Risk Management Policy

NHS Devon

Version	**2.0**
Policy Sponsor	Chief Communications and Partnerships Officer
Policy Lead	Company Secretary
Approved by	NHS Devon Board
Approved on	04/10/2023
To be reviewed by	04/10/2026

Document change history (to add rows, copy and paste)		
Date	**Change**	**Comments**
06/09/2023	New Policy	
23/02/2024	Policy Amendment	Updated for minor changes and to address Internal Audit recommendations (Report Ref. DICB03/24A

Equality, Diversity, and Inclusion Statement

NHS Devon is committed to the promotion of equal opportunities, addressing health inequalities, and fostering of good relations between people protected under the terms of the Equality Act 2010, the Health and Social Care Act 2012 and Human Rights legislation. We are equally committed to the elimination of unlawful discrimination, harassment, and victimisation. To demonstrate this commitment, we develop, promote, and maintain policies, strategies, and operating procedures. Every effort is made to ensure that patients, employees, contractors, or visitors do not experience discrimination; either directly or indirectly, because of their vulnerability; disadvantage; age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion and belief; sex (gender) or sexual orientation.

All staff must comply with this policy. Compliance must reflect our organisational commitment to and policy on, equality, diversity, and inclusion. In addition, each manager and member of staff involved in implementing this policy must give due regard to the needs of those protected under law.

If you, or any other groups, believe you are discriminated against under the terms of the Equality Act, the Health and Social Care Act 2012 or Human Rights legislation by anything contained in this document; or you need this document in an alternative format, for example, large print, Braille, Easy read, or other languages; please contact our Patient Advice and Complaints Team (PACT):

Tel: 0300 123 1672
Email: pals.devon@nhs.net

Contents		
Section	**Title**	**Page**

** All appendices to this policy are procedural documents*

1. Introduction

1.1 Risk management plays a critical role in helping NHS Devon understand and manage risks to the achievement of its priorities. It helps us to determine an appropriate control environment and balance of strategies to address risk, so that we use resources both efficiently and effectively. It involves making decisions and establishing governance systems that embed and support effective risk processes, as well as building an organisational culture that supports integrity, accountability, honesty, openness, and responsiveness to change.

1.2 This policy sets out the key principles that guide risk management within NHS Devon.

1.3 Further advice and guidance is available from the Corporate Governance team by emailing d-icb.governance@nhs.net.

2. Purpose and Objectives

2.1. Risks will always occur. Many risks are manageable, but others pose a more serious possibility of impact on the organisation, staff, patients and / or the general public. Once identified, risks must be assessed, recorded, managed according to severity, reported and scrutinised.

2.2. NHS Devon is required by statute and by guidance from the Department of Health and Social Care (DHSC), to systematically identify and control all significant strategic and operational risks. These arise across the organisation and include clinical and corporate services.

2.3. The Board is required to ensure that robust risk management processes exist and assured that there are systems in place to control and manage risk and that these systems are working effectively. This involves the proactive identification and management of risks that may threaten achievement of NHS Devon's objectives, its statutory or regulatory duties and the response to adverse events or learning from audits and other independent reviews.

2.4. The Chief Executive Officer (CEO) is required to sign an Annual Governance Statement (as part of the Annual Report and Accounts) to provide reasonable assurance that NHS Devon has been properly informed about the totality of its risks and can evidence they have identified NHS Devon's strategic and corporate objectives, and managed the principal risks to achieving them. This includes all measures and practices that are used to control and manage risks. The system operates at all levels within NHS Devon and is continuously monitored for effectiveness on behalf of, and by, the Board.

2.5. This policy will:

- Establish a framework for risk management and board assurance which embraces organisational, financial, clinical, and non-clinical risks and in which all parts of the organisation are involved.
- Provide an environment for proactive decision making.
- Empower all staff to manage risk within delegated limits.
- Provide a proactive early warning system and enable a comprehensive response to mitigate risk where indicated.
- Establish a platform for managing risks within partnership working.
- Ensure the integration of risk management with NHS Devon's strategies and objectives and with local (directorate / team) objectives that these support.

2.6. This policy also helps to reduce the risk of fraud and bribery by providing a robust system of internal control for risk management. It supports and complements NHS Devon's Counter Fraud, Bribery and Corruption Policy and has been reviewed by the organisation's Local Counter Fraud Specialist. Fraud and bribery risks will be included in NHS Devon's risk register and its performance against standards will be assessed annually via completion of the NHS Counter Fraud Authority (CFA) Counter Fraud Functional Standard Return.

2.7. The NHS Devon Board recognises that risk management is an integral part of good management practice and an effective corporate governance framework and, to be most effective, it must become part of the organisation's culture. The Board is therefore committed to ensuring that risk management forms a part of the NHS Devon philosophy, practice, and planning, rather than being viewed or practised as a separate programme, and that responsibility for implementation is accepted at all levels of the organisation.

2.8. The Board acknowledges that the provision of appropriate training is central to the achievement of this aim.

2.9. A critical role of any Board is to focus on the risks that may compromise the achievement of the organisation's strategic and corporate objectives its statutory or regulatory duties. In order to be confident that the systems of internal control are robust, the NHS Devon Board must be able to provide evidence that it has systematically identified its strategic objectives and managed the principal risks to achieving them.

2.10. The NHS Devon Board is committed to the following key principles:

- **A Just Culture** – Staff reporting or directly involved in incidents are assured that any investigation will be carried out fairly, openly, transparently, without prejudice and with the aim of identifying learning and correcting underlying causes of the incident to prevent recurrence.
- **Freedom to Speak Up (Whistleblowing)** – All staff should be familiar with NHS Devon's Freedom to Speak Up: Raising Concerns (Whistleblowing) Policy, available on the staff intranet, which sets out

procedures and guidance to staff on raising concerns. NHS Devon has Freedom to Speak Up Guardians to whom staff may raise concerns; their details can be found on the staff intranet.

3. Definitions

3.1. For a full glossary of terms used within this policy document and in risk management in general, please refer to **Appendix A**.

Risk

3.2. Risk is defined as:

"An uncertain event or set of events, that should it occur, will have an effect on the achievement of objectives. A risk is measured by the combination of the probability of perceived threat or opportunity occurring and the magnitude of its perceived impact on objectives".

(Management of Risk: Guidance for Practitioners, Officer of Government Commerce, 2010)

3.3. For example, the potential occurrence of an event that may either cause harm or have an impact on patients, visitors, partner organisations, strategic objectives, assets and / or reputation.

3.4. In particular:

- Any element which has the potential to damage or threaten the achievement of the statutory or regulatory duties, strategic and corporate objectives, programmes, or service delivery of NHS Devon.
- Anything that could damage the reputation of NHS Devon and undermine the public's confidence in NHS Devon.
- Failure to guard against impropriety, malpractice, waste and / or poor value for money.
- Non-compliance with regulations and / or legislation such as those covering health and safety, safeguarding and the environment.
- An inability to respond to, or manage, changed circumstances in a way that prevents or minimises adverse effects on the delivery of NHS Devon's statutory or regulatory duties, strategic and corporate objectives.

3.5. NHS Devon distinguishes between **inherent risks** and **residual risks**. An inherent risk is one that is unmitigated whilst a residual risk is the risk that remains once the inherent risk has been mitigated or managed. **Appendix B** provides an illustration of the difference between these two types of risk.

Issues

3.6. An issue is an event that has happened or is happening. It is a 'known' as opposed to an 'unknown' quantity. The outcome of the actions and events is no longer subject to uncertainty as in the case of a risk. The consequences may be observed and measured. However, that is not to say that new risks will not emerge as the 'issue' continues.

In simplistic terms, the difference comes down to whether the event has the **potential to occur** (i.e. it is a risk), or **has already occurred** and the impact / consequence is now present (i.e. it is an issue).

Appendix C provides more detailed information in relation to the key differences between risks and issues. This policy does not mandate the recording of issues; it is for teams / directorates to decide whether to do so. Where this is the case, the level of detail and the related action plans to address an issue should be proportionate to the nature of the issue that has arisen.

Risk Management Principles

3.7. Risk management within NHS Devon will be carried out in accordance with the principles set out in **Appendix D**. Examples include alignment with objectives, fits the context, promotes, guides, and supports a clear and consistent approach, informs decision-making, facilitates continual improvement, and achieves measurable value.

4. Risk Management Activities and Processes

4.1. Risk management involves the following activities (see **Appendix E**):

4.1.1. **Identify the risk:** Consider how and why the successful achievement of a goal / objective might be prevented. Hazards, barriers, and challenges to achievement of objectives, at strategic and operational level, can be identified from a variety of internal and external sources such as staff resource issues, workforce recruitment problems, incompatibility of IT systems, a lack of assurance on areas of quality and performance data or information from staff and / or patients etc.

4.1.2. **Assess the risk:** Describe the risk and give it a succinct title which clearly identifies the risk, the area to which it relates and, where appropriate, the financial year to which it relates. Consider how the risk could occur, who or what might be involved, what the effect(s) would be if the risk were to materialise and how this could be reduced or minimalised. Describe the risk clearly and concisely; think in terms of the "**if**", "**then**", "resulting in" statement e.g. **if** (the cause – why the risk is happening) -, **then** (the risk event, that if it happened, could

have an impact on objectives) **resulting in** (the effect or impact of the risk – what will happen if the risk realises).

4.1.3. **Analyse, evaluate and score the risk:** Assess the likelihood of the risk materialising, and the level of its impact should it occur; it informs the risk score matrix. See **Appendix F** to assess whether the risk scores highly enough to take action. The total risk score will also determine whether the risk is managed at a team / directorate level or via the NHS Devon Corporate Risk Register (CRR).

4.1.4. **Treat the risk:** Determine which of the following actions will be required:

Treatment	Treatment Description
Treat	Draw up a specific action plan (which includes consideration of funding / associated costs) to reduce the impact or likelihood scores to an acceptable level, as articulated in the 'risk appetite' agreed by the NHS Devon Board, in order to gain further control.
Tolerate	It is not always possible to identify and then fully implement actions that eliminate or minimise the risk. Where this is the case, it is essential that the significance of the risk that remains (the residual risk) is understood and the organisation, in accordance with the level of authority for risk management, confirms that it is prepared to accept that level of risk.
Transfer	Transfer the risk to another organisation (this is rare).
Terminate	Close the risk (subject to approval) – for example, decide to no longer do the activity that is causing the risk.

4.1.5. **Report the risk:** All identified risks should be recorded on a risk register; the risk score determines where it is reported:

4.1.5.1. **All team / directorate risks** (generally scoring 10 or below) are reported and managed locally via a team / directorate risk register. The risk register should be reviewed monthly and escalated to the relevant Chief Officer as required.

A quarterly review of all team / directorate risk registers should be undertaken by the Corporate Governance team to ensure oversight of any risks that may need to be escalated.

All teams / directorates should maintain their own risk registers.

If a risk is deemed to be a risk to the achievement of NHS Devon's statutory or regulatory duties, corporate objectives or statutory purposes, and not just those of the team / directorate, and scores 12 or above, then it can be escalated for inclusion on the NHS Devon Corporate Risk Register (CRR).

4.1.5.2. **All project / programme risks** (any score) are reported and managed locally via a project / programme risk register. The risk register should be reviewed regularly by the Project / Programme Manager. Where there is a significant risk to the non-achievement of the project / programme objective which may then pose a further risk to the achievement of an organisational statutory or regulatory duty, objective, operational or strategic, the Project / Programme Manager will discuss with the most senior officer with portfolio responsibility for the risk and seek advice and guidance from the central Corporate Governance team as appropriate.

4.1.5.3. **All operational risks** (generally scoring 12 and above) are added to the NHS Devon Corporate Risk Register (CRR); this is done in conjunction with a member of the Corporate Governance team. Operational risks are reviewed on a monthly basis. The review is overseen by a member of the Corporate Governance team.

Operational risks scoring 15 and above are reported alongside the Board Assurance Framework (BAF) to the Executive Committee.

4.1.5.4. **All strategic risks** (generally scoring 15 and above) are included on the Board Assurance Framework (BAF) and are reviewed regularly and reported alongside operational risks (scoring 15 and above) to the Executive Committee, the NHS Devon Board, and where appropriate, its associated Assurance Committees.

Refer to **Appendix G** for a summary of risk action and reporting requirements.

4.1.6. **Monitor / review the risk:** Monitor the risk impact and review the effectiveness of action / actions taken. It is important to consider whether the risk score / risk priority has changed as a result.

4.1.7. **Communicate with and consult those impacted by the risk:** It is important to identify who is affected by the risk and who needs to know about it e.g. internally and / or externally.

5. Strategic and Operational Risks

5.1. Risk related activity within NHS Devon is derived from two directions

- **Bottom up:** Individuals, teams, directorates, Chief Officers, the Executive Committee, and Board Assurance Committees can identify a risk and this risk would then be recorded and managed accordingly in accordance with the details laid out in this policy document. These risks are operational risks. Those risks scoring 10 or below are included on team / directorate risk registers and those scoring 12 or above form the NHS Devon Corporate Risk Register (CRR).
- **Top down:** The NHS Devon Board discusses and agrees those strategic risks that it considers the organisation faces in the achievement of its statutory or regulatory duties, agreed corporate objectives or other statutory functions. These form the strategic risks of NHS Devon and are recorded in its Board Assurance Framework (BAF).

5.2. Both operational and strategic risks should be aligned to NHS Devon's statutory or regulatory duties and objectives (as articulated in the Integrated Care Strategy and Joint Forward Plan (JFP)). In the absence of corporate objectives at any point, operational and strategic risks should be expressed and recorded against

either one of the four statutory purposes of Integrated Care Boards:

- Improve outcomes in population health and healthcare.
- Reduce health inequalities in outcomes, experience, and access.
- Enhance productivity and Value for Money (VfM).
- Support broader social and economic development.

or one of the six themes of the NHS Oversight Framework:

- Quality of care, access & outcomes.
- Preventing ill-health and reducing inequalities.
- Finance and use of resources.
- People.
- Leadership & capability.
- Local strategic priorities.

5.3. **Risk Scores** are calculated in accordance with the National Patient Safety Agency (NPSA) Model Risk Matrix and are the product of the impact / consequence and the likelihood of the risk arising (see **Appendix F**).

5.4. NHS Devon adheres to the Nolan Principles of openness and accountability, however occasionally there is the requirement to make a risk **confidential** which means that it is not reported within the public domain. A risk can be classified as confidential, with the approval of the Corporate Governance team and Chief Officer, if it contains clinically or commercially sensitive information. The classification of a risk as being confidential due to clinically sensitive

information also requires the approval of either the Chief Medical Officer (CMO) or the Chief Nursing Officer (CNO).

6. Corporate Risk Register (CRR)

6.1. **Risk escalation to the NHS Devon Corporate Risk Register** (CRR) - All teams / directorates should maintain their own risk registers. If a risk is deemed to be a risk to the achievement of NHS Devon's statutory or regulatory duties or corporate objectives, and not just those of the team or directorate, and score 12 or above, then it can be escalated for inclusion on the NHS Devon Corporate Risk Register (CRR). The Corporate Governance team reviews any such risk with the risk assessor and owner to establish whether this is appropriate, and the scoring is proportionate. If the risk is deemed appropriate for inclusion, it is added to the NHS Devon Corporate Risk Register (CRR).

6.2. **Risk Management System** – All managers have a responsibility to record identified corporate risks on NHS Devon's risk management system. This ensures risks at all levels are held in a central location which is fully auditable (please contact the Corporate Governance team for access to and training on how to use the risk management system if required). The use of the risk management system enables staff to add new risks or make updates to existing risks at any time. Corporate risks must be reviewed and updated every month by the named assessor. Following this review the update will be agreed by the risk owner and reported as appropriate.

6.3. Regular reviews are undertaken across NHS Devon to ensure that:

- New risks are identified and assessed.
- A careful watch is maintained on cumulative risk across NHS Devon to ensure that this is identified and properly escalated.
- Existing risks and their mitigating actions are tracked and kept up to date.
- A summary of all incidents within teams / directorates is reviewed and this information is disseminated to ensure that appropriate learning takes place to reduce future risks.
- Risks that are no longer being faced by NHS Devon are closed.

6.4. The full process for the identification, scoring, management and reporting of risks is detailed withinthe Standard Operating Procedures (SOPs) that support this policy document.

7. Board Assurance Framework (BAF)

7.1. The Board Assurance Framework (BAF) provides a structure and process that enables NHS Devon to focus on the risks that might compromise achieving its most important goals and objectives, to map the controls that should be in place to manage those objectives, and to confirm that the Board has sufficient

assurance regarding the effectiveness of those controls. The Board Assurance Framework (BAF) also identifies any gaps in control and / or assurance and articulates action plans in place to address them.

7.2. In advance of each financial year, the NHS Devon Board should agree overarching corporate goals for that year. These goals have a number of underpinning corporate objectives. The Board Assurance Framework (BAF) captures these corporate goals and the strategic risks applicable to them. Each goal and the strategic risks associated with this goal will be assigned to a Board Assurance Committee for scrutiny, monitoring, and testing of whether evidence provided to substantiate the levels of control applied. In the absence of corporate objectives at any point, operational and strategic risks are expressed and recorded against

either one of the four Statutory Purposes for Integrated Care Boards, those being:

- Improve outcomes in population health and healthcare.
- Reduce health inequalities in outcomes, experience, and access.
- Enhance productivity and Value for Money (VfM).
- Support broader social and economic development.

or one of the six themes of the NHS Oversight Framework:

- Quality of care, access & outcomes.
- Preventing ill-health and reducing inequalities.
- Finance and use of resources.
- People.
- Leadership & capability.
- Local strategic priorities.

7.3. Any Board Assurance Committee responsible for scrutinising an area of risk can escalate a risk onto the Board Assurance Framework (BAF) when one or more of the following criteria are met:

- The current score is significantly in excess of the target score;
- It is a long-standing risk that shows little or no reduction in current risk score; or
- The Committee has not received sufficient assurance that the risk is being appropriately and effectively managed.

7.4. The Board Assurance Framework (BAF) is updated by Chief Officers in conjunction with the Corporate Governance team, on a bi-monthly basis, and reported to the Executive Committee for recommendation to the NHS Devon Board. The Board Assurance Framework (BAF) will set out the controls, assurances, gaps and associated mitigating actions relating to each gap. The details in relation to mitigating actions will also require an ‘action owner’, the ‘action status’ and ‘planned implementation date’ to be recorded; this is so that progress against plan can be monitored, and corrective action taken where there is deviation from plan.

7.5. The Board Assurance Framework (BAF) will be used as a tool for setting the agendas of Board meetings and development sessions (as well as Board Assurance Committee agendas). It will be presented at each formal meeting. To be an effective tool, it should be possible to map items identified in the Board Assurance Framework (BAF) to papers presented to the meeting which address those items. This may be through specific papers, or within standing agenda items such as finance, quality, or performance report.

8. Risk Appetite

8.1. NHS Devon's **Risk Appetite Statement** documents the delegation of risk taking from the Board to senior management. It specifies the overall risk levels that the Board is willing to accept whilst operating in full compliance with regulatory and legal requirements.

8.2. **Risk appetite** is defined as "the amount and type of risk that an organisation is prepared to pursue, retain or take in pursuit of its strategic aims and objectives" and is key to achieving effective risk management. It can be influenced by personal experience, political factors, and external events.

8.3. It represents a balance between the potential benefits of innovation and the threats that change, and improvement inevitably bring. It should be at the heart of the systems and processes in place to manage risk within NHS Devon, as well as how decisions are taken.

8.4. The NHS Devon Board should articulate, as part of the annual risk cycle, its appetite in relation to each of the statutory or regulatory duties or corporate objectives, expressed using the following Corporate Governance Institute (CGI) Framework:

Risk Appetite Level	Risk Appetite Level - Description
Avoid	The avoidance of risk and uncertainty is a key organisational objective
Minimal	(ALARP – As Little As Reasonably Possible): The preference for ultra-safe delivery options that have a low degree of inherent risk and only for limited reward potential
Cautious	The preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward
Open	Willing to consider all potential delivery options and choose while also providing an acceptable level of reward and Value for Money (VfM)
Seek	Eager to be innovative and to choose options offering potentially

Risk Appetite Level	Risk Appetite Level - Description
	higher business rewards despite greater inherent risk
Mature	Confident in setting higher levels of risk appetite because controls, forward scanning and responsiveness systems are robust

8.5. Based on risk appetite, a 'target' risk score is set for individual risks, this is the level to which the risk is managed to. The benefits of this approach include:

- Management focus on risks that can be managed / reduced;
- Identification of targeted actions to reduce risks to 'target';
- Timely reduction of risks;
- Identification of static risks / ineffective actions; and
- Management focus on risks that are not reducing.

8.6. The process for setting and reviewing risk appetite (including 'target' risk scores) is detailed in **Appendix H** together with the current risk appetite statement agreed by the NHS Devon Board.

9. Accountabilities, Duties and Responsibilities

9.1. The **NHS Devon Board** is ultimately responsible for the organisation's systems of internal control (financial, organisational, clinical, and non-clinical) and risk management arrangements, and for demonstrating leadership, active involvement, and support for risk management across the organisation. It is supported in the discharge of its responsibilities by the Audit & Risk Committee (ARC), other Assurance Committees, and the Executive Committee.

The Board receives assurance as to whether operational and strategic risks are being effectively managed. It reviews and approves the Board Assurance Framework (BAF) on a regular basis to monitor the actions and assurances against the strategic risks and assesses the overall impact on delivery of the NHS Devon statutory/regulatory duties or corporate objectives.

In addition to the above, it is also responsible for determining the risk appetite of NHS Devon and for approving the organisation's Risk Management Policy.

9.2. The **Audit & Risk Committee** (ARC) provides an objective view on internal control and risk management systems to the NHS Devon Board that is independent of the executive. The Audit & Risk Committee (ARC) also:

- Reviews the adequacy and effectives of the system of integrated governance and risk management and internal control across the whole of the NHS Devon activities that support the achievement of its objectives, and to highlight any areas of weakness to the NHS Devon Board.

- Reviews the adequacy and effectiveness of the assurance processes that indicate the degree of achievement of NHS Devon's statutory/regulatory duties or objectives, the effectiveness of the management of principal risks.
- Maintains oversight of organisational and system risks where they relate to the achievement of NHS Devon's statutory or regulatory duties or objectives; the Board maintains overall responsibility for risk management.
- Seeks reports and assurance from directors and managers as appropriate, concentrating on the systems of integrated governance, risk management and internal control, together with indicators of their effectiveness.
- Reviews the outcome of the annual internal audit of governance and risk management arrangements which, along with other assurances received, will enable the committee to recommend the Annual Governance Statement is signed off by the Chief Executive Officer (CEO) at the end of each financial year.
- Identifies opportunities to improve governance, risk management and internal control processes across NHS Devon.

The Chair of the Audit & Risk Committee (ARC) will provide a summary to the NHS Devon Board of its assurances and where necessary, request deep dives to be undertaken in areas of risk where further assurances are required.

9.3. The **Head of Internal Audit** (HoIA) is responsible for implementing a programme of verification to ensure that the risk management systems and controls NHS Devon has in place are sufficient and will enable the provision of an audit assurance opinion to the Chief Executive Officer (CEO) and the Audit & Risk Committee (ARC).

9.4. The **NHS Devon Board Assurance Committees** have specific roles in relation to the statutory/regulatory duties or strategic risks assigned to them and as set out in their Terms of Reference.

9.5. The Executive Committee provides oversight and delivery of risk management arrangements. It regularly has oversight of the NHS Devon Corporate Risk Register (CRR) to review whether individual operational risks are being effectively managed and whether the action plans are sufficient and having the desired effect within the agreed timescales. In addition, it regularly has oversight of the Board Assurance Framework (BAF) to monitor the actions and assurance against the strategic risks and to assess the overall impact on delivery of NHS Devon's statutory/regulatory duties or corporate objectives, and approves its submission to the NHS Devon Board.

9.6. The **Chief Executive Officer** (CEO) has overall responsibility for ensuring that an effective risk management system is in place. They are also responsible for ensuring that there is an adequate system of internal control in place. The work of ensuring that this system is in place is delegated to the Company Secretary in practice, who is also responsible for overseeing the management and maintenance of the Board Assurance Framework (BAF) and ensuring the Board follows due process with regards to the overall

management of risk. The Company Secretary is accountable to the Chief Communications and Partnerships Officer and is responsible for ensuring (and reporting to the Board and to the Audit & Risk Committee (ARC)) that systems and structures are in place for the effective management of financial risk and organisational controls.

The Chief Executive Officer (CEO) is responsible for the preparation of an Annual Governance Statement setting out how these responsibilities have been discharged.

9.7. The **Chief Nursing Officer** (CNO) is accountable to the Chief Executive Officer (CEO) and is responsible for ensuring (and reporting to the Board or appropriately established committees) that systems and structures are in place for the effective management of clinical quality and safety. As the **Caldicott Guardian** they ensure that the Caldicott principles for managing information and ensuring its security and integrity are adhered to by staff within NHS Devon.

9.8. The **Chief Medical Officer** (CMO) provides Clinical Leadership for NHS Devon and is accountable to the Chief Executive Officer (CEO) and is responsible for providing strategic and operational leadership and management of the clinical risk within NHS Devon and organisational assurance on all matters of clinical risk and clinical outcomes to the NHS Devon Board.

9.9. The **Corporate Governance team** is responsible for overseeing the day-to-day management and co-ordination of the risk management system.

9.10. The **Risk Manager** is responsible for providing support and advice on risk management issues across NHS Devon. In addition, they will work closely with specialist advisers within NHS Devon who provide advice on specific areas of risk management, for example, Health and Safety; Fire; Infection Control; Manual Handling; Security; Fraud and Information Governance. The Risk Manager will provide information about corporate and strategic risks for the Executive Committee, Board Assurance Committees, and the NHS Devon Board. This forms the basis of 'bottom up' population of the risk register and will be used to inform the Corporate Risk Register (CRR) and the Board Assurance Framework (BAF). They are responsible for the ongoing development, implementation, and evaluation of risk management systems. These systems will align with the requirements of related regulatory bodies such as NHS England and the Care Quality Commission (CQC).

9.11. The **Senior Information Risk Owner** (SIRO) is accountable to the Chief Executive Officer (CEO) and is responsible for managing information assets and risks across the organisations. The role of the Senior Information Officer (SIRO) for NHS Devon is undertaken by the Chief Communications and Partnerships Officer.

9.12. The **Company Secretary** reports to the Chief Communications and Partnerships Officer and is responsible for ensuring the development and

implementation of Risk Management Policy across NHS Devon, ensuring that risk management processes are effectively coordinated, implemented, and monitored. This responsibility incudes:

- Maintenance of the Board Assurance Framework (BAF) and the NHS Devon Corporate Risk Register (CRR) as active documents with clear monitoring of mitigation and action plans.
- Supporting the implementation of NHS Devon's Risk Management Policy (including the provision of advice and training).
- Overseeing and reporting on risk management compliance requirements.

9.13. All **Chief Officers*, Senior Leadership Team** members and **Managers** are responsible for:

- Implementing the Risk Management Policy and procedures within their scope of responsibility.
- Ensuring that NHS Devon's risk management processes, including risk assessments, monitoring and escalation of cumulative risks and regular reviews are embedded in their team / programme management functions, included as a standing item on the monthly team meeting agenda and ensuring risk discussions are minuted or included in an action log.
- Ensuring that NHS Devon's risk management processes, including risk assessments, are in place within their scope of responsibility.
- Ensuring that relevant risks are identified, assessed, reviewed, and appropriately managed.
- Ensuring that they discuss risks with relevant senior managers and directors as appropriate.
- Implementing and monitoring any risk management actions within their designated area. Where local actions are considered to be inadequate, senior managers are responsible for escalating these risks through the agreed committee or management structure if local resolution has not been satisfactorily achieved.
- Reviewing a summary of all incidents within their teams or their scope of responsibility on a regular basis and disseminating this information to ensure that appropriate learning takes place in order to reduce risks.
- Ensuring that all staff are given the necessary information and training to enable them to be aware of the risks to their local objectives, those in their work environment and of their personal responsibilities and responsibilities towards working safely.
- Ensuring that staff undertake all relevant mandatory training.
- Ensuring staff compliance with this document.

* *It should be noted that a Chief Officer can delegate any of the responsibilities outlined above to their deputy but delegation below this level is not permitted.*

Where delegation is granted, this should be communicated by the Chief Officer in writing to the Corporate Governance team (and specifically the Risk Manager).

9.14. All **Staff** have a responsibility to co-operate with managers and they are encouraged to identify risks and advise their line managers accordingly. Risk management is the responsibility of all employees. Key responsibilities include:

- Being familiar, and complying with, the Risk Management Policy and supporting procedures and with all other relevant policies and procedures.
- Reporting incidents, accidents and "near misses" following procedures set out in the Incident Reporting Policy and supporting procedures.
- Being aware of their duty under legislation to take reasonable care for personal safety and the safety of all others who may be affected by the business of NHS Devon.
- Complying with NHS Devon rules, regulations, and instructions to protect the health, safety, and welfare of anyone affected by the business of NHS Devon.

10. Monitoring Compliance and Effectiveness

Training

10.1. Knowledge of how to manage risk is essential in embedding and maintaining an efficient risk management system. To this end, the Corporate Governance team will work in conjunction with Human Resources (HR) to conduct a Training Needs Analysis (TNA) to ensure that the necessary training and education needs, and methods needed to implement this policy and any supporting procedure(s) are identified and resourced as required. This may include identification of external training providers and / or development of an internal training process. Once the TNA has been undertaken, the Risk Management Training Schedule will be appended to this policy document at **Appendix I**.

10.2. The TNA and Risk Management Training Schedule will be reviewed and updated periodically so that it reflects the changing needs of the organisation and / or when there are significant changes in risk management arrangements (including changes to this policy or any of its related processes).

Implementation

10.3. NHS Devon Managers, or their designated representatives, will implement this policy by:

- Notifying all staff of its existence. New staff will be informed of this policy as part of their induction.
- Destroying all superseded paper-based versions of the policy and electronic versions retained in their area.

- Having adequate knowledge of, and / or access to, all relevant legislation in order to ensure that compliance with such legislation is maintained.
- Discussing with staff as part of their regular one-to-ones how they seek to achieve their individual objectives around policy review and maintenance.

Review

10.4. NHS Devon will review its performance on risk management through a specific annual internal audit on Risk and Assurance Processes. This annual audit is submitted to the Audit & Risk Committee (ARC) and is reflected in the Head of Internal Audit Opinion (HIAO) on the organisational arrangements for risk management and internal control.

10.5. The Chief Executive Officer (CEO) will review compliance with, and effectiveness of, the risk management system of internal control annually in preparing the Annual Governance Statement.

10.6. The Audit & Risk Committee (ARC) will review risk through information submitted to it throughout the year. In addition to this, risk reports will be submitted to the NHS Devon Board Assurance Committees as appropriate. These Committees can request information on specific risks to seek further assurance and details of actions being taken to address the risk.

10.7. The NHS Devon Risk Appetite will be reviewed annually by the NHS Devon Board.

10.8. Any trends resulting from possible policy non-compliance will be raised with staff through appropriate management routes.

10.9. Delivery and records of attendance at risk management awareness training will be reviewed annually by the Corporate Governance team.

11. References

Other related policy documents

11.1 Freedom to Speak Up: Raising Concerns (Whistleblowing) Policy
11.2 Internal Incident Policy
11.3 Serious Incidents Policy

Legislation and statutory requirements

11.4 Equality Act 2010:
www.legislation.gov.uk/ukpga/2010/15/contents

11.5 Freedom of Information Act 2000:
www.legislation.gov.uk/ukpga/2000/36/contents
ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

11.6 Health and Safety at Work Act 1974:
www.hse.gov.uk/legislation/hswa.htm

11.7 Human Rights Act 1998:
www.legislation.gov.uk/ukpga/1998/42/contents

11.8 Management of Health and Safety at Work Regulations 1999:
www.legislation.gov.uk/uksi/1999/3242/contents/made
www.hse.gov.uk/pubns/hsc13.pdf

Best practice recommendations and other key guidance

11.9 Caldicott Principles:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/942217/Eight_Caldicott_Principles_08.12.20.pdf

11.10 Department of Health and Social Care Group Accounting Manual 2021/2022:
www.gov.uk/government/publications/dhsc-group-accounting-manual-2020-to-2021

11.11 Good Governance Institute ‘The New Good Governance Handbook 2016’:
www.good-governance.org.uk/wp-content/uploads/2017/04/The-new-Integrated- Governance-Handbook-2016.pdf

11.12 Federation of European Risk Management Associations (FERMA):
www.ferma.eu/about/about-ferma

11.13 Financial Reporting Council ‘UK Corporate Governance Code 2018’:
www.frc.org.uk/directors/corporate-governance-and-stewardship/uk-corporate-governance-code

11.14 Health and Safety Executive ‘Managing for Health and Safety 2013’:
www.hse.gov.uk/pubns/books/hsg65.htm

11.15 The Institute of Risk Management ‘A Risk Management Standard 2002’:
www.theirm.org/media/4709/arms_2002_irm.pdf

11.16 International Organisation for Standardisation (ISO) Guide ‘73:2009 Risk Management’ (Revised 2016):
www.iso.org/standard/44651.html

11.17 NHS England - Learning from patient safety events:
https://www.england.nhs.uk/patient-safety/patient-safety-insight/learning-from-patient-safety-events/

11.18 NHS Resolution:
resolution.nhs.uk/

11.19 NHS Leadership Academy – The Healthy NHS Board 2013:
www.leadershipacademy.nhs.uk/wp-content/uploads/2013/06/NHSLeadership-HealthyNHSBoard-2013.pdf

11.20 HM Government: The Orange Book – Management of Risk – Principles and Concepts:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1154709/HMT_Orange_Book_May_2023.pdf

APPENDIX A: Glossary of Terms

Terms	Definition
Acceptance	Informed decision to take a particular risk.
Avoidance	Informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk.
Consequence	Outcome of an event affecting objectives.
Control	Measure that is modifying risk. Control include any process, policy, device, practice, or other actions which may modify risk.
Governance	Is a system by which organisations are directed and controlled. It defines accountabilities, relationships and the distribution of rights and responsibilities among those who work with and in the organisation, determines the rules and procedures through which the organisation's objectives are set, and provides the means of attaining those objectives and monitoring performance. This includes the establishing, supporting, and overseeing the risk management framework.
Likelihood	Chance of something happening.
Monitoring	Continual checking, supervising, critically observing, or determining the status in order to identify change from the performance level or expected. Monitoring can be applied to a risk management framework, risk management process, risk, or control.
Residual Risk	Risk remaining after risk treatment.
Resilience	Capacity of an organisation to adapt in a complex and changing environment.
Risk	Is the effect of uncertainty on objectives. Risk is usually expressed in terms of causes, potential events, and their consequences.
Risk Appetite	Amount and type of risk that an organisation is willing to pursue or retain.
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation.
Risk Management	Is the co-ordinated activities designed and operated to manage risk and exercise internal control within an organisation.
Risk Management Process	Systematic application of management policies, procedures, and practices to the activities of communicating, consulting, establishing context, and identifying, analysing, evaluating, treating, monitoring, and reviewing risk.

Terms	Definition
Risk Matrix	Tool for ranking and displaying risks by defining ranges for likelihood and impact.
Risk Owner	Person with the accountability and to make a decision regarding the management of a risk.
Risk Profile	Description of any set of risks.
Risk Register	Record of information about identified risks. The term 'risk log' is sometimes used instead of 'risk register'.
Risk Reporting	Form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management.
Risk Source	Element(s) which alone or in combination has the intrinsic potential to give rise to risk.
Stakeholder	Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.
Treatment	Process to modify risk. Risk treatment can involve: ▪ Avoiding the risk by deciding not to start or continue with the activity that gives risk to the risk; ▪ Taking or increasing the risk in order to pursue an opportunity; ▪ Removing the risk source; ▪ Changing the likelihood; ▪ Changing the impact; ▪ Sharing the risk with another party or parties (including contracts); and ▪ Retaining the risk by informed decision. Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".

APPENDIX B: Inherent and Residual Risk

NB: This is a procedural document separate to the Risk Management Policy and may be amended without requiring the amendment of the policy.

Event	Inherent Risk
Event: Getting into the driving seat of a car, turning on the engine and moving of off	**Inherent Risk:** Damage to vehicles and injury to driver, other road users and pedestrians
Risk Management Action	***Residual Risk***
▪ Instructions to check mirrors and use indicators appropriately before moving off and to wear a seat belt	▪ Reduced possibility of damage to vehicles and injury to driver, other road users and pedestrians
Further Risk Management Action	***Residual Risk***
▪ Driver must obtain permission to move off from passenger who will ensure that mirrors are checked, indicator used appropriately, and seat belt is properly worn	▪ Further reduced of the possibility of damage to vehicles and injury to driver, other road users and pedestrians
Further Risk Management Action	***Residual Risk***
▪ In addition to the two measures above the car is immobilised, that is mechanically unable to move, until such a time as the passenger is satisfied that all safety precautions have been undertaken. The passenger will then flick a switch which will disengage the immobiliser	▪ Even less possibility of damage to vehicles and injury to driver, other road users and pedestrians

APPENDIX C: Risks and Issues

NB: This is a procedural document separate to the Risk Management Policy and may be amended without requiring the amendment of the policy.

The table below summarises the key differences between 'risks' and 'issues':

RISK	ISSUE
An event that **may** occur	An event that is **currently happening or has happened**
Described in the **future tense**	Described in the **present tense**
Has a material impact on objectives[1]	Has a material impact on objectives[1]
Can be **beneficial or harmful / positive or negative**	**Issue itself is always negative** *(however, the outcome of solving an issue may still be beneficial, albeit it may take more time and effort)*
Can be mitigated against to prevent the risk from becoming an issue	**Prevention is not possible**; action is needed to mitigate its impact or to resolve the issue
Management Techniques: **Reduce risk; transfer the risk; manage the risk; contingency plan; accept risk or terminate risk**	Management Techniques: **Problem solving; decision-making**

[1] *Material Impact on Objectives – this can be in terms of programme / project objectives, team objectives, directorate objectives, corporate objectives, or strategic objectives.*

APPENDIX D: Risk Management Principles

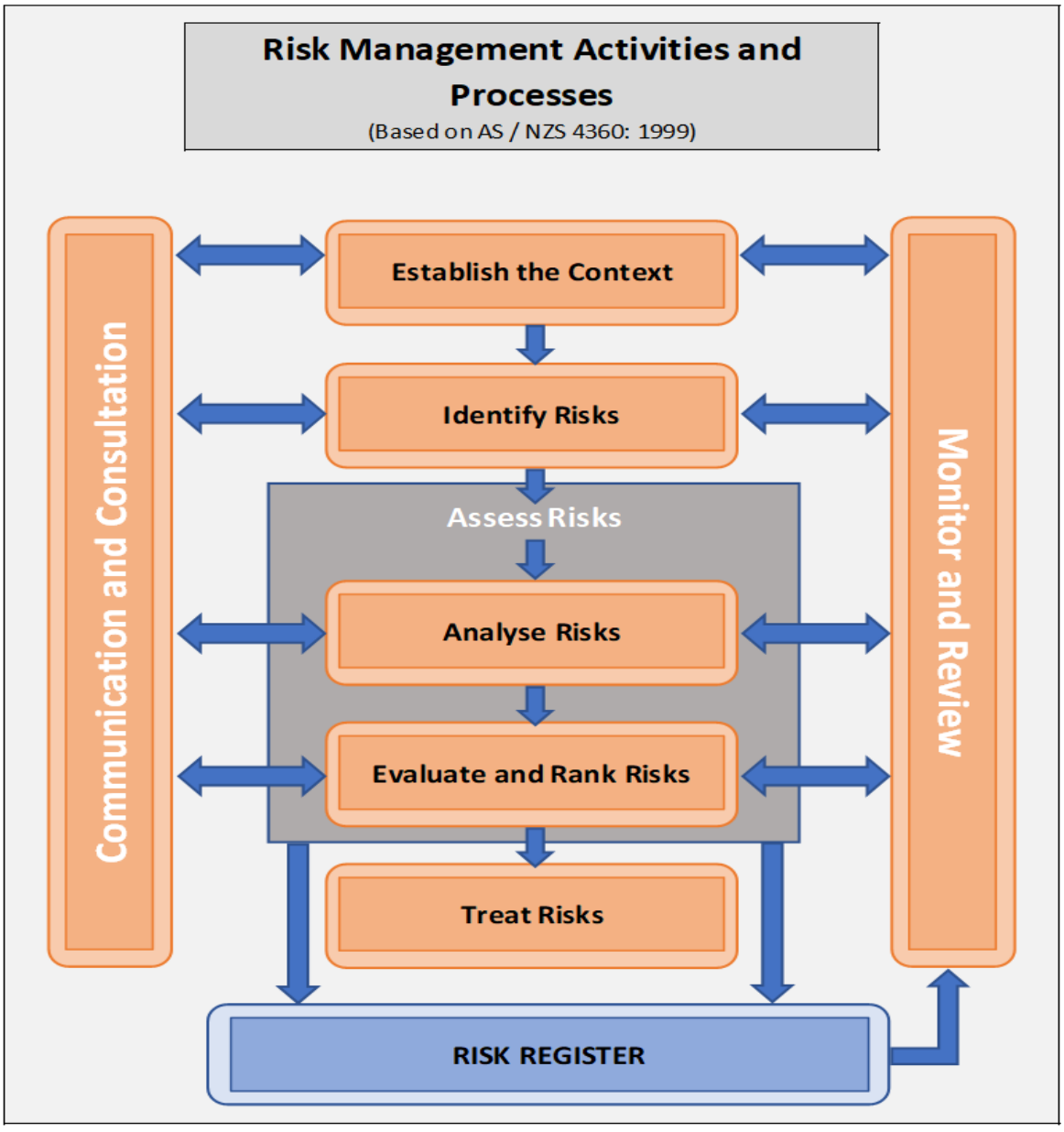
NB: This is a procedural document separate to the Risk Management Policy and may be amended without requiring the amendment of the policy.

Principle	Principle Description
Proactive	Risk management will be used proactively to manage key risks and used as an active management tool. This helps to ensure that risks are considered, and future actions planned in a visible, consistent, and controlled manner. Risk management will form part of plans with work on risk management being front loaded.
Aligns with Objectives	Risk management will be focused on the key uncertainties which may impact on the achievement of one or more objectives. Risks will be identified and given the appropriate priority for action.
Fits the Context	The risk management approach will be designed to fit the internal and external environment in which NHS Devon operates and so that time, effort, resources, and energy will be used in the appropriate way.
Engages Partners and Stakeholders	Risk management will engage with the right partners and stakeholders in the Integrated Care System (ICS) and deal with different perceptions of risk. Appropriate risks will be identified early and dealt with at the right level.
Promotes, Guides and Supports a Clear and Consistent Approach	Risk management will provide clear and coherent guidance to staff and key stakeholders so everyone can see how NHS Devon identifies, assesses, and controls key risks, and is consistent across the organisation. This enables people to compare results with plans and enable better decision making about how resources will be deployed. It also provides clear guidance on roles within risk management and explains responsibilities and accountabilities.
Informs Decision Making	Risk management will be linked to and inform decision making across the organisation. This enables important decisions to be made with explicit consideration of the impact of risks and the status of risk management. This also helps to safeguard the decision making process to allow for good decision making.
Facilitates Continual Improvement	Risk management will be used to help NHS Devon to improve by proactively managing risks and increasing organisational risk maturity. The organisation will use its experience of risk management to continually improve through 'lessons learned' and best use of the resources available.
Creates a Supportive Culture	NHS Devon will create a culture that recognises uncertainty and supports considered risk taking. The organisation recognises that zero risk taking is neither possible nor desirable.
Achieves Measurable Value	Risk management will help to achieve measurable value through the effective identification and management of key risks. In general, it costs less to anticipate and manage a risk than it does to recover from an issue.

APPENDIX E: Risk Activities and Processes

NB: This is a procedural document separate to the Risk Management Policy and may be amended without requiring the amendment of the policy.

The following diagram sets out NHS Devon's approach to risk management:



APPENDIX F – Model Risk Matrix

NB: This is a procedural document separate to the Risk Management Policy and may be amended without requiring the amendment of the policy.

Instructions for use:

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

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

3. Use **Table 2** to determine the likelihood score (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 by multiplying the impact by the likelihood: I (impact) x L (Likelihood) = R (risk score) - **See Table 3**.

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, the risk ratings and the organisations' risk management system. Include the risk in the organisations' risk register at the appropriate level.

Table 1 – Impact (Consequences) - Scores

Impact (Consequence) Score (Severity Levels) and Examples of Descriptors					
	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

Impact (Consequence) Score (Severity Levels) and Examples of Descriptors					
	1	2	3	4	5
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Quality of Service	Peripheral element of treatment or service suboptimal Informal complaint	Overall treatment or service suboptimal Formal complaint (stage 1) Local resolution Single failure to meet internal standards Minor implications for patient safety if unresolved Reduced performance rating if unresolved	Treatment or service has significantly reduced effectiveness Formal complaint (stage 2) complaint Local resolution (with potential to go to independent review) Repeated failure to meet internal standards Major patient safety implications if findings are not acted on	Non-compliance with national standards with significant risk to patients if unresolved Multiple complaints / independent review Low performance rating Critical report	Totally unacceptable level or quality of treatment / service Gross failure of patient safety if findings not acted on Inquest / ombudsman inquiry Gross failure to meet national standards
Human Resources / Organisational Development / Staffing / Competence	Short-term low staffing level that temporarily reduces service quality (< 1 day)	Low staffing level that reduces the service quality	Late delivery of key objective / service due to lack of staff Unsafe staffing level or competence (>1 day) Low staff morale Poor staff attendance for mandatory / key training	Uncertain delivery of key objective / service due to lack of staff. Unsafe staffing level or competence (>5 days). Loss of key staff. Very low staff morale. No staff attending mandatory / key training	Non-delivery of key objective / service due to lack of staff Ongoing unsafe staffing levels or competence Loss of several key staff No staff attending mandatory training / key training on an ongoing basis

Impact (Consequence) Score (Severity Levels) and Examples of Descriptors					
	1	2	3	4	5
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Statutory Duty / Inspections	No or minimal impact or breach of guidance / statutory duty	Breach of statutory legislation Reduced performance rating if unresolved	Single breach in statutory duty Challenging external recommendations / improvement notice	Enforcement action. Multiple breaches in statutory duty. Improvement notices Low performance rating Critical report	Multiple breaches in statutory duty. Prosecution Complete systems change required. Zero performance rating. Severely critical report
Adverse Publicity / Reputation	Rumours Potential for public concern	Local media coverage – short- term reduction in public confidence	Local media coverage –long-term reduction in public confidence	National media coverage with service well below reasonable public expectation <3 days	National media coverage with service well below reasonable public expectation >3 days MPs concerned (questions in the House).
Business Objectives / Projects	Insignificant cost increase / schedule slippage	Elements of public expectation not being met. <5 per cent over project budget Schedule slippage <5 per cent	5–10 per cent over project budget Schedule slippage 5–10 per cent over	11–25 per cent over project budget Schedule slippage 11–25 per cent over Key objectives not met	Incident leading to >25 per cent over project budget Schedule slippage >25 per cent over Key objectives not met

Impact (Consequence) Score (Severity Levels) and Examples of Descriptors					
	1	**2**	**3**	**4**	**5**
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Finance, Including Claims Service / Business Interruption Environmental Impact	Small loss Risk of claim remote Business loss / interruption of >1 hour Minimal or no impact on the environment	Loss of 0.1 – 0.25 per cent of budget Claim less than £10,000 Business loss / interruption of >8 hours Minor impact on environment	Loss of 0.26 – 0.5 per cent of budget Claim(s) between £10,000 and £100,000 Business loss / interruption of >1 day Moderate impact on environment	Uncertain delivery of key objective / Loss of 0.6 – 1.0 per cent of budget Claim(s) between £100,001 and £1 million Purchasers failing to pay on time Business loss / interruption of >1 week Major impact on environment	Non-delivery of key objective Loss of >1 per cent of Budget. Failure to meet specification / slippage. Payment by results Claim(s) >£1 million Permanent loss of service or facility Catastrophic impact on environment

Table 2 - Likelihood Scores (L)

What is the likelihood of the risk occurring?

The frequency-based score is appropriate in most circumstances and is easier to identify. It should be used whenever it is possible to identify a frequency.

Likelihood Score	**1**	**2**	**3**	**4**	**5**
Description	**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 / recur occasionally	Will probably happen / recur but it is not a persisting issue	Will undoubtedly happen / recur, possibly frequently

Table 3 - Risk Scoring = Impact x Likelihood (I x L)

Impact / Consequence	**Likelihood**				
	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 as follows:

	1 to 6	**Low Risk**
	8 to 10	**Moderate Risk**
	12	**High Risk**
	15 to 25	**Extreme Risk**

APPENDIX G:
Risk Action and Reporting Requirements

NB: This is a procedural document separate to the Risk Management Policy and may be amended without requiring the amendment of the policy.

Score	Risk	Action	Reporting Requirements
1 to 6	Low	**Tolerate / Managed Through Normal Control Measures**	• Report to Line Manager. • Enter onto the local Team / Directorate Risk Register (TRR / DRR). • Managed by Local Manager and escalated to relevant Chief Officer (or delegated Deputy) as required.
8 to 10	Moderate	**Consider Treat / Review Control Measures**	
12	High	**Treatment Plans to be Developed, Implemented, and Monitored**	• Entered onto the Corporate Risk Register (CRR) in liaison with Corporate Governance team. • Included in Corporate Governance team's bi-monthly report to the Executive Committee. • Oversight by the Executive Committee through bi-monthly report from Corporate Governance team.
15 to 25	Extreme	**Immediate Action Required. Treatment Plans to be Developed, Implemented, and Monitored**	• Report immediately to Corporate Governance team. • Entered on to the Risk Register in liaison with the Corporate Governance team. • Included in the Corporate Governance team's Board Assurance Framework (BAF) reporting bi-monthly to the Executive Committee. • Reported in Corporate Governance team's Board Assurance Framework (BAF) reporting to each meeting of the NHS Devon Board and Committee-specific risks reported via Board Assurance Committees where appropriate.

In addition the NHS Devon Board receives the Board Assurance Framework (BAF) at each meeting with:

- Details of all of the strategic risks, their control measures, and assurances.
- Changes to the strategic risks since the previous report, including scoring.
- Current review narratives for each of the strategic risks.
- The level of assurance on each of the NHS Devon corporate objectives or Statutory Purposes in light of the risks which may impact on those objectives.
- Changes in the totality of risk facing NHS Devon (the total of the strategic level risks) and how this may have changed in the previous twelve months.

This process, its robustness and its deployment is scrutinised by the NHS Devon Audit & Risk Committee (ARC). The Risk Management System is subject to annual review by the Internal Auditors and a report is received by the Audit & Risk Committee (ARC).

APPENDIX H – Risk Appetite

NB: This is a procedural document separate to the Risk Management Policy and may be amended without requiring the amendment of the policy.

Risk appetite specifies the overall risk levels NHS Devon is willing to accept while operating in full compliance with regulatory and legal requirements. In addition, it establishes principles for risk taking to ensure that the totality of risk remains within the defined risk appetite boundaries.

The 'Risk Appetite' will be reviewed and agreed at least annually by the NHS Devon Board.

The 'Risk Appetite' is framed around the priorities set out in the Risk Management Policy and the statement was agreed by the NHS Devon Board at its meeting on 26 March 2024. The statement is based on the premise that the lower the risk appetite, the less NHS Devon is willing to accept in terms of risk and consequently the higher levels of controls that must be in place to manage the risk.

NHS Oversight Framework Theme	Risk Appetite	Tolerance Level for Residual Risk
Quality of care, access and outcomes	AVOID	8-12
Preventing ill-health and reducing inequalities	AVOID	8-12
Finance and use of resources	OPEN	15
People	SEEK	20-25
Leadership & capability	SEEK	20-25
Local strategic priorities	OPEN	15

APPENDIX I:
Risk Management Training Schedule

NB: This is a procedural document separate to the Risk Management Policy and may be amended without requiring the amendment of the policy.

To be included once the Risk Management Training Needs Analysis (TNA) has been completed.