NHS
Yorkshire
Ambulance Service
NHS Trust

Risk Management Policy

Document Author: Risk and Assurance Manager

Date Approved: March 2025

Document Reference	PO – Risk Management Policy – February 2028
Version	V: 4.0
Responsible Director (title)	Director of Corporate Services and Company Secretary
Document Author (title)	Risk and Assurance Manager
Approved By	Risk and Assurance Group
Date Approved	March 2025
Review Date	March 2028
Equality Impact Assessed (EIA)	Yes
Document Publication	Internal and Public Website

Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
1.0	15/01/2014	Mark Hall	A	Approved SMG 15/01/14
2.0	May 2017	Maxine Travis	A	Approved at TMG 10/05/2017
3.0	Jan 2021	Risk Team	A	Approved by TMG
3.1	April 2023	Risk Team	A	TMG approved extension until September 2023
3.2	Jan 2024	Risk Team	A	Clare Ashby approved extension until April 2024
3.3	March 2024	Risk Team	A	Extension approved within March Risk and Assurance Group
3.4	July 2024	Risk Team	A	Extension approved within July Risk and Assurance Group
3.5	January 2025	Levi MacInnes	D	Full review of policy, presented to RAG for approval.
4.0	March 2025	Risk Team	A	RAG approval of the policy.
A = Approved D = Draft				
Document Author = Levi MacInnes, Risk & Assurance Manager				
Associated Documentation: • Risk Management and Assurance Strategic Framework • Health and Safety Risk Assessment Procedure • Health and Safety Policy • Records Management Policy • Information Governance Strategy • Business Continuity Planning Policies and Procedures				

Staff Summary

Risk is inherent in all activities and at all levels of the Trust. Risks can arise or be identified at any time in the course of day-to-day work across the organisation.
All members of staff are responsible for identifying and reporting risks in their area of work. Risk management is everybody's business.
The Trust seeks to adopt good practice in the identification, evaluation and cost effective control of risks.
This policy sets out the Trust's expectations and key processes regarding the identification and management of risks.
All risks must be recorded in the Trust's risk management system. The Risk and Assurance team will provide training and support for staff to help them use the risk management system.
This policy includes requirements and guidance to help staff to: • Identify, scope and describe a risk • Evaluate the consequence, likelihood and overall rating of a risk • Understand the controls and gaps in controls associate with a risk • Develop and manage actions to mitigate a risk • Record and manage risk information on the Trust's risk management system • Maintain risk registers at the appropriate level of the organisation • Review and update the status of a risk • Escalate, de-escalate and close a risk
This policy sets out the key roles and responsibilities of designated risk owners and designated action owners
Risk register reviews should be a regular agenda item for management teams, specialist groups, governance bodies, and project or programme governance groups
The Risk and Assurance team will regularly support the designated Risk Leads to implement this policy in their business area.

1.0 Introduction

1.1 Yorkshire Ambulance Service NHS Trust (henceforth, 'the Trust') is committed to identifying and managing all risks associated with service delivery, support functions and the organisation as a whole.

1.2 Risk is inherent in all activities and at all levels of the Trust, therefore risk management is everybody's business. Actively recognising the risks associated with service delivery and support functions enables the Trust to plan and implement strategies to mitigate the likelihood and consequence of a risk materialising.

1.3 Risk management is a statutory and regulatory requirement for the Trust. It is also a core component of good practice in all aspects of strategy, planning, and operational management.

1.4 At the operational level good risk management is essential for the delivery of safe, efficient, and high-quality services. Dynamic risk assessment links to other resilience and business continuity activities to help sustain impactful frontline operations and support functions.

1.5 The Trust recognises that failure to identify and address risk in a timely and effective manner could result in:

- Harm to patients, staff, volunteers, or others in their activities for the Trust.
- Failure to deliver the Trust's strategic objectives and operational priorities.
- Failure to achieve sufficient levels of resilience and business continuity.
- Loss or damage to the Trust's reputation as an influential and impactful system partner at national, regional or community level.
- Loss or damage to the Trust's property, assets, systems, and data.
- Financial and commercial losses.
- Adverse publicity, complaints, and litigation.
- Failure to meet statutory, policy or regulatory requirements.

1.6 Managing risk is not just about avoiding adverse future events. Risk management good practice also includes considered, well-controlled risk-taking in pursuit of opportunities to develop, improve and add value to the services and functions of the Trust.

1.5 Through its risk management and assurance arrangements, including proactive risk assessment, resilience and business continuity processes, the Trust supports an open, dynamic and balanced approach to managing risk and pursuing opportunities to innovate, change, and improve.

2.0 Purpose/Scope

2.1 This policy sets out the Trust's expectations and key processes regarding the identification and management of risks.

2.2. This policy applies to all activities associated with the Trust, including service delivery, support functions, internal business developments and change, wider system interactions and other external factors affecting any constituent part of the organisation and the Trust as a whole.

2.3 This policy applies to all categories of risk, including, but not limited to: strategic, operational, clinical, technology (including healthcare technology), financial, fraud, commercial, programme/project, security, business continuity, information, regulatory, environmental and reputational risks.

2.4 This policy applies to all directly employed staff, agency staff, contractors and volunteers engaged in work or other activities on behalf of the Trust.

2.5 This policy aligns with and supports implementation of the Trust's Risk Management and Assurance Strategic Framework.

2.6 This policy is supported by a user guide that provides a practical, step-by-step approach to using the Trust's risk management system (RLDatix) available from the Risk and Assurance Team.

2.7 The scope of this policy does not include the Trust's requirements regarding dynamic risk assessment relating to safer responding practice. These requirements are set out in the Safer Responding Policy and associated documents.

2.8 The scope of this policy includes only brief reference to the Trust's requirements regarding Health and Safety risk assessments. These requirements are set out fully in the Health and Safety Risk Assessment Policy and associated documents.

3.0 Process

3.1 Risk Management Objectives

3.1.1 The Trust seeks to adopt good practice in the identification, evaluation, and cost-effective control of risks to ensure that they are reduced to an acceptable level or are eliminated as far as is reasonably practicable. In addition, the Trust seeks to maximise appropriately controlled opportunities to deliver its strategic objectives and operational priorities, and to continuously improve its service provision and support functions.

