NHS
Rotherham Doncaster
and South Humber
NHS Foundation Trust

Risk Management Framework

DOCUMENT CONTROL	
Version:	12.1
Unique Reference Number:	1075
Ratified by:	Board of Directors
Date ratified:	
Name of originator/Author:	Head of Risk Management
Name of responsible committee/individual:	Director of Corporate Assurance
Summary of Changes	The updated Risk Management Framework enhances risk culture by embedding the PACED principles and the "Managing Risk the RDaSH Way" approach. Key improvements include: • Introduction of the PACED principle for managing risk. • Enhanced Risk Classification • Enhancing risk culture and aligning it to the trust's core values • Standard Operating Procedures for Opening and closing Risk • Introduction of Control Types • Clear risk treatment procedures. • More Frequent Review of Tolerated Risks • Integration of External Registers. • Four Levels of Assurance section to evaluate the effectiveness of risk mitigation controls. • Non-Compulsory Issue Log Implementation
Date issued:	
Next Review	
Target Audience	All Staff

Table of Contents

1. Introduction 5
2. Scope 6
3. Structure 6
4. Risk Culture-Managing Risk the RDaSH Way 7
5. Strategic Delivery Risk 8
6. Partnership Risks 9
7. Risk Management Process 9
7.1 Risk Identification 10
7.1.1 Risk Identification Techniques 11
7.1.2 Risk articulation 11
7.1.3 Risk Classification 13
7.1.4 Standard Operating Procedures (SOP) for Risk Identification 15
7.2 Risk Assessment 15
7.2.1 Risk Analysis 16
7.2.2 Risk Evaluation 17
7.3 Risk Treatment 18
7.3.1 Treat 18
7.3.2 Tolerate 19
7.3.3 Transfer 19
7.3.4 Terminate (Avoid) 19
7.3.5 Criteria for Risk Treatment 19
7.4 Monitoring, Review and Escalation 20
7.4.1 Monitoring and Review 20
7.4.2 Assurance Over Controls 21
7.4.3 Closing a Risk 22
7.4.4 Reporting 22
8. Risk Appetite and Statement 23
9. Risk Governance 23
9.1 Assurance 24
9.2 Roles and Responsibilities 24
10. Risk Registers 27
10.1 Integration of Other Risk Registers 27

11. Training and Development 27
12. Risk System 28
13. Emergency Preparedness, Resilience and Response (EPRR) 28
14. Continuous improvement 28
15. Issue Logs 28
16. Equality Impact Assessment Screening 29
16.1 Privacy, Dignity and Respect 29
16.2 Mental Capacity Act 29
17. Links to Associated Documents 29
18. References 30
Appendix 1 – Monitoring and Evaluation Arrangements 31
Appendix 3 – Risk Scoring Methodology 33
Appendix 4 – Risk Form 37
Appendix 5 – Risk Classification Definitions 39

1. Introduction

Risk management is a core component of good corporate governance and an essential element in the delivery of safe healthcare services. At RDaSH, the effective management of risk underpins our strategic aims, operational effectiveness, and duty of care to both staff and patients. By adopting this framework, we ensure that all staff are equipped with the necessary knowledge, tools, and support to recognize and manage risks systematically and consistently.

Successful risk management enhances strategic planning and prioritisation, assists in achieving objectives and strengthens the ability to be agile to respond to the challenges that our Trust faces. If we want to meet our objectives successfully, improve service delivery and achieving value for money, risk management must be an essential and integral part of planning and decision-making. This risk management framework has been developed to improve risk management further and to embed this as a routine part of how we operate.

Risk is inherent in everything we do to deliver high-quality services and must be an integral part of informed decision-making, from policy, through implementation to the everyday delivery of services. This isn't about adding new processes; it is about ensuring that effective risk management is integrated in the way we lead, direct, manage and operate.

The effectiveness of risk management depends on the individuals responsible for operating the systems put in place. Our risk culture must embrace openness, support transparency, welcome constructive challenge and promote collaboration, consultation and co-operation. We must invite scrutiny and embrace expertise to inform decision-making.

Risk Management is everybody's responsibility and is a fundamental part of the Trust's Governance Structure providing the following benefits:

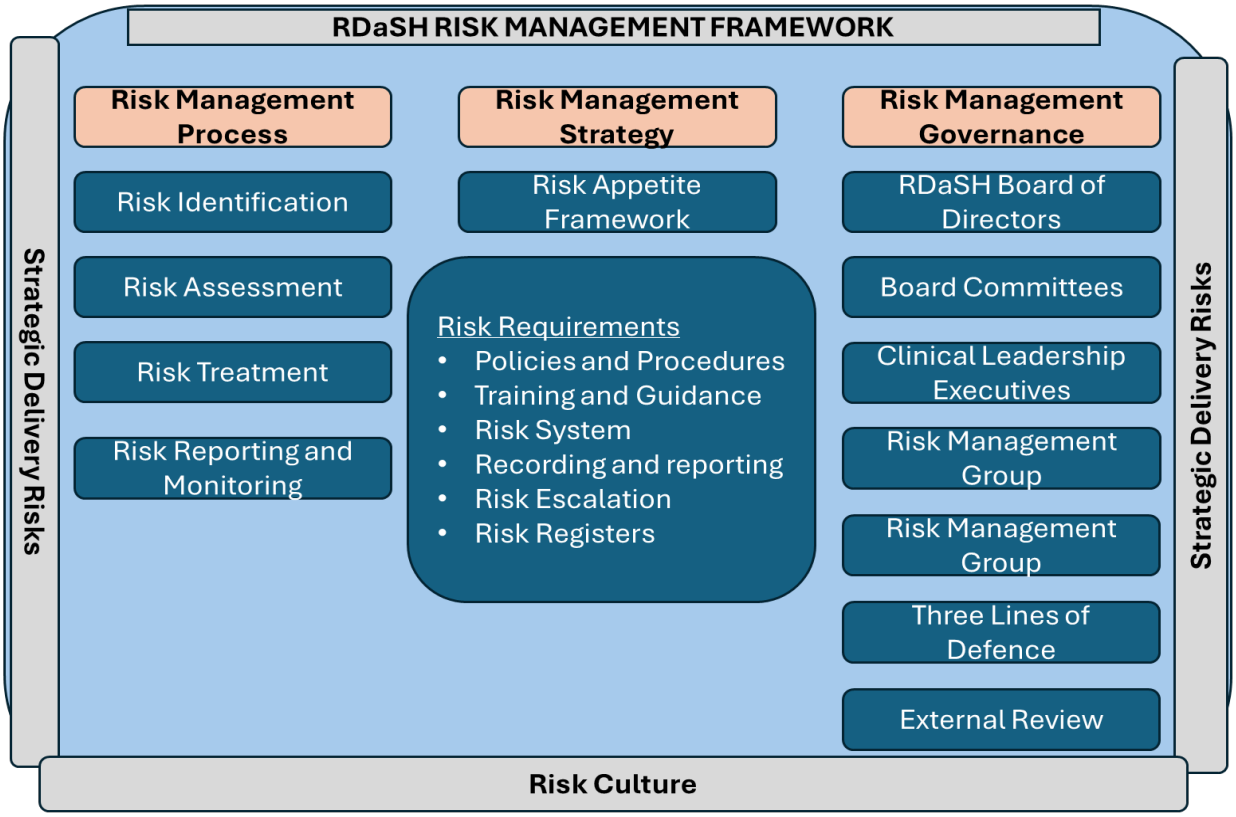
2. Scope

This Framework is designed to be the overarching document for risk, articulating the principles of how risk is managed within the trust and is intended for use by all directly employed, agency staff engaged on RDaSH NHS Trust business in respect of any aspect of that work. It is recognised that actions contain inherent risks.

RDaSH NHS Trust Strategic Delivery Risk and organisational and Corporate Risk Registers provide a central record of risks to the organisation. The Trust Board identifies and monitors the key strategic risks against the Trust's strategic aims and objectives and staff throughout the Trust identify, monitor and manage operational risks on a day-to-day basis.

3. Structure

RDaSH's Risk Management Framework (RMF) is designed to ensure that risk identification, assessment, treatment, and reporting align with the size and nature of our operations. This framework is broadly patterned after HM Treasury's Orange Book (which provides principles and concepts for managing risk in the public sector) and incorporates elements of the COSO (Committee of Sponsoring Organizations) framework, ensuring industry best practice is embedded throughout RDaSH's risk management approach.



The Risk Management Framework offers a structured approach to managing risks by focusing on processes, strategy, and governance. The framework ensures risks are identified, assessed, treated, and monitored effectively, supported by policies, training, risk systems, and escalation pathways. The strategy component defines the organization's risk appetite and ensures risk registers and reporting systems are in place.

Governance is central to the framework, with accountability spread across the Board of Directors, committees, clinical leadership, the Risk Management Group, and external reviews. It incorporates the Three Lines of Defence model for oversight and assurance. The framework is underpinned by a strong risk culture that promotes proactive risk management the RDaSH way and integrates with the Strategic Delivery Risk to align risk management with broader organizational objectives.

Our approach to risk management will be guided by the application of the key risk management principle of **PACED**. This shows our commitment to maintaining a systematic yet adaptable approach to enterprise risk management, ensuring that our risk processes are fully integrated, strategically aligned, and proportionate to the threats and opportunities faced by the Trust. The principle of PACED requires our risk management effort to be:

Proportionate
We scale our risk management to the significance and potential impact of each risk. We allocate more resources to high-severity risks that could significantly affect patient safety, service delivery, or financial stability.

Aligned
We ensure our approach aligns with RDaSH's objectives and strategic priorities. By integrating risk considerations into business planning and decision-making, we actively support Trust-wide goals such as quality care, patient safety, and continuous improvement.

Comprehensive
We identify, assess, and manage all major risks across clinical, operational, and strategic areas, considering both internal factors and the external environment.

Embedded
We embed risk management into our culture and day-to-day operations. It is woven into key workflows, policies, and decision-making so that proactive risk awareness becomes second nature to all staff

Dynamic
We keep our practices flexible and responsive to changing circumstances. Through continuous monitoring, stakeholder engagement, and periodic reviews, we adapt to emerging threats and opportunities, ensuring resilience and service continuity

4. Risk Culture-Managing Risk the RDaSH Way

At RDaSH, our approach to managing risk is guided by our Core Values—Passionate, Reliable, Caring and Safe, Supportive, Open, and Progressive. These values shape our culture, define our standards, and underpin the "RDaSH way" of delivering quality, safe services. They influence how we identify, assess, treat, and monitor risks, ensuring that every team member from frontline staff to leadership understands risk management as a daily responsibility. In essence, managing risk the RDaSH way means

1. **Passionate**
We bring energy and commitment to our risk management practices, recognizing that identifying, analysing, and mitigating risks is essential to delivering the highest standard of care. Staff at all levels are encouraged to approach risk management enthusiastically.

2. **Reliable**

Our processes and protocols are designed to provide consistent, dependable outcomes, fostering trust among staff, patients, and the wider community. By adhering to clear procedures, regularly reviewing controls, and maintaining transparent reporting, we ensure reliability in how risks are managed and escalated.

3. Caring and Safe
Patient safety and staff well-being lie at the heart of our risk culture. We prioritize actions that safeguard clinical quality, reduce harm, and create a secure environment. Every decision and intervention are evaluated through the lens of caring and safety, underscoring our responsibility to protect those we serve and those who deliver care.

4. Supportive
We believe that risk management is a collective endeavour. We aim to foster a culture in which staff feel supported to speak up about concerns, learn from incidents, and collaborate in finding solutions. Through open channels of communication, training, and accessible guidance, we empower individuals and teams to manage risk effectively.

5. Open
Honesty and transparency underpin our entire risk management framework. We encourage open dialogue, timely reporting of incidents and near-misses, and frank discussions about the effectiveness of current controls, as well as the timescales for resolving identified risks. By having these honest conversations, we cultivate trust and drive a continuous cycle of learning and improvement.

6. Progressive
Our approach is forward-looking and adaptable. We continuously seek opportunities to refine processes, integrate new technologies, and stay abreast of best practice in risk management. We remain agile in responding to emerging threats and evolving healthcare landscapes, ensuring our commitment to patient safety remains unwavering.

5. Strategic Delivery Risk

In accordance with the Annual Reporting Manual, foundation trusts are required to present in their Annual Report an annual governance statement signed by the Chief Executive and underpinned by a supporting Strategic Delivery Risks (SDR). This aims to provide the Board of Directors with assurance that systems are safe and subject to appropriate scrutiny and that the Board of Directors can demonstrate that they are informed of key strategic risks. The SDR contains all the strategic risks that can undermine the Trust's Strategic Objectives.
The SDR is built up of the strategic risks and includes:

- Current and Target Risk scores
- Lead Committee and Lead Director
- Key Controls intended to manage the risk
- Sources of Assurance to evidence that control measures in place are working effectively to manage risk.
- Gaps in either control or assurance and actions to address the gaps
- Risk Appetite

6. Partnership Risks

RDaSH recognizes the importance of managing partnership risks to ensure safe and effective service delivery. As collaboration and partnerships increase, systematically managing associated risks becomes essential.

Partnership risks will be identified and documented early during partnership formation, and joint risk assessments will be conducted collaboratively with partner organisations. Identified partnership risks will then be integrated into RDaSH's risk registers where appropriate. Joint action plans will also be developed with partners to effectively manage and mitigate these risks, with regular reviews and clear reporting through RDaSH's governance structures.

Regular monitoring and review of partnership arrangements will ensure the ongoing effectiveness of risk management. Lessons learned from any partnership-related incidents or near misses will be captured and implemented to enhance future practices. Embedding these practices will support the management of partnership risks effectively and safeguard the delivery of our strategic objectives

7. Risk Management Process

Risk management processes are the activities that deliver management and control of risks. In the context of RDaSH's Risk Management Framework, a risk is defined as the chance of something happening that will have an impact on business objectives, and this can be in terms of:

- A threat - a possible event we want to try to reduce the chances of occurrence or limit the impact to us if it did happen.

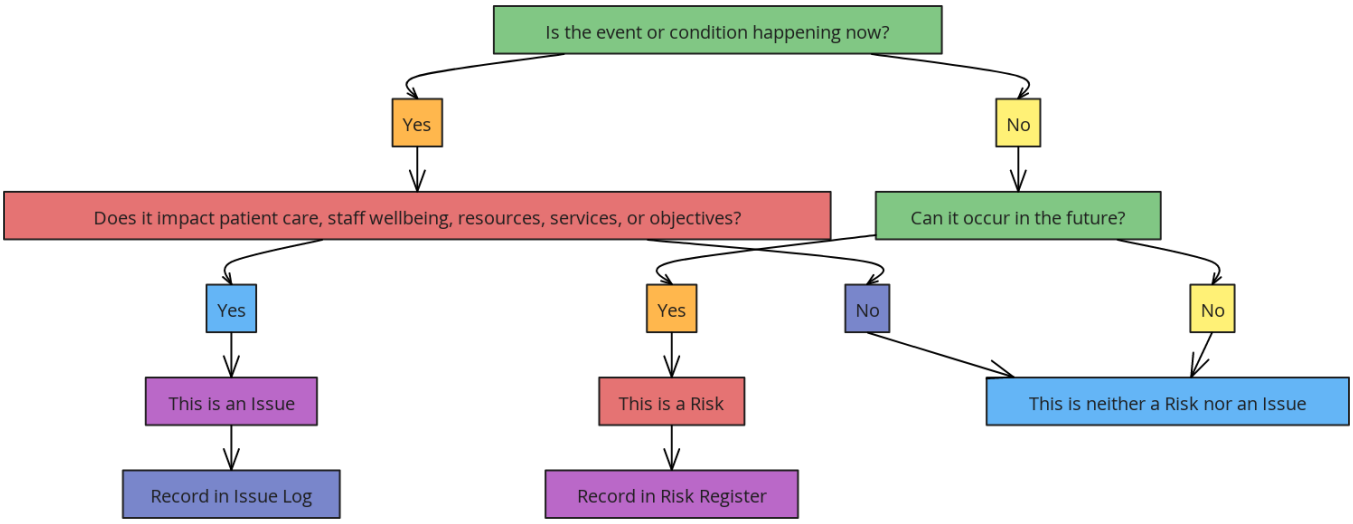
or

- An opportunity - a possible event that we might exploit by action which could deliver a benefit or positive effect for our Trust.

So how does this differ from an issue? **An issue** is an unplanned event that has already happened. As the issue has already happened it is not a risk. However, that does not mean there is no risk associated with the issue.

For example:

Patients waiting excessive time on a waiting list is an issue as this is happening. Not having an adequate process to manage the care of those patients poses the potential risk of harm.



Risk management is the process of identifying and evaluating potential consequences and determining the most effective method of controlling and responding to the risk(s) that we face. It is an ongoing cyclical process, not just a point in time that requires a corporate approach across the whole Trust.

The Risk Management Process at RDaSH consists of five main stages: Risk Identification, Risk Assessment, Risk Treatment, and Monitoring, Review & Reporting. An essential, ongoing element at each stage is communication & consultation with relevant stakeholders. Together, these activities ensure that risks are managed in line with RDaSH's objectives, values, and regulatory requirements.

7.1 Risk Identification

At RDaSH, we recognize that effective risk management starts with identifying both threats and opportunities. By knowing what could impact our objectives, we can protect the safety of our patients and the success of our Trust. We take a two-pronged approach:

- Top-Down: Our Board of Directors, executive leaders, and senior managers highlight strategic and systemic risks that could hinder organizational goals.
- Bottom-Up: Frontline staff, clinical teams, and department managers surface operational and clinical risks at the ground level.

This dual approach provides a well-rounded view, minimizing threats and maximizing opportunities to help us deliver safe, effective care.
time.

7.1.1 Risk Identification Techniques

Risks can be identified from many sources of information. Some of these are reactive (e.g. incidents), proactive (e.g. risk assessments), internal (e.g. staff consultations) or external (e.g. inspections).

Reactive

- Current incidents complaints and claims
- External decisions which could impact the organisation
- External recommendations, CQC HSE MHRA etc
- Audits; quality, internal or external
- National Initiatives

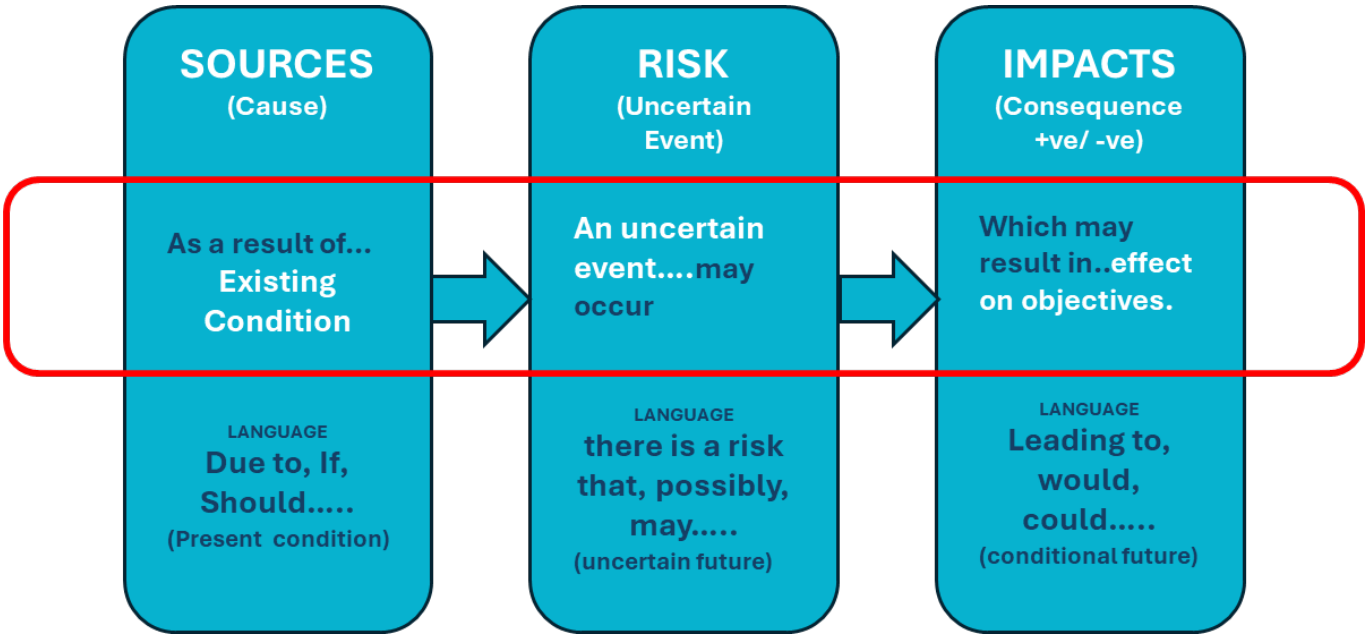
Proactive

- Delivery plans, corporate planning & objective setting
- Looking at lessons learned and previous issues
- Benefits of proposed projects and improvement actions
- Horizon scanning Risk assessments
- Staff, staff and stakeholder consultations
- Benchmarking
- Workshops and Brainstorming

Helpful Resource Appendix 2 – Prompts for identifying risk – to assist in identifying risks

7.1.2 Risk articulation

Accurate and clear risk articulation is essential for ensuring that identified risks are properly understood and managed. When formulating a risk statement, RDaSH follows a structured approach to capture three key components:



The Cause (What could/has go/gone wrong?)

- Identifies the underlying factors or triggers that might result in an adverse event or situation.
- For example, "Due to inadequate staff training…"

The Risk Event (What might happen?)

- Describes the specific event or scenario that could materialize because of the cause.
- For example, "…there is a risk that clinical procedures are not carried out correctly…"

Effect/Impact/Consequence (What would be the impact?)

- Explains the potential outcome or implications for patients, the Trust, or stakeholders.
- For example, "…leading to compromised patient safety and reputational harm.

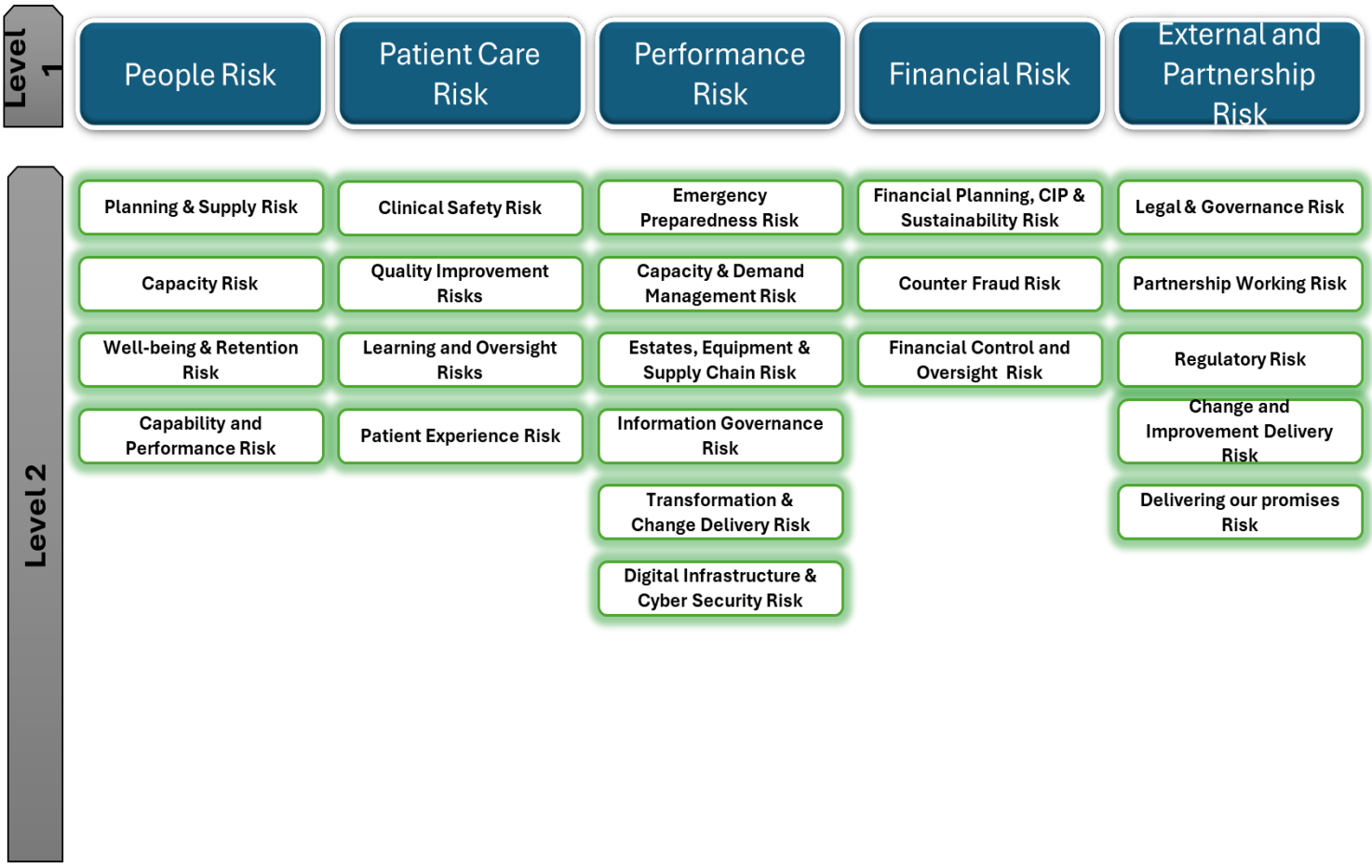
Example

Due to inadequate staff training, there is a risk that clinical procedures are not carried out correctly, leading to compromised patient safety and reputational harm.

Helpful Resource Appendix 4 - Risk form - for use when risk identified to aid discussion and articulate the risk

7.1.3 Risk Classification

RDaSH employs a two-level classification system to categorize risks in a manner that is both broad enough to capture all high-level threats and sufficiently detailed to address specific operational and clinical concerns. This Level 1 and Level 2 approach provides clarity in ownership, reporting, and escalation, while enabling tailored mitigation strategies.



- **Risk Types**
  Broad groupings that encompass major risk domains (e.g., performance, financial, People, Financial). These categories capture large-scale or complex risks that may affect multiple areas of the Trust.
- **Risk Categories**
  More specific classifications nested under each Level 1 category (e.g.IT Systems, Supply Chain, etc.). These subcategories pinpoint precise risk drivers and potential impacts, facilitating focused action planning.

Helpful Resource Appendix 5 - Detailed breakdown and definitions of each category

When classifying a risk, you are ultimately categorizing the risk itself, that is the event or scenario that could occur rather than just its cause or its impact.

- Cause helps you understand what triggers the risk (root cause).
- Impact helps measure how severe or disruptive it could be.
- The Risk Event is what you classify into the relevant domain (e.g., Clinical, Financial, Operational), because that domain best describes where and how the organization will experience the threat or opportunity.

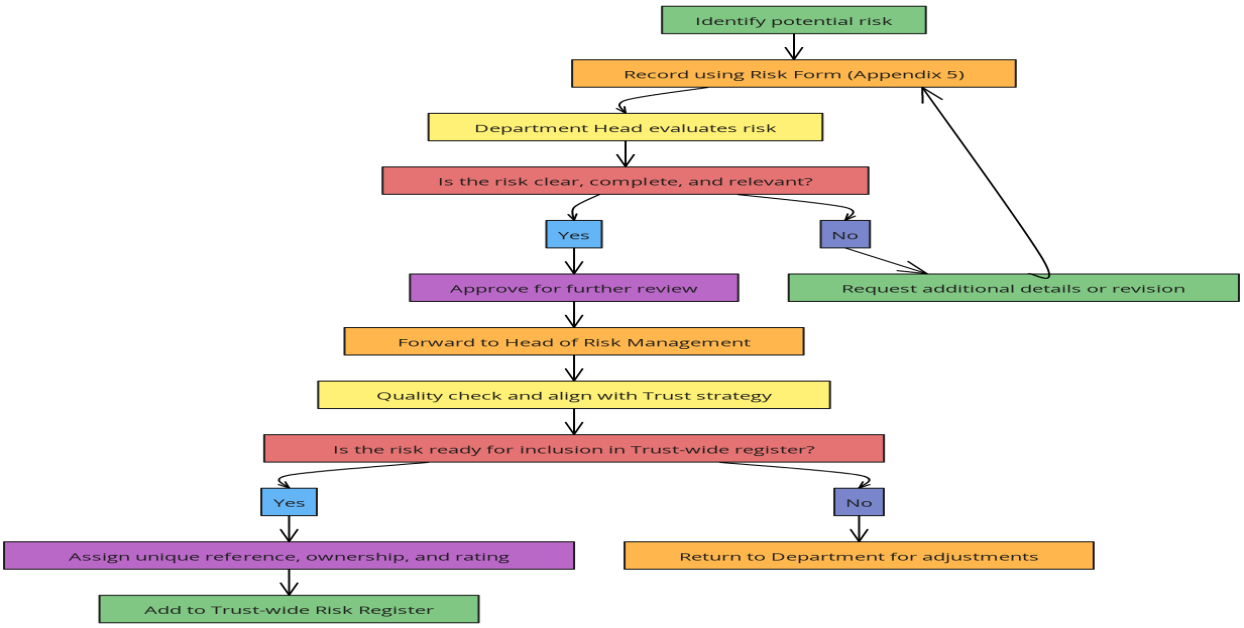
In other words, the cause and impact inform why and how seriously RDaSH should treat the risk, but the category is typically determined by the primary domain or nature of the risk event itself.

