as a result of partnership/ joint working crossing organisational boundaries. In such cases it is important that all organisations involved are aware of the risk and understand and accept responsibility for controls and actions.

To ensure learning and appropriate adaptation occurs in order to minimise recurrence of risks across the organisation, cross Directorate and Operational Division analysis will be undertaken. This will enable similar and cross cutting risks to be grouped and shared, enabling learning and adaptation of controls or actions.

7. Adding risks to the Risk Register

Where risks are identified, these should be communicated to line managers who should discuss the risk at the next team/ management meeting, and where it is agreed the risk should be added to the risk register, a risk assessment should be undertaken, and full details of the risk documented via the Risk Capture Form held on the DATIX system.

8. Accountability and Responsibility for Risk

The responsibility for managing an identified risk rests with the individual who has identified it unless, and until, that risk is accepted by another.

Although a named individual may be responsible for the risk, the mitigations in place to manage the risk are the responsibility of all staff. For example, a building/ fixtures risk relating to safety may be the responsibility of a member of the estates personnel in terms of taking forward plans for repair; however processes/procedures put in place to manage and maintain the safety of staff, patients and visitors within the vicinity, are the responsibility of all staff within the unit.

The accountability for managing risks identified within a Directorate rests with the Executive Lead, and within Operational Divisions, the Chief Operating Officer but they may delegate day to day responsibility to an appropriate manager or colleague.

9. Board Assurance Framework

All NHS Trusts are required to use a Board Assurance Framework, as this has been proven good practice for many years in both healthcare and a range of other high-risk organisations. It is a “live” document that changes over time, and it picks up all the controls that we have in place to manage, minimise the principal risks we’ve identified and points towards concise and comprehensive evidence that the controls are working.

The Board Assurance Framework documents the overall level of risk to the achievement of the Trust’s strategic objectives, bringing together the assurances that effective controls are in place and actions are being completed. The required assurances reflected in the document also inform the Board and Committee agendas, ensuring that key assurances are provided to the Board in a timely manner.

The Board Assurance Framework is updated on a quarterly basis and led by the Trust Executive Directors who will update their assigned sections of the BAF with support from the Corporate Risk and Incident Manager. A quarterly review will then be undertaken by the Executive Management Team collectively to ensure that the strategic risks are appropriately recorded and managed.

Each of the Trust's strategic goals and the associated section of the Board Assurance Framework have an assigned board sub-committee, and the relevant sections of the BAF document are reviewed at committee meeting to provided further assurance around the management of risks. This review will take place on a quarterly basis ahead of the final agreed version of the BAF being presented to Trust Board. This provides an opportunity for the assuring committee to review the content of the BAF for the quarters and offer any amendments / additions ahead of the final version for the quarter being produced.

10. Emergency Preparedness, Resilience and Response (EPRR) Risks

Key risks facing the organisation regarding emergency preparedness, resilience and response are identified and captured under the Operations directorate risk register and reviewed on a quarterly basis ~~at~~ by the Trust's Emergency Preparedness, Resilience and Response (EPRR) team taking into account any new or emerging risks highlighted by the National, Local or Community Risk Registers.

Risks will be captured where threat or hazards are identified which may affect the ability of the Trust to deliver its functions. Actions to mitigate the assessed risks where required are agreed at the meeting and form part of the Trust's EPRR work programme. Progress against the actions and the current level of risk posed is regularly monitored.

A monthly report to the Trust Operational Delivery Group details the current open EPRR risks facing the Trust, allowing for review of any current issues being faced and monitoring of identified mitigations, as well as further areas of action required. The report also highlights any new or closed risks within the reporting period and supports with the escalation of any significant risks within the Trust.

Quarterly risk management reports to Trust Board include the total number of EPRR risks as well as a breakdown of risk ratings. Should any EPRR risk be graded at a current rating of 15+ (significant risk) it would be escalated to the Executive Management Team for review and considered for inclusion in the organisations' Trust-wide risk register. Identified EPRR risks will also be considered for inclusion on the Trust's Board Assurance Framework if they present significant risk to the achievement of one of the organisations strategic goals.

11. Roles and Responsibilities

Role	Responsibility
Chief Executive (CE)	Accountable for having effective risk management systems and internal controls in place and for achieving statutory requirements. The Chief Executive has delegated overall duty to ensure risk management is discharged appropriately to the Director of Nursing.
Director of Nursing	Has overall duty to ensure risk management is discharged appropriately and has the overall responsibility for the implementation of the strategy.
Executive Directors and Senior Operational / Corporate Managers	Responsible for identifying, communicating and managing the risks associated with their portfolios in accordance with the framework set out in this strategy. They are responsible for understanding the approach towards risk management of all key clients, contractors, suppliers and partners and mitigate where necessary, where gaps are found. They are responsible

Role	Responsibility
	for identifying risks that should be escalated to and from the Trust-wide Risk Register.
Non-Executive Board Members	Responsible for challenging and seeking assurance that integrated systems are in place within the organisations.
Specialist Managers / Leads	Responsible for ensuring all risks within their specialist area are assessed and managed.
Corporate Risk and Compliance Manager	Responsible for the development and implementation of the Risk Management Strategy and framework, and for leading and coordinating risk management across the Trust.
All employees and contractors	Expected to be familiar with the Trust's approach to risk management, take a risk-managed approach to their own work and take responsibility for the management of the risks they own.

Management of risk is a fundamental duty of all staff whatever their grade or role. All staff must follow the Trust policy and procedures which explain how this duty is to be undertaken and attend any relevant training provided by the Trust. In particular, all staff must ensure that identified risks are dealt with swiftly and effectively, and reported to their immediate line manager, so that further action may be taken where necessary.

12. Risk Management Governance – Structural Arrangements

Each Board Committee and its sub-groups has a collective responsibility to ensure effective risk management to ensure good governance as they discharge their duties, and this is reflected in their respective terms of reference. Through their work plans they will contribute towards reducing the organisation's exposure to risk. Risks identified by Committees and reporting groups will be communicated and recorded on the appropriate directorate / divisional risk register and subject to overview, monitoring and intervention by the Corporate Risk and Incident Manager, providing assurance to the Audit Committee (AC) and Trust Board.

Committee / Forum	Responsibility
Trust Board	Has overarching responsibility for risk management throughout the Trust and currently considers the Trust-wide Risk Register and Board Assurance Framework four times a year. It considers the strategic and high-level Trust-wide operational risks facing the Trust as part of its routine business to satisfy itself collectively that risks are being managed appropriately. The Trust Board continuously strives to strengthen the culture of risk management throughout the organisation.
Audit Committee (AC)	Board Committee with overarching responsibility for risk. The role of the Committee is to scrutinise and review the Trust's systems of governance, risk management, and internal control. It seeks regular assurance on the Trust's risk management arrangements to enable it to review the organisation's approach to risk management as well as reviewing the Trust-wide risk register and Board Assurance Framework regularly. The Committee reviews the adequacy of all risk and control related disclosure statements (in particular the Annual Governance Statement), together with any accompanying Head of Internal Audit statement, External Auditor opinion or other appropriate independent assurances. On occasion it will commission internal or external auditors to review and report

Committee / Forum	Responsibility
	on aspects of risk management or on the management of significant risks.
Finance and Investment Committee (FIC)	Board Committee with overarching responsibility for oversight of the Trust's Finances and whose remit it is to conduct independent and objective review and oversight of the Trust's trading and commercial investment activities on behalf of the Board, and to ensure compliance with Investment Policy and Strategic Objectives. The role of the Committee is to scrutinise and review the Trust's financial position and activity. It seeks regular assurance on the Trust's risk management arrangements specifically related to finance risks and is responsible for one section of the Board Assurance Framework, which it also reviews as a standing agenda item at each meeting.
Quality Committee (QC)	Board Committee with overarching responsibility for oversight of the Trust's quality and improvement agenda. The role of the Committee is to scrutinise the Trust's quality and improvement work programmes seeking assurance on all related areas covering the Trust's clinical risk management arrangements. This work includes CQC compliance, service improvements and redesign linked to quality improvement, research and clinical governance. The Quality Committee also reviews the quality-related risks held across the Trust's risk register and the relevant sections of the Board Assurance Framework.
Workforce and Organisational Development Committee (WFOD)	Board Committee with overarching responsibility for oversight of the Trusts' workforce and organisational development agenda. The committee scrutinises the Trust's workforce-related metrics and seeks regular assurance regarding the Trust's risk management arrangements specifically related to workforce. The committee is also responsible for the relevant section of the Board Assurance Framework.
Mental Health Legislation Committee (MHL)	Board Committee whose remit it is to provide strategic leadership pertaining to the Mental Health Act, the Mental Capacity Act and their respective Codes of Practice and other mental health related legislation, as well as to monitor, provide challenge and seek assurance of compliance with external standards relating to Mental Health Legislation and approve and review Mental Health Legislation polices and protocols. The committee also regularly reviews the Trust's Board Assurance Framework as well key risks linked to mental health related legislation.
Executive Management Team (EMT)	Involves all Executive Directors and is chaired by the Chief Executive. The Executive Management Team provides the leadership for risk management across the Trust, considering and approving the development of systems and processes, as well as championing risk management within their areas of responsibility. This Group is the lead for managing the Trust-wide Risk Register, monitoring the management of risk. They consider and accept new items on to the Trust-wide Risk Register, reviewing and revising risk entries on a regular basis, as well as the approval/removal of any risks from the Register at the request of the Corporate Risk and Incident Manager.

Committee / Forum	Responsibility
Operational Delivery Group (ODG)	Chaired by the Chief Operating Officer considers the operational risk registers, as well as thematic risks from directorate risk registers. This group is responsible for ensuring that risk assessments are consistent, timely and appropriate actions to manage and mitigate risks are being taken, and that similar risks across the Trust are identified, cross-referenced and considered as a whole.
Directorate Business meetings	Meeting held within each Directorate that is responsible for ensuring that appropriate risk registers are in place, risks are being effectively captured and appropriate mitigating actions are being taken. They are also responsible for highlighting risks for escalation/ de-escalation, based on the current risk score and perceived business impact for the Trust, to/from the Trust-wide risk register via the Executive Management Team.
Operational Business meetings	Held within each business division and are responsible for ensuring that appropriate risk registers are in place, risks are being effectively captured and appropriate mitigating actions are being taken. They are also responsible for highlighting risks for escalation/ de-escalation, based on the current risk score and perceived business impact for the Trust, to/from the Trust-wide risk register via the Executive Management Team.
Quality and Patient Safety Group (QPAS)	Accountable to the Quality Committee. It oversees and coordinates all aspects of quality improvement (patient experience/patient safety & clinical effectiveness), assurance and clinical governance activity and delivery. The group has responsibility to escalate any issues which may have a potential impact on the delivery of the organisational objectives to the Executive Management Team.
Clinical Risk Management Group (CRMG)	Sub-group feeding into QPAS. Has responsibility for ensuring clinical risk management systems, processes and related clinical risk management strategies and policies are regularly reviewed and implemented Trust-wide. They ensure systems and processes are developed and maintained to enable Trust-wide monitoring and review of all clinical risks to ensure appropriate investigation, and maximisation of learning from incidents.
Health and Safety Group	Receives updates from multiple infrastructure, safety and compliance related subgroups, ensuring that strategic decisions are made and appropriate action taken to resolve, mitigate or appropriately escalate issues and risks. It also feeds into the CPB, CRMG, and EMT.
Emergency Preparedness Resilience and Response (EPRR)	Sub- group reporting to ODG on the delivery of the objectives of the sub-group including the identification, management and reporting of EPRR risks.
Capital Programme Board	Reports to EMT following the assessment and prioritising of capital applications based on underlying risk.

13. Training

Guidance on populating risk registers and managing risks is available to all staff via the Trust intranet. Risk Management training is open to all Trust staff monthly and is delivered by the Corporate Risk and Incident Manager. Bespoke training for teams / services is also provided upon request to ensure that the training needs in relation to risk management are met across the Trust. Risk management is also introduced to all staff as part of the Trust's induction training.

All staff employed by the Trust, are required to attend the mandatory and statutory training that is relevant to their role and to ensure they meet their own continuous professional development requirements.

14. Monitoring

The Trust's arrangements for risk management are evaluated annually against the 'Alarm National Model for Risk Management', from which areas for further development will be identified. These are included the work plan for the coming year, against which progress will be measured and reported regularly to the Executive Management Team, Audit Committee and the Trust Board. The annual review will be undertaken in Quarter 1 2024/2025 for the Trust's risk management processes through 2023/24.

The outcome of the annual review of the Trust's arrangements for risk management, in particular risk registers, will be considered by the Audit Committee, and the Committee will report to the Board on its findings of its annual risk review as a covering statement to the annual assurance report.

Cyclical review of Operational Division and Directorate Risk Registers are undertaken by the Audit Committee (AC) to ensure that appropriate risk registers are being maintained, risks are being effectively captured and assessed, scoring is appropriate and consistent, appropriate mitigating actions are being taken, and risks escalated/ de-escalated in line with Trust policy. The Risk Management Strategy, Policy and related guidance and documentation will be reviewed and updated annually considering the assessment, as well as any changes to external and internal factors.

15. Communication

The Risk Management Strategy and supporting policies and guidance will be made available to all staff via the Trust Intranet.

The Risk Management Strategy will be made available to stakeholders and the public via publication on the Trust Internet.

16. Related Documents

Risk Management is reflected in many Trust Policies, as well as interlinking to all Trust strategies and policies. The following documents directly support this policy:

- Risk Management Strategy 2021-2024
- Risk Management guidance documents (via **Trust Intranet**)

Links to these documents and specific areas of risk management and related policies are available on the **Trust's Risk Management intranet page**, along with links to additional guidance and information.

17. Definitions

Board Assurance Framework	A method for presenting effective and focused assurances over the key risks to meeting strategic objectives.
Likelihood	Used as a general description of probability or frequency.
Probability	The likelihood of a specified event or outcome occurring. This is measured by the ratio of specific events or outcomes to the total number of possible events or outcomes. Probability is expressed along a scale ranging from 'rare' to 'almost certain'.
Risk	Defined as uncertainty/ possibility of loss, damage, missed opportunity, injury or failure to achieve objectives or deliver our plans as a result of an uncertain action or event.
Risk Appetite -	Statement of intent from the organisation about the level risk it is prepared to accept, tolerate, or be exposed to at any point in time.
Risk Assessment	The evaluation of risk with regard to the impact should the risk be realised, and the likelihood of the risk being realised.
Risk Identification	This is the process of determining what, where, when, why and how something could happen.
Risk Management	The systematic identification of risk within a system or process and the implementation of actions to minimise harm arising. A key aspect of risk management is learning from events, errors, or near misses in order to reduce the risk of them recurring.
Risk Management Strategy	The overall organisational approach to risk management as defined by the Trust Board, which is documented and easily available throughout the organisation.
Risk Maturity	Overall quality and embeddedness of the risk management arrangements.
Risk Mitigation	The action that can be taken to reduce either the probability or impact of a risk.
Risk Reduction	Actions taken to lessen the *likelihood*, negative *consequences* or both associated with *risk*.
Risk Register	A tool for recording identified risks, the results of their analysis and evaluation, and monitoring actions and plans against them. The Risk Register is an important component of the organisation's risk management framework.
Risk Treatment	Process of selection and implementation of measures to modify risk.

18. Equality and Diversity

An **Equality and Diversity Impact Assessment** has been carried out on this document using the Trust approved EIA.

Appendix 1 - Document Control Sheet:

Document Type	Policy		
Document Purpose	This policy defines the Trusts approach to risk management and the processes to be followed to ensure risks are identified, captured, the impact understood and managed, and reported to the Trust Board.		
Consultation/ Peer Review:	Date:	Group / Individual	
list in right hand columns consultation groups and dates -	QPaS		
Approving Body:	EMT	Date of Approval:	23 May 2024
Ratified at:	Trust Board	Date of Ratification:	29 May 2024
Training Needs Analysis: *(please indicate training required and the timescale for providing assurance to the approving committee that this has been delivered)*		Financial Resource Impact	
Equality Impact Assessment undertaken?	Yes [/]	No [ ]	N/A [ ] Rationale:
Publication and Dissemination	Intranet [/]	Internet [ ]	Staff Email [ ]
Master version held by:	Author [ ]	HealthAssure [/]	
Implementation:	*Describe implementation plans below - to be delivered by the Author:*		
	• • •		
Monitoring and Compliance:			

Document Change History:			
Version Number / Name of procedural document this supersedes	*Type of Change i.e. Review / Legislation*	*Date*	*Details of Change and approving group or Executive Lead (if done outside of the formal revision process)*
3.0	*Review*	*Nov-19*	*Reviewed and updated Approved at EMT 27-Nov-19 with ratification at Trust Board Nov-19*
4.0	*Review*	*Jan-21*	*Reviewed and approved at QPaS 21-Jan-21. Agreed should have annual review on policy Changes include -link to Risk Management strategy -updates regarding divisional risk registers -monitoring of mortality review of risk through ODG Update to structural governance – structural arrangement Ratified by Trust Board January 2021s*
4.1	*Review*	*Jan-22*	*Reviewed with minor changes Approved at QPaS 27 January 2022*
4.2	*Review*	*Mar-24*	*Full review, with minor amends made. Approved at EMT (11 March 2024) and ratified at Board (27 March 2024).*
4.3	*Review*	*May-24*	*Review of new EPRR risk section. Approved at EMT (23 May 2024) and ratified at Board (29 May 2024).*

Appendix 2 - Equality Impact Assessment (EIA) Toolkit

For strategies, policies, procedures, processes, guidelines, protocols, tenders, services

1. Document or Process or Service Name: **Risk Management Policy**
2. EIA Reviewer (name, job title, base and contact details): **Oliver Sims, Corporate Risk and Incident Manager**
3. Is it a Policy, Strategy, Procedure, Process, Tender, Service or Other? **Policy**

Main Aims of the Document, Process or Service To set out the requirements that must be met for approval, ratification and dissemination of all Humber Teaching FT policies.
Please indicate in the table that follows whether the document or process has the potential to impact adversely, intentionally or unwittingly on the equality target groups contained in the pro forma

Equality Target Group Age Disability Sex Marriage/Civil Partnership Pregnancy/Maternity Race Religion/Belief Sexual Orientation Gender re-assignment	Is the document or process likely to have a potential or actual differential impact with regards to the equality target groups listed? **Equality Impact Score** Low = Little or No evidence or concern (Green) Medium = some evidence or concern(Amber) High = significant evidence or concern (Red)	How have you arrived at the equality impact score? 1. who have you consulted with 2. what have they said 3. what information or data have you used 4. where are the gaps in your analysis 5. how will your document/process or service promote equality and diversity good practice

Equality Target Group	Definitions	Equality Impact Score	Evidence to support Equality Impact Score
Age	Including specific ages and age groups: Older people, Young people, Children, Early years	Low	No evidence potential or actual differential impact or concern. Policy is applicable to all Trust staff.
Disability	Where the impairment has a substantial and long term adverse effect on the ability of the person to carry out their day to day activities: Sensory, Physical, Learning, Mental Health (and including cancer, HIV, multiple sclerosis)	Low	No evidence potential or actual differential impact or concern. Policy is applicable to all Trust staff.
Sex	Men/Male, Women/Female	Low	No evidence potential or actual differential impact or concern. Policy is applicable to all Trust staff.
Married / Civil Partnership		Low	No evidence potential or actual differential impact or concern. Policy is applicable to all Trust staff.
Pregnancy / Maternity		Low	No evidence potential or actual differential impact or concern. Policy is applicable to all Trust staff.
Race	Colour, Nationality, Ethnic/national origins	Low	No evidence potential or actual differential impact or concern. Policy is applicable to all Trust staff.
Religion or Belief	All Religions Including lack of religion or belief and where belief includes any religious or philosophical belief	Low	No evidence potential or actual differential impact or concern. Policy is applicable to all Trust staff.
Sexual Orientation	Lesbian, Gay Men, Bisexual	Low	No evidence potential or actual differential impact or concern. Policy is applicable to all Trust staff.
Gender Re-assignment	Where people are proposing to undergo, or have undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attribute of sex	Low	No evidence potential or actual differential impact or concern. Policy is applicable to all Trust staff.

Summary

Please describe the main points/actions arising from your assessment that supports your decision above
The Risk Management policy impacts on a process rather than individuals and is to be applied consistently to all risk management across the Trust. When individuals carry out risk assessments on situations/services and put in place mitigation, they should apply a situation/service specific equality impact assessment.

EIA Reviewer	Oliver Sims		
Date completed;	March 2024	Signature	O. Sims