3.1.2 The objectives of risk management across the Trust are to:

- Minimise the potential for harm to patients, staff, volunteers and visitors, reducing this to levels that are as low as is reasonably practicable.
- Protect everything of value to the Trust (such as high-quality patient care, staff and patient safety, reputation and influence, physical and intellectual assets, current and future income streams, information systems and data).
- Enable the Trust to anticipate, respond to, and remain resilient during periods of system transformation, organisational change, and operational pressure.
- Maximise opportunities for development, innovation, and improvement of services and functions in a safe, considered and controlled manner.

- Ensure that the Trust achieves and sustains compliance with statutory, policy, regulatory and legal frameworks and other similar requirements.
- Inform the Trust's strategy, policies, business plan and operational management by identifying risks and their likely impact, and by developing actions and controls to manage these risks well.
- Ensure that risk management and assurance activity is embedded into standard management practice across the Trust and is not regarded as separate or niche.
- Ensure that risk management and assurance activity is seen as a live and dynamic process that is embedded in the work of governance bodies and managerial groups at all levels of the Trust.
- Provide a standard set of policies, procedures, and processes to support consistent risk management practice across all functions and at all levels of the Trust.

3.1.3 To achieve these objectives the Trust will:

Consider risk when:

- Developing, approving and implementing strategies, plans and policies.
- Developing and approving business cases or other investment proposals.
- Scenario planning for exceptional circumstances (such as major incidents, catastrophic cyber-attack, pandemic response, industrial action, and other severe demand pressures).
- Planning and delivering transformation programmes and change projects.
- Planning and implementing cost improvement plans or other efficiency and productivity initiatives.
- Planning and implementing service improvements.
- Planning and implementing digital change projects and product upgrades.
- Entering into contractual relationships or other formal or commercial partnership arrangements.
- Any other strategic and operational decisions.
- Preparing and presenting reports and proposals for governance bodies.
- Clearly define risk management roles, responsibilities and reporting lines within the organisation.
- Apply appropriate and proportionate risk management principles and practice in all activities of the Trust.
- Reinforce the importance of effective risk management as part of the everyday work of all staff and volunteers employed or engaged by the Trust.
- Ensure that the importance of effective risk management and assurance is reflected in the role and responsibilities of internal governance bodies and captured as appropriate in the approved terms of reference of these bodies.
- Maintain a single risk management information system to record timely, accurate, and comprehensive intelligence about all identified risks. Use this system to produce corporate and local risk registers and other forms of risk analysis and reporting.
- Ensure that appropriate actions and controls are in place to mitigate risks and that these are well understood by those expected to apply them.
- Ensure that gaps in controls are identified and rectified in a timely and appropriate manner.
- Provide training and engagement activities to strengthen risk management capacity and capability within the workforce and to generate and sustain a good level of general awareness and understanding of risk management across the

Trust.

- Maintain appropriate linkages between risk management and other relevant governance, assurance, and internal control frameworks, policies and processes (such as business continuity, information governance, physical and cyber security).
- Work with its internal audit provider to plan and deliver an annual programme of risk-based reviews and related assurance activity and implement improvement actions and learning opportunities arising from these in a timely and appropriate manner.
- Monitor, review, and seek continuous improvement in risk management and assurance arrangements across the organisation.

3.2 Risk Identification

3.2.1 Risk is inherent in all activities and at all levels of the Trust. Risks can arise or be identified at any time in the course of day-to-day work across the Trust. All members of staff are responsible for identifying and reporting risks in their area of work.

3.2.2 Risks to Trust activity can be identified from many and varied valid sources. The following are examples of such sources. *This list is illustrative only and is not intended to be exhaustive.*

- Risk Assessment
- Quality Impact Assessment
- Incidents and Near Misses
- Complaints and Concerns
- Claims and Litigation
- Central Alerting System
- Triangulation of Information
- Horizon Scanning
- Inspections for Improvement
- Central Alerts
- Coronial Investigations
- Policy Development and Review
- Internal and External Audit
- Business Continuity Plans and Exercises
- Regulatory Frameworks
- Compliance Reporting
- Management Reviews
- Risk Workshops
- Programme / Project Assurance
- Debriefs

3.2.3 Important sources of risk information include the various types of proactive risk assessment carried out across the Trust as outlined in the Health and Safety Risk Assessment Policy. Proactive risk assessments aim to protect the interests of staff, patients, the public, and other stakeholders by embedding risk assessment in the day-to-day working practices of all employees. In so doing it enables the Trust to fulfil its duty of care towards staff and others, and supports compliance with health and safety legislation and related regulations.

3.2.4 Themes and trends identified from Health and Safety risk assessments may be articulated as individual risks and recorded in the Trust's risk management system.

3.2.5 When an area of potential or emerging risk is identified. This should be raised via the local governance arrangements and the Risk Lead for that area. Alternatively, an emerging risk can be raised to the Risk and Assurance team and subsequently the Risk and Assurance Group (RAG) pending further investigation/ information.

3.3 Recording Risks

3.3.1 All risks must be recorded in the Trust's risk management system. This applies to all categories and types of risk, including programme and project risks as well as operational business risks.

3.3.2 Where the system functionality allows, the following information should be recorded about each risk:

- Risk title
- Risk description ("IF…THEN….RESULTING IN…")
- Risk register
- Risk type and sub-type
- Context of risk identification
- Risk review date
- Initial risk score
- Target risk score
- Risk Treatment (4T's)
- Controls and gaps in controls
- Actions, including action owners and action due dates

3.3.3 The risk treatment is the response to the risk being identified, the four T's are as follows:

1. **Treat:** take actions to control and reduce the level of risk, either likelihood or impact through effective risk management.

2. **Terminate:** avoid/eliminate the risk by completely terminating the activity/cause and removing the risk.

3. **Tolerate:** accept and/or retain the level of risk, this would typically be for lower-level risks.

4. **Transfer:** transfer the liability to a 3rd party for example utilising insurance or contractual agreements.

3.3.4 Risks with a score below 12 should be recorded on the system in local risk registers only (for example, at directorate, business area or project level). Risks with a score of 12 and above should be recorded on the system in local risk registers and submitted for escalation to the corporate risk register.

3.3.5 The escalation of a risk to the corporate risk register will be moderated and approved at the Risk and Assurance Group and subsequently presented to the Trust Executive Group (TEG). The Risk and Assurance Manager (or equivalent) will review the risks before being presented to the group.

3.3.6 As part of the risk reporting to TEG, the relevant Executive Director (or equivalent) will be asked to confirm any new corporate risks proposed in their area. Individual Executive Directors (or equivalent), or TEG collectively, are able to request further review and moderation of proposed new corporate risks.

3.3.7 Risks recorded on the corporate risk register continue to be owned by the original risk owner. Other than in exceptional circumstances, where a risk is escalated from a local risk register to be recorded on the corporate risk register this does not result in a transfer of risk ownership.

3.3.8 The Trust will provide training to the support identified staff to use the risk management system effectively.

3.3.9 The Risk and Assurance team will provide guidance and support for staff to help them use the risk management system effectively.

3.4 Describing a Risk

3.4.1 The description of a risk should convey the key element of that risk in a clear and concise way. The Trust has a standard formula for describing a risk, as follows:

"IF….THEN….RESULTING IN…"

3.4.2 Application of this standard formula for describing a risk allows the user to always define these three key elements of the risk:

- The potential threat ("IF…")
- What will happen if the threat materialises ("THEN…")
- The impact ("RESULTING IN…")

3.4.3 All risks recorded in the Trust's risk management system (RLDatix) should be expressed using the standard formula.

3.4.4 The Risk and Assurance team will provide examples and further guidance regarding risk description.

3.5 Controls; and Gaps in Controls

3.5.1 **Controls** are measures or arrangements that are already in place to mitigate or manage a risk. Examples of controls might include policies, plans, systems and procedures, approvals processes, management information, compliance reporting, audits, and training.

3.5.2 Every control should be relevant to the risk it is intended to mitigate. It should be clear that the control directly impacts on that risk. The strength and effectiveness of each control should be considered when deciding the influence it will have on the risk rating.

3.5.3 **Gaps in controls** are issues directly relevant to the mitigation of a risk that are not yet controlled adequately or at all. Examples of gaps in controls could include the absence of any of the controls mentioned above (3.5.1).

3.5.4 Gaps in controls should be addressed via clear, effective and proportionate remedial actions.

3.6 Action Planning

3.6.1 The risk owner is responsible for developing an action plan to mitigate the risk. The risk owner must ensure that the planned actions are proportionate to the gaps in control and are relevant to the treatment of the risk.

3.6.2 Each identified gap in control associated with a risk should be addressed by at least one remedial action. The action should be specific to the gap identified, be time-limited, and have a designated owner who is responsible for delivering the action (or for ensuring its completion via delegation to others).

3.6.3 The Trust's risk management system includes functionality to record actions associated with risks. All actions to address gaps in controls, or otherwise to mitigate a risk, should be recorded in the Trust's risk management system.

3.6.4 It is recognised that once a new risk has been identified it can take time to develop and agree appropriate mitigation actions. However, actions associated with a risk must be recorded on the Trust's risk management system no more than one calendar month after the risk is first recorded on that system

3.6.5 An individual gap in controls might require multiple remedial actions. In such circumstances each action must be recorded separately to ensure that an audit trail of implementation progress is captured for each individual action.

3.6.6 Actions plans should include for each action a designated owner, priority for completion, and due date for completion.

3.6.7 The Trust's risk management system will alert action owners by email to prompt them when actions are recorded and due for completion. Section 3.8 outlines the expectations of risk owners/reviewers and action owners in respect of responding to prompts received from the risk management system.

3.6.8 To summarise:

- Controls are measures or arrangements that are already in place in order to manage or mitigate a risk.
- Gaps in controls are the additional issues to be addressed in order to mitigate the risk further.
- Actions describe the remedial measures set out in an action plan in order to address gaps in controls.

3.7 Risk Rating

3.7.1 The Trust uses a standard evaluation matrix to score and apply a rating to each identified risk. The model utilises a 5 x 5 matrix of consequence and likelihood scores in order to calculate an overall score for each risk. Appendix C presents the Trust's risk evaluation matrix.

3.7.2 The score calculated for each risk determines the rating of the risk, as follows:

Risk Rating		Risk Score
	High ('Red')	15 - 25
	Moderate ('Amber')	8 - 12
	Low ('Green')	1 -6

3.7.3 The rating applied to a risk determines how that risk should be managed in the organisation. This is set out in the table below:

Key to Risk Ratings		
Risk Score	**Risk Rating**	**Risk Management Approach**
15-25	**High**	Managed at local team or departmental level and / or Directorate or Trust level or by a subject specific group depending on management control, treatment plan, or wider strategic implications for the Trust. Risk Leads consider escalation and review at Risk and Assurance Group where consideration is given to escalating the risk into the Corporate Risk Report and / or the Board Assurance Framework
8-12	**Moderate**	Managed at local team or departmental level, unless escalated to Directorate or Trust level or to a subject specific group. Where there is a consequence score of 4 or 5 alone this may be considered for escalation to the Risk and Assurance Group regardless of the likelihood score.
1-6	**Low**	Managed at a local team or departmental level. Local management to determine and develop risk treatment plans or to manage through routine procedures; and consider including on the risk register. This level of risk may be short-lived or aggregated into a higher risk.

3.7.4 Risk Domains: the Trust's risk evaluation matrix presents a number of 'domains' or categories of risk against which to assess the consequence and likelihood of any given. Appendix D outlines risk domain descriptors to support with evaluating the risk.

These domains are:

- Safety
- Staff
- Statutory duty or inspections
- Service or business interruption
- Business programmes / projects
- Safeguarding
- Coroners' requests / inquests
- Complaints
- Financial loss
- Information Governance
- Adverse publicity / reputation
- Litigation

3.7.5 Consequence: the consequence element of a risk concerns the level of impact of the threat associated with a risk if it were to materialise. For each risk domain the Trust's risk evaluation matrix contains five descriptors (1-5) that are used to score the consequence element of any given risk.

The five consequence (C) descriptors are:

Consequence		Descriptor
	1	Negligible
	2	Minor
	3	Moderate
	4	Major
	5	Catastrophic

3.7.6 Likelihood: the likelihood element of a risk concerns the probability or chance that the threat associated with a risk will actually materialise. The Trust's risk evaluation matrix contains five descriptors (1-5) that are used to score the likelihood element of any given risk. Appendix E outlines the likelihood descriptors to support with evaluating the risk.

The five likelihood (L) descriptors are:

Likelihood		Descriptor
	1	Rare
	2	Unlikely
	3	Possible
	4	Likely
	5	Almost Certain

3.7.7 The risk evaluation matrix should be applied in six steps as follows:

Step 1: Identify the appropriate domain that describes the potential adverse outcome that would result if the risk materialises. This relates to the 'RESULTING IN…' element of the risk description.

Step 2: Determine the consequence score (C) that best fits the potential adverse outcome if it materialised

Step 3: Determine the likelihood score (L) that best fits the probability of the potential adverse outcome occurring

Step 4: Calculate the overall risk score by multiplying the consequence score (C) by the likelihood score (L)

Step 5: Use the risk score to identify the appropriate rating to apply to the risk (low, moderate, or high)

Step 6: Record the controls, gaps in controls and determine and action plan.

3.8 Risk Ownership

3.8.1 The risk management system (RLDatix) provides three key profiles to support risk ownership. These are as follows:

- **Register Owner**: Responsible risk lead for their function/department and management of the risk register within the system (as outlined in Appendix B). They may also be the Risk Owner / Reviewer for individual risks.

- **Risk Owner / Reviewer**: Responsible for the overall management of a singular risk, including the ongoing assessment, review and action planning.

- **Action Owner**: An individual responsible for delivering an action to reduce / mitigate the risk.

3.8.2 The risk owner/reviewer and the action owner can be the same individual. They can also be different individuals and located in different services or directorates. It is permissible for the risk owner/reviewer to develop the action plan associated with a risk and then to allocate or transfer some or all the actions to other individuals for them to manage through to completion. In such circumstances the risk owner/reviewer remains the same, but these other individuals become the designated action owners.

3.8.3 Each risk can have multiple actions. Each of these actions must have a designated action owner. Where a risk has multiple actions, it can have multiple action owners.

3.8.4 The risk owner/reviewer must always consult with the proposed action owner(s) prior to recording actions and allocating responsibility for their delivery. This is a matter of professional courtesy in line with the Trust's values and behaviours. It also ensures that the proposed action owner(s) formally accept ownership of the action(s) and take responsibility for delivery as set out in the action plan.

3.8.5 A designated risk owner/reviewer can transfer overall ownership of a risk to another individual.

3.8.6 When transferring a risk, the current risk owner/reviewer must always consult with the proposed new risk owner/reviewer prior to transferring ownership of the risk. This is a matter of professional courtesy in line with the Trust's values and behaviours. It also ensures that the proposed new risk owner/reviewer agrees to take ownership of the risk and be responsible for its management and action plan.

3.8.7 Upon leaving the organisation, the risk owner/reviewer and action owners must identify an appropriate successor and enact the transfer of ownership.

3.9 Risk Reviews

3.9.1 All risks should be reviewed by the risk owner/reviewer on a routine basis within the risk management system (RLDatix). No risk should go more than four months without being subject to a formal review. All risks should be reviewed by the risk owner on a routine basis in accordance with the minimum review periods (shown in the table below).

Note that these review periods are the required minimum and more frequent risk reviews are encouraged (for example, it is recommended that red risks are subject to formal review on a monthly basis).

Risk Rating		Minimum Review Frequency
	High ('Red')	Every 2 Months
	Moderate ('Amber')	Every 3 Months
	Low ('Green')	Every 4 Months

3.9.2 Risks recorded on the corporate risk register (CRR) will also be reviewed and moderated collectively by the Risk and Assurance Group in line with Terms of Reference.

3.9.3 Risk reviews should include an evaluation of the current risk score (using the risk evaluation matrix), review and confirmation of the target risk score, and a review of progress in completing the mitigation actions.

3.9.4 Following a risk review the 'current risk score' together with the 'initial risk score' and the 'target risk score' provides a view of progress towards reducing the risk to the target level.

3.9.5 If, as a result of a risk review, the current risk score increases from 'below 12' to '12 or above' then the risk will be submitted for escalation to the corporate risk register (CRR) via the Risk and Assurance Group as outlined in section 3.3.4.

3.9.6 If, as a result of a risk review, the current risk score decreases from '12 or above' to 'below 12' then the risk will be submitted for de-escalation from the corporate risk register (CRR) via the Risk and Assurance Group.

3.9.7 Unless otherwise specified, upon de-escalation from the corporate risk register a risk remains open and active. This will remain in the system on the local risk register only.

3.10 Responding to System Auto-Prompts

3.10.1 The Trust's risk management system will automatically send a prompt to register owners, risk owners/reviewers and action owners to inform them that a review is due.

3.10.2 Risk owners and action owners should respond to system prompts in a timely manner.

3.10.3 It is not necessary to wait until a system auto-prompt is received before reviewing and updating the information recorded about a risk or an action. Progress about a risk or an action can and should be updated at any time there is a relevant update.

3.10.4 For any given risk, the overall risk review date and the individual action due dates may differ. This is entirely appropriate as there may be multiple actions to be completed over a period of time, each with a different completion date.

3.11 Completing Actions and Closing Risks

3.11.1 The action owner is responsible for updating and closing actions as and when these are completed.

3.11.2 When an action has been completed consideration should be given to the impact on the risk score and rating. If the completed action has a significant impact on the likelihood or consequence of the risk occurring, the risk score and rating should be reviewed and potentially reduced.

3.11.3 A risk that remains open can have a number of completed actions recorded against it. However, when all the planned actions have been complete, the risk owner/reviewer should consider whether further actions are required to manage the risk, or whether the risk should be closed.

3.11.4 Where the completion of all actions results in a risk being reduced to its target risk score, or being eliminated entirely, that risk can be closed.

3.11.5 Risks can be closed without reaching the target risk level where the relevant business area recognises that any remaining residual risk will not or cannot be mitigated and is willing to tolerate the outstanding level of risk. In most circumstances the current risk rating should be 'low' (a score of 1 to 6) prior to removing a risk from the risk register.

3.11.6 Risks held on the corporate risk register will be submitted for closure to the Risk and Assurance Group (RAG). The risk owner/reviewer will provide assurance to the group the risk is mitigated or reduced with no further action that can be taken.

4.0 Risk Oversight Arrangements

4.1 The Trust's Risk Management and Assurance Strategic Framework sets out the overarching principles and processes that enable the Trust to manage risk well and uphold high standards of risk governance and assurance. It describes how the Trust's risk management activities dovetail with other governance and assurance arrangements to form a coherent system of internal control. This framework supports the Trust to deliver its objectives by ensuring that:

- Risks to objectives are identified and managed in a timely and effective manner
- Opportunities for strategic development and service improvement are embraced and delivered safely
- The prevailing risk management and assurance culture is open and constructive
- Risk management and assurance activity, including risk assessment and business continuity, adds value to the life and work of the Trust

4.2 The Board Assurance Framework is owned by the Trust Board. It represents ownership by the Trust Board of the key areas of risk to the achievement of the Trust's strategic objectives. The Board Assurance Framework sets out the main strategic risks to the organisation's objectives and the associated controls and mitigation actions. It presents an assessment of the strength of internal controls in place to reduce the likelihood and impact of key risks materialising, and it identifies the main sources of internal and external assurance regarding the effectiveness of those internal controls.

4.3 The corporate risk register (CRR) captures all recorded risks with a score of '12 and above'. The CRR is reviewed by the Risk and Assurance Group (RAG). Material changes to the CRR are reported to the Trust Executive Group (TEG), either in the RAG Chair's monthly report or in formal periodic (e.g. quarterly) risk reports.

4.4 Risks with a score 'below 12' are managed via local risk registers held at directorate, business area, specialist group, or project/programme level. These local level risk registers should be maintained by the appropriate risk lead in conjunction with other appropriate managers involved in that area of work.

4.5 Risk register reviews should be a regular agenda item for meetings of directorate and business area management teams, specialist groups and governance bodies, and project or programme governance and assurance meetings. The requirement to hold regular risk register reviews should be included in the terms of reference for such bodies. Risk register reviews should include the following standard elements:

- Review existing risks
- Review progress of mitigation actions
- Re-assess risk scores
- Consider emerging risks

4.6 Each directorate, business area or project/programme will have a designated Risk Lead. The role of this Risk Lead is to maintain oversight of all risks for their area, be the representative for their business area at Risk and Assurance Group (RAG) and provide updates to RAG on behalf of their service on existing and emerging risks. Appendix B presents a descriptor for the Risk Lead role.

4.7 The Risk and Assurance Manager (or equivalent) will meet with Risk Leads on a regular basis in order to review existing risks and discuss areas of emerging risk.

4.8 The Risk and Assurance team will continuously monitor compliance with the outlined risk management arrangements, reporting to risk leads and risk owner/reviews to ensure risks are being actively managed.

5.0 Training Expectations for Staff

5.1 All designated risk leads, and others with significant involvement in risk management, will receive training in use of the Trust's risk management system (RLDatix) from the Risk and Assurance Team.

5.2 The Trust may identify and mandate specific additional risk management training requirements for any individual or staff groups in accordance with the responsibilities of their role(s) and the needs of the service.

5.3 Board members and other senior leaders will receive specialist risk management development opportunities throughout their service with the Trust where this is relevant to their role.

5.4 The Head of Risk and Assurance and the Risk and Assurance Manager will continuously review any additional training needs and action accordingly upon identification for the Trust and/or individuals.

6.0 Implementation Plan

6.1 The latest approved version of this policy will be posted on the Trust intranet site for all members of staff to access.

6.2 Additional implementation measures will be applied in teams or functions as required. These will be supported through local induction processes, staff engagement and development processes, and other relevant management arrangements.

6.3 The Risk and Assurance team will support Risk Leads to implement this policy in their business area.

7.0 Monitoring Compliance With this Policy

7.1 For the Trust to be assured that the processes described within this policy are working, monitoring arrangements are shown in the table below.

Auditable Standards	Methodology	Frequency	Monitoring Committee
All services and business areas should be represented at Risk and Assurance Group	Review of attendance register by the Risk and Assurance Manager	Annual	Risk and Assurance Group
	Review of RAG membership	Annual	Risk and Assurance Group
All recorded risks should be kept up to date and reviewed in line with policy.	Review of Corporate Risk Register at RAG in line with Terms of Reference.	**Monthly:** escalations, de-escalations, new and closed. **Quarterly:** full governance review	Risk and Assurance Group
	Risk review meetings: Risk Leads and Risk and Assurance Manager	Quarterly	Risk and Assurance Team

All risk registers are monitored to ensure compliance of risk management arrangements.	Review of risks including; risk details, scoring, controls and gaps, actions recorded, ongoing risk reviews undertaken	**Monthly:** risks 12 and above recorded on the CRR. **Quarterly:** risks below 12 recorded on local risk register.	Risk and Assurance Team

7.1 The Risk and Assurance Group will receive a periodic (e.g. quarterly) report on risk management quality and compliance.

8.0 APPENDICES

8.1 This policy includes the following appendices.

Appendix A: Roles and Responsibilities in Risk Management and Assurance

Appendix B: Key Individual Roles

Appendix C: Risk Evaluation Matrix

Appendix D: Risk Evaluation Descriptors

Appendix E: Likelihood Risk Evaluation Descriptors

Appendix A – Roles and Responsibilities in Risk Management and Assurance

All Staff

All members of staff across the Trust have a responsibility to ensure they make themselves aware of and comply with the Risk Management Policy. All members of staff are responsible for reporting identified potential risks within their area of work. Staff will be required to participate in activities which are commensurate with the Trust's Risk Management Policy and statutory or legislative requirements.

All members of staff are responsible for:

- Understanding and complying with Trust policies and procedures.
- Undertaking any training provided by the Trust as a requirement of this policy.
- Ensuring the safety of themselves, their colleagues, the patient and others who may be affected by their acts or omissions.
- Acting in accordance with Trust values and expected behaviors.

Trust Board

The Trust Board owns the strategic framework for risk management and assurance, oversees the system of internal controls which enables risk to be assessed and managed, and sets the organisations' risk appetite. The Board sets the Trust's strategic aims and ensures that resources are in place to meet its objectives. It receives reports at each meeting on the most significant risks and associated mitigation actions as detailed in the Trust's Board Assurance Framework.

Audit and Risk Committee

The Audit and Risk Committee is a formal committee of the Trust Board. It provides overview and scrutiny of risk management and of the Trust's system of internal control more generally.

Quality Committee

The Quality Committee is a formal assurance committee of the Trust Board. It undertakes scrutiny of the Trust's clinical governance, quality and safety plans, compliance with external quality regulations and standards, and key associated functions. The committee oversees risks to delivery of plans and functions related to this remit.

Finance and Performance Committee

The Finance and Performance Committee is a formal assurance committee of the Trust Board. It undertakes scrutiny of the Trust's financial plans, revenue and capital budgets, investment decisions, contract management and procurement, information technology, estates and fleet. The committee oversees risk to delivery of plans and functions related to this remit.

People Committee
The People Committee is a formal assurance committee of the Trust Board. It undertakes scrutiny of the Trust's workforce recruitment and retention plans, organisational development, organisational culture, diversity and inclusion, training and development, leadership and management. The committee oversees risk to delivery of plans and functions related to this remit.

Trust Executive Group
The Trust Executive Group (TEG) is formally designated as the senior executive, managerial and operational decision-making body of the Trust. In this role TEG oversees the development and delivery of the Trust's strategy, enabling strategies, and business plan priorities, the delivery of the Trust's clinical, operational, workforce and financial plans objectives, the achievement of the required statutory duties, regulatory compliance, clinical standards, and performance targets, the development and determination of key operational policies, development proposals, and business cases. TEG oversees risk to delivery of plans and functions related to this remit.

Risk and Assurance Group
The Risk and Assurance Group is a formally constituted management group that reports to the Trust Executive Group. It reviews, moderates and assures corporate-level risks and associated controls and mitigations. The Group receives reports on all directorate risk registers and specific risk issues from its members, including representatives from all other associated risk management groups.

Other Groups involved in risk management include:

Strategic Health and Safety Committee
This strategic Committee is responsible for the review and monitoring provision of a healthy, safe and secure environment for all employees, contractors and members of the public who may be affected by the activities of the Trust. The Committee is responsible for instigating appropriate action to address risks identified from issues that may compromise the above.

Clinical Governance Group
The Clinical Governance Group provides a focus for clinical risk and quality issues. It receives reports by exception on clinical risk issues and is responsible for directing action to manage clinical risk.

Patient Safety Learning Group
The Patient Safety Learning Group provides a focus for risks and issues relating to patient safety and learning from serious incidents.

Incident Review Group
The Incident Review Group is responsible for reviewing and instigating appropriate action to address issues identified in relation to incidents, potential serious incidents and near misses, along with identifying themes and trends from the following specialty areas:

- Formal Complaints/Concerns
- Claims
- Coroner's Inquests
- Clinical Case Reviews
- Debriefs following incidents and exercises

Information Governance Working Group
The Information Governance Working Group is responsible for advising upon and overseeing the management of all issues associated with information risk, confidentiality and information governance/security.

Appendix B - Key Individual Roles

Chairman and Non-Executive Directors

The Chairman and Non-Executive Directors are responsible for ensuring that systems for governance, risk management and internal control are effective and maintained across all functions and at all levels of the Trust. They set the Trust's objectives, identify risks relating to these, set the Trust's risk appetite, and own the Board Assurance Framework. They constructively challenge and contribute to the development of risk management systems. One of the Non-Executive Directors is appointed as the Chair of the Audit Committee which has oversight of for risk management, assurance and internal controls.

Chief Executive, as the Trust's Chief Accounting Officer

The Chief Executive has overall responsibility for ensuring that an effective system of risk management and assurance is in place and that the Trust meets its statutory and regulatory requirements in respect of good corporate governance. The Chief Executive is accountable to the Board for maintaining a sound system of internal control and is responsible for the Annual Governance Statement that sets out how the Trust's risk management and assurance arrangements support the achievement of the organisation's objectives.

Deputy Chief Executive

The Deputy Chief Executive has overall lead responsibility the direction, development, management and implementation of the Trust's strategic framework for risk management and assurance. This role is also the Trust's designated Senior Information Risk Owner (SIRO).

Executive Directors

All Executive Directors have responsibility for ensuring that the Trust's Risk Management Policy is implemented within their directorates and that risk management is embedded within their governance arrangements. The Executive Medical Director has specific designated responsibilities relating to clinical risk.

Director of Corporate Services and Company Secretary

The Director of Corporate Services and Company Secretary is responsible for developing, supporting and embedding effective risk management and assurance processes within the Trust, and for risk reporting to various governance bodies. This Director chairs meetings of the Risk and Assurance Group and is the overall custodian of the Board Assurance Framework.

Risk and Assurance Team

The Risk and Assurance Team, led by the Head of Risk and Assurance, is responsible for operational implementation of the Risk Management Policy and related systems and procedures. The team provides risk management support, guidance and training and owns the production and reporting of the corporate risk register.

Managers

All managers within the Trust are responsible for identifying and managing risk within the remit of their roles and responsibilities. They are expected to comply with the designated risks management policies, systems and associated procedures, and ensure all efforts are made to encourage their teams to escalate potential risks they become aware of. In addition, there are managers with specific interest and responsibility for oversight of risk management within specialist areas of work. These include, but are not limited to, the following:

- Health and Safety Manager
- Security Management Specialist

- Caldicott Guardian
- Head of Risk and Assurance; Risk and Assurance Manager
- Head of Safeguarding
- Head of Safety

Risk Leads

Risk Leads will operate with their designated directorates/committees/groups to manage the identification, management, escalation and review of risk in order to promote and support effective risk management and encourage compliance with the Trust's Risk Management Policy.

Risk Leads are expected to attend all meetings of the Risk and Assurance Group. In their absence, nominated deputies are encouraged to ensure that all services and functional areas are represented in the proceedings of the Group.

Attendance by designated Risk Leads at meetings of the Risk and Assurance Group will be subject to monthly review by the Chair and the Risk and Assurance Manager. Where a service or functional area has not been represented at two consecutive meetings this will be escalated to the appropriate member of the Trust Executive Group.

No decisions about corporate risks relating to a particular service or function will be taken by the Risk and Assurance Group if those services or functions are not represented in the meeting by the respective Risk Lead or nominated deputy, unless, and at the discretion of the Chair, sufficient information has been provided in advance to the Risk and Assurance Manager to enable the Group to make an informed decision

Risk Leads will:

- Ensure risk registers and risk treatment plans are produced in their respective directorates/committees and groups and filed correctly in a timely manner, and that they are considered appropriate to mitigate risks.
- Attend relevant directorates/committees and group forums to discuss and present new/revised risks (particularly any risks rated 12 or more for consideration and/or addition to the directorate level risk register or for further escalation).
- Conduct regular updates and maintenance of their respective directorates/committees and group risk registers.
- Ensure that risks are acted upon immediately including the assignment of Risk Owner/Reviewer if not themselves.
- Ensure risks are reviewed/agreed at regular intervals and support Risk Owners/Reviewers.
- Monitor and review progress against directorates/committees and group risk registers and risk treatment plans, in the respective areas.
- Ensure completion of risk register assessment forms, where appropriate e.g. to identify and transfer risks.
- Ensure action is taken as soon as possible, at the lowest possible level to eliminate, transfer or reduce risk.
- Ensure any risks scoring 12 or above, or other risks that have significant

consequence to Trust objectives, are acted upon immediately (escalate extreme risks to the attention of the Risk and Assurance Group).

- Monitor and progress identified actions from the Corporate Risk Register, appropriate to their respective directorates/committees and groups,
- Attend the Risk and Assurance Group monthly to present new and revised risks in the form of a report (particularly any risks scored as ‘12’ or more and/or with a consequence score of 5 alone, for consideration to the Corporate Risk Register).
- Ensure the risk escalation and reporting procedure is adhered to within their respective directorates/committees and groups.

Appendix C – Risk Evaluation Matrix

Risk Evaluation Matrix: Consequence x Likelihood

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

The scores obtained from the risk matrix are used to assign ratings to risks as follows:

Key to Risk Ratings		
Risk Score	**Risk Rating**	**Risk Management Approach**
15-25	High	Managed at local team or departmental level and / or Directorate or Trust level or by a subject specific group depending on management control, treatment plan, or wider strategic implications for the Trust. Risk Leads consider escalation and review at Risk Assurance Group where consideration is given to escalating the risk into the Corporate Risk Report and / or the Board Assurance Framework
8-12	Moderate	Managed at local team or departmental level, unless escalated to Directorate or Trust level or to a subject specific group. Where there is a consequence score of 4 or 5 alone this may be considered for escalation to the Risk Assurance Group regardless of the likelihood score.
1-6	Low	Managed at a local team or departmental level. Local management to determine and develop risk treatment plans or to manage through routine procedures; and consider including on the risk register. This level of risk may be short-lived or aggregated into a higher risk.

Appendix D – Risk Evaluation Descriptors

Consequence Score Guidance

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

RISK DOMAINS	RISK CONSEQUENCE SCORE AND EXAMPLES OF DESCRIPTORS				
	1	2	3	4	5
	NEGLIGIBLE	MINOR	MODERATE	MAJOR	CATASTROPHIC
SAFETY **Harm to patients/staff and/or public** **(including physical and/or psychological harm)**	Minor injury not requiring first aid or no apparent injury	Minor injury or illness, requiring minor intervention 1-2 people affected No long term consequences.	Moderate injury which impacts on an individual or a small number of people Some degree of harm up to a year. RIDDOR/MHRA/agency reportable incident	Major injury leading to long-term incapacity/disability Serious mismanagement of care with long-term effects 16-50 people affected	Death /life threatening harm Multiple permanent injuries or irreversible health effects More than 50 people affected
STAFF **Competence and training, poor staff attendance for mandatory/key training**	Insignificant effect on delivery of service objectives due to failure to maintain professional development or status	Minor error due to a lack of appropriate skills, knowledge and competence to undertake duties.	Moderate error due to limited skills, knowledge and competence to undertake duties	Major effect on delivery of service objectives due to failure to maintain professional development or status	Significant effect on delivery of service objectives due to failure to maintain professional development or status
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 Critical report	Multiple breeches in statutory duty Prosecution Severely critical report, zero performance rating

RISK DOMAINS	RISK CONSEQUENCE SCORE AND EXAMPLES OF DESCRIPTORS				
	1	2	3	4	5
	NEGLIGIBLE	MINOR	MODERATE	MAJOR	CATASTROPHIC
BUSINESS PROGRAMMES/ PROJECTS	Temporary defects causing minor short term consequences to time and quality	Poor project performance shortfall in area(s) of minor importance	Poor project performance shortfall in area(s) of secondary importance	Poor performance in area(s) of critical or primary purpose	Significant failure of the project to meet its critical or primary purpose
FINANCIAL LOSS – OPERATIONAL / BUSINESS AREA	Small loss of budget (£0 -£5,000)	Medium financial loss (£5,000 -£10,000)	High financial loss (£10,000 - £100,000)	Major financial loss (£100,000 - £250,000) Purchasers failing to pay on time	Huge financial loss (£250,000 +), loss of contract / payment by results Unrecoverable financial loss by end of financial year
INFORMATION GOVERNANCE RISKS	Minimal or no loss of records containing person identifiable data. Only a single individual affected.	Loss/compromised security of one record *(electronic or paper)* containing person identifiable data.	Loss/ compromised security of 2-100 records *(electronic or paper)* containing confidential/ person identifiable data.	Loss/ compromised security of 101+ records *(electronic or paper)* containing person identifiable data.	Serious breach with potential for ID theft compromised security of an application / system / facility holding person identifiable data *(electronic or paper).*
ADVERSE PUBLICITY/ REPUTATION/PUBLIC CONFIDENCE	Rumours No public/political concern	Local media area interest – short-term reduction in public confidence	Extended local/regional media interest. Regional public/political concern.	Regional/national media interest with less than 1 day service well below reasonable public expectation	National media interest with more than 1 day service well below reasonable public expectation.

RISK DOMAINS	RISK CONSEQUENCE SCORE AND EXAMPLES OF DESCRIPTORS				
	1	2	3	4	5
	NEGLIGIBLE	MINOR	MODERATE	MAJOR	CATASTROPHIC
LITIGATION	Likely repudiation at pre-action stage.	Damages valued at less than £10,000 Minor concerns relating to care highlighted, no systemic issues identified Allegations not substantiated and claim likely to be successfully defended and discontinued at pre-action stage.	Civil action / Criminal prosecution / Prohibition notice-proceedings issued Likelihood of success at trial >50% Damages) valued between £10,000 and £100,000 Concerns relating to treatment/care/systemic issues identified which are not likely to have impacted on the outcome Low level risk of reputational damage.	Civil action / Criminal prosecution/Prohibition notice – proceedings issued Likelihood of success at trial <50% Damages between £100,000 and £1 million Major concerns as to treatment/care/systemic issues which are likely to have impacted on the outcome Reputational damage (local level) Raises individual employee failings and or Trust policy concerns	Civil action/Criminal prosecution/Prohibition notice – indefensible Damages >£1 million Catastrophic / significant systemic issues/concerns which have significantly contributed to the outcome Damage due to never event Reputational damage (national level)
SERVICE/BUSINESS INTERRUPTION	Loss of ability to provide services (interruption of >1 hour)	Loss of ability to provide services (interruption of >8 hours)	Loss of ability to provide services (interruption of >1 day)	Loss of ability to provide services (interruption of >1 week)	Permanent loss of service or facility

RISK DOMAINS	RISK CONSEQUENCE SCORE AND EXAMPLES OF DESCRIPTORS				
	1	2	3	4	5
	NEGLIGIBLE	MINOR	MODERATE	MAJOR	CATASTROPHIC
CORONER'S REQUESTS / INQUESTS	No issues or concerns identified No identified risk of criminal or civil litigation No identified risk of reputational damage Witness statements admitted under Rule 23 YAS not an Interested Person	Minor concerns identified unrelated to management of patient No identified risk of criminal or civil litigation No identified risk of reputational damage YAS not an Interested Person.	Concerns relating to treatment/care/systemic issues which are not likely to have impacted on the outcome Does not raise significant individual or Trust policy failings Low level risk of civil litigation claim Low level risk of reputational damage Family and/or other Interested Persons legally represented	Significant concerns to treatment/care/systemic issues which are likely to have impacted on the outcome Areas of concern not addressed receiving a Coroner's Prevention of Future Death report (PFD). Consideration given to legal representation at Inquest YAS has Interested Person Status Concerns raised by Coroner/other Interested Persons Potential for Prevention of Future Deaths report-issues addressed pre-inquest Notification of civil claim- contemplated or actual	Catastrophic / significant issues/concerns which are likely to have significantly contributed to the outcome High likelihood of a Coroner's Prevention of Future Death report-issues not addressed pre-inquest YAS has interested person status. Raises issues of national importance Potential to result in public national enquiry (i.e. London Bombings, Mid Staffordshire enquiry) Potential for criminal prosecution or civil claim proceedings issued

				Reputational damage (local level) Jury/Article 2 inquest Family and/or other Interested Persons legally represented	Reputational damage (national level) Jury/Article 2 inquest Family and/or other Interested Persons legally represented.

RISK DOMAINS	RISK CONSEQUENCE SCORE AND EXAMPLES OF DESCRIPTORS				
	1	2	3	4	5
	NEGLIGIBLE	MINOR	MODERATE	MAJOR	CATASTROPHIC
COMPLAINTS	Minor injury not requiring first aid or no apparent injury Misunderstanding of an element of the service which can be corrected Distress, inconvenience or hurt feelings but no failing	Minor injury or illness, requiring minor intervention Single failure to meet internal standards Single failing resulting in delay to appointment or care, distress, inconvenience or hurt feelings Single failure to meet organisational policy Poor practice, apparent lack of consideration	Moderate injury sustained Single failing resulting in loss of appointment or care Repeated failure to meet internal standards for the individual Single failure to meet organisational code of conduct Repeated failure to meet organisational policy for the individual Unacceptable level or quality of treatment/service.	Major injury leading to long-term incapacity/disability Repeated failure to meet organisational code of conduct for the individual Repeated failings resulting in loss of appointment or care for the individual Inappropriate behaviour	Death /life threatening harm Grossly substandard care Failure to meet legislative requirements/breach of the law

RISK DOMAINS	RISK CONSEQUENCE SCORE AND EXAMPLES OF DESCRIPTORS				
	1	2	3	4	5
	NEGLIGIBLE	MINOR	MODERATE	MAJOR	CATASTROPHIC
SAFEGUARDING CHILDREN AND ADULTS AT RISK ***Actual or alleged abuse; sexual abuse, physical or psychological ill-treatment, or acts of omission which constitute neglect, exploitation, financial or material abuse, discriminative and organisational abuse, self-neglect, domestic abuse, human trafficking and modern day slavery***	No issues or concerns identified clinically or with reputation Progression to strategy meeting or multi-agency review unlikely No media interest Response to query responded to within 2 working days No, or minimal impact or breech of guidance/statutory duty	Minor concerns over patient care CDOP/Form B with uncomplicated information gathering Minor delay in response to external agency request (more than 5 working days) No allegations against Trust or employees Short term service impact from brief investigation involving discussions Police, Social care and HR	Moderate concerns about patient care, response times, clinical interventions CDOP requiring moderately complex information gathering and analysis Referral to LADO and Police. Disciplinary process commenced, suspension from front line duties Possible media interest anticipated Single failure to meet organisational code of conduct	Major concerns with patient care that could have affected outcome Major injury leading to incapacity or disability Repeated failure to reach internal standards Regional media statement requested Abuse enquiry becomes public enquiry Inappropriate behaviour	Incident leading to death or permanent disability Healthcare did not take appropriate action/intervention to safeguard against abuse occurring Abuse that resulted in (or was identified through) a SCR, DHR, LLR Inquest requiring safeguarding information Staff/ex-staff member is found guilty of abuse and convicted Media interest highly likely Inappropriate behaviour

RISK DOMAIN	RISK CONSEQUENCE SCORE AND EXAMPLES OF DESCRIPTORS				
	1	2	3	4	5
	NEGLIGIBLE	MINOR	MODERATE	MAJOR	CATASTROPHIC
ROAD TRAFFIC COLLISIONS	Minor collisions where minimal damage is caused to property or the vehicle, *i.e. reversing, scratch or minor dent*	Collisions generally at lower speed where there is damage to vehicles and/or property but no injuries are sustained *i.e. broken mirror, obvious dent to wing etc.*	Collisions where there are minor injuries to staff or members of the public (patient, pedestrian or other road user). Damage to vehicle – 3rd party *i.e. A&E assessment or GP, but no further treatment*	Collisions, usually at higher speeds or where there are serious injuries to staff or members of the public (patient, pedestrian or other road user) Damage to vehicle – 3rd party. *i.e. serious trauma resulting in medical attention and hospitalisation*	Serious collisions, usually at higher speed resulting in the death or permanent incapacity of a member of staff or the public *i.e. Fatal road traffic collision which could result in a criminal prosecution*

Appendix E – Likelihood Risk Evaluation Descriptors

Likelihood Score Guidance

What is the likelihood of threat associated with a risk actually occurring?

The frequency-based score is in many circumstances the easier to identify. It should be used whenever it is possible to determine the likelihood of the risk materialising.

	RISK LIKELIHOOD SCORE AND EXAMPLES OF DESCRIPTORS				
	1	2	3	4	5
	RARE	UNLIKELY	POSSIBLE	LIKELY	ALMOST CERTAIN
PROBABLILITY	LESS THAN 5% 1 in 100,000 chance	6-20% 1 in 10,000 chance	21-50% 1 in 1000 chance	50-80% 1 in 100 chance	MORE THAN 81% 1 in 10 chance
FREQUENCY	This will probably never happen/recur Will only occur in exceptional circumstances	Unlikely to occur Do not expect it to happen/recur but it is possible it may do so	Reasonable chance of occurring Might happen or recur occasionally	Likely to occur Will probably happen/recur but it is not a persisting issue	More likely to occur than not Will undoubtedly happen/recur, possibly frequently