

Risk Management Policy

July 2026 – July 2029

Policy purpose and key messages

This joint policy sets out how NHS Derby and Derbyshire Integrated Care Board (ICB), NHS Lincolnshire ICB, and NHS Nottingham and Nottinghamshire ICB manage strategic and operational risks through a common risk management framework developed in support of their formal partnership arrangements.

The policy promotes a positive risk culture and supports informed decision-making by establishing consistent arrangements for the identification, assessment, management, escalation and monitoring of risks across the three ICBs. It defines the ICBs' approach to risk appetite and tolerance, outlines the governance, roles and responsibilities that support effective risk management, and describes how strategic, operational and local risks are managed through the Board Assurance Framework, Operational Risk Register, and Risk Logs.

The policy supports organisational resilience, delivery of strategic objectives and statutory duties, and provides assurance to Boards, patients, partners and the public that risks are being managed appropriately and proportionately.

CONTROL RECORD	
Title	Risk Management Policy
Reference number	DLN-GOV-001
Version	2.0
Status	Draft
Author	Director of Corporate Governance and Assurance, supported by the Risk Management Team
Sponsor	Amanda Sullivan, Chief Executive
Team	Corporate Governance and Assurance
Amendments	General streamlining of content as appropriate to policy requirements. Specific updates to the ICBs' risk appetite framework and risk domains, following review by the Boards. Associated updates to the Risk Scoring Matrix in Appendix B to align with updated risk domains.
Superseded documents	DLN-GOV-001 Risk Management Policy v1.2
Audience	All staff within NHS Derby and Derbyshire Integrated Care Board, NHS Lincolnshire Integrated Care Board, and NHS Nottingham and Nottinghamshire Integrated Care Board.
Consulted with	Board members
Equality Impact Assessment	September 2025
Approving body	Boards of NHS Derby and Derbyshire Integrated Care Board, NHS Lincolnshire Integrated Care Board, and NHS Nottingham and Nottinghamshire Integrated Care Board
Date approved	To be confirmed
Date of issue	July 2026
Review date	July 2029
Policy retention period	Life of organisations plus six years
This is a controlled document and whilst this policy may be printed, the electronic version available on the ICBs' document management system is the only true copy. As a controlled document, this document should not be saved onto local or network drives.	

Table of Contents

1. Introduction	1
2. Purpose	1
3. Scope.....	2
4. Definitions	2
5. Roles and responsibilities	2
6. Risk appetite and tolerance	4
7. Strategic risk management	7
8. Operational risk management.....	8
9. Risk logs	8
10. Risk management lifecycle	9
11. Fraud risks	13
12. Information risks	14
13. Performance against key delivery priorities	14
14. Management of issues.....	15
15. Equality and diversity statement	15
16. Communication, monitoring and review	15
17. Confidentiality	16
18. Staff training.....	16
19. Interaction with other policies.....	16
20. References	17
21. Equality Impact Assessment.....	18
Appendix A: Definitions and Glossary of Terms.....	22
Appendix B: Risk Scoring Matrix	25

1. Introduction

- 1.1 This is a joint Risk Management Policy of NHS Derby and Derbyshire Integrated Care Board (ICB), NHS Lincolnshire ICB, and NHS Nottingham and Nottinghamshire ICB ("the ICBs"). The policy has been developed in accordance with the formal partnership arrangements established between the ICBs and sets out a common framework for risk management that enables consistent oversight, assurance and reporting across the organisations, whilst preserving the statutory sovereignty and accountability of each ICB.
- 1.2 The ICBs recognise that effective risk management is essential to the achievement of strategic objectives, the discharge of statutory duties, and the delivery of safe, effective and sustainable services. Effective risk management supports informed decision-making, organisational resilience and the provision of assurance to Boards and stakeholders.
- 1.3 Whilst operating within a formal partnership arrangement, each ICB remains a separate statutory body accountable for its own governance and decision-making. Risk management arrangements therefore support the management of both sovereign risks, which are specific to an individual ICB, and joint risks, where the causes, consequences, controls or mitigations extend across more than one ICB. Definitions of sovereign and joint risks are provided in Appendix A.
- 1.4 Risk management is an integral part of organisational governance, planning, transformation, programme delivery and day-to-day operations. All employees, officers and members share responsibility for identifying and managing risks within their area of responsibility.
- 1.5 The ICBs are committed to maintaining proportionate and effective risk management arrangements that support a positive risk culture and informed risk-taking within agreed levels of risk appetite and tolerance.
- 1.6 This policy is supported by associated procedures, guidance and risk management tools and is aligned to the principles of ISO 31000:2018 Risk Management Guidelines.