7.1.3.1 Quick Guide to Risk Classification

- **Identify the Risk Event**
    - **Tip:** Focus on the event itself (e.g., “a cyberattack compromising patient data”) rather than only the cause (e.g., “insecure systems”) or the impact (e.g., “service disruption”).
- **Pinpoint the Primary Domain**
    - **Ask:** “Which area of the organization is most affected if this event occurs?”
    - **Examples:**
        - **Clinical**: Risks that directly affect patient care or clinical outcomes.
        - **Operational**: Risks that compromise day-to-day activities (staffing, IT systems, facilities).
        - **Financial**: Risks that impact budgets, revenues, or significant investments.
        - **Strategic**: Risks that threaten long-term objectives or the organizational direction.
- **Check for Level 2 Subcategories**
    - **Ask:** “Within this main category, which subcategory best captures the nature of the risk?”
    - **Examples:**
        - If **Operational**, consider subcategories like health and safety, information governance, IT Infrastructure etc.
        - If **Clinical**, you might look at Patient safety and outcomes, Infection Control, Capacity Planning etc.

If unsure about which category or subcategory applies, reach out to the Risk Team or the Head of Risk Management. They can offer advice and ensure accurate alignment with the classification framework.

7.1.4 Standard Operating Procedures (SOP) for Risk Identification



RDaSH follows clear procedures to ensure that every newly identified risk is captured and recorded in a timely, accurate manner. By adhering to the steps below, staff and managers can maintain consistency, accountability, and alignment with the Trust's overarching risk management approach.

1. Risk identification is the responsibility of all staff. Any team member who identifies a potential risk should promptly record it using the Risk Form in appendix 5. All staff reporting or reviewing a newly identified risk must ensure the risk is described in line with the articulation guidelines set out in the Framework.
2. Once a risk is recorded, it will need to be approved by the department heads (or equivalent managers/directors) review the details for clarity, completeness, and relevance to their service area.
   If the risk is valid and warrants further assessment, the manager formally approves its inclusion in the Risk Register. If additional information is required or if the risk is not applicable, the manager requests clarification or suggests revision.
3. Approved risks are forwarded to the Head of Risk Management, who performs a quality check to ensure consistent application of the Trust's risk framework and rating criteria and ensures that all newly added risks follow standard formatting, classification, and alignment with RDaSH's overarching strategy and risk appetite.
4. After sign offs, the validated risk is recorded in the Trust-wide Risk Register with a unique reference number, ownership details, and initial rating

7.2 Risk Assessment

RDaSH's Risk Assessment process consists of two interlinked components: **Analysis and Evaluation**. This approach ensures each risk is understood in terms of both its current (residual) score and the desired (target) score, thereby guiding decisions on whether additional actions or resources are required.

7.2.1 Risk Analysis

RDaSH focuses on the residual (current) level of risk—that is, the level of risk that remains once the existing controls and mitigation measures are considered. This approach recognizes that many controls are already in place (e.g., policies, procedures, training, monitoring systems) that reduce the likelihood or impact of the risk. Therefore, the analysis phase determines the current (residual) risk score for each identified risk by examining the likelihood of occurrence and potential impact, considering any existing controls already in place. In analysing risk, we:

1. Explore what key controls are in place already, what is in place that reduces either impact or the likelihood of the risk occurring.
   The key controls are the processes, plans, measures that are in place to assist in the impact of the risks or likelihood of the risk occurring, such as:
   - Operational plans.
   - Statutory frameworks, for instance standing orders, standing financial instructions and associated scheme of delegation.
   - Actions in response to audits, assessments and reviews.
   - Workforce training and education.
   - Clinical governance processes.
   - Incident reporting and risk management processes.
   - Complaints and other patient and public feedback procedures.
   - Strategies/Policies/Procedures/Guidance.
   - Robust systems/programmes in place.
   - Objectives set and agreed at appropriate level.
   - Frameworks in place to provide delivery.
   - SLA/Contracts/Agreements in place

2. Each risk once identified needs to be assessed using a risk evaluation tool called the risk matrix. This tool measures the impact of the risk occurring and the likelihood that the risk will occur.
   Impact x Likelihood = Risk score

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

The **impact** is the consequence or 'how bad' it would be if the risk occurred. When assessing this you should not use the worst-case scenario, think what the most probable outcome would be.

The **likelihood** is a measure of how likely the risk will occur. When looking at this you should consider the current environment. Consider the adequacy and effectiveness of the controls already in place and likeliness of the risk being materialised

Helpful Resource - Appendix 4 – Risk scoring methodology – to aid scoring both the impact and likelihood.

This rating reflects the actual level of risk faced by RDaSH **with** existing controls in place.

3. After the risk score has been established, it is also important to establish what the target score is. Target score is the desired future rating, typically reflecting RDaSH's risk appetite or an acceptable, achievable level of residual risk. The target score guides subsequent action planning, helping determine the extent and urgency of any additional actions required.

It is important to note that where **risk appetite** has been implemented, the **risk tolerance level** for the class of risk being recorded will serve as the **target score**. This ensures alignment with the Trust's defined thresholds for acceptable risk.

In scenarios where the **risk appetite** is under review or yet to be fully implemented, the Trust will adopt the principle of **ALARP (As Low as Reasonably Practicable)** as the guiding standard for determining the target score. **ALARP** requires that risks are reduced to a level where the cost, effort, or inconvenience of additional controls would be disproportionate to the benefits gained. This ensures a balanced approach to risk management that is both cost-effective and responsible.

In simple terms, **ALARP** means that:

1. Risks should be mitigated as far as **reasonably practicable** without imposing excessive burdens on resources.
2. When deciding on additional controls, the Trust will assess whether the cost or complexity of implementation is justified by the level of risk reduction achieved.

7.2.2 Risk Evaluation

Once risks have been analysed, it will be necessary to decide how to respond to the risks. Risk evaluation is, in effect, a decision point at which to decide whether to respond or not to respond to the risk.

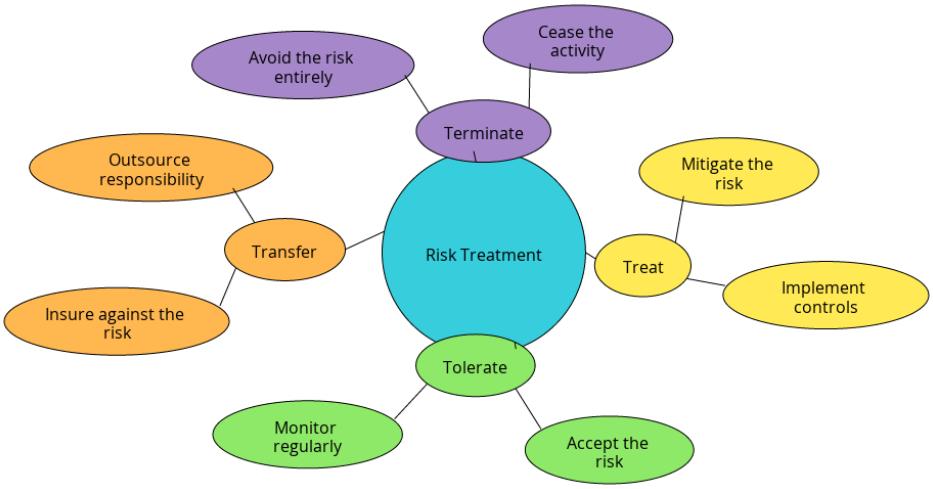
To do so, this implies there is a threshold that the risk will need to cross before action is taken. This threshold is termed risk appetite, which can simply be explained as the amount of risk required to achieve objectives. The following operating procedures will apply for evaluating risks in RDaSH

1. If the current rating is higher than the desired target, prioritize developing and implementing **risk treatment actions** (refer to risk treatment section) to close the gap. In some cases, achieving the target risk score may be challenging or require significant resources—these considerations factor into treatment planning and resource allocation
2. High or Extreme risks that surpass the Trust's appetite or strategic thresholds receive immediate attention and possible escalation to senior leadership through the Risk Management Group (RMG).
3. If a risk significantly exceeds its target or the Trust's risk appetite, it is escalated to relevant committees or executive teams for further review and endorsement of actions.
4. The Strategic Delivery Risk (SDR)may be updated if the risk impacts core strategic objectives.

5. Lower-rated risks may only require periodic monitoring, provided they align with the target score and do not pose imminent threats to operations or patient safety.

7.3 Risk Treatment

Risk treatment is how we manage and respond to risks. It is the process of determining and implementing the best course of action for managing identified risks, based on their **likelihood** and **impact** ratings and the Trust's **risk appetite**. In RDaSH, the goal is to **reduce current risk** to a level that is acceptable and aligned with our commitment to patient safety, regulatory compliance, and operational integrity. Risk treatment includes **Treat, Tolerate, Transfer, and Terminate (sometimes referred to as "Avoid").**



7.3.1 Treat

Treating a risk means introducing or strengthening controls to reduce its likelihood or minimize its impact. When a risk is likely to occur but has a relatively low potential impact, the Trust typically chooses to Treat.

When identifying actions or controls, it is important to determine whether they address the likelihood of the risk or its impact. This distinction helps re-evaluate the risk score more accurately after implementation, providing a clearer understanding of their effectiveness.

7.3.1.1 Controls

Controls are measures or safeguards that address the root causes or triggers of a risk, and they can also mitigate the impact. By selecting the right type of control, we can better ensure that resources are allocated effectively to reduce the residual risk to an acceptable.

- **Preventive Control:** These are the most important type of risk controls. They eliminate or reduce the cause of a risk, making it less likely to occur. Examples include firewalls, staff vetting processes, and routine maintenance schedules.
- **Corrective Controls**: Corrective controls are repair or correct measures after a risk event happens but must be in place beforehand. Examples include disaster recovery plans, backup power generators, and rapid response teams.
  This form of controls affects the impact level of a risk, has it is aimed at minimising harm or rectifying incidents.

- **Directive Controls:** Guide or influence behaviour and processes to reduce the likelihood of incidents. Examples include clear policies, SOPs, training modules, and leadership directives. These controls also impact on the likelihood of risks
- **Detective Controls:** Identify when a risk has materialized, allowing early intervention to prevent escalation. Examples include widespread testing and environmental monitoring tools.

Summary Table

Control Type	Purpose	Effect on Risk Score
Preventive	Stop the risk from occurring.	Reduces likelihood.
Corrective	Minimize harm if the event occurs.	Reduces impact.
Directive	Guides behaviours to avoid risks.	Reduces likelihood.
Detective	Identify issues early.	Reduces likelihood and impact.

All risks that are been treated will have the status of been a **live** risk and will be reviewed monthly. Reviews will assess how effectively controls are working and whether current risk levels have improved.

7.3.2 Tolerate

Tolerating a risk means accepting the residual risk level without taking further actions to mitigate it, provided it remains within the Trust's appetite or cannot be cost-effectively reduced further. Risks that are tolerated will have **tolerated status** on the risk register and will be reviewed every quarter to ensure they remain stable and do not escalate.

7.3.3 Transfer

Transferring a risk involves shifting the financial or operational consequences of the risk to a third party, often through insurance or contractual agreements.

7.3.4 Terminate (Avoid)

Terminating a risk involves discontinuing the activity or process that generates the risk, so it is no longer an issue for the Trust. If an activity is not central to RDaSH's mission and poses undue risk, it may be discontinued to protect resources or avoid compliance breaches.

7.3.5 Criteria for Risk Treatment

Risk Score	Recommended Treatment Option(s)	Criteria	Review Frequency
1 – 3 (Low)	**Tolerate** (Treat only if further mitigation is straightforward and cost-effective)	Risk falls well within the Trust's appetite. - Further controls would be disproportionate. - Likelihood typically **1 or 2** (Rare/Unlikely).	Bi-Annually

Risk Score	Recommended Treatment Option(s)	Criteria	Review Frequency
4 – 6 (Moderate)	**Treat or tolerate**	Risk is within or slightly above acceptable boundaries. - If likelihood ≤ 2, may still tolerate if cost-benefit of extra controls is negative. - If likelihood ≥ 3, treat unless authorized otherwise by RMG	Quarterly if tolerating. Monthly if treating
8 – 12 (High)	**Treat** (or tolerate only with authorization form RMG)	Risk surpasses normal tolerance and typically has a **likelihood ≥ 3** or **impact ≥ 3**. - Additional controls are feasible.	Monthly
15 – 25 (Extreme)	**Treat**, **Transfer**, or **terminate**	Risk is unacceptable under normal circumstances (e.g., serious patient safety issues). - If no feasible controls exist, consider terminating the activity or service. - Transfer if an external party can manage better.	Monthly, with monthly escalation and moderation by RMG.

7.4 Monitoring, Review and Escalation

7.4.1 Monitoring and Review

Monitoring involves the continuous oversight of risks to ensure that new risks are recorded, existing risks are effectively managed, and all treatments stay aligned with the Trust's risk framework and appetite.

Because risks evolve with changes in both the external and internal environments, regular reviews help track how quickly a risk may develop, and whether mitigation efforts remain timely and effective. These reviews also re-evaluate action plans to confirm that initial assumptions still apply—without periodic checks, a mitigation measure could itself become a hidden risk.

All risk registers, which are managed on the Risk Management System (RMS) contains risks managed at directorate level and each risk is allocated a Risk Owner. The Risk Owner is responsible for taking appropriate action and ensuring the risk is kept current, with updates recorded in line with the status of the risk i.e. live risk or tolerated risk.

Each risk is allocated a Director of the Board and along with the risk owner, are responsible for ensuring changes to the risk are captured, that actions are implemented, and the risk is updated accordingly. Reviews of each risk are to be undertaken with support from the Head of Risk Management as follows:

- 'Live'/Treated risks on at least a monthly basis
- 'Tolerated' risks on at least quarterly basis

All risks must be robustly and routinely monitored and updated, and the following should be considered:

- Risk Description – does it still reflect the current situation and potential/actual impact of the risk occurring?
- Gaps in control/assurance – are all gaps covered?
- Actions:
    - what is the progress being made?
    - have the actions created new controls? If so, does this now affect the risk scoring, can it be reduced?
    - Are more actions required?

1. Tolerated risks
    - is the risk still to be tolerated?
    - are the controls up to date and still in place/ are there any additional controls to be added?

Action plan due dates drive timely and effective risk mitigation. Progress is tracked against these timelines, and any delays require a clear justification and approval for revised deadlines. Due dates should be realistic, reflecting resource availability and operational constraints, and must not be changed arbitrarily.

The risk management team meets regularly (usually monthly for most directorates) to review emerging or evolving risks. At least once a year, a high-level review of risk registers and key controls confirms continued alignment with strategic objectives and regulations. Strategic-level risks are also cross-referenced with the SDR, ensuring top-level threats and opportunities remain visible and up to date.

7.4.2 Assurance Over Controls

Control assurance at RDaSH evaluates whether each proposed or existing control is suitably designed to address an identified risk. It focuses on reducing the likelihood or impact of a risk by verifying the control's design adequacy and relevance. Actual implementation effectiveness is assessed through independent reviews (e.g., Internal Audit)

1. **Assignment of Control Review**
    - The Head of Risk Management (HoRM) may assign new or revised controls to a relevant technical department (e.g., IT for cyber risks). The department checks if the proposed control follows best practices and tackles the identified vulnerabilities.
2. **Scope of Evaluation**

Experts confirm whether the control:

- Targets the risk's root cause.
- Meets regulatory or compliance obligations.
- Is robust enough to lower the likelihood or impact.
- They may recommend additional or alternative controls if needed

3. **Levels of Assurance on Control Selection**

Based on the technical review, an assurance level is assigned in the risk management system to reflect confidence that the correct control has been identified and recommended:

- **Minimal Assurance**: Little confidence the control addresses core risk drivers. Major redesign or alternative solutions may be needed.
- **Limited Assurance**: Partial alignment with the risk; gaps or uncertainties remain. Further refinement or supplemental measures are advised

- **Substantial Assurance:** Strong confidence the control addresses primary causes and meets standards. Only minor improvements might be suggested.
- **Full Assurance:** Complete alignment with best practice; no further design changes are necessary.

4. **Reporting and Continuous Improvement**
    - The assigned assurance level is recorded in the risk register, providing clear visibility of whether the control design is adequate.
    - Moderate risks with Minimal or Limited Assurance are escalated to the Risk Management Group (RMG), which may seek alternative solutions, request more detailed proposals, or involve additional experts.
    - High or Extreme risks require strong confidence and should have controls rated at least Substantial. If any such risk has Limited or Minimal Assurance, it is also escalated to the RMG.
    - Internal Audit or other independent reviewers may periodically or on demand verify that controls are properly implemented and effectively reducing risk.

7.4.3 Closing a Risk

- Closing a risk formally ends active management because it is either mitigated to an acceptable level or no longer relevant. Before closing:

- **Mitigation Success**: All actions and controls are in place, with evidence the residual risk is now acceptable
- **Sustained Improvements**: Reviews confirm no likely re-escalation of the risk.
- **Documentation and Verification**: The risk register is updated with the final assessment and rationale.
- **Approval and Communication**: Closure is approved by the relevant manager and verified by the Head of Risk Management, then communicated to stakeholders.

Closed risks remain in the historical record for reference in future assessments and audits. Periodic reviews confirm that conditions haven't changed enough to require reopening or reclassifying the risk.

7.4.4 Reporting

Timely and accurate reporting keeps everyone from frontline teams to Board-level committees informed about current risk exposures, mitigation actions, and emerging trends.

Escalation for strategic risks will be to the Board of Directors as follows Approves changes to risk descriptions and scores.

- Agree any change of risk description
- Agree and increase or decrease in risk score
- Provide support where the implementation of the action plan is not producing the anticipated results and further support, and guidance is required

Risk Management Group (RMG)

- Receives detailed reports on new or evolving risks.
- Identifies when more support or escalation is needed.
- Reviews exceptions (e.g., tolerating higher risk levels, severe incidents impacting strategic goals).

Strategic Delivery Risk (SDR)

- Highlights key strategic risks and aligns them with Trust-wide objectives.

- Summaries from SDR ensure the Board and committees maintain oversight, directing resources to critical threats or opportunities.

Board Audit Committee

- Receives regular updates on the implementation and performance of the Risk Management Framework.
- Monitors staff training, the effectiveness of controls, and adherence to risk management procedures.

Clinical Leadership Executive (CLE)

- Reviews regular risk reports related to their areas.
- Receives updates from the Head of Risk Management at scheduled committee meetings

8. Risk Appetite and Statement

The Trust recognises that it is impossible to deliver its services and achieve positive outcomes for its stakeholders without taking risks. Only by taking risks can the Trust realise its aims. It must, however, take risks in a controlled manner, thus reducing its exposure to a level deemed acceptable from time to time by the Board and, by extension, external inspectors/regulators, and relevant legislation. This is the risk appetite – defined as “the amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time” (HM Treasury Orange Book).

“The Trust recognises that its long-term sustainability depends on the delivery of its strategic objectives and, its relationships with its communities, including service users and families, the public and partners. Patient and staff safety is paramount and as such the Trust will not accept risk that materially provide a negative impact on quality and governance. The Trust acknowledges the challenging business environment in which it operates and has a greater appetite to take considered risks in terms of the impact to achieve innovation and excellence.”

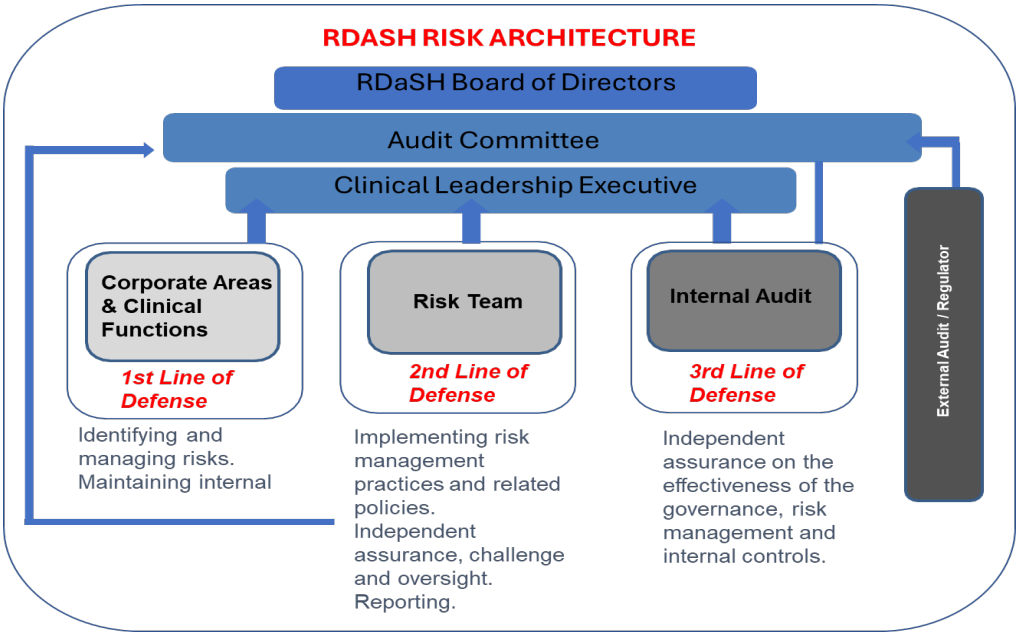
In agreeing the Strategic Delivery Risk, the Board will consider and agree a risk appetite statement in respect of each strategic risk. The risk appetite framework contains details and levels of risk the trust is willing to accept in the achievement of its objectives.

9. Risk Governance

Risk Governance in the trust provides the framework of roles, responsibilities, and structures through which risks are identified, escalated, and monitored. It ensures alignment between day-to-day operational activities and the strategic direction set by the Board of Directors.

9.1 Assurance

At its core, risk governance ensures accountability at all levels of the organization. The Board of Directors sets the strategic direction, defines the Trust's risk appetite, and oversees significant or emerging risks through the Strategic Delivery Risk (SDR). The Audit Committee scrutinizes the effectiveness of internal controls and governance processes, ensuring that risk management practices are robust and aligned with best practices.



Operational oversight is provided by the Risk Management Group (RMG), which acts as a central hub for coordinating risk activities. It reviews risk registers, authorizes exceptions to standard treatment criteria, and escalates unresolved or extreme risks to the Executive Management Team or the Board. Frontline teams, supported by line managers, are responsible for day-to-day risk identification and treatment, with guidance and technical support from the Risk Management Team

The Trust's governance model is aligned with the Three Lines of Defence framework. Frontline teams and managers form the first line, owning and managing risks within their domains. The second line consists of oversight functions, such as the Risk Management Team, providing frameworks, tools, and guidance. Independent audits and regulatory reviews form the third line, offering assurance that the system is functioning as intended.

9.2 Roles and Responsibilities

The board of Directors is responsible for:

- Setting the vision, mission, and strategic direction for RDaSH, including the overarching risk appetite and tolerance levels.
- Endorses the Risk Management Framework and ensures resources are available for its effective implementation
- Receives and reviews high-level risk reports (e.g., via the Strategic Delivery Risk), holding senior executives to account for managing significant or emerging risks.

- Ensuring that roles and responsibilities for risk management are clear to support effective governance and decision-making at each level with appropriate escalation, aggregation and delegation.
- Assessing compliance with the Corporate Governance Code and ensures that explanations of any departures are recorded within the governance statement of the annual report and accounts.

The Audit Committee is responsible for supporting the Board of Directors in leading the assessment and management of risk through:

- Critically challenging and reviewing the risk management framework, to evaluate how well the arrangements are actively working in our Trust.
- Conducts independent scrutiny of the Trust's internal controls and risk management processes
- Advises the Board of Directors on significant risks or deficiencies in the Trust's risk management practices, ensuring appropriate escalation and resolution
- Reviews the performance of the Risk Management Framework to ensure it remains effective and relevant, making recommendations for updates or enhancements as needed.
- Critically challenging and reviewing the adequacy and effectiveness of control processes in responding to risks within our Trust's governance, operations, compliance and information systems.

The Chief Executive as accounting officer for the trust's risk management activities is responsible for**:**

- ensuring that expected values and behaviours are communicated and embedded at all levels to support the appropriate risk culture.
- demonstrating leadership and articulate their continual commitment to and the value of risk management.
- ensuring that risk is considered as an integral part of appraising option choices, evaluating alternatives and making informed decisions.
- Allocates appropriate resources for managing and mitigating risks

The Clinical Leadership Executive is responsible for

- Ensuring risk management is embedded into all processes.
- Ensure that risk management activities align with the Trust's strategic objectives and risk appetite, addressing risks that could impact organizational priorities
- Act as the escalation point for unresolved or Extreme risks, ensuring timely decisions and actions are taken to mitigate threats.
- Lead by example to foster openness and proactive risk management throughout the organization, emphasizing learning and continuous improvement.

The Risk Management Group is responsible for

- Acts as the Trust-wide hub for risk oversight, consolidating updates from various departments and projects.
- Monitors the Trust's risk registers, ensuring risks are consistently identified, scored, and escalated.
- Ensures action plans for high or extreme risks are executed effectively, tracking progress and identifying resource needs
- Escalates unresolved or particularly severe risks to the Clinical Leadership Executive

- Overseeing work to mitigate risks, supporting leaders to do so, where necessary by bringing together expertise across the group
- Taking responsibility for resolving *cross-trust* risks that are thematic or escalating such concerns for resolution through the Clinical Leadership Executive (CLE) and/or within delivery reviews
- Ensuring that the risk management framework is being implemented effectively and to advise CLE or the Audit Committee where this is not the case
- Ensuring that risks to delivery of the strategy are reflected within the risk register or, where relevant, the Strategic Delivery Risk.

The Director of Corporate Assurance/Board Secretary is responsible for ensuring that all risk and assurance processes are devised, implemented and embedded throughout the Trust and for reporting of any significant issues arising from the implementation of the Framework including non-compliance or lack of effectiveness arising from the monitoring processes. Additionally advises the Board, Chief Executive, and other senior leaders on critical governance or assurance gaps that could expose the Trust to unacceptable levels of risk.

The Head of Risk Management is responsible for

- Maintaining, updating, and disseminating the Risk Management Framework, policies, and procedures
- Provides tools, training, and advice to line managers, risk owners, and project managers on risk identification, assessment, and treatment.
- Prepares high-level risk analyses and dashboards for the Risk Management Group, Executive Management Team, and the Board.
- Ensuring risks are articulated clearly, scored consistently using the Trust's risk matrix, and classified appropriately in alignment with the Risk Management Framework and Risk Appetite.
- Monitor and oversee the Trust-wide risk registers, ensuring all risks are documented, regularly updated, and linked to the Trust's strategic objectives or operational priorities.
- Design and deliver risk management training programs to staff and managers, fostering a culture of proactive risk awareness and competence across the Trust.
- Work with departments, clinical teams, and corporate functions to integrate risk management practices into their day-to-day activities and decision-making processes.

All Staff

- Identify and report potential risks, incidents, or near misses promptly
- Adhere to established policies, standard operating procedures, and mitigation measures
- Take part in risk-related training and actively contribute to a culture of continuous improvement
- Escalate any developments that might raise the likelihood or impact of known risks

Line Managers

- Own and manage risks within their departments or services
- Ensure risks are documented, scored, and treated according to Trust policy
- Escalate High or Extreme risks to the Risk Management Group or senior leadership

- Oversee the implementation of action plans and monitor the effectiveness of controls

Risk Owners

- Assume primary accountability for assigned risks, including developing and tracking mitigation actions
- Reassess residual risk regularly and update registers to reflect status
- Communicate progress, challenges, or changes to line managers and relevant committees
- Document all relevant information on causes, controls, and potential impacts

Project Managers

- Identify and manage project-specific risks throughout the project lifecycle
- Align project risk management activities with the Trust's overall Risk Management Framework
- Conduct regular project risk reviews, updating registers and action plans as needed

10. Risk Registers

The Risk Register is both a recording and management tool for all identified risks within RDaSH. In addition to serving as a single repository for detailed risk information, it provides a structured way to track, prioritize, and address risks throughout their lifecycle.

All risks are recorded on a risk register which is the formal record of the risks that the Trust has identified. There are 23 risk registers within the Trust, one for each of the 23 directorates in RDaSH.

10.1 Integration of Other Risk Registers

In addition to the Trust's central risk registers, Certain specialized areas (e.g., fraud, EPRR, climate resilience, and cybersecurity) keep separate risk registers for specific compliance or operational needs. Any risks in these registers that exceed the Trust's risk appetite are escalated and added to the corporate Risk Register. This ensures a comprehensive view of all significant exposures, consistent reporting, effective decision-making, and timely cross-functional collaboration when extra resources are required

11. Training and Development

Staff can complete the mandatory "000 Risk Management and Governance" training on ESR and are encouraged to undertake additional short video modules on risk and risk management. Risk owners responsible for directorate-level registers have access to one-to-one training with the Risk Management Team, supported by an Easy Step Guide.

This section should be read alongside the Risk Management Training Framework, which details the Trust's mandatory training, advanced courses for specific roles, and refresher sessions. Together, these resources ensure all staff are equipped to identify, assess, and manage risks effectively.

12. Risk System

RDaSH uses a dedicated risk system called RADAR as the central platform for capturing, storing, and monitoring all identified risks. Staff at every level can log new risks, update records, and access real-time data, supporting timely, informed decision-making. The system's tiered permission structure (view-only, edit, approval) ensures data integrity and security, with access levels aligned to each user's risk management responsibilities. The Head of Risk Management oversees the system, keeping it current and aligned with organizational goals.

13. Emergency Preparedness, Resilience and Response (EPRR)

RDaSH is committed to safeguarding its services and ensuring a coordinated response during major incidents or disruptions. The EPRR Team oversees planning, training, and exercises that strengthen the Trust's ability to maintain patient care and protect staff under challenging circumstances. The Trust's EPRR Team will maintain a Trust-wide register for all EPRR risks within the Trust. This register will be produced in line with the Trust EPRR Policy. The EPRR Group reviews all risks on the EPRR risk register on a bi-monthly basis, escalating risks within defined parameters to the corporate risk register and review by the Risk Management Group where necessary.

14. Continuous improvement

The Risk Management Framework is dynamic, evolving with new risks, organizational changes, and audit feedback. Changes follow a structured review process involving performance assessments, stakeholder consultations, and periodic reviews by the Risk Management Group (RMG). All proposed updates are documented, reviewed by the Head of Risk Management and Director of Corporate Assurance, and approved by both the RMG and Board of Directors.

If no urgent issues or audit findings arise, the framework undergoes a formal review every four years. This ensures it remains effective, current, and aligned with the Trust's strategic objectives and best practices, supporting robust risk management across RDaSH.

15. Issue Logs

The Issue Log is an optional tool for directorates to capture and track operational challenges, process weaknesses, or near misses. Its primary purpose is to keep the Risk Register focused on strategic risks by separating routine issues that don't meet the threshold for formal risk classification.

- **Details are Recorded**: Include a brief description, potential causes, proposed corrective actions, and responsible individuals
- **Regular Review is Conducted**: Management periodically reviews the log, tracks progress and decides if any issues need escalation to the formal risk management process.
- **Integration with Risk Management**: Persistent or broadly significant issues that become risks should be escalated and added to the Risk Register through established channels.

16. Equality Impact Assessment Screening

The completed Equality Impact Assessment for this Policy has been published on this policy's webpage on the Trust Policy Library/Archive website.

16.1 Privacy, Dignity and Respect

Requirement - The NHS Constitution states that all patients should feel that their privacy and dignity are respected while they are in hospital. High Quality Care for All (2008), Lord Darzi's review of the NHS, identifies the need to organise care around the individual, 'not just clinically but in terms of dignity and respect'.

Consequently, the Trust is required to articulate its intent to deliver care with privacy and dignity that treats all service users with respect. Therefore, all procedural documents will be considered, if relevant, to reflect the requirement to treat everyone with privacy, dignity, and respect, (when appropriate this should also include how same sex accommodation is provided).
Trust Response – No issues have been identified in relation to this policy.

16.2 Mental Capacity Act

Requirements - Central to any aspect of care delivered to adults and young people aged 16 years or over will be the consideration of the individual's capacity to participate in the decision-making process. Consequently, no intervention should be carried out without either the individual's informed consent, or the powers included in a legal framework, or by order of the Court.

Therefore, the Trust is required to make sure that all employees working with individuals who use our service are familiar with the provisions within the Mental Capacity Act. For this reason, all procedural documents will be considered, if relevant to reflect the provisions of the Mental Capacity Act 2005 to ensure that the rights of individual are protected, and they are supported to make their own decisions where possible and that any decisions made on their behalf when they lack capacity are made in their best interests and least restrictive of their rights and freedoms.
Trust Response - All individuals involved in the implementation of this policy should do so in accordance with the Principles of the Mental Capacity Act 2005.

17. Links to Associated Documents

The Risk Management Framework is supported by the Trusts suite of policies as listed on the RDaSH website. There is a strong link to a range of policies including:

- Risk Appetite Framework
- Clinical Risk Assessment and Management Policy
- Incident Management Policy
- Listening and Responding to Concerns and Complaints Policy
- Suite of Health & Safety policies
- Claims Handling policy
- Standing Financial Instructions
- Information Risk Management Policy

18. References

The Orange Book - Management of risk – Principles and Concepts
https://assets.publishing.service.gov.uk/media/6453acadc33b460012f5e6b8/HMT_Orange_Book_May_2023.pdf

From the cube to the rainbow double helix: a risk practitioner's guide to the COSO ERM Frameworks
https://www.theirm.org/media/6885/irm-report-review-of-the-coso-erm-frameworks-v2.pdf

Understanding, Evaluating and Implementing Effective Enterprise Risk Management
6th Edition, Hopkin and Thompson

Appendix 1 – Monitoring and Evaluation Arrangements

Both operational and strategic risk is subject to continual review and monitoring by the relevant meeting structure, and this is facilitated by the Corporate Assurance Team in producing reports as outlined below.

Strategic Risk Oversight

Board of Directors will receive reports on:

- All strategic risks within Strategic Delivery Risk for approval - as and when required.
- Any changes to the strategic risk description and /or risk scoring for approval - as and when required.
- Oversight on progress of mitigation of all the strategic risks within Strategic Delivery Risk – 3 times a year.
- Extreme rated operational risks – as when identified.

Board Committees will receive reports on:

- Oversight on progress of mitigation of the strategic risks within Strategic Delivery Risk as assigned to the applicable Committee(s) – 3 times a year.
- Any changes to the risk description and /or risk scoring to provide comment and recommend approval - as and when required.

Systems of Internal Control Oversight

Audit Committee will receive reports on:

- An overview of risk management which outlines the process for managing and monitoring risk and provides assurance on achievement to date - each meeting.
- An annual evaluation of the implementation and impact of the Risk Management Framework, confirming that all aspects of the Framework have been completed. This includes the receipt and acceptance of the Framework (and its requirements) by designated staff, in line with the Trust's Policy tracking mechanism.
- Risk management as undertaken by the Trust's Internal Auditors on a cyclical basis. Risk management and governance are standing items within their plan and their work to deliver the Head of Internal Audit Opinion.

Operational Risk Oversight

Clinical Leadership Executive will receive reports on:

- Outbrief from the Risk Management Group summarising decision and any areas of escalation.
- Extreme rated risks – as and when identified

Risk Management Group will receive reports on:

- Longstanding risks – on a rolling programme basis
- Thematic reviews – on a rolling programme basis
- Cross Trust risks – on an as and when basis
- Escalating risks – on an as and when basis

- Compliance data (for example the frequency of reviews undertaken by risk owners) – on a rolling programme basis

Delivery Review meetings will receive reports on based on the applicable risk register:

- Current state of risks – each meeting
- Top 3 risks – each meeting

Care Group Business meetings will**:**

- have oversight of the Care Group risks – at each meeting.

Risk Owners will:

- monitor and review all live risks on a monthly basis.
- monitor and review all tolerated risks at least quarterly (high/Moderate risks) /annually (low risks).
- escalate any risks deemed to be extreme to the Risk Management Group for moderation and approval though the Head of Risk Management.
- escalate any risks that require further support and guidance to the Risk Management Group.

Appendix 3 – Risk Scoring Methodology

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.

Impact score	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 On-going unsafe staffing levels or competence Loss of several key staff No staff attending mandatory training /key training on an on-going basis
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

Impact score	1	2	3	4	5
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
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
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 Claim(s) >£1 million
Information Governance/ Confidentiality / Information security	Minor breach of confidentiality. Less than 5 people affected or risk assessed as low e.g. media interest unlikely, small number of encrypted files.	Serious potential breach and risk assessed high e.g. unencrypted clinical records lost. Up to 20 people affected.	Serious actual breach of confidentiality affecting up to 100 people, media interest and damage to reputation possible. Reportable as an SI if encrypted	Serious actual breach of confidentiality involving particularly sensitive records (e.g. sexual health or child protection) affecting up to 1000 people. Media interest and damage to reputation Reportable as an SI	Serious actual breach of confidentiality involving over 1000 individuals. Damage to reputation, national media coverage, potential for litigation or prosecution of Trust under Data Protection Act. Reportable as an SI and Information Commissioner
Objectives / Project	Barely noticeable reduction in scope/ schedule Insignificant cost increase /schedule slippage	Minor reduction in scope / quality/ schedule <5 per cent over project budget. Schedule slippage	Reduction in scope or quality, project objectives or schedule 5-10 per cent over project budget. Schedule slippage	Non-compliance with national project 10-25 per cent over project budget Schedule slippage Key objective not met	Incident leading to significant inability to meet project objectives, reputation of the organisation seriously damaged >25 per cent over project budget. Schedule slippage Key objectives not met
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

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	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it is not a persisting issue	Will undoubtedly happen/recur, possibly frequently
Probability	**0- 5%** Extremely unlikely or virtually impossible	**6 – 20%** Low but not impossible	**21 – 50%** Fairly Likely to occur	**51 – 80%** More likely to occur than not	**81 – 100%** Almost certainly will occur

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

For grading risk, the scores obtained from the risk matrix are assigned grades as follows

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

Instructions for use

1 Define the risk(s) explicitly in terms of the adverse consequence(s) that might arise from the risk.

2 Use table 1 (page 13) to determine the impact score(s) (I) for the potential adverse outcome(s) relevant to the risk being evaluated.

3 Use table 2 (above) to determine the likelihood score(s) (L) for those adverse outcomes. If possible, score the likelihood by assigning a predicted frequency of occurrence of the adverse outcome. If this is not possible, assign a probability to the adverse outcome occurring within a given time frame, such as the lifetime of a project or a patient care episode. If it is not possible to determine a numerical probability then use the probability descriptions to determine the most appropriate score.

4 Calculate the risk score the risk multiplying the consequence by the likelihood: I (impact) x L (likelihood) = RS (risk score)

5 Identify the level at which the risk will be managed in the organisation, assign priorities for remedial action, and determine whether risks are to be accepted on the basis of the colour bandings and risk ratings, and the organisation's risk management system. Include the risk in the organisation risk register at the appropriate level.

Appendix 4 – Risk Form

Date Identified	Click here to enter a date.	**Source**	Choose an item.
RISK DESCRIPTION			
What is Causing the risk? **(Due to/If)**			
What is the specific risk or issue? **(there is a risk that…)**			
What could happen if this risk occurs? **(Which may result in/Could/Would lead to)**			
Risk Description in full (combination of cause, risk, and effect)			
RISK OWNER AND DIRECTORATE			
Accountable Director	Choose an item.	**Risk lead**	
Care Group/ Directorate/Project Log	Choose an item.	**Mitigation managed**	Choose an item.
Monitoring Committee			
EXISTING CONTROLS			
Control 1			
Control 2			

Control 3			
Control 4			
RISK SCORING			
Current Impact Score	Choose an item.	**Current Likelihood Score**	Choose an item.
Rationale or Justification for Scoring: (Why was this likelihood and impact score selected? Provide a justification based on the available data or evidence.)			

PROPOSED ACTIONS/ADDITIONAL CONTROLS			
	Action	**Action Owner**	**Target Completion Date**
1.			Click here to enter a date.
2.			Click here to enter a date.
3.			Click here to enter a date.
4.			Click here to enter a date.

RISK TREATMENT			
Risk Treatment	Choose an item.		
Target Impact Score	Choose an item.	**Target Likelihood Score**	Choose an item.

Appendix 5 – Risk Classification Definitions

People Risk	The risk of not having a sufficient, healthy, capable and appropriately deployed workforce to deliver services safely and sustainably.
Planning & Supply Risk	**Securing and forecasting sufficient numbers and skill-mix of staff (recruitment, succession, training pipelines) for clinical and backbone services**
Capacity Risk	**To ensure the Trust deploys effectively the right mix of skills and capacity.**
Well-being and Retention Risk	**To ensure the Trust retains the right people with the right skills and supports the mental and physical health of its staff, preventing burnout and stress.**
Capability and Performance Risk	**Ensuring colleagues possess the competence, training and productivity needed to meet clinical and corporate standards**

Financial Risks	The risk of financial loss, mismanagement, or unsustainable planning that impacts the Trust's ability to deliver services, invest in future priorities, or comply with financial and regulatory expectations. This includes planning, oversight, control, and fraud-related exposures.
Financial Planning, CIP & Sustainability Risk	The Trust's ability to balance income, expenditure and capital over the planning cycle, including delivery of cost-improvement plans, cash-flow and access to capital funding and capacity to achieve best value for money through procurement, contract management, productivity benchmarking and whole-life costing of assets and services
Counter Fraud Risk	The adequacy of preventative and detective measures that deter, detect and respond to fraud, bribery, corruption or other irregularities that could cause financial loss or reputational damage. (internal and external) from committing acts of fraud against the Trust and its patients.
Financial Control and Compliance	Effectiveness of the Trust's financial governance to safeguard resources and meet regulatory requirements and ensure that financial information reported internally and externally is correct, true and fair and does not contain material misstatement

Patient Care Risks	The risk that care delivered fails to meet required safety, quality, and experience standards. This includes risks of clinical harm, ineffective improvement efforts, poor learning systems, or suboptimal patient involvement that compromise outcomes or regulatory compliance.
Clinical Safety Risk	Potential for service-users to experience physical or psychological harm because safety controls or practices are ineffective.
Quality Improvement Risks	Potential for improvement initiatives to be poorly prioritised, resourced, designed, implemented or evaluated
Learning and Oversight Risks	The risk of weaknesses in oversight, assurance, incident investigation, audit or organisational learning to limit continuous improvement of care quality.
Patient Experience Risks	To ensure the Trust meets patient, carer and family expectations of dignity, involvement, communication and satisfaction.

Performance Risks	The risk that operational systems and support infrastructure fail to meet service, resilience, or compliance expectations. This covers emergency preparedness, demand-capacity mismatch, estates and equipment, digital infrastructure, information governance, and overall delivery capability.
Emergency Preparedness Risk	Readiness to withstand, respond to and recover from disruptive events—pandemic, flood, cyber-attack, mass-casualty, utility loss—while maintaining critical functions.
Capacity & Demand Management	The organisation's ability to match beds, clinic slots, caseloads and workforce hours to actual and forecast demand so that waiting-time, flow and productivity targets are met.
Estates, Equipment & Supply Chain Risk	The condition, suitability and resilience of the Trust's physical estate, engineering plant, medical devices, fleet and supply chains, including PPE, drugs and consumables—so they support safe, continuous care.
Information Governance Risk	To ensure that the Trust has the right processes and systems for collecting, storing, managing and maintaining information (includes archiving and deletion) in all its forms to support business needs and comply with regulations.

Digital Infrastructure & Cyber Security Risk	Reliability, availability and performance of networks, servers, clinical applications and end-user devices, together with technical cyber-defence measures that protect them

External and Partnerships Risks	**The risk arising from the Trust's interface with external stakeholders, legal frameworks, strategic partners, and regulatory bodies. This includes the risk of failure to comply, collaborate, deliver agreed outcomes, or influence change in ways that affect strategic goals or reputation.**
Change and Improvement Delivery Risk	Capability to plan, resource, govern and realise the benefits of strategic programmes, digital deployments, estate redevelopments and service redesigns within agreed scope, time and cost.
Legal & Governance Risk	Complying with statutory obligations (e.g., Mental Health Act, GDPR, Health & Safety) and corporate-governance duties to avoid litigation or sanctions.
Partnership Working Risk	To ensure the Trust has effective partnership working arrangements in place, working in conjunction with health, social care, voluntary, local authorities and private sectors
Regulatory Risk	To ensure the Trust has effective processes in place for monitoring performance and progress against regulatory standards, including constitutional standards as set out in the national Contract, liaising with local and specialist commissioners.
Delivering our promises Risk	The possibility that the Trust fails to honour the commitments, service standards or partnership deliverables it has agreed with patients, communities, commissioners or partner organisations, resulting in loss of trust, reputational damage, strained relationships and reduced future collaboration

NHS
Rotherham Doncaster
and South Humber
NHS Foundation Trust

Risk Appetite Framework

Table of Contents

Section 1: Our Risk Management Framework 3

Framework Summary 3

Common Risk Language 3

Risk Types 3

Section 2: Our Risk Appetite 4

Background 4

Why is Risk Appetite important? 4

Definitions 4

Risk Appetite Scales 5

Risk Appetite Statements by Categories 5

Section 3: Applying Risk Appetite 8

Risk Tolerance Bands 8

Risk Appetite Breaches 9

Appendix A - Risk Types and Risk Categories 10

Appendix B - Risk category Definitions 11

Appendix C- Appetite Levels by Risk Category 15

Section 1: Our Risk Management Framework

Framework Summary

The Risk Management Framework explains how a variety of processes fit together to create a consistent and effective way of managing risk across the Trust. The key elements of risk management encompass the activities relating to risk identification, assessment, control, monitoring and reporting of risk. The framework promotes an open risk culture, encouraging staff at all levels to raise concerns and proactively manage uncertainty. It supports both upward escalation of risks that may impact strategic delivery and downward alignment of risks to local service areas, ensuring a dynamic connection between operational realities and strategic oversight.

A standardised classification system is in place to help structure risks by theme, and risk scoring is guided by Trust-wide impact and likelihood matrices. The framework is underpinned by regular training, continuous improvement, and assurance mechanisms to test the effectiveness of controls. This framework is reviewed periodically and was most recently revised following wide consultation with stakeholders across the organisation to ensure it remains fit for purpose and reflective of the Trust's current operating context.

Common Risk Language

The Trust has defined five Risk Types (known as Level 1 Risk Types). These are the principal risks which arise from the nature of the Trust's operating environment. The Trust has also defined twenty-one Risk Categories (known as Level 2 Risk Categories), each aligned to one of the five Risk Types. These were determined by aligning the specific risks contained within the trust's risk registers to a broader risk category.

Appendix A sets out the list of the agreed Risk Types and Risk Categories.

Appendix B provides the definitions for each Level 2 Risk Category.

Risk Types

Definitions for each of the five Level 1 Risk Types are set out below:

- People Risk - The risk that the Trust is unable to attract, retain, deploy or support a capable and healthy workforce. This includes risks to workforce supply, capacity, wellbeing, and performance that could affect the safe and effective delivery of services.
- Financial Risks - The risk of financial loss, mismanagement, or unsustainable planning that impacts the Trust's ability to deliver services, invest in future priorities, or comply with financial and regulatory expectations. This includes planning, oversight, control, and fraud-related exposures.
- Patient Care Risks - The risk that care delivered fails to meet required safety, quality, and experience standards. This includes risks of clinical harm, ineffective improvement efforts, poor learning systems, or suboptimal patient involvement that compromise outcomes or regulatory compliance.
- Performance Risk - The risk that operational systems and support infrastructure fail to meet service, resilience, or compliance expectations. This covers emergency preparedness,

demand-capacity mismatch, estates and equipment, digital infrastructure, information governance, and overall delivery capability.

- External and Partnerships Risk - The risk arising from the Trust's interface with external stakeholders, legal frameworks, strategic partners, and regulatory bodies. This includes the risk of failure to comply, collaborate, deliver agreed outcomes, or influence change in ways that affect strategic goals or reputation.

Section 2: Our Risk Appetite

Background

The development of the Trust's risk appetite follows a period of growing maturity in how we identify, assess, and manage risk. As our strategic ambitions evolve and system pressures increase, setting clear appetite levels has become essential to guide decision-making, prioritise resources, and enable innovation where appropriate. This approach recognises that not all risks can or should be avoided and that informed risk-taking is sometimes necessary to deliver better outcomes. The appetite framework reflects both our internal priorities and the external environment we operate in and has been shaped through engagement with leaders across clinical, corporate roles.

Why is Risk Appetite important?

Risk appetite is more than a statement of preferred risk levels. It is a practical guide that shapes day to day choices and long-term commitments across the Trust. Clear appetite statements matter because they:

- Supporting informed decision-making;
- Reducing uncertainty;
- Improving consistency across governance mechanisms and decision making;
- Supporting performance improvement;
- Focusing on priority areas within the Trust; and
- Informing spending review and resource prioritisation processes.

Since budgetary constraints may prevent achievement of Risk Appetite (at least in the short-term), the defining of a Risk Tolerance enables the Trust to clearly set an acceptable position in pursuit of its strategy and vision.

Definitions

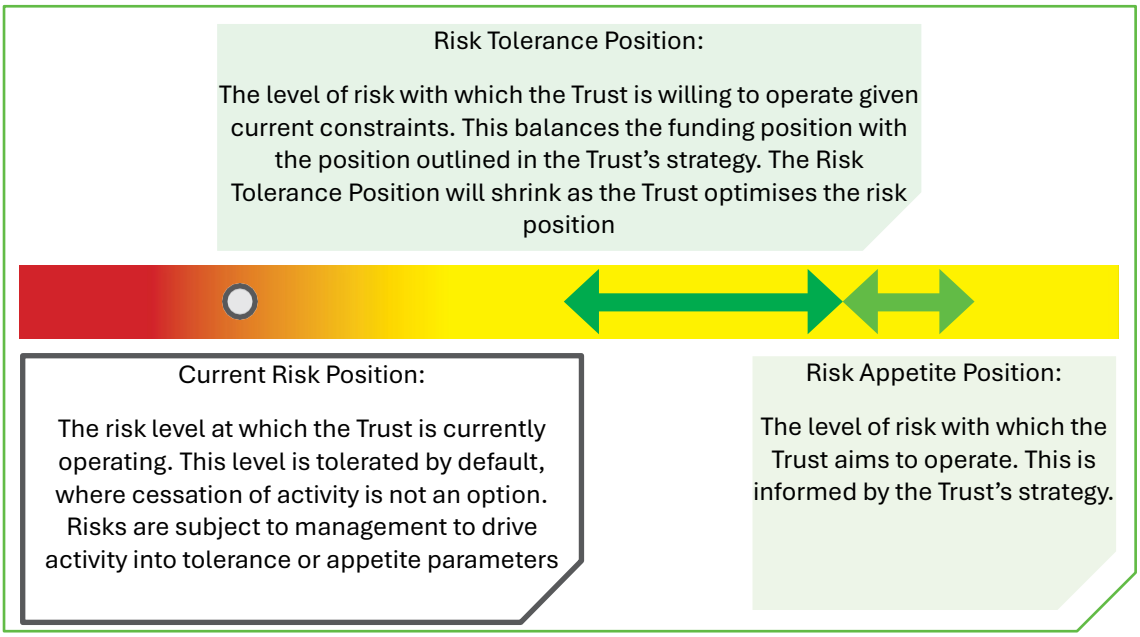
The Trust has adapted definitions for Risk Appetite and Risk Tolerance from the 'Orange Book – Risk Appetite guidance notes', Government Finance Function (October 2020), which are stated below:

Risk Appetite: the level of risk with which the Trust aims to operate.

Risk Tolerance: the level of risk with which the Trust is willing to operate.

It is worth noting that these terms should not be used interchangeably.

The diagram below demonstrates the interaction between these two concepts:



Risk Appetite Scales

Following consultation with the executive group, we have agreed to utilise the following risk appetite scales that broadly show the different appetites an organisation could have to meet its strategic objectives. See Appendix C:

1. Averse - We will not accept this risk under any circumstances; immediate mitigation or avoidance is required.
2. Low Tolerance- We accept only a small, tightly controlled exposure where benefits are essential, and controls are proven.
3. Moderate Tolerance - A balanced position: we will accept risk when the benefit clearly outweighs it and effective controls are in place.
4. High Tolerance- We are willing to take a sizeable, well-understood risk in pursuit of significant benefit, provided controls are monitored.

Risk Appetite Statements by Categories

The Trust has set out the Risk Appetite level for each Risk Type. While the matrix adopts the five-point scale for all risk types, the definition of what constitutes an 'averse Risk Appetite will differ across Risk Types.

1. People Risk

Sub-category	Appetite	Risk Appetite Statement
Planning & Supply	Moderate Tolerance	We will take calculated risks in developing new workforce pipelines and sourcing models, provided staffing remains safe and sustainable.

Sub-category	Appetite	Risk Appetite Statement
Capacity	Low Tolerance	We accept only minimal risk in having the right number and mix of staff; unsafe or inadequate coverage must be escalated immediately.
Well-being & Retention	Low Tolerance	We have low tolerance for working conditions or practices that may compromise staff wellbeing, morale, or retention.
Capability & Performance	Low Tolerance	We accept only minimal risk that staff lack the skills, training, or supervision required to meet clinical or operational standards.

2. Financial Risks

Sub-category	Appetite	Risk Appetite Statement
Financial Planning, CIP & Sustainability	Low Tolerance	We accept minimal risk in financial planning and cost improvement initiatives; budgets must remain balanced, and sustainability protected.
Counter Fraud	Averse	We have no tolerance for fraud, bribery, or corruption; all suspicions must be reported and addressed.
Financial Control & Oversight	Averse	We do not tolerate breaches of financial control or non-compliance with reporting and oversight requirements.

3. Patient Care Risks

Sub-category	Appetite	Risk Appetite Statement
Clinical Safety	Averse	We do not tolerate risks that could result in avoidable harm or serious compromise to patient safety.
Quality Improvement	High Tolerance	We support innovation and experimentation in quality improvement, accepting some controlled risk in pursuit of better outcomes.
Learning and Oversight	Low Tolerance	We accept minimal risk in the operation of governance, audit, and learning systems that assure care quality.
Patient Experience	Moderate Tolerance	We are willing to take limited risk to improve experience where dignity, communication, and outcomes are protected.

4. Performance Risks

Sub-category	Appetite	Risk Appetite Statement
Emergency Preparedness	Moderate Tolerance	We tolerate limited, well-managed risk to improve resilience and emergency response capability through ongoing learning and stress-testing.
Capacity & Demand	Low Tolerance	We accept minimal risk of demand exceeding capacity; service delays or access issues must be actively managed.
Estates, Equipment & Supply Chain	Moderate Tolerance	We accept limited risk while modernising our estate or reconfiguring supply chains, provided patient safety is not compromised.
Information Governance	Averse	We do not tolerate breaches of information confidentiality, integrity, or availability.
Digital Infrastructure & Cyber Security	Low Tolerance	We accept minimal risk to core digital infrastructure and cyber defences; outages or vulnerabilities must be minimised and quickly addressed.

5. External and Partnerships Risk

Sub-category	Appetite	Risk Appetite Statement
Change and Improvement Delivery	Moderate Tolerance	We are prepared to accept limited risk in delivering improvement programmes or transformation, provided governance remains effective.
Legal & Governance	Averse	We do not tolerate breaches of legal duties, regulatory obligations, or governance standards.
Partnership Working	High Tolerance	We are open to new partnerships and collaborations, accepting uncertainty where aligned to strategic goals and public benefit.
Regulatory	Averse	We do not tolerate non-compliance with regulatory standards and reporting obligations.
Delivering our promises	Low Tolerance	We accept minimal risk in failing to meet agreed commitments to our partners and communities; delivery must be reliable and transparent.

Section 3: Applying Risk Appetite

It is now essential that the Trust determines how best to embed its approach to Risk Appetite into routine planning and decision-making. To support this, the following key processes have been identified where active consideration of Risk Appetite is particularly important:

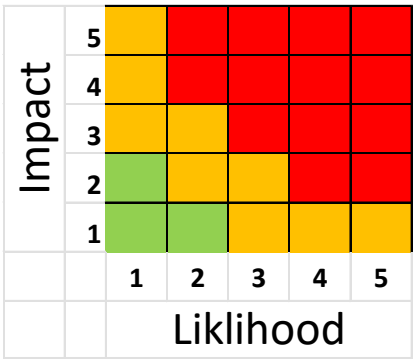
- Strategic Planning - Risk Appetite should be considered as part of strategic planning, ensuring that proposed objectives and initiatives align with the Trust's appetite for risk in relevant areas.
- Decision Making - Staff decision making as well as Committee proposals should consider their impact upon the Trust's risk profile and Risk Appetite adherence.
- Key Risk Escalations - Where risks are identified that do not adhere to the Trust's Risk Appetite, these instances must be escalated.
- Project and Programme Delivery – Using Risk Appetite to guide decision-making around innovation, resource allocation, and risk-taking in transformation efforts

Risk Tolerance Bands

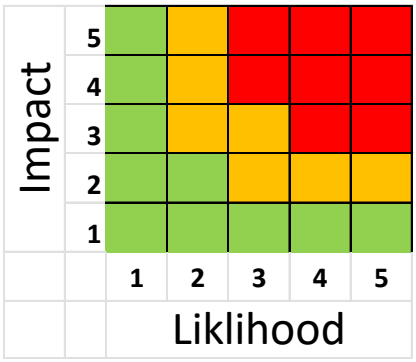
Appendix C sets out the appetite definitions for each Risk Type. While the matrix adopts the five-point scale for all Risk Types the definition of what constitutes a 'moderate tolerance' Risk Appetite will differ across Risk Types. Each appetite definition by Risk Category has also been aligned to the applicable residual risk score range, as per the Risk Scoring Matrix.

Illustrative Risk Appetite matrices have been set out below to show residual risk scores for the Risk Appetite scale, within Risk Appetite (Green), within Risk Tolerance (Amber) and outside of Risk Appetite and Tolerance (Red).

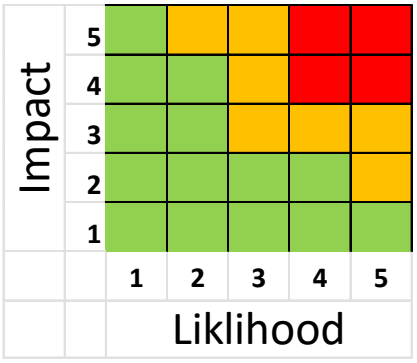
Averse



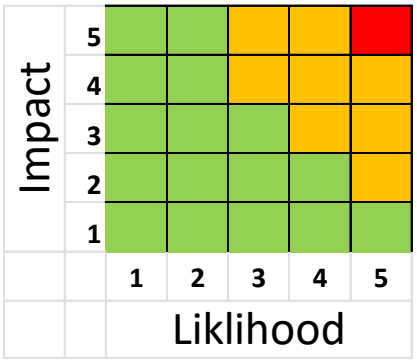
Low Tolerance



Moderate Tolerance



High Tolerance



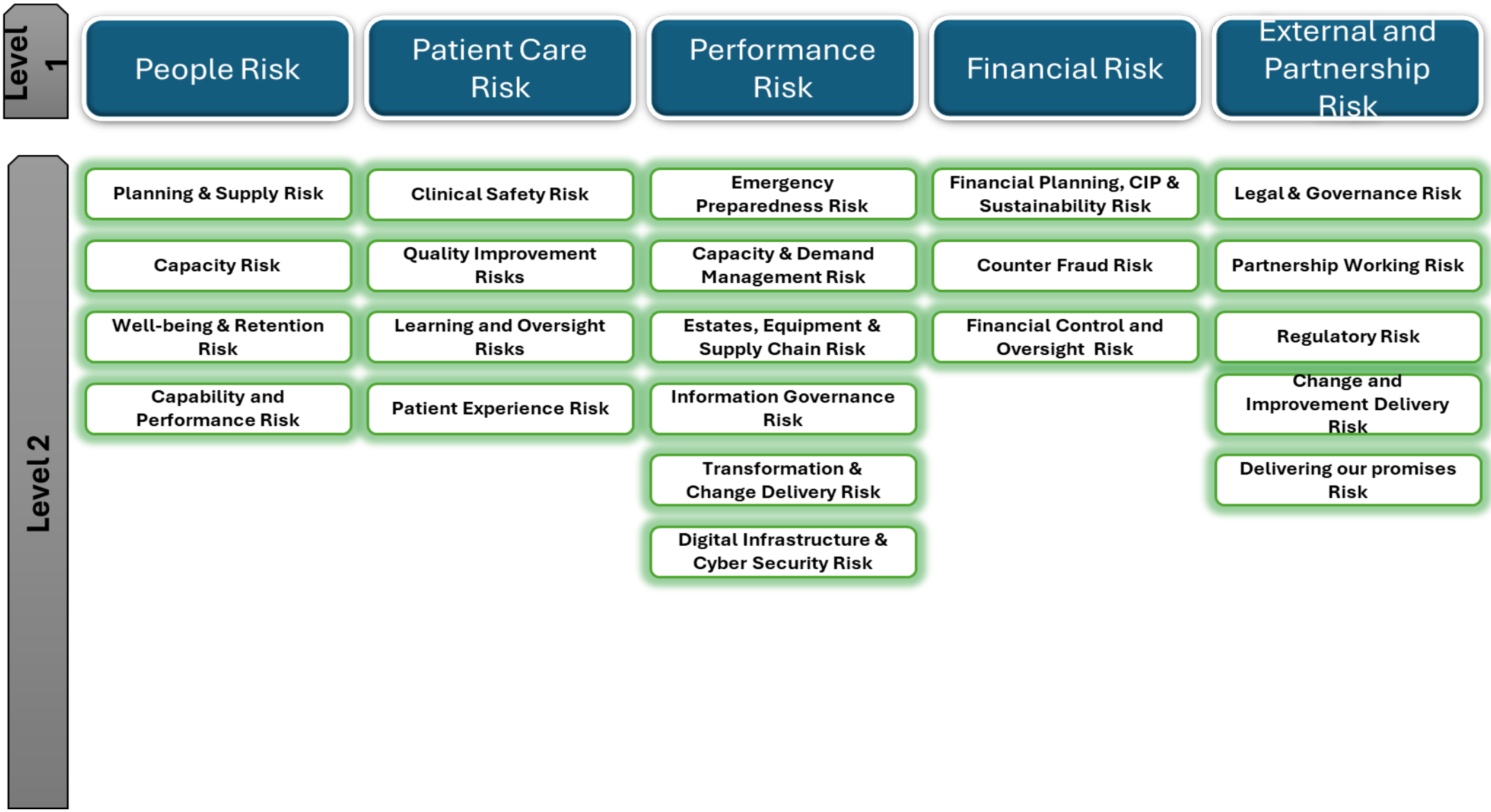
Appetite scale	Green (within appetite)	Amber (within tolerance)	Red (escalate ≥)	Typical stance
Averse	1 – 2	3 – 6	≥ 7	Avoid or stop.
Low Tolerance	1 – 5	6 – 10	≥ 11	Accept very limited risk under strict control.
Moderate Tolerance	1 – 8	9 – 15	≥ 16	Hold most amber risks with close monitoring.
High Tolerance	1 – 10	12 – 20	≥ 21	Innovate; escalate only extreme risks.

Risk Appetite Breaches

Risks that fall outside the Trust's agreed tolerance band for their appetite level, whether the appetite is Averse, Low, Moderate or High, or whose narrative conflicts with the declared appetite, are automatically scheduled for review by the Risk Management Group, RMG, within its rolling work programme. RMG first checks the fundamentals: is the residual score calculated correctly and is the appetite classification appropriate?

If the answer is yes and the risk remains above tolerance, the risk owner presents a brief paper analysing current controls, identifying gaps and proposing practical actions to reduce the score into at least the amber band that sits within tolerance for that appetite level. Each action is assigned to a named lead with clear deadlines. RMG tracks delivery of these actions through monthly updates until the residual score demonstrably returns to tolerance. Should the risk stay red, or if it scores twenty-one or above, RMG escalates it to the CLE and notes it for the Audit Committee.

Appendix A - Risk Types and Risk Categories



Appendix B - Risk category Definitions

People Risk	The risk of not having a sufficient, healthy, capable and appropriately deployed workforce to deliver services safely and sustainably.
Planning & Supply Risk	Securing and forecasting sufficient numbers and skill-mix of staff (recruitment, succession, training pipelines) for clinical and backbone services
Capacity Risk	To ensure the Trust deploys effectively the right mix of skills and capacity.
Well-being and Retention Risk	To ensure the Trust retains the right people with the right skills and supports the mental and physical health of its staff, preventing burnout and stress.
Capability and Performance Risk	Ensuring colleagues possess the competence, training and productivity needed to meet clinical and corporate standards

Financial Risks	The risk of financial loss, mismanagement, or unsustainable planning that impacts the Trust's ability to deliver services, invest in future priorities, or comply with financial and regulatory expectations. This includes planning, oversight, control, and fraud-related exposures.
Financial Planning, CIP & Sustainability Risk	The Trust's ability to balance income, expenditure and capital over the planning cycle, including delivery of cost-improvement plans, cash-flow and access to capital funding and capacity to achieve best value for money through procurement, contract management, productivity benchmarking and whole-life costing of assets and services

Counter Fraud Risk	The adequacy of preventative and detective measures that deter, detect and respond to fraud, bribery, corruption or other irregularities that could cause financial loss or reputational damage. (internal and external) from committing acts of fraud against the Trust and its patients.
Financial Control and Compliance	Effectiveness of the Trust's financial governance to safeguard resources and meet regulatory requirements and ensure that financial information reported internally and externally is correct, true and fair and does not contain material misstatement

Patient Care Risks	The risk that care delivered fails to meet required safety, quality, and experience standards. This includes risks of clinical harm, ineffective improvement efforts, poor learning systems, or suboptimal patient involvement that compromise outcomes or regulatory compliance.
Clinical Safety Risk	Potential for service-users to experience physical or psychological harm because safety controls or practices are ineffective.
Quality Improvement Risks	Potential for improvement initiatives to be poorly prioritised, resourced, designed, implemented or evaluated
Learning and Oversight Risks	The risk of weaknesses in oversight, assurance, incident investigation, audit or organisational learning to limit continuous improvement of care quality.
Patient Experience Risks	To ensure the Trust meets patient, carer and family expectations of dignity, involvement, communication and satisfaction.

Performance Risks	The risk that operational systems and support infrastructure fail to meet service, resilience, or compliance expectations. This covers emergency preparedness, demand-capacity mismatch, estates and equipment, digital infrastructure, information governance, and overall delivery capability.
Emergency Preparedness Risk	Readiness to withstand, respond to and recover from disruptive events—pandemic, flood, cyber-attack, mass-casualty, utility loss—while maintaining critical functions.
Capacity & Demand Management	The organisation's ability to match beds, clinic slots, caseloads and workforce hours to actual and forecast demand so that waiting-time, flow and productivity targets are met.
Estates, Equipment & Supply Chain Risk	The condition, suitability and resilience of the Trust's physical estate, engineering plant, medical devices, fleet and supply chains, including PPE, drugs and consumables—so they support safe, continuous care.
Information Governance Risk	To ensure that the Trust has the right processes and systems for collecting, storing, managing and maintaining information (includes archiving and deletion) in all its forms to support business needs and comply with regulations.
Digital Infrastructure & Cyber Security Risk	Reliability, availability and performance of networks, servers, clinical applications and end-user devices, together with technical cyber-defence measures that protect them

External and Partnerships Risks	The risk arising from the Trust's interface with external stakeholders, legal frameworks, strategic partners, and regulatory bodies. This includes the risk of failure to comply, collaborate, deliver agreed outcomes, or influence change in ways that affect strategic goals or reputation.
Change and Improvement Delivery Risk	Capability to plan, resource, govern and realise the benefits of strategic programmes, digital deployments, estate redevelopments and service redesigns within agreed scope, time and cost.
Legal & Governance Risk	Complying with statutory obligations (e.g., Mental Health Act, GDPR, Health & Safety) and corporate-governance duties to avoid litigation or sanctions.
Partnership Working Risk	To ensure the Trust has effective partnership working arrangements in place, working in conjunction with health, social care, voluntary, local authorities and private sectors
Regulatory Risk	To ensure the Trust has effective processes in place for monitoring performance and progress against regulatory standards, including constitutional standards as set out in the national Contract, liaising with local and specialist commissioners.
Delivering our promises Risk	The possibility that the Trust fails to honour the commitments, service standards or partnership deliverables it has agreed with patients, communities, commissioners or partner organisations, resulting in loss of trust, reputational damage, strained relationships and reduced future collaboration

Appendix C- Appetite Levels by Risk Category

Risk Category	Averse	Low Tolerance	Moderate Tolerance	High Tolerance
People Risk	We will not accept any risk that could result in unsafe staffing levels, burnout, or compromised capability that impacts patient safety.	We accept only tightly controlled risk in workforce planning, wellbeing, or capability where clear mitigation is in place.	We are willing to test new recruitment or deployment approaches where risks are understood and do not compromise patient care.	We actively support bold workforce innovations and flexible staffing models, accepting uncertainty where long-term gain outweighs short-term disruption.
Financial Risks	We will not accept financial practices or decisions that put the Trust's solvency, regulatory compliance, or ability to fund care at risk.	We tolerate only small, controlled financial risk where it is necessary to sustain core operations or ensure value for money.	We accept moderate risk in planning or investment decisions where there is a clear, measurable path to improved efficiency or outcomes.	We support ambitious financial strategies or funding models that involve uncertainty, provided there is strong governance and recovery planning.
Patient Care Risks	We do not accept any risk of avoidable patient harm, serious safety incidents, or breach of core clinical standards.	We accept minimal risk to patient care when all controls are in place and where mitigation is prompt and effective.	We will tolerate limited care delivery risk when piloting new models or innovations, provided dignity, safety, and outcomes remain protected.	We support experimental approaches to care delivery that challenge current practice, accepting a higher level of risk for transformative benefit.
Performance Risk	We will not accept operational risks that would disrupt critical services or breach regulatory or contract standards.	We accept low levels of operational disruption risk where services remain resilient and recovery is assured.	We tolerate moderate inefficiencies or backlogs when tied to transformation, provided core services and response times are safeguarded.	We accept performance volatility and experimentation with service models to support broader strategic shifts or innovation.

Risk Category	Averse	Low Tolerance	Moderate Tolerance	High Tolerance
External & Partnerships Risk	We will not accept any breach of legal, regulatory, or partnership commitments that damages trust or public confidence.	We tolerate only tightly managed risks in partnership delivery, legal exposure, or reputation, with close monitoring and escalation.	We accept measured risk in new collaborations or regulatory engagement when benefits are likely and dependencies are transparent.	We encourage ambitious external collaborations, accepting uncertainty where aligned to long-term system goals or innovation.

ROTHERHAM DONCASTER AND SOUTH HUMBER NHS FOUNDATION TRUST

Report Title	Committee Supporting Paper	**Agenda Item**	Paper Z
Sponsoring Executive	Kathryn Lavery, Chair		
Report Author	Various		
Meeting	Board of Directors	**Date**	29 May 2025

Suggested discussion points (two or three issues for the meeting to focus on)

The following reports, received and discussed by the Quality Committee is presented today to be noted by the Board of Directors:

Learning from Deaths Annual Report 2024-2025 – The Quality Committee was assured that the systems, processes and mechanisms in place for learning from deaths is robust.

Alignment to strategic objectives (indicate with an 'x' which objectives this paper supports)

Business as usual	x

Previous consideration

The documents have been presented to the Quality Committee (21 May 2025).

Recommendation

The Board of Directors is asked to:

x	**CONSIDER** and note the appended report for information

Impact

Trust Risk Register							
Strategic Delivery Risks	x	SO4					
System / Place impact							
Equality Impact Assessment	Is this required?	Y		N	x	If 'Y' date completed	
Quality Impact Assessment	Is this required?	Y		N	x	If 'Y' date completed	

Appendix (please list)

Refer to Agenda Pack B

Rotherham Doncaster and South Humber NHS Foundation Trust

Learning from Deaths Annual Report 2024-2025

Dr D Sinclair
Chief Medical Officer

Kimberley Gostolo
Structured Judgement Reviewer, Coroner and Mortality Support

Melanie Ketton
Structured Judgement Reviewer, Coroner and Mortality Support

April 2025

1 Introduction

This report is an overview of mortality surveillance and learning from deaths within Rotherham Doncaster and South Humber NHS Foundation Trust (RDaSH) and highlights the work undertaken with respect to such during this period.

2 National / Regional Context

RDaSH is a member of the North of England Learning from Deaths Alliance which is a group of nine mental health trusts covering the area from South Yorkshire up to the border of Scotland. The Alliance shares good practice, documentation, and benchmarks quality standards in relation to mortality management with the aim to develop consistency in mortality surveillance practice across organisations.

We are also members of the Regional Mortality Meeting which includes representatives from both acute hospitals and community trusts.

3 Mortality Surveillance

The Chief Medical Officer for the Trust is the Executive Lead for Mortality and reports to both the Quality Committee and the Board of Directors . The Chief Medical Officer is supported by the Medical Lead for Mortality and the Structured Judgement Reviewers / Coroner and Mortality support team.

3.1 Prevention and Learning from Future Deaths Group (PLFDG) previously Mortality Surveillance Group (MSG)

PLFD oversees all aspects of mortality surveillance within the Trust. The meeting takes place bimonthly and chaired by the Chief Medical Officer and is required to have leadership representation from all of the directorates and care groups.

The meeting also incorporates Resuscitation Surveillance Operational Group (RSOG).

It is a national requirement that a quarterly report on mortality data is presented to the Board of Directors. This offers current data issues in relation to mortality surveillance management.
It is presented via the Quality Committee and summarised to the board by the chair of that committee.

Between April 2024 and March 2025, the PLFD meetings were held bimonthly. Due to the absence of Care Group Representatives, none of the meetings were quorate during 2024 - 2025. This matter has been raised with the Care Group Directorates and Leadership Teams.

Where meetings were not quorate, decisions were made via email consultation to avoid delays of the action log outcomes and for any progress to be able to actively move forward.

3.2 Mortality Operational Group (MOG)

The group meets on a weekly basis to ensure that reported deaths within the Trust are reviewed in a timely manner. This group is chaired by the Medical Lead for Mortality, currently a Consultant Psychiatrist. MOG reports to the PLFD in line with the requirements from the Learning from Deaths policy.

Each mortality form identified as being in 'scope' and currently submitted via the Ulysses reporting tool is scrutinised by MOG. A decision is then determined to identify the level of escalation. Currently as directed by the Learning from Deaths policy, a decision is made to complete either a Structured Judgement Review or if identified, to escalate the incident to the Patient Safety Team for further review under the Patient Safety Incident Response Approach.
Following the scrutiny of submitted mortality forms, MOG will make a decision to close the incident if no further concern is identified in care,

3.3 Policies, Processes and Procedures.

The terms of reference for the PLFD group were reviewed and approved in October 2024.

The terms of reference for the Mortality Operational Group were reviewed in April 2025 and awaiting approval .

The Learning from Deaths Policy recently had an amendment in September 2024 to include the changes to the Medical Examiners Certification of Death. The policy was reviewed and approved by the Board of Directors in January 2025.

This policy is next due for review in January 2026.

3.4 Reporting Deaths

Guidance is available for staff on the Trust Intranet as to how mortality forms should be completed using the current Ulysses system.

As the Trust move forward to introducing RADAR healthcare system for reporting of events, previously known as incidents, information and guidance on the reporting of

deaths has been produced in conjunction with members from MOG and the RADAR implementation team and in readiness for go live on the 01.05.2025.

3.5 Reviewing Deaths

From 1st April 2024 – 31st March 2025 there were 608 deaths reported on the Rotherham Doncaster & South Humber NHS Trust mortality Ulysses system.

This figure is up by 15, compared to 2023 – 2024 (593)., however down by 96 in 2022 -2023. (704) .

The figures for April 2024 – March 2025 relate to patients who had contact with the Trust within six months prior to death.

Between April 2024 – March 2025 , MOG reviewed all 608 deaths of which 44 were subject to Structured Judgement Reviews.

Table 1

Quarter	No of deaths	No of deaths reviewed	No of SJRs indicated
Quarter 1	146	146	12
Quarter 2	157	157	8
Quarter 3	157	157	10
Quarter 4	148	148	14
Total	608	608	44

No deaths during April 2024 – March 2025 have been identified as a direct problem in care.

4 Learning from Deaths

4.1 Structured Judgement Reviews

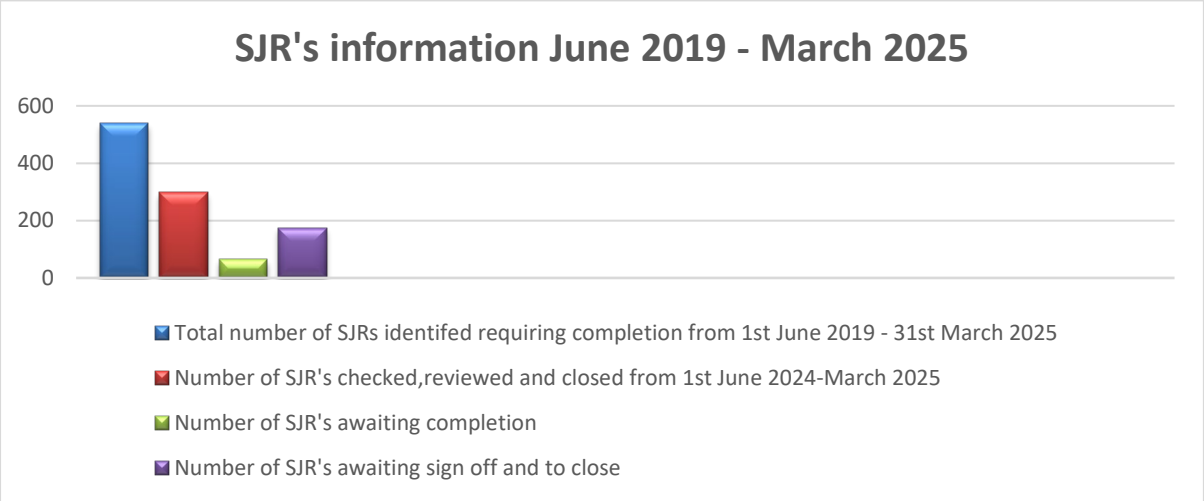
Number of Historic Structured Judgement Reviews completed dated from 2019

Due to unexpected changes in the Mortality team in May 2024, focus for the Structured Judgement Reviewers has been to support the coronial work for the Trust.

Over recent months a plan has been agreed to work through the outstanding numbers of SJR’s.

The two SJR reviewers have worked extra hours to support this plan and to clear the back log of those which require completion.

Graph 1



4.2 Structured Judgement Review Process

The Structured Judgement Reviews undertaken over the past months have identified the following areas of good practice. The points below have been discussed in the MOG meetings and where members from the Patient Safety Team attend.
Information of the findings is discussed through the PLFD group and to be then considered at the Quality meetings.
This supports the wider organisational and future learning for Trust.

- Good physical health monitoring particularly around patients prescribed antipsychotic medications
- Timely documentation in care records
- Good dysphagia care plans and appropriate reviews with risk assessments updated to reflect changes.
- Timely communication with other professionals to address identified issues and supportive of patients' needs
- Good multidisciplinary team and person-centred approach to patient care
- Good timely and responsive assessments following initial referral for people with learning disabilities

Identified areas of learning

- Documentation of capacity using appropriate form available on the electronic patient record
- Risk assessments not always reflective of most up to date care plans
- Lack of documentation of carer or family involvement

- Hospital passports or Traffic Light document for people with learning difficulties not being updated and added to the electronic patient record to reflect changes in health or social circumstances
- Entries added to patient records being ambiguous of involvement from professionals and not identifying purpose of the contact

4.3 Regional Changes

Medical Examiners.

On the 9th of September 2024 new statutory systems were introduced across England and Wales regarding the reporting of deaths.

All deaths in any health setting that are not investigated by a coroner are reviewed by NHS medical examiners.

Prior to this date, RDaSH had initiated some initial systems in support of this change. Following discussion with the Trust and the Doncaster medical examiners, an agreement was reached whereby the medical examiners serve as the single point of contact for all areas of the Trust.

This provides a supportive and reliable approach for staff across the organisation when reporting a death.

4.4 Coroner Inquests

National

Regulation 28 - Prevention of Future Deaths. (PFD)

Under paragraph 7 of schedule 5, Coroners and Justice Act 2009 ,Regulation 28 empowers coroners to issue PFD reports to a person, organisation , local authority , government department or agency where the coroner believes that action should be taken to prevent future deaths.

The Chief Coroner receives all reports and responses, and these are published on the Courts and Tribunals Judiciary website.

From April 2024 to March 2025, the Trust solicitors, Browne Jacobson, have been instructed on seven occasions to represent the Trust at scheduled inquests. Two of the inquests have now been concluded, the remaining are pending cases for the Trust.

From January 2024 to March 2025, the Trust has been issued with one PFD Regulation 28 report.

Table 2 Regulation 28 Prevention of Future Deaths issued to the Trust Jan 2024 – March 2025

Date issued to the Trust	Concerns raised by the coroner	Response sent	Actions completed
16.09.2024	Crisis provision for older adults out of hours	31.10.2024	Changes made to Crisis services for Doncaster and Rotherham to align with services in North Lincolnshire. All persons presenting in Crisis are assessed by the team regardless of age or time of day.

Over the past year the Coroner Liaison and Mortality Team have received 130 enquiries from different coroners and from a number of jurisdictions across the country for information about the deceased person and their contact with our services.

Staff within the Trust have provided 136 statements or reports to assist the coroners for 96 inquests held.

There have been 19 witnesses called to provide evidence at court and to assist the coroner to reach a conclusion in relation to the death of the deceased.

The coroner has made the decision on 98 occasions where the witnesses from the Trust have been stepped down from appearing in person to provide evidence to the court. The statements which have been submitted have been read out in court under Rule 23.

Over the past year the Structured Judgement Reviewers / Coroner and Mortality support have attended 10 pre inquest review hearings (PIRH) at the coroners courts.

The purpose of the pre inquest hearings are for the coroners to establish more specific detail from named persons, authorities or organisations which have been concerned with the deceased.

This offers a further opportunity for the coroner to identify if additional and more specific information is required prior to the scheduled inquest date.

4.5 Recent attendance at inquests has highlighted specific areas of focus for the Trust .

Following the conclusions of inquests attended over the past year, particular areas have been highlighted as points mentioned by the coroners for further consideration-

- For staff to improve on professional curiosity
- For improved communication across organisations and authorities
- Importance of full accurate record keeping and documentation, including communication and agreed treatment plans including risk assessment
- The importance of sharing organisational learning across the Directorates within the Trust .

These points have been shared with the Patient Safety Team and for wider organisational learning.

4.6 Improvements within the Trust for organisational learning for inquests.

From the beginning of June 2024 and due to the unexpected changes in the mortality team, the two full time structured judgement reviewers were asked to support the mortality and coroner work for the Trust.

Since this time, the work has been addressed by the two full time SJR staff and from August 2024, a full-time administrator is now part of the team .

Areas for improvement were identified, and changes were made to the coordination of requests from the coroner's office. This included a systemised process to provide a preplanned flow for requested reports to be returned to the coroner in a timely manner.

Improvements were added to the existing inquest spreadsheet and therefore offering real time data of all enquires received and for the coronial process for RDaSH patients.

The team meet daily where correspondence from the coroner or matters

concerning inquests are discussed. This provides a level of assurance around the current and pending inquests where any outstanding actions can be proactively addressed.

In December 2024 to the beginning of February 2025, the two structured judgement reviewers within the Trust had additional support two days a week with a solicitor seconded from Browne Jacobson Law firm to gain a better understanding of the coronial and inquest process.

Opportunities were explored as to how the organisation can better prepare for inquests and provide support to staff colleagues.

In January as part of the Trusts half day learning, 2 x ninety-minute sessions were offered to all staff to better understand the formal procedures for all areas concerning coroners' inquests. These sessions were attended by approximately 110 staff from within the Trust with a presentation delivered by an expert solicitor on inquests and the law.

In March 2025 Browne Jacobson offered a six-module training package covering all aspects of coroners inquests and 115 staff, including medics, undertook this training. These modules have been made available to these staff until the end of June 2025.

Within the modules, staff have had the opportunity to listen and pose questions directly to serving coroners. The topics of learning have also included mock inquests based on real cases and with a retired senior coroner. This offered a realistic insight as to the formal proceedings of what to expect when attending coroners court.

4.8 Future support for staff regarding inquests.

Since June 2024, the two structured judgement reviewers / coroner and mortality staff have been providing ongoing support to all staff in respect to coroner requests. This has included support around all aspects of the process and attendance at court.

Additional support has also been provided to the care groups in the promptness for reports for the coroner via the administration support in the team sending reminders with guidance for completion and accuracy for reports being submitted to court. This has allowed for a continuous provision of support for staff involved with coroner inquests.

Next steps

It is hoped that during 25-26 the team will continue to be able to deliver further training opportunities to all staff and provide the necessary assistance around coronial work for the Trust and in partnership with the Learning and Development Team.