Joint Policy on Risk Management

NHS Devon
NHS Cornwall and Isles of Scilly

Document Reference	Policy on Risk Management
Version	V1
Senior Responsible Officer	Company Secretary
Author/s	Head of Corporate Governance
Approved by	NHS Devon Integrated Care Board NHS Cornwall and Isles of Scilly Integrated Care Board
Date Approved	28 May 2026
Date Issued	1 June 2026
Date of next Review	31 March 2027

Equality, diversity and inclusion statement

NHS Devon and NHS Cornwall and Isles of Scilly are committed to promoting equal opportunities, addressing health inequalities, and fostering good relations between people protected under the Equality Act 2010, the Health and Social Care Act 2012, and Human Rights legislation. We are equally committed to eliminating 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):

Policy Summary

Summary & Key Aims	Target Audience
Aim: Acknowledge that risk exists and empower staff to assess, record, and manage it by severity, report it, and scrutinise it within NHS Devon, NHS Cornwall and Isles of Scilly. **Purpose:** Provide a comprehensive risk management and assurance framework covering organisational, financial, clinical, and non-clinical risks, engaging all parts of the ICB.	All staff (including interim and temporary staff, contractors and seconded staff) have a duty to comply with this Policy.
Key Requirements	**Previous Policy Names**
Risk management is everyone's responsibility. Staff must cooperate with managers, identify risks, and advise their line managers. Key responsibilities include: Be familiar with and follow the Joint Policy on Risk Management, along with all relevant policies and procedures. Report incidents, accidents, and near misses per the Incident Reporting Policy. Be aware of legal duty to ensure personal and others' safety. Comply with NHS Devon, NHS Cornwall, and Isles of Scilly rules to safeguard health, safety, and welfare.	This Policy supersedes the individual policies of NHS Cornwall and Isles of Scilly and NHS Devon of the same name.
Risks to the ICB if the policy isn't followed	**What could happen if staff don't follow the policy**
Not following the risk management policy can lead to increased unmanaged risks threatening strategic objectives and duties, failure to address strategic risks, regulatory scrutiny, operational disruptions, reputational damage, and financial or legal liabilities, including potential collapse.	If an employee fails to follow the agreed-upon risk mitigation measures, the consequences may vary based on the severity of the violation. The employee's reputation within the ICB may suffer. The employee may be required to undergo additional training or retraining to address knowledge gaps or compliance issues.

Table of Contents

1. **Introduction** 5
2. **Purpose** 5
3. **Definitions** 8
4. **Risk Management Activities and Processes** 9
5. **Risk impact domains** 12
6. **Strategic and Operational Risks** 13
7. **Corporate Risk Register (CRR)** 14
8. **Board Assurance Framework (BAF)** 16
9. **Risk Appetite** 17
10. **Accountabilities and Responsibilities** 18
11. **Impact Assessment** 23
12. **Monitoring Compliance and Effectiveness** 24

Training 24

Implementation 24

Review 25

13. **References** 25

APPENDIX 1 - Glossary of Terms 27

APPENDIX 2 - Inherent and Residual Risk 30

APPENDIX 3 - Risks and Issues 31

APPENDIX 4 - Risk Management Principles 32

APPENDIX 5 - Risk Activities and Processes 33

APPENDIX 6 - Model Risk Matrix 34

APPENDIX 7 - Risk Action and Reporting Requirements 40

APPENDIX 8 – Risk Appetite 42

APPENDIX 9 – External references 45

1. Introduction

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

1.2. This policy sets out the key principles that guide risk management within NHS Devon and NHS Cornwall and Isles of Scilly.

1.3. Further advice and guidance are available from the Corporate Governance team at d-icb.swpeninsulagovernance@nhs.net.

2. Purpose

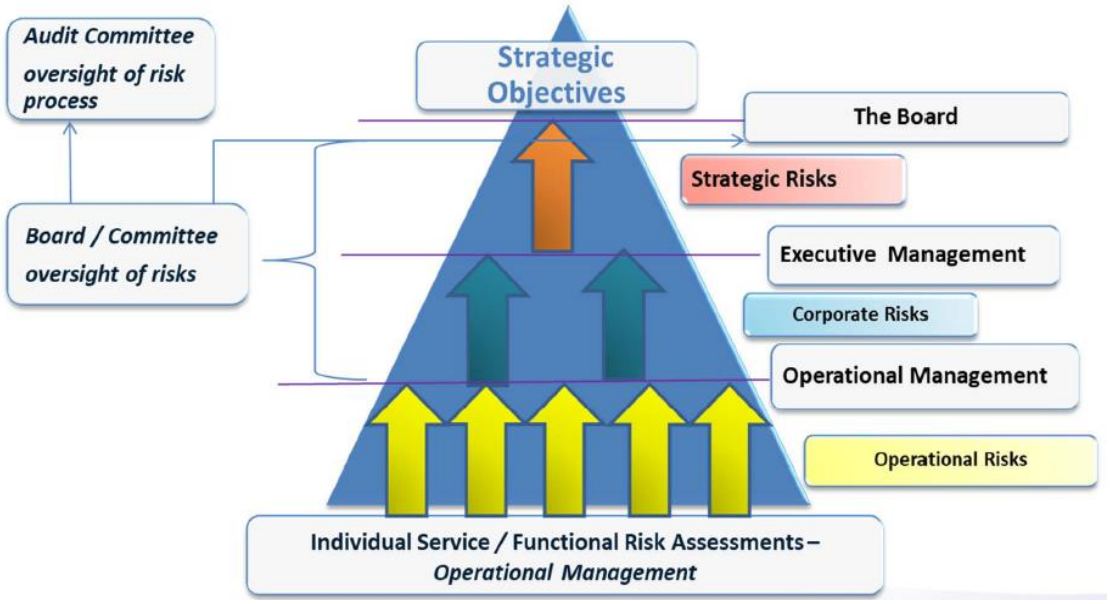
2.1. Risks will always occur. Many risks are manageable, but others pose a greater risk of impact on the organisation, staff, patients, and /or the general public. Once identified, risks must be assessed, recorded, managed according to severity, reported and scrutinised.

2.2. NHS Devon and NHS Cornwall and Isles of Scilly are 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, including clinical and corporate services.

2.3. The Boards of NHS Devon and NHS Cornwall and Isles of Scilly (through the South West Peninsula Board) set the organisational strategy from which risks to delivery are identified; the Board is required to ensure that robust risk management processes exist, it is 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 the achievement of NHS Devon and NHS Cornwall and Isles of Scilly objectives, its statutory or regulatory duties, and its response to adverse events or to learning from audits and other independent reviews.

2.4. Figure 1 shows the flow of risk between operational, corporate and strategic levels

Figure 1: Risk Hierarchy



2.5. It should be noted that the primary focus across healthcare systems is population health, but there is a clear distinction between the objectives of each organisation within the health system. Whilst partner provider organisations (e.g., Acute, Community and Mental Health Trusts) are directly accountable for patient safety, typically Integrated Care Boards (ICBs) face risks around the visibility of patient safety, challenges in identifying and investigating cross-organisational risks, resource constraints, and potential declines in performance and financial stability due to mergers and cuts in running costs. Should such risks materialise, NHS Devon and NHS Cornwall and Isles of Scilly ICB's duty to commission and oversee statutory health system functions effectively could be adversely affected, resulting in reputational damage and a lack of public confidence.

2.6. This policy applies to all employees and Committee Members of NHS Devon and NHS Cornwall and Isles of Scilly:

- Establishes 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.
- Provides an environment for proactive decision making.
- Empowers all staff to manage risk within delegated limits.
- Provides a proactive early warning system and enable a comprehensive response to mitigate risk where indicated.

- Establishes a platform for managing risks within partnership working.
- Ensures the integration of risk management with the NHS Devon and NHS Cornwall and Isles of Scilly's strategies and objectives and with local (directorate / team) objectives that these support.

2.7. 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 and NHS Cornwall and Isles of Scilly's Counter Fraud, Bribery and Corruption Policy and has been reviewed by the organisation's Local Counter Fraud Specialist. Fraud and bribery risks may be included in NHS Devon and NHS Cornwall and Isles of Scilly risk registers and its performance against standards will be assessed annually via completion of the NHS Counter Fraud Authority (CFA) Counter Fraud Functional Standard Return.

2.8. NHS Devon and NHS Cornwall and Isles of Scilly recognise 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 South West Peninsula Board is therefore committed to ensuring that risk management forms a part of NHS Devon and NHS Cornwall and Isles of Scilly 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.

2.9. NHS Devon and NHS Cornwall and Isles of Scilly acknowledge that the provision of appropriate training is central to the achievement of this aim.

2.10. 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. To be confident that internal control systems are robust, NHS Devon and NHS Cornwall and Isles of Scilly must provide evidence that they have systematically identified their strategic objectives and managed the principal risks to achieving them. Evidencing assuring through specific documentation is a key feature of the NHS Devon and NHS Cornwall and Isles of Scilly risk management system, **4risk** (see paragraph 7.4 for more information on levels of assurance).

2.11. NHS Devon and NHS Cornwall and Isles of Scilly are 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 the NHS Devon and NHS Cornwall and Isles of Scilly Freedom to Speak Up: Raising Concerns (Whistleblowing) Policies, available on the staff intranet, which sets out procedures and guidance to staff on raising concerns. NHS Devon and NHS Cornwall and Isles of Scilly have Freedom to Speak Up Guardians to whom staff may raise concerns; their details are available 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 1.

3.2. **A risk** is defined as:

"The effect of uncertainty on objectives".

(ISO31000: 2018)

For example, the potential occurrence of an event that may have an impact on strategic objectives, duties, assets and / or reputation of the organisation.

3.3. 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 and NHS Cornwall and Isles of Scilly.
- Anything that could damage the reputation of NHS Devon and NHS Cornwall and Isles of Scilly and undermine the public's confidence in NHS Devon and NHS Cornwall and Isles of Scilly.
- 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 and NHS Cornwall and Isles of Scilly's statutory or regulatory duties, strategic and corporate objectives.

3.4. NHS Devon and NHS Cornwall and Isles of Scilly distinguish 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 2 provides an illustration of the difference between these two types of risk.

3.5. **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.

3.6. 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).

3.7. Appendix 3 provides more detailed information on the key differences between risks and issues. NHS Devon and NHS Cornwall and Isles of Scilly do not hold a corporate issue log.

3.8. Risk management within NHS Devon and NHS Cornwall and Isles of Scilly will be carried out in accordance with the principles set out in Appendix 4. 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 5):

- **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.

- **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 minimised. 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 materialises).

- **Analyse, evaluate and score the risk:** Assess the likelihood of the risk materialising, and the level of its impact should it occur using the risk score matrix. Note: all assessments must be based on the likelihood and impact domains set out in Appendix 6. The calculated risk score will determine whether the risk is managed at the team/directorate level or via the NHS Devon and NHS Cornwall and Isles of Scilly Corporate Risk Register (CRR).

- **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 South West Peninsula 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.

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

  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 and updated 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. Note: it is the risk owner's responsibility to raise awareness about the risk.

All teams / directorates should maintain their own risk registers.

If a risk is deemed to be a risk to the achievement of NHS Devon and NHS Cornwall and Isles of Scilly'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 and NHS Cornwall and Isles of Scilly Corporate Risk Register (CRR).

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.

All operational risks (generally with a validated residual score of 12 and above) are added to the NHS Devon and NHS Cornwall and Isles of Scill**y** Corporate Risk Register (CRR); this is done in conjunction with a member of the Corporate Governance team. Operational risks are reviewed monthly. The review is overseen by a member of the Corporate Governance team.

Extreme operational risks (scoring 15 and above) are reported alongside the Board Assurance Framework (BAF) to NHS Devon and NHS Cornwall and Isles of Scilly Chief Officers.

All strategic risks are included on the Board Assurance Framework (BAF) and are reviewed regularly and reported alongside corporate risks to Chief Officers and the South West Peninsula Board, and where appropriate, its associated Assurance Committees.

Refer to Appendix 7 for a summary of risk action and reporting requirements.

- **Monitor / review the risk:** Monitor the risk impact and review the effectiveness of action / actions taken. It is expected that the risk score / risk priority has changed as a result.

- **Communicate with and consult those impacted by the risk:** It is the risk owner's responsibility to identify who is affected by the risk and who needs to know about it, e.g. internally and/or externally.

5. Risk impact domains

5.1. In NHS commissioning, risk management frameworks are essential to ensure that commissioned services are safe, effective, and deliver value for money. Risk impact domains provide a structured way to identify, assess, and manage risks across different aspects of commissioning.

Safety and Quality of Care

- Example: Risk that a commissioned provider fails to meet infection control standards, leading to patient harm.
- Guidance: Commissioners include safety indicators in contracts, conduct quality assurance visits, and require incident reporting.

Clinical Effectiveness

- Example: Risk that services do not follow NICE guidelines, resulting in suboptimal patient outcomes.
- Guidance: Commissioners specify clinical standards in service specifications and use audit data to assess compliance. They may commission clinical reviews or second opinions.

Workforce and Staff Wellbeing

- Example: Risk that provider staff burnout affects service quality.
- Guidance: Commissioners consider workforce sustainability in service design, support staff wellbeing initiatives, and include workforce metrics in performance reviews.

Regulatory and Legal Compliance

- Example: Risk of non-compliance with NHS England commissioning regulations or data protection laws.
- Guidance: Commissioners ensure contracts include compliance requirements, provide training on legal obligations, and conduct regular compliance audits.

Publicity and Stakeholder Confidence

- Example: Risk that poor service quality leads to negative media coverage and loss of public trust.
- Guidance: Commissioners engage with patient groups, maintain transparent communication, and have crisis management plans. They also monitor media and social media sentiment.

Business Objectives

- Example: Delays or underperformance in implementing new care pathways or service transformation projects, leading to missed health outcomes or efficiency targets.
- Guidance: Commissioners establish clear roles and responsibilities for risk ownership. Ensure leadership oversight through committees and board reporting.

Financial and Resource Management

- Example: Risk of overspending on commissioned services or fraud.
- Guidance: Commissioners implement robust financial controls, regular audits, and value-for-money assessments. They may use activity and cost data to detect anomalies.

Information Governance and Cybersecurity

- Example: Risk of data breaches in shared patient records systems.
- Guidance: Commissioners require providers to adhere to NHS Digital standards, conduct data protection impact assessments, and monitor cybersecurity incidents.

5.2. The risk impact risk scoring matrix can be seen at Appendix 6

6. Strategic and Operational Risks

6.1. Risk-related activity within NHS Devon and NHS Cornwall and Isles of Scilly is derived from two directions:

- **Top down:** NHS Devon and NHS Cornwall and Isles of Scilly Boards and the South West Peninsula Board discuss and agree those strategic risks that they consider the ICBs face in the achievement of their statutory or regulatory duties, agreed corporate objectives or other statutory functions. These form the strategic risks of NHS Devon and NHS Cornwall and Isles of Scilly and are recorded in their Board Assurance Frameworks (BAFs).

- **Bottom up:** Individuals, teams, directorates, Chief Officers, the South West Peninsula Board, and its 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 and NHS Cornwall and Isles of Scilly Corporate Risk Register (CRR).

6.2. Both operational and strategic risks should be aligned to NHS Devon and NHS Cornwall and Isles of Scilly'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 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.

6.3. 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 6).

6.4. NHS Devon and NHS Cornwall and Isles of Scilly adhere 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 the 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 Place and Transformation Officer or the Chief Clinical Officer.

7. Corporate Risk Register (CRR)

7.1. **Risk escalation, de-scalation and moderation** - All teams / directorates should maintain their own risk registers. If a risk is deemed to be a risk to the achievement of NHS Devon and NHS Cornwall and Isles of Scilly'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 and NHS Cornwall and Isles of Scilly Corporate Risk Register (CRR). The Risk Management Group* reviews any such risk with the risk assessor and owner to determine whether it is appropriate and whether the scoring is proportionate. If the risk is deemed appropriate for inclusion, it is added to the NHS Devon and NHS Cornwall and Isles of Scilly Corporate Risk Register (CRR).

7.2. **Risk Management System** – All managers have a responsibility to record identified corporate risks on the NHS Devon and NHS Cornwall and Isles of Scilly risk management system (4risk). 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 risk management system allows staff to add new risks (once appropriately approved) or update existing ones at any time. Corporate risks must be reviewed and updated by the named assessor in line with 4risk rules (e.g., red-rated risks must be reviewed at least monthly to be compliant). Following this review the update will be agreed by the risk owner and reported as appropriate.

7.3. Regular reviews are undertaken across NHS Devon and NHS Cornwall and Isles of Scilly to ensure that:

- New risks are identified and assessed.
- A careful watch is maintained on cumulative risk NHS Devon and NHS Cornwall and Isles of Scilly to ensure that this is identified and properly escalated via the Risk Management Group.
- 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 and NHS Cornwall and Isles of Scilly are closed.

7.4. **Assurance** should be provided using the Three Lines (of defence) model to govern our risks and demonstrate that we are managing the organisation well. The three lines model provides a structure for describing the assurance activity related to risk management across the organisation. It gives regions and corporate teams autonomy for identifying, managing and reporting risk; with our specialist functions such as the corporate risk management and legal teams providing oversight; and internal/external audit providing independent assurance.

<u>The first line of defence</u>

7.5. The first line of defence relates to functions that own and manage risk. Staff and managers working within ICB teams have direct ownership, responsibility, and accountability for identifying, managing and controlling risks to their objectives. Assurance is provided through the monitoring and reporting of risk and control activities through senior leadership/management team meetings. This can include the review of performance metrics, deep dive reviews of concern areas, etc. and it is ongoing.

<u>The second line of defence</u>

7.6. The second line of defence relates to functions that oversee or specialise in risk management and compliance. They guide, support, and challenge the first line by bringing expertise and subject matter knowledge to help ensure risks and controls are effectively managed and assured. The Corporate Governance team, and other internal oversight teams such as legal, IT,

performance/business planning, finance and HR (among others) form the second line of defence and are responsible for co-ordinating, facilitating and overseeing the organisation's effectiveness and integrity. Each directorate and should consider and document how the second line will be enacted within their area of the organisation, such as raising awareness across senior leadership teams and Board Assurance Committees.

The third line of defence

7.7. The third line of defence relates to functions that provide independent assurance, namely audit. It provides assurance to senior management and the Board over both the first and second lines' efforts. Internal audit and external scrutiny through the National Audit Office provide independent, objective assurance and challenge concerning the integrity and effectiveness of risk management and internal control. Assurance is provided through monitoring and reporting of strategic/corporate risk and control activities through the Audit and Risk Committee (ARC)

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

8. Board Assurance Framework (BAF)

8.1. The BAF provides a structure and process that enables NHS Devon and NHS Cornwall and Isles of Scilly 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 risks, and to confirm that the Board has sufficient assurance regarding the effectiveness of those controls.

8.2. In advance of each financial year, NHS Devon and NHS Cornwall and Isles of Scilly should agree on overarching strategic objectives for that year underpinned by several corporate objectives. The BAF captures these strategic objectives and the strategic risks applicable to them. Each objective, along with the strategic risks associated with it, will be assigned to a Board Assurance Committee to ascertain levels of assurance through scrutiny, monitoring, testing and challenge of controls through associated evidence. Operational and strategic risks may also be expressed and recorded against 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.

8.3. Any Board Assurance Committee responsible for scrutinising an area of risk to the delivery of one or more strategic objectives can recommend the escalation of a risk to the Board when one or more of the following criteria are met:

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

8.4. The BAF is routinely updated by Chief Officers in conjunction with the Corporate Governance team and reported to NHS Devon and NHS Cornwall and Isles of Scilly Chief Officers for recommendation to the South West Peninsula Board. The BAF will set out the controls, assurances, and mitigating actions. 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.

8.5. The BAF will be used as a tool for setting the agendas of Board meetings and development sessions (as well as Board Assurance Committee agendas). To be an effective tool, it should be possible to map items identified in the 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 and performance reports.

9. Risk Appetite

9.1. NHS Devon and NHS Cornwall and Isles of Scilly'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.

9.2. **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.

9.3. 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 and NHS Cornwall and Isles of Scilly, as well as how decisions are taken.

9.4. NHS Devon and NHS Cornwall and Isles of Scilly, through the South West Peninsula 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 framework:

Risk Appetite Level	Risk Tolerance Level
Very Low	1-5
Low	6-10
Moderate	11-15
High	16-20
Very High	21-25

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

- Management focuses 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 focuses on risks that are not being reduced

9.6. The process for setting and reviewing risk appetite (including 'target' risk scores) is detailed in Appendix 8 together with the current risk appetite statement agreed by the South West Peninsula Board.

10. Accountabilities and Responsibilities

10.1. NHS Devon and NHS Cornwall and Isles of Scilly, operating through the South West Peninsula Board, are 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. They are supported in the discharge of their responsibilities by the Audit and Risk Committees meeting in

common (ARC), Risk Management Group, other Assurance Committees, and the NHS Devon and NHS Cornwall and Isles of Scilly Chief Officers.

10.2. The South West Peninsula Board receives assurance as to whether operational and strategic risks are being effectively managed. It reviews and approves the Board Assurance Framework (BAF) regularly to monitor actions and assurances against strategic risks and assesses the overall impact on the delivery of NHS Devon and NHS Cornwall and Isles of Scilly's statutory/regulatory duties and corporate objectives.

10.3. In addition to the above, it is also responsible for determining the risk appetite of NHS Devon and NHS Cornwall and Isles of Scilly and for approving the Joint Policy on Risk Management.

10.4. The **Risk Management Group** (RMG) is chaired by the Company Secretary and constituted by key members of the senior leadership team, overseeing the risk environment of NHS Devon and NHS Cornwall and Isles of Scilly at an operational level and provides assurance to the ARC on the efficacy of the risk control system. RMG challenges risks identified and presented by directorates, validating new and/or escalating risks for inclusion on the Corporate Risk Register as appropriate. RMG also recommends new and/or escalating risks for consideration by the South West Peninsula Board for the inclusion within the Board Assurance Framework. The core purpose of RMG is to:

- Moderate risk scoring of all risks and ensure due process (as described within this policy) has been observed in all cases
- Review all risks with a risk score of 15 or above as a standing item
- Ensure all existing and new risks have appropriate assurances in place
- Rank the validated risks in priority order to inform Executive Directors, Assurance Committees, System Capital Meeting and the Board

10.5. The **Audit and Risk Committee** (ARC) provides an objective view on internal control and risk management systems to NHS Devon and NHS Cornwall and Isles of Scilly that is independent of Chief Officers. ARC also:

- Reviews the adequacy and effectives of the system of integrated governance and risk management and internal control across the whole of NHS Devon and NHS Cornwall and Isles of Scilly activities that support the achievement of its objectives, and to highlight any areas of weakness to the South West Peninsula Board.
- Reviews the adequacy and effectiveness of the assurance processes that indicate the degree of achievement of NHS Devon and NHS Cornwall and Isles of Scilly'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 and NHS Cornwall and Isles of Scilly's statutory or regulatory duties or objectives; the Board maintains overall responsibility for risk management.
- Seeks reports and assurance from RMG, 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 and NHS Cornwall and Isles of Scilly.

10.6. The Chair of the ARC will provide a summary to NHS Devon and NHS Cornwall and Isles of Scilly of its assurances and where necessary, request assurance reports to be undertaken in areas of risk where further assurances are required.

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

10.8. **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.

10.9. NHS Devon and NHS Cornwall and Isles of Scilly **Chief Officers** provide oversight and delivery of risk management arrangements. Seek assurance from RMG 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, they regularly have 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 and NHS Cornwall and Isles of Scilly's statutory / regulatory duties or corporate objectives and approve its submission to the South West Peninsula Board.

10.10. 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 an adequate system of internal control is 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 CEO and is responsible for ensuring (and reporting to the South West Peninsula Board and to the Audit and Risk Committees meeting in common (ARC)) that systems and structures are in place for the effective management of financial risk and organisational controls.

10.11. The CEO is responsible for the Annual Governance Statement, setting out how these responsibilities have been discharged.

10.12. The **Chief Clinical Officer** is accountable to the 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.

10.13. The **Chief Clinical Officer** provides Clinical Leadership for NHS Devon and NHS Cornwall and Isles of Scilly and is accountable to the CEO and is responsible for providing strategic and operational leadership and management of the clinical risk within NHS Devon and NHS Cornwall and Isles of Scilly and organisational assurance on all matters of clinical risk and clinical outcomes to the South West Peninsula Board.

10.14. The **Chief Place and Transformation Officer** is the appointed **Caldicott Guardian** and ensures that the Caldicott principles for managing information and ensuring its security and integrity are adhered to by staff within NHS Devon and NHS Cornwall and Isles of Scilly.

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

10.16. The allocated **Risk Manager** is responsible for providing support and advice on risk management issues NHS Devon and NHS Cornwall and Isles of Scilly. In addition, they will work closely with specialist advisers within NHS Devon and NHS Cornwall and Isles of Scilly 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 to NHS Devon and NHS Cornwall and Isles of Scilly Chief Officers, Board Assurance Committees, and the South West Peninsula 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).

10.17. The Company Secretary, reporting to the CEO is responsible for ensuring the development and implementation of Risk Management Policy across NHS Devon and NHS Cornwall and Isles of Scilly, ensuring that risk management processes are effectively coordinated, implemented, and monitored. This responsibility includes:

- Maintenance and development of the Board Assurance Framework (BAF) and the NHS Devon and NHS Cornwall and Isles of Scilly Corporate Risk Register (CRR) as active documents through the implementation of appropriate mechanisms to enable clear monitoring of mitigation and action plans.
- Supporting the implementation of the NHS Devon and NHS Cornwall and Isles of Scilly Joint Policy on Risk Management (including the provision of advice and training).
- Overseeing and reporting on risk management compliance requirements.

10.18. The Company Secretary is also the appointed **Senior Information Risk Owner** (SIRO), accountable to the CEO and is responsible for managing information assets and risks across the organisations.

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

- Implementing the Joint Policy on Risk Management and procedures within their scope of responsibility.
- Ensuring that NHS Devon and NHS Cornwall and Isles of Scilly's risk management processes, including risk assessments, monitoring and escalation / de-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 and NHS Cornwall and Isles of Scilly'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 and escalated via RMG.
- Ensuring that they discuss risks with relevant senior managers and directors as appropriate.
- Implementing and monitoring any risk management actions within their designated area. When local actions are considered inadequate, senior managers are responsible for escalating these risks through RMG if local resolution cannot be 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 and RSET training.
- Ensuring staff compliance with this document.
- Having adequate knowledge of, and / or access to, all relevant legislation in order to ensure that compliance with such legislation is maintained.

* *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 allocated Risk Manager).*

10.20. 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 Joint Policy on Risk Management 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 and NHS Cornwall and Isles of Scilly.
- Complying with NHS Devon and NHS Cornwall and Isles of Scilly rules, regulations, and instructions to protect the health, safety, and welfare of anyone affected by the business of NHS Devon and NHS Cornwall and Isles of Scilly.

11. Impact Assessment

11.1. An Equality Quality Impact Assessment (EQIA) has been completed in respect of this policy. No concerns were highlighted.

12. Monitoring Compliance and Effectiveness

Training

12.1. Risk Management training, although not currently part of the Mandatory Training requirement is considered as Role Specific Essential Training (RSET).

12.2. RSET can affect a small or large amount of staff. It may be defined by local risk or quality assessments, guidance from a professional body, regulatory guidance or other sources, such as workforce and business planning. It should not be seen as secondary to core Mandatory Training, but as an equal. Where a manager is unsure of a requirement, advice should be taken either from internal subject experts or from external bodies as appropriate.

12.3. Knowledge of how to manage risk is essential in embedding and maintaining an efficient risk management system. Risk management training is mandatory at induction and will form part of the annual review of staff development as part of an individual's annual appraisal review. The implementation of risk management by individuals will be performance managed through staffs' individual appraisal reviews. To this end, the Corporate Governance team will work in conjunction with Human Resources (HR) to conduct an annual 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 identifying external training providers and/or developing an internal training process.

12.4. 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

12.5. Chief Officers, Directors and Managers, and/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 and directed to the staff intranet to read the policy.

- Discussing with staff as part of their regular one-to-ones how they seek to achieve their individual objectives around policy review and maintenance.
- All staff will be informed of the Policy's approval and subsequent changes via the Staff Bulletin, which will include a link to the document on the staff Intranet.

Review

12.6. NHS Devon and NHS Cornwall and Isles of Scilly 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 and Risk Committees meeting in common (ARC) and is reflected in the Head of Internal Audit Opinion (HIAO) on the organisational arrangements for risk management and internal control.

12.7. 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.

12.8. The ARC will review risk information submitted throughout the year. In addition, risk reports will be submitted to Board Assurance Committees as appropriate. These Committees can request information on specific risks to seek further assurance and details on actions being taken to address them.

12.9. NHS Devon and NHS Cornwall and Isles of Scilly Risk Appetite will be reviewed annually by the South West Peninsula Board.

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

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

12.12. This policy will be reviewed annually to ensure that it remains fit for purpose.

13. References

13.1. This policy does not stand alone and should be considered alongside the following related policies mentioned in this document. These are available on the staff intranet.

- Freedom to Speak Up: Raising Concerns (Whistleblowing) Policy

- Counter Fraud, Bribery, and Corruption Policy
- Internal Incident Policy
- Serious Incidents Policy
- EQIA Policy

APPENDIX 1 - 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.
Reputational Risk	The adverse perception of the image of NHS Devon and NHS Cornwall and Isles of Scilly by patients, partner organisations and individuals, the local community or regulators.
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.

Terms	Definition
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.
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

Terms	Definition
	▪ 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 2 - 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
<u>Event:</u> Getting into the driving seat of a car, turning on the engine and moving of off	**<u>Inherent Risk:</u>** 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 3 - 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 4 - Risk Management Principles

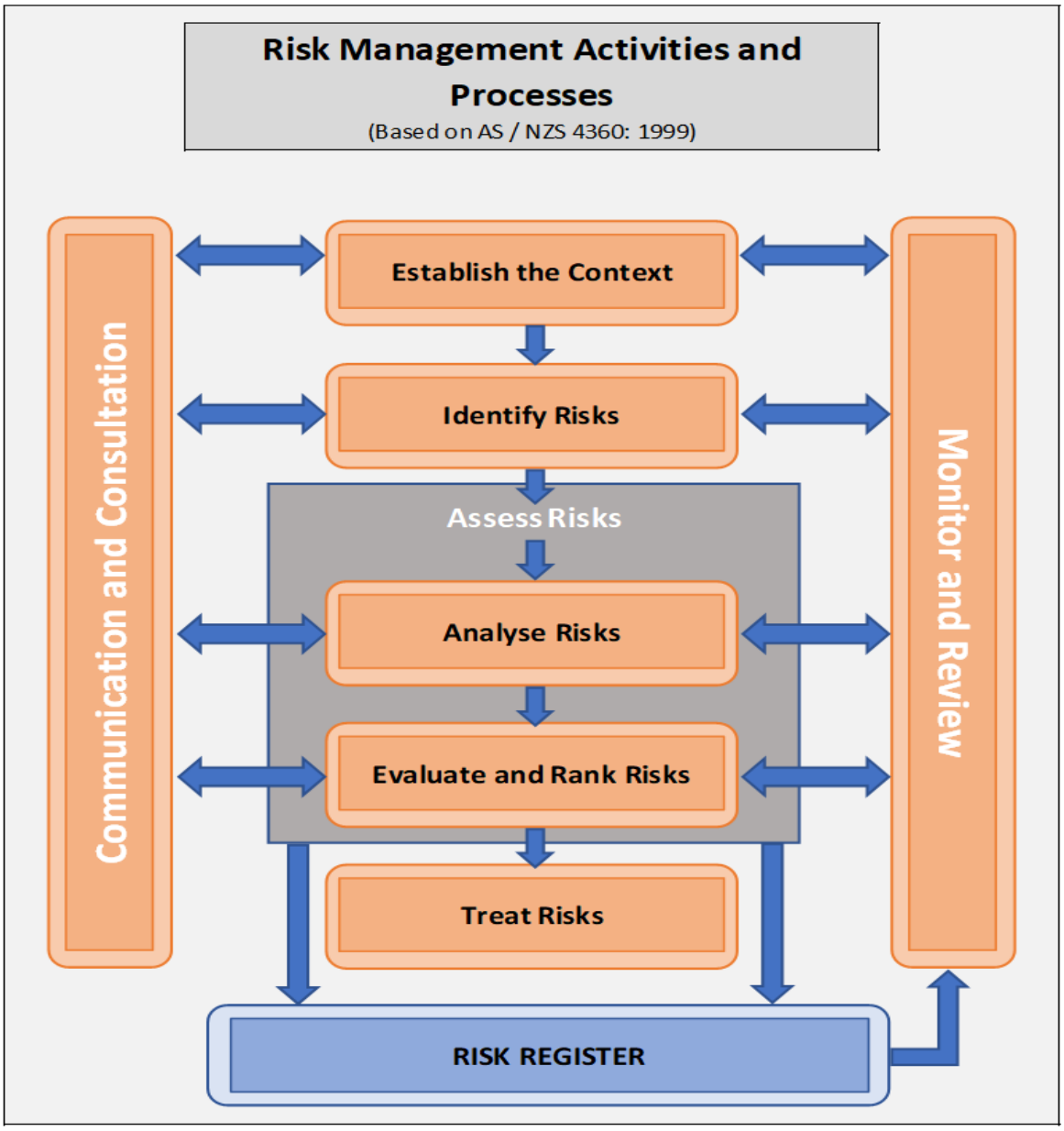
NB: This is a procedural document separate to the Risk Management Policy and may be amended without requiring the amendment of the policy.

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 and NHS Cornwall and Isles of Scilly 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 and NHS Cornwall and Isles of Scilly identify, assess, and control 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 and NHS Cornwall and Isles of Scilly 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 and NHS Cornwall and Isles of Scilly 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 5 - 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 the NHS Devon and NHS Cornwall and Isles of Scilly approach to risk management:



APPENDIX 6 - 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**
Patient Safety and Quality of Care Including capacity / resilience	Minimal injury, requires 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**
Clinical Effectiveness Including clinical incidents / reviews / complaints	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
Workforce and Staff Wellbeing Includes Human Resources functions / Organisational Development / Staffing / Competencies	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**
Regulatory and Legal Compliance Including 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
Publicity and stakeholder confidence Including reputational damage	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 Including Project governance	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**
Financial and resource management Including Claims / Environmental Impact	Small loss Risk of claim remote Minimal or no impact on the environment	Loss of 0.1 – 0.25 per cent of budget Claim less than £10,000 Minor impact on environment	Loss of 0.26 – 0.5 per cent of budget Claim(s) between £10,000 and £100,000 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 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 Catastrophic impact on environment
Information Governance and Cybersecurity Including Service / Business Interruption	Minor, unlikely unauthorised disclosure with no harm Minor data inaccuracies with no effect on care or operations Business loss / interruption of >1 hour	Limited unauthorised access affecting a small number of individuals, causing some concern Data errors causing minor workflow disruptions or delays in care Business loss / interruption of >8 hours	Unauthorised access to patient data causing distress Alteration of clinical or operational data impacting patient care or decision-making Business loss / interruption of >1 day	Large-scale data breach affecting many patients Corruption or manipulation of critical data leading to serious clinical errors or operational failures Business loss / interruption of >1 week	Severe breach causing widespread harm and legal penalties Systematic data tampering causing life-threatening clinical errors or widespread operational collapse Permanent loss of service or facility

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 7 - 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**	• Liaise with Corporate Governance team as appropriate to present to Risk Management Group. If approved, enter onto the Corporate Risk Register (CRR). • Included in Corporate Governance team's bi-monthly report to NHS Devon and NHS Cornwall and Isles of Scilly Chief Officers. • Oversight by NHS Devon and NHS Cornwall and Isles of Scilly Chief Officers through bi-monthly report from Corporate Governance team.
15 to 25	Extreme	**Immediate Action Required. Treatment Plans to be Developed, Implemented, and Monitored**	• Liaise with Corporate Governance team as appropriate to present to Risk Management Group. If approved, enter onto the Corporate Risk Register (CRR). • Included in the Corporate Governance team's Board Assurance Framework (BAF) reporting bi-monthly to NHS Devon and NHS Cornwall and Isles of Scilly Chief Officers. • Reported in Corporate Governance team's Board Assurance Framework (BAF) reporting to each meeting of the South West Peninsula Board

Score	Risk	Action	Reporting Requirements
			and Committee-specific risks reported via Board Assurance Committees where appropriate.

In addition, the South West Peninsula 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 and NHS Cornwall and Isles of Scilly 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 and NHS Cornwall and Isles of Scilly (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 Audit and Risk Committees meeting in common (ARC). The Risk Management System is reviewed annually by Internal Auditors, and a report is provided to the Audit and Risk Committees meeting in common (ARC).

APPENDIX 8 – 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 and NHS Cornwall and Isles of Scilly are 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 South West Peninsula Board.

The 'Risk Appetite' is framed around the priorities set out in the Risk Management Policy and the statement is agreed by the South West Peninsula Board annually. The statement is based on the premise that the lower the risk appetite, the less NHS Devon and NHS Cornwall and Isles of Scilly are willing to accept in terms of risk and consequently the higher levels of controls that must be in place to manage the risk.

Risk Theme	Risk Appetite Statement	Risk Appetite	Tolerance Level for Residual Risk
Safety failures in commissioned services	The Board has a **low** appetite for risk in relation to safety failures within commissioned services. Our primary focus is the elimination of avoidable harm and the maintenance of a robust culture of clinical safety. We prioritize compliance with national safety standards and regulatory requirements	Low	**6-10**
Quality failures in commissioned services	The Board has a **moderate** appetite for risks in relation to quality failures within commissioned services. We are receptive to innovative service models and transformation programmes that aim to improve long-term clinical outcomes, acknowledging that such changes may carry a degree of short-term delivery risk or temporary variability in quality metrics.	Moderate	**11-15**

Risk Theme	Risk Appetite Statement	Risk Appetite	Tolerance Level for Residual Risk
System financial sustainability	The Board has a **low** appetite for risks that could jeopardise the long-term financial sustainability of the ICS. We prioritize the delivery of a balanced budget and adherence to statutory financial duties over the pursuit of innovative but high-risk financial ventures.	Low	**6-10**
Delivery of constitutional standards and recovery priorities	The Board has a **moderate** appetite for risks associated with the delivery of constitutional standards and recovery priorities. We are receptive to innovative delivery models and transformative changes that may cause short-term operational disruption or require temporary trade-offs in performance, provided these actions are essential to securing long-term service sustainability and improved patient outcomes. While we accept a degree of inherent risk in these pursuits, all such activities must be managed within a controlled environment with robust performance oversight to ensure no significant or lasting detriment to patient safety or core clinical quality	Moderate	**11-15**
Workforce sustainability and leadership resilience	The Board has a **moderate** appetite for risks associated with workforce sustainability and leadership resilience. We recognise that maintaining the 'status quo' is a significant risk in itself; therefore, we are willing to accept calculated risks to transform our workforce models and leadership structures.	Moderate	**11-15**
Failure to reduce health inequalities	The Board has a **moderate** appetite for risks associated with our duty to reduce health inequalities. We recognise that traditional, 'one-size-fits-all' service models have failed to close the equity gap; therefore, we are willing to take calculated risks to pilot unconventional, targeted interventions for our most underserved populations.	Moderate	**11-15**
Digital, data and analytics capability (incl	The Board has a **low** appetite for risks that could compromise our cyber security posture, the integrity of our data assets, or our compliance	Low	**6-10**

Risk Theme	Risk Appetite Statement	Risk Appetite	Tolerance Level for Residual Risk
cyber security and information governance)	with IG and Data Protection legislation. Our primary objective is to maintain a secure, stable, and resilient digital environment.		
Provider and system alignment	The Board has a **moderate** appetite for risks associated with provider alignment and system integration. We recognise that achieving a 'one system' approach requires moving beyond traditional organisational boundaries; therefore, we are willing to accept calculated risks in the delegation of functions and the pooling of resources	Moderate	**11-15**
Reconfiguration and service change	The Board has a **high** appetite for risks associated with large-scale service reconfiguration and system-wide transformation. We believe that incremental change is no longer sufficient to meet the needs of our population; therefore, we are proactively seeking opportunities to fundamentally redesign how and where care is delivered	High	**16-20**

APPENDIX 9 – External references

Legislation and statutory requirements

- Equality Act 2010
- Freedom of Information Act 2000
- Health and Safety at Work Act 1974
- Human Rights Act 1998
- Management of Health and Safety at Work Regulations 1999

Best practice recommendations and other key guidance

- Caldicott Principles
- Department of Health and Social Care Group Accounting Manual 2021/22
- Good Governance Institute - The New Good Governance Handbook 2016
- Federation of European Risk Management Associations (FERMA):
- Financial Reporting Council "UK Corporate Governance Code 2018"
- Health and Safety Executive 'Managing for Health and Safety 2013'
- The Institute of Risk Management 'A Risk Management Standard 2002'
- International Organisation for Standardisation (ISO) Guide '73:2009 Risk Management' (Revised 2016):
- NHS England - Learning from patient safety events
- NHS Resolution
- NHS Leadership Academy – The Healthy NHS Board 2013
- HM Government: The Orange Book – Management of Risk – Principles and Concepts:
- ISO 31000:2018 Risk Management Guidelines:
- NHS England Risk Management Framework (June 2025)