2. Purpose

- 2.1 This policy describes the approach of the ICBs to the management of strategic and operational risks across the respective statutory organisations.
- 2.2 The purpose of this policy is to encourage a culture where risk management is viewed as an essential process of the activities of the ICBs. It provides assurance to the public and partner organisations that the ICBs are committed to managing risk appropriately.
- 2.3 This policy aims to achieve several key objectives, including to:

- a) Outline the benefits of risk management.
- b) Explain the risk appetite and approach to tolerance within the ICBs.
- c) Set out the ambition of the ICBs to continuously improve risk management arrangements.
- d) Outline the approach to implementation and monitoring.
- e) Describe the relevant compliance and assurance arrangements regarding risk management within the ICBs.
- f) Ensure there is a robust system in place to manage risk effectively.

3. Scope

- 3.1 This policy covers all employees, including Members of the ICBs' Boards, those appointed by the ICBs, and anyone working within the ICBs on a temporary basis or under a contract for services (either individually or through a third-party supplier), collectively referred to as "individuals".

4. Definitions

- 4.1 Definitions and a glossary of terms referenced in this policy are described in Appendix A.

5. Roles and responsibilities

- 5.1 Accountability for managing risks rests with strategic and operational leaders across the ICBs. Governance forums provide oversight and assurance, whilst the Risk Management Team facilitates the operation of the framework and supports its consistent application. Key responsibilities for specific roles and forums are described in the table below:

Role / Forums	Responsibilities
Boards	The Boards retain overall accountability for the effectiveness of risk management within their respective organisations. The Boards approve the Risk Management Policy, Risk Appetite Statement and Board Assurance Framework, determine whether strategic risks are being managed within agreed risk appetite, and seek assurance that appropriate controls, mitigations and governance arrangements are in place to support the achievement of strategic objectives and statutory duties.
Audit Committees	The Audit Committees provide independent assurance to the Boards regarding the adequacy and effectiveness of the ICBs' risk management framework, systems of internal control and assurance processes. The Committees scrutinise the robustness of arrangements relating to the Board Assurance Framework and

Role / Forums	Responsibilities
	Operational Risk Register and advise the Boards on the effectiveness of risk management arrangements. The Committees do not own or manage risks.
Committees of the Boards	All committees of the Boards are responsible for overseeing strategic and operational risks related to their delegated responsibilities as outlined within their respective terms of reference. This will include monitoring the progress of actions, robustness of controls and timeliness of mitigations. They are also responsible for identifying risks that arise during meeting discussions and ensuring that these are captured on the Operational Risk Register.
Executive Management Team	The Chief Executive has overall responsibility for maintaining a sound system of internal control in support of the ICBs' aims, objectives, and duties. Executive Directors are responsible for ensuring effective systems of risk management, commensurate with this policy, are in place within their respective Directorates. Working collectively, the Executive Management Team (EMT) promotes the risk culture within the ICBs and provides executive oversight of strategic and operational risks. The EMT ensures appropriate ownership and management of risks, scrutinises the effectiveness of mitigating actions, and monitors trends to support proactive risk management and continuous improvement.
Senior Leadership Team	Members of the Senior Leadership Team are responsible for leading risk management arrangements within their teams, which includes, but is not limited to, ensuring that: • Risk Logs are in place, as appropriate, to support delivery of team, place and project/programme objectives. • Operational risks are appropriately escalated from Risk Logs to the Operational Risk Register. • Mitigating actions are in place to manage risks in line with the risk appetite statement. • Staff are suitably trained in relation to risk management.
Risk Owners	Risk Owners are responsible for the effective management of the risks assigned to them. They are responsible for ensuring risks remain accurately described and assessed, controls and mitigations are effective, actions are progressed, and risk records are reviewed and updated in accordance with agreed timescales.
Director of Corporate Governance and Assurance / Risk Management Team	The Director of Corporate Governance and Assurance leads on the implementation of corporate governance and risk and assurance systems across the ICBs. They are supported by a Risk Management Team that facilitates the operation of the risk management framework. The Risk Management Team provides specialist advice, training and support, maintains the Board Assurance Framework and Operational Risk Register, coordinates reporting and review processes, and promotes consistent application of this policy. The Risk Management Team does not own risks or mitigations, which remain the responsibility of designated risk owners.

Role / Forums	Responsibilities
Senior Information Risk Owner	The Senior Information Risk Owner (SIRO) provides Board-level leadership for information risk management and is accountable for ensuring that information risks are appropriately identified, managed and escalated. The SIRO provides assurance to the Boards on the effectiveness of information risk management arrangements and compliance with relevant information governance requirements.
Information Asset Owners	Information Asset Owners (IAOs) are responsible for the management of information risks associated with the information assets under their control. They ensure appropriate controls are in place to protect information, identify emerging risks and incidents, and escalate significant information risks through established governance arrangements.
Information Governance, Data Protection and Cyber Steering Group	Oversees information governance, cyber security and data protection risks and ensures significant information risks are escalated through appropriate governance arrangements.
Individuals	All individuals have a responsibility to identify, manage and report risks arising from their activities and to comply with this policy. Risk considerations should form part of routine decision-making, planning, service delivery, programme management and procurement activities.

6. Risk appetite and tolerance

- 6.1 The ICBs recognise that the achievement of their strategic objectives and statutory responsibilities requires informed and proportionate risk-taking. Risk appetite defines the level and type of risk that the ICBs are willing to accept in pursuit of their objectives and in the interests of improving health outcomes, reducing health inequalities, and commissioning sustainable health services for the populations they serve.
- 6.2 The ICBs are committed to managing risk in a manner that supports innovation, transformation and continuous improvement whilst ensuring that risks are understood, appropriately controlled and remain within agreed levels of tolerance. The ICBs do not seek to eliminate all risk; rather, they seek to make informed decisions that balance potential opportunities and benefits against potential adverse impacts.
- 6.3 A common risk appetite framework has been adopted across the ICBs in support of their formal partnership arrangements. The framework provides a consistent basis for decision-making, prioritisation, escalation and assurance, whilst recognising that each ICB remains responsible for the management of its own sovereign risks and statutory responsibilities.
- 6.4 The Boards approve the risk appetite framework and ensure that it is considered when:

- a) Setting strategic objectives and priorities.
- b) Making significant decisions and investments.
- c) Assessing strategic and operational risks.
- d) Determining the need for additional controls or mitigating actions.
- e) Considering whether risks require escalation through governance arrangements.

6.5 Risk tolerance represents the level of residual risk that the ICBs are willing to accept following the implementation of controls and mitigating actions. Risk tolerance is expressed through target risk score ranges, which provide a practical mechanism for applying the risk appetite framework and determining whether further action is required to reduce risk exposure. The risk appetite matrix and associated risk domain tolerances should be used to support consistent risk assessment, management, escalation and reporting.

6.6 The ICBs' risk appetite is described using five categories, ranging from Averse (little or no appetite for risk) to Significant (high appetite for risk where strong controls and assurance arrangements exist). The associated target risk score ranges provide an indication of the level of residual risk that may be tolerated within each category.

Risk appetite level	Description	Target risk score range*
Averse	Preference for ultra-safe delivery options that avoid or minimise risk as much as possible.	1-5
Cautious	Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward.	4-10
Open	Willing to consider all potential delivery options while also providing an acceptable level of reward (and value for money).	8-15
Eager	Seek to be innovative and to choose options offering potentially higher rewards with greater uncertainty (i.e. despite greater inherent risk).	15-20
Significant	Confident in setting high levels of risk appetite because controls, forward scanning and responsiveness systems are robust.	25

* Note that there is some overlap in the risk tolerance ranges, as the scores depend on whether the impact or likelihood score is higher. For example, the risk appetite may be classified as 'averse' if the risk is scored as Impact 5 x Likelihood 1, or 'cautious' if the risk is scored as Impact 1 x Likelihood 5.

6.7 The ICBs have determined their appetite and corresponding target risk score ranges across the principal risk domains set out below. These should be used

when assessing risks, determining the appropriateness of mitigating actions, and considering whether risks remain within acceptable limits.

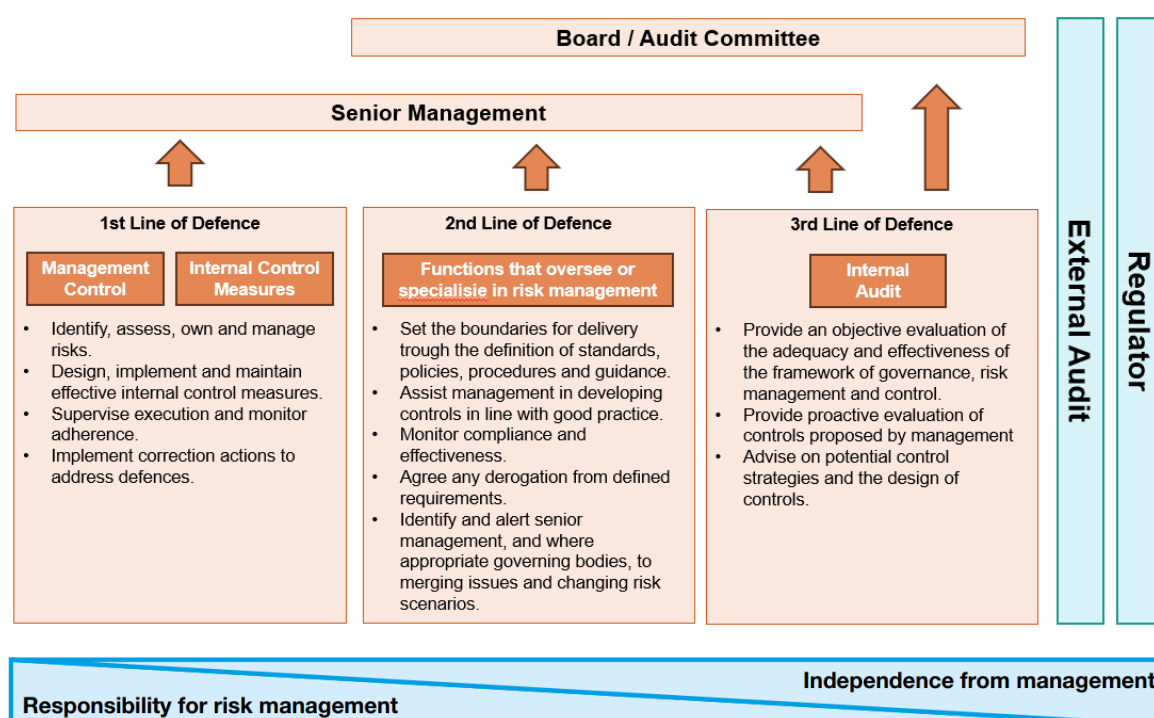
Risk domain	Risk appetite level	Target risk score range
Quality and Access: Risks that people do not receive safe, effective, high-quality and timely care due to failures in quality oversight, service access, capacity, performance or patient experience.	Cautious	4-10
Legal and Regulatory Compliance: Risks of non-compliance with legislation, statutory duties, regulatory requirements, or other mandatory obligations, resulting in enforcement action, legal challenge or loss of public confidence.	Cautious	4-10
Health Outcomes and Inequalities: Risks that the ICBs fail to improve population health outcomes or reduce health inequalities, including failure to target interventions effectively, address unwarranted variation, deliver prevention activity, or achieve improvements in health and wellbeing for the populations served.	Open	8-15
Workforce and Organisational Capability: Risks that the ICBs lack the workforce capacity, capability, leadership, culture or organisational resilience required to deliver its objectives and statutory responsibilities effectively.	Open	8-15
Financial Sustainability and Resource Allocation: Risks that the ICBs fail to achieve financial sustainability or maximise value from available resources, including ineffective resource allocