University Hospitals of Derby and Burton NHS Foundation Trust

TRUST POLICY FOR THE MANAGEMENT OF RISK

Reference Number POL-CLIN/4186/23	**Version: 1.1**		**Status: Final**	**Author:** Jo Ralph **Job Title:** Head of Clinical Governance and Risk
Version / Amendment History	**Version**	**Date**	**Author**	**Reason**
	1	April 2023	Jo Ralph	New Document
	1.1	August 2023	Jo Ralph	Separation of appendices and amendment to risk descriptors
Intended Recipients: All Trust Staff				
Training and Dissemination: All staff at local induction and compulsory updates for band 6 and above through the Trust Mandatory training				
To be read in conjunction with: Trust policies related to incident management and learning, Health & Safety and procedure specific risk assessment & management.				
In consultation with and Date: Risk Management Steering Group, Trust Delivery Group, Audit Committee, Trust Board Risk Management Steering Group on 25 April 2023				
EIRA stage One Completed Yes stage Two Completed No - Not Applicable				
Approving Body and Date Approved	Trust Delivery Group - 26 June 2023 **Minor amendments approved by Executive Lead 01.09.2023**			
Date of Issue	September 2023			
Review Date and Frequency	May 2026 and every then three years			
Contact for Review	Corporate Nursing			
Executive Lead Signature	 Garry Marsh, Executive Chief Nurse			

CONTENTS

TRUST POLICY FOR THE MANAGEMENT OF RISK

1. INTRODUCTION

The purpose of the Trust Policy for the Management of Risk is to communicate why and how risk management will be implemented throughout the Trust to support the realisation of its strategic priorities.

The Trust is committed to establishing a transparent risk management culture and process where effective management of risk is an integral part of day-to-day management and delivery of healthcare.

Everyone working for and with University Hospitals of Derby and Burton NHS Foundation Trust (UDHB) will take a proactive approach in the management of risk and ensure risks are identified, assessed, controlled and when necessary, escalated in line with this policy.

The Board is committed to establishing an environment where staff feel able and are supported to identify risks. We expect and encourage staff to do this and in return are committed to actively respond. In so doing we aim to improve services for patients and the wider community and the working lives of our people.

2. PURPOSE AND OUTCOMES

This document sets out the University Hospitals of Derby and Burton NHS Foundation Trust's (hereafter referred to as "the Trust") Policy to manage risks arising from activities including governance (incorporating information governance and research governance), finance and mandatory services, clinical, emergency preparedness resilience and response, human resource, safety, environmental, service development and business.

The Trust aims to be pro-active in its approach to the management of risk and, through its strategic approach and the processes identified within this document, will endeavor to identify, control and, where possible, eliminate risk before incidents of actual loss or harm occur. Effective risk management requires a culture where all staff engage in reducing risks and improving quality and safety. Risk management is a responsibility for all members of staff and should form part of objective setting in every business and management planning cycle and of every service development.

This document provides the framework from which the Trust will implement and embed its ethos for a consistent and robust identification and management of opportunities and risks within the organisation, supporting openness, challenge, innovation and excellence in the achievement of its objectives.

3. KEY INDIVIDUAL RESPONSIBILITIES

All Staff are expected to:

- Be aware of the principles for the management of risk
- Follow the risk management systems and processes
- Adopt the appropriate practices to mitigate risk
- Follow the risk and incident reporting procedures
- To participate in induction and all relevant mandatory training as defined by the Trust

policies
- Provide safe and high-quality patient care

All staff - are encouraged to use risk management processes as a mechanism to highlight areas they believe need to be improved. Where staff feel that raising risks may compromise them or may not be effective, they will be aware and encouraged to follow the 'Freedom to Speak Up' Policy incorporating guidance on raising concerns.

Risk Handler - is responsible for the day-to-day management of the risk(s) assigned to them. It is the responsibility of the risk handler to keep the risk record updated including details of risk reviews, dates of upcoming reviews, re-evaluation of the current risk scoring and associated actions. The Risk Handler should be familiar with the risks on their workload and their associated actions and should they face any difficulties with managing the risk, be familiar with the routes of escalation and how to seek assistance. If the 'current score' of risk increases to 15 and/or above, the risk will need to be agreed at the Risk and Compliance Group meeting prior to the risk 'going live' and the status on Datix changing to 'Live Risk'

Risk Manager/Owner - is responsible for the overall management of the risk(s) assigned to them. The Risk Owner should be familiar with the risks on their workload and their associated actions and should they face any difficulties with managing the risk, be familiar with the routes of escalation and how to seek assistance. If the 'current score' of risk increases to 15 and/or above, the risk will need to be agreed at the Risk and Compliance Group meeting prior to the risk 'going live' and the status on Datix changing to 'Live Risk'

Action Owner - are responsible for the management of action(s) assigned to them, to assist with mitigating a particular risk. It is the responsibility of the action owner, to ensure that the action linked to the risk is up to date, and progress is being made to close this action down. Action owners should maintain regular contact with the risk handler, to provide a progress update, and assurance that the action is being managed and evidenced uploaded and provided through the Risk Module on Datix.

Clinical Governance Facilitators - are accountable to the Divisional Directors of Nursing/Midwifery/AHPs for:

- Implementing the Trust Policy for the Management of Risk at Business Support Unit level, through the documented Divisional, Business Support Unit and departmental structures;
- Monitoring activity to provide assurance that local structures are effective and escalating issues as appropriate.
- Supporting the Risk Handlers and Action Owners with risk assessment and management
- To provide education and training on risk assessment and management to the Division

General Managers, Divisional Therapy Managers, Clinical Directors and Matrons - are responsible for identifying, assessing, responding to, reporting and reviewing risks within their ward, department, or service. They will ensure risks are identified, evaluated, mitigated, escalated where necessary, reviewed, and updated according to the risk level. In addition, they will ensure that all their employees have an understanding of the risks to their service and at all times ensure compliance with health and safety policies and procedures and all relevant legislation and regulation.

The Divisional Nursing/Midwifery/AHPs and Medical Directors are accountable to the Divisional Associate Director for: -

- Implement and embed the Risk Management Policy at Divisional level, through the documented Divisional and Business Support Unit structures;
- The meetings have responsibility for establishing a pro-active approach to risk management across the division and to ensure that risks are correctly described, evaluated with robust mitigations in place
- Monitoring activity to provide assurance that local structures are effective and escalating issues as appropriate;
- Ensuring the agreed risk management procedures, systems and processes are implemented, embedded and effective in the service for which they are accountable; and
- Ensuring clinical and non-clinical risks; health and safety; emergency planning and business continuity, relevant project and operational risks are identified and managed.

All Divisional Directors (including Nursing/Midwifery/AHPs/Medical) are responsible for ensuring the identification, assessment, approval, response, reporting and review of all risks to the achievement of objectives and delivery of services in line with the requirements set out in this document. They shall, at all times, ensure compliance with health and safety policies and procedures and all relevant legislation and regulation.

Head of Clinical Governance and Risk – is accountable to the Director of Quality, Clinical Governance, Risk and Compliance

- Supporting the development of the risk management policy, procedure and guidance;
- Ensuring that a comprehensive training programme covering risk and patient safety issues is developed, delivered and accessible to all levels of the organisation, meeting the Trust's legal obligations and the educational needs of the staff
- Maintaining the Trust's Risk Management Database, Datix
- Providing expert advice on the management of risks
- Providing reports to the Trust's Committees and sub-Committees.

Director of Quality, Clinical Governance, Risk and Compliance - is accountable to the Chief Nurse for the overall performance of risk management systems and supporting processes for risk registers.

Executive Director of Corporate Development – is the lead for Corporate Governance and is responsible for the production and maintenance of the high-level committees' terms of reference. They will ensure the identification and management of organisational risk and oversee progress against the Board Assurance Framework in its entirety.

Executive Director of People & Culture – is the Board lead for Workforce Development, Human Resource Management, Health and Safety, Organisational Development, Employee Services and Flexible Staffing. He or she is accountable to the Chief Executive Officer for risks arising from these areas. He or she will ensure the identification and management of risk and oversee progress against the Board Assurance Framework for his or her areas of responsibility.

Chief Operating Officer - is the Board lead for Operational Performance, Emergency Planning and Business Continuity, Clinical and Service Planning, Service Transformation, Space

Utilisation and Private Patients' Services. He or she is accountable to the Chief Executive Officer and has a specific responsibility for identifying, recording, advising on and coordinating actions around operational and performance risks. He or she is accountable to the Chief Executive Officer for risks arising from these areas. He or she will ensure the identification and management of risk and oversee progress against the Board Assurance Framework for his or her areas of responsibility.

Executive Director of Finance – is the Board lead for Finance, Performance Monitoring and Contracting, NHSI Compliance, Estates and Capital Investment, Supplies and Procurement, Charitable Funds and Commercial Development. He or she shall ensure that activities are controlled and monitored through effective audit and accounting mechanisms that are open to public scrutiny and presented annually. He or she is accountable to the Chief Executive Officer for risks arising from these areas. He or she will ensure the identification and management of risk and oversee progress against the Board Assurance Framework for his or her areas of responsibility.

He or she shall also fulfill the function of Senior Information Risk Officer (SIRO) and so be responsible for the management of information risks and provision of leadership and training for Information Asset Owners. He or she will ensure the identification and management of risk and oversee progress against the Board Assurance Framework for his or her areas of responsibility.

Executive Medical Director – has Board level responsibility for the delivery of patient safety and the Quality Strategy with the Executive Chief Nurse. He or she is the Board lead for, Clinical Effectiveness, Clinical Audit, Compliance with NICE Guidance, Education & Research, Medical Practice (including professional lead for pharmacists) and Clinical Coding. He or she is accountable to the Chief Executive Officer for risks arising from these areas. He or she will ensure the identification and management of risk and oversee progress against the Board Assurance Framework for his or her areas of responsibility.

Executive Chief Nurse - is the Board lead for Risk Management, Patient Experience, Nursing Midwifery and Allied Health Professional practice, Infection Prevention and Control, End of Life and Safeguarding. He or she shares joint responsibility with the Executive Medical Director for the delivery of patient safety and the Trust Quality Strategy. He or she is accountable to the Chief Executive Officer for risks arising from these areas and the provision of a risk management system. He or she will ensure the identification and management of risk and oversee progress against the Board Assurance Framework for his or her areas of responsibility.

The Chief Executive Officer - is the accountable officer with the overall responsibility for risk management including Health and Safety. As such, the Chief Executive Officer must take assurance from the systems and processes for risk management and ensure that these meet statutory requirements and the requirements of the regulators. The Chief Executive Officer chairs the Trust Delivery Group meeting, which reports to the Board, and will sign the Annual Governance Statement in accordance with UHDBFT governance arrangements. He or she shall ensure that reporting mechanisms clearly demonstrate that the Chief Executive Officer is informed of all significant risk issues and that their responsibility for management can be fulfilled. The Chief Executive Officer will ensure, via the Executive Chief Nurse and Trust Secretary, robust oversight of all risk management processes and the production of reports on risk.

4. KEY ORGANISATIONAL RESPONSIBILITIES

The organisational management of risk forms part of the Trust's overall approach to governance. The key forums for the management of risk in the Trust are outlined below: -

Trust Board - Executive and Non-Executive Directors share responsibility for the success of the organisation including the effective management of risk and compliance with relevant legislation.

They have a collective responsibility as a Board to:

- protect the reputation of the Trust and everything of value;
- provide leadership on the management of risk;
- reduce, eliminate and exploit risk in order to increase resilience;
- determine the nature and extent of the significant risks it is willing to take in achieving its strategic objectives;
- agree and review the Trust's risk appetite statement on a regular basis; and
- review the Trust's strategic objectives and ensure the BAF is fit for purpose, providing thorough oversight of strategic risks.

Audit Committee - is responsible for keeping the Trust Board informed of any material matters which have come to the committee's attention. He or she will provide the Board with an opinion letter about the proposed Annual Governance Statement, and report to the Board on the effectiveness of the risk management system.

The Assurance Committees of the Board - Assurance Committees of the Board has a role for risks pertaining to their area of focus. They have roles in reviewing the management of the risks held on the Risk Register and Board Assurance Framework. They review the Board Assurance Framework and ensure that the Board of Directors receive assurance that effective controls are in place to manage risk and report on any significant risk management and assurance matters.

Each of these Committees has oversight responsibility for a section of the Risk Register within the remit of their own Terms of Reference and performs detailed scrutiny of controls and assurances. Via their Non-Executive Chair, each reports formally to the Board of Directors, to confirm delivery of assurance or to escalate matters, as necessary.

Risk and Compliance Group - Provides a forum for Divisions to present risks the extreme risks (and others for escalation and of concern) for peer review and challenge and thus ensure Divisional risk management is robust and consistent.

Business Unit Support Meetings/Divisional Governance Board Meetings - to ensure that Section 5 Process for Assessing and Managing Risk are delivered and that there is a clear line of review and escalation process across the Divisional Governance structure.

5. PROCESS FOR ASSESSING AND MANAGING RISK

The Trust follows a process that is presented as a set of iterative steps that are undertaken in a coordinated manner, but not necessarily in a strict sequence as in practice, these steps are iterative.

Risk Identification

Risk can be identified proactively by assessing the Trusts strategic objectives, work related activities, analysing adverse events trends and outcomes, and anticipating external

possibilities or scenarios that may require mitigation. Listed below are examples of the sources of intelligence that can be used to assist with risk identification: -

Internal Sources

- Organisational key performance indicators (e.g. Quality and Performance reports)
- Risk, incidents, complaints and claims reporting and analysis
- Internal audits/ reviews
- Process analysis, including compliance with Trust strategies, policies, plans & procedures
- NHS core standards for Emergency Preparedness, Resilience and Response
- Surveys (e.g. FFT and staff satisfaction surveys)

External Sources

- Reports from inspections from external bodies, e.g. Care Quality Commission, Health and Safety Executive, External Audit
- Coroner reports
- National standards, guidance and new/updated legislation
- Horizon scanning of the external healthcare environment and learning from others
- Working partnerships with other local and national healthcare organisations
- National Central Alerting System broadcasts

Once a risk has been identified, it should be described unambiguously by outlining the event, cause, and effect of the risk. The following convention shall be used for all risk descriptions:

- **A Risk of……..**
- **Caused by….**
- **May Result in….**

All identified risks shall have a designated risk handler (a named person) who is responsible for its management. This should be the person best placed to manage the risk with sufficient level of authority to make decisions relating to management of the risk.

All identified risks shall be formally recorded onto the Trust risk register on Datix. It is the risk

Handler's responsibility to ensure the risk is escalated to their Business Unit Support/ Divisional/Corporate governance meeting for awareness and approval.

The recording of risks onto the risk register for/within a Division other than your own without seeking prior approval from the respective Divisional Leadership Team is strongly discouraged. Risks found to have been recorded without prior approval will be removed from the register.

Risk Assessment

To enable meaningful assessment of risks and for proportionate responses to be decided upon, planned and implemented, the two main components below must be evaluated;

- Consequence
- Likelihood

In this context, consequence is defined as the potential harm or loss if the risk occurs and must be scored using the risk scoring matrix table (see Appendix A).

The likelihood score reflects how likely it is that the risk will occur. Frequency may not be useful when scoring risks associated with time- limited or one-off projects and for these risks the likelihood score should be based on the probability of the risk occurring.

The assessment process should aim to be as objective as possible, making use of available evidence to support the risk consequence and likelihood. Where possible, the assessment should evolve relevant stakeholders.

Appendix B provides a Risk Assessment Tool which can be used to assess a risk before submission to the Risk Module on Datix.

Risk Scoring

The risk scoring matrix guidance at Appendix A shall be used for obtaining a numerical value to the consequence and the likelihood of the risk occurring. The rating is calculated by multiplying the consequence score by the likelihood score.

When scoring a risk there are three risk scores that need to be established, these are:

- **Initial score** – this is the score when the risk is first identified and initially assessed without controls in place. This score will not change for the duration of the risk.
- **Current score** – the level of the risk at present time considering the effectiveness of current controls (existing systems and processes). The current score will/should alter following periodic review of the risk as actions to treat the residual risk are incrementally implemented.
- **Target score** – the level of the risk expected following the full implementation of the proposed smart actions to reduce the residual risk.

If the current risk score is 15 or above, the risk handler and relevant stakeholders must seek approval from their Divisional/Corporate Leadership Team, prior to the risk being made active on the Trust risk register. In the interim, the risk shall be recorded on risk register and placed under the approval status of **"being reviewed."**" on Datix until the risk score has been endorsed at the Risk and Compliance Group. Once endorsed, the risk status shall be changed to **"live/approved."**

If the current risk score is equal to or lesser than the target risk score it implies that the risk has been managed to a level, as agreed by the risk handler and relevant stakeholders, and shall be subject to periodic reviews and remain part of discussions at Divisional governance forums.

Risk Treatment

Selecting the most appropriate risk treatment strategy involves balancing the potential benefits
to the achievement of objectives against the time, costs and efforts. The risk handler and relevant stakeholders should decide on the treatment strategy from below. In general there are four potential responses to address a risk once it has been identified and assessed: Tolerate, Treat, Transfer and Terminate (referred to as the '4 Ts'). The Trust will use the '4 Ts' to address and manage risks at all levels of the organisation.

- **Tolerate the risk**: The risk may be considered manageable without the need for further mitigating action, for example if the risk is rated LOW or if the Trust's ability to mitigate the risk is constrained or if taking action is disproportionately costly. If the

decision is to tolerate the risk, consideration should be given to develop and agree contingency arrangements for managing the consequences if the risk is realised.

- **Treat the risk**: Incorporate checks within the process to identify and correct an error; Standardise processes; Prevent access to the hazard (e.g. by guarding equipment or the use of personal protective equipment); Organise work to reduce exposure to the hazard (e.g. rotating or training of staff); Identify contingences to compensate for system failure.
- **Transfer the risk**: Risks may be transferred for example by conventional insurance or by sub-contracting a third party to take the risk. This option is particularly suited to mitigating financial risks or risks to assets. It is important to note that reputational risk cannot be fully transferred.
- **Terminate the risk**: Cease to carry out a risky operation; Remove the risk by using alternative resources (people, equipment or materials or by moving to a new environment).

Review/Monitoring of Risks

Active risks on the Trusts risk register regardless of risk score should entail the following key lines of enquiry:

- Consideration of the current risk scoring (does the score reflect current position)
- Review and ascertain the effectiveness of current control measures
- Update on outstanding actions to bridge gaps or address weaknesses in control
- Provide a progress update and set the next risk review date on Datix.
- Does the risk require escalation for additional support.

Low, Moderate and High Risks are managed within the Divisions. Extreme Risks may be managed within the Division or Corporate areas but will be subject to scrutiny from Risk and Compliance Group and assurance Committee to ensure adequate actions are taken and risk reduction occurs.

The minimum frequency for formal review of risks on the Trusts risk register are specified below;

Current Risk Grade /Score	Decision to Accept Risk	Level of Monitoring	Frequency of Review At least……
Low 1-3	Business Support Unit	Business Support Unit/ Ward/Dept	Annually
Moderate 4-6	Business Support Unit	Division	Six Monthly
High 8-12	Divisional Governance Board Meeting	Division	Three Monthly
Extreme 15-25	Divisional Governance Board Meeting and then Risk and Compliance Group	Division/Risk and Compliance Group/Trust Delivery Group/UHDB Committees / Trust Board	Monthly

This requirement relates to the process of formal review and updating of the risk register. A more frequent (monthly) reviews is encouraged, as and when significant changes to the risks are identified.

The risk handler and relevant stakeholders can determine the preferred method of risk review. It does not need to take place at a formal meeting.

The responsibility for updating the risk record on the risk register rests with the assigned risk handler.

Following each formal review, the risk record should be updated with meaningful progress updates, and a new review date set as the last day of the relevant month regardless of review frequency to provide assurance that a review has taken place.

Risk Reporting and Escalation

An effective risk management framework anticipates, detects, acknowledges and responds to changes and events in an appropriate and timely manner. Risk reporting provides a regular mechanism to direct updates to key stakeholders, ensuring the right information is given to the right people, at the right level, at the right time. In doing so risk reporting enhances the quality of decision-making, informs prioritisation of activity, and strengthens organisational oversight.

The timely escalation and de-escalation of risks is an important facet of risk management and there are mechanisms in place within the Trust for this to happen. Risks are expected to be monitored at Department/Business Support Unit/Divisional governance meetings and at the Risk Management and Compliance Group, subject specific group and Executive Leadership Team and Board Assurance Committee levels. Within these meetings, confirm and challenge is expected to take place when discussing risks to seek assurance that risks have been accurately described, scored, appropriate risk handler assigned, and robust controls applied, gaps in controls identified and where required smart actions are in place.

To promote good governance, a specific subject group meeting may opt to monitor a particular risk as there may be cross-divisional / cross-corporate impact of the risk – for example, Health and Safety, Information Governance, estates and facilities, and IT

Risk's scoring 15 & above are considered as extreme risks and as such, will appear on the monthly risk reports produced by the Head of Clinical Governance and Risk to the relevant forums for discussion and decision making and escalation to the specific UHDB Committee and Trust Board.

Risks and themes of risks identified through analysis as fast movers that could potentially impact on strategic objectives shall feature in risk reports produced by the Head of Clinical Governance and Risk to help recipients of the report with their decision making.

Risks that have been determined to have a strategic impact must be escalated to the executive lead for each BAF risk for consideration and inclusion, as necessary. After receiving approval from the next formal Board and the assurance committee, the risk must then be monitored going forward to ensure that it is being appropriately mitigated.

Risks projected to exceed the Trust Boards predefined risk appetite levels must initially be escalated to the Risk & Compliance Group (R&CG) discussion and scrutiny. The decision on subsequent action including escalation to Board for approval will be made by this group.

Any Division may escalate risks that cannot be managed/treated within the Divisions to the R&CG for discussion and or additional support with managing the risk.

Risk Acceptance and Closure

When all mitigating action to address the gaps identified in the control have been completed, consideration should be made as to whether the risk becomes an accepted risk (tolerated). This is a decision, which should be made at the relevant monitoring committee / subject specific group, to accept the risk at its current risk scoring (if it is within the risk appetite levels for that type of risk). Accepted risks shall be subject to periodic reviews if the risk remains present.

Risk shall be considered for closure when the risk has been removed e.g. the activity or process which gave birth to risk is no longer undertaken, and the informed decision for closure has been endorsed at the respective monitoring committee or subject specific group. Once endorsed, the risk shall be closed on the risk register via Datix by changing its approval status to **"closed/archived"** and populating the closed date filed with the date closure was endorsed.

6. RISK APPETITE

University Hospitals of Derby and Burton NHS Foundation Trust (UHDB) aims to provide high quality, effective and safe care to its population. It recognises that its long term sustainability depends upon the delivery of its strategic objectives and its relationships with its patients, the public and strategic partners and stakeholders.

The Board recognises risk is inherent in the provision of healthcare and its services, and therefore a defined approach is necessary to identify risk context, ensuring that the Trust understands and is aware of the risks it's prepared to accept in the pursuit of the delivery of the Trust's aims and objectives.

The Trust's Risk Appetite statement outlines the Board's strategic approach to risk-taking by defining its boundaries and thresholds, thereby supporting delivery of the Trust's Risk Management approach. It sets out the Board's appetite for risk at a given time. It is a live and dynamic statement which may be subject to change over time. It is therefore reviewed by the Board at the beginning of each Confidential Board Meeting. The current risk appetite statement is accessible via the Trust's website

7. DEFINITIONS

Risk Management	A central database used to prioritise risks according to their assessment scores and provide a tracking mechanism for implementation of actions and risk reduction.
Risk	The effect of uncertainty on objectives, recognising threats and opportunities.
Risk Assessment	Application of an assessment tool to define the level of risk based on the likelihood and consequence of that risk occurring.
Risk Handler	Is responsible for the day-to-day management of the risk(s) assigned to them. It is the responsibility of the risk handler to keep the risk record updated including details of risk reviews, dates of upcoming reviews, re-evaluation of the current risk scoring and associated actions.

Datix	An electronic software application which the Trust uses to manage and record its risks, incidents, inquests, claims, complaints and safety alerts.
Consequence	Identification of the level of the impact. This can range from negligible to catastrophic.
Likelihood	Identification of the level of probability of consequences occurring. This can range from rare to almost certain.
Initial Risk	The extent of risk that is present prior to controls are considered.
Current/Residual Risk	The extent of risk that remains after current controls are considered
Controls	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 (a poor Internal Audit report for example) highlights gaps in control. Where there are gaps in current controls or controls that are in development prior to maturity, then risk handler need to establish the most appropriate way forward and develop a risk action plan for implementation.
Assurances	Provide details of assurances that the control is in place and is operating effectively. These assurances are obtained from a variety of sources, such as management reports, minutes of meetings, internal and external audit and other external assessors such as the Care Quality Commission.
Risk Appetite	The amount of risk that the Trust is prepared to accept, tolerate, or be exposed to at any point in time.
Board Assurance Framework (BAF)	A structured means of identifying and mapping the main sources of assurance in an organisation, and co-ordinating them to best effect.
Annual Governance Statement	Statement signed by the Chief Executive as the Accountable Officer and sets out the organisational approach to internal control.

8. MONITORING COMPLIANCE AND EFFECTIVENESS

This policy will be published internally and made accessible to all staff.

Monitoring Requirement:	Management of Risk Process	Training Requirement	Implementation
Monitoring Method:	➢ Consistency with risk descriptions ➢ Application of robust control to risks ➢ Smart actions assigned to risks ➢ Reduction in	The facilitation of risk awareness training for Band 6 and above	Effectiveness of the Trust's Risk Management Framework

	overdue risk reviews ➢ Reduction in overdue robust actions		
Monitoring Report presented to:	Risk and Compliance Group	Risk and Compliance Group	Audit Committee
Frequency of Report:	Monthly Divisional and Business Unit reports	Monthly Divisional and Business Unit reports	Biennial internal audit

9. REFERENCES

- A Risk Matrix for Risk Managers, National Patient Safety Agency (2008)
- NHS Audit Committee Handbook, Department of Health (2011)
- UK Corporate Governance Code, Financial Reporting Council (2010)
- The Orange Book (Management of Risk – Principles and Concepts), HM Treasury (2020)
- Government Finance Function – Risk Appetite Guidance Note V2.0 (2021)

APPENDIX A: Risk Scoring Matrix and Guidance

Table 1: How do I assess the consequence?

To enable meaningful assessment of risks and for proportionate responses to be decided upon, planned and implemented, the two main components below must be evaluated:

- The consequence
- The likelihood or probability of the risk occurring

Consequence scores

Choose the most appropriate domain for the identified risk from the left hand side of the table Then work along the columns in same row to assess the severity of the risk on the scale of 1 to 5 to determine the consequence score, which is the number given at the top of the column

Table 1:

	1	2	3	4	5
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**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	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	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	Non-compliance with national standards with significant risk to patients if unresolved Multiple complaints/ independent review Low performance rating Critical report	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
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
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	Non-compliance with national 10–25 per cent over project budget Schedule slippage Key objectives not met	Incident leading >25 per cent over project budget Schedule slippage Key objectives not met
Finance including claims	Small loss 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
Service/ business interruption Environmental impact	Loss/interruption of >1 hour Minimal or no impact on the environment	Loss/interruption of >8 hours Minor impact on environment	Loss/interruption of >1 day Moderate impact on environment	Loss/interruption of >1 week Major impact on environment	Permanent loss of service or facility Catastrophic impact on environment

Table 2: - How do I assess the likelihood?

Using available evidence, consider how likely it is that the risk will occur using the following descriptors:

Likelihood Score		Descriptor – how often might it/does it happen		
5	**ALMOST CERTAIN**	Will undoubtedly happen/recur, possibly frequently	Expected to occur at least daily	>75%
4	**EXPECTED**	Will probably happen/recur but it is not a persisting issue	Expected to occur at least weekly	50-74%

3	**LIKELY/POSSIBLE**	Might happen or recur occasionally	Expected to occur at least monthly	25-49%
2	**UNLIKELY**	Do not expect it to happen/recur but it is possible it may do so	Expected to occur at least annually	11-24%
1	**RARE**	This will probably never happen/recur	Not expected to occur for years	<10%

Table 3: Grading Matrix (NPSA 5x5 Risk Matrix)
Use the table below to identify the Consequence and Likelihood. The risk score is calculated by multiplying the consequence score by the likelihood score.

		Consequence				
		1	**2**	**3**	**4**	**5**
Likelihood Score		**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
	5 Almost Certain	5	10	15	20	25
	4 Likely	4	8	12	16	20
	3 Possible	3	6	9	12	15
	2 Unlikely	2	4	6	8	10
	1 Rare	1	2	3	4	5

Consequence x Likelihood = Risk Score

1 - 3	Low risk	4 - 6	Moderate risk
8 - 12	High risk	15 - 25	Extreme risk

APPENDIX B: Risk Assessment Tool

UNIVERSITY HOSPITALS OF DERBY & BURTON NHS FOUNDATION TRUST RISK ASSESSMENT TOOL			
Division:		Site:	
Business Unit:		Ward/Department:	
Risk Description			
A Risk of …			
Caused by …			
May Result in …			

Domains/Descriptors (Circle as appropriate)			
Impact on the safety of patients, staff or public (physical/ psychological harm)	Quality/complaints/ audit	Human resources/ organisational development/ staffing/ competence	Statutory duty/ inspections
Adverse publicity/ reputation	Business objectives/ projects	Finance including claims	Service/ business interruption Environmental impact

Summary of current controls in place:

Consider equipment, staffing, environment, policy / procedure, training, documentation, information (this list is not exhaustive)

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.

Summary of current assurances in place

Provide details of assurances that the control is in place and is operating effectively. These assurances are obtained from a variety of sources, such as management reports, minutes of meetings, internal and external audit and other external assessors such as the Care Quality Commission.

LEVEL OF HARM/CONSEQUENCE **See descriptors below**		**LIKELIHOOD**	
Insert domain/descriptor	**Catastrophic**	**ALMOST CERTAIN** Expected to occur at least daily	**>75%**
Insert domain/descriptor	**Major**	**LIKELY** Expected to occur at least weekly	**50-74%**
Insert domain/descriptor	**Moderate**	**POSSIBLE** Expected to occur at least monthly	**25-49%**
Insert domain/descriptor	**Minor**	**UNLIKELY** Expected to occur at least annually	**11-24%**
Insert domain/descriptor	**Negligible**	**RARE** Not expected to occur for years	**<10%**

NPSA Risk Matrix 5x5: -

		Consequence (see below descriptions)				
		1	2	3	4	5
Likelihood Score		Negligible	Minor	Moderate	Major	Catastrophic
	5 Almost Certain	5	10	15	20	25
	4 Likely	4	8	12	16	20
	3 Possible	3	6	9	12	15
	2 Unlikely	2	4	6	8	10
	1 Rare	1	2	3	4	5

IDENTIFY THE LEVEL AT WHICH RISK WILL BE MANAGED

E	Extreme risk, immediate action required, reviewed within 1 month	**H**	High risk, action planned immediately, commenced within one month, reviewed within 3 months
M	Moderate risk, action planned within one month, commenced within three months, reviewed within 6 month	**L**	Low risk, action planned within three months, reviewed within 1 year

Action plan of further control measures required:

Priority	Action	Person Responsible	Date Started	Date Completed

Target Risk Assessment once all control measures are implemented ***NB see guidance notes if category remains E, H or M***	Level of Harm/ Consequence	Likelihood	Category (L, M, H, E)	Predicted date to reach Target Score

Risk Assessors Name:		Designation:		Date:	
Managers Name		Designation:		Date:	

Review Date	Risk Evaluation			Print Name & Signature	Date of next review
	Level of Consequence	Likelihood	Category (E, H, M or L)		

Risk Assessment Replaced		
Name	Designation	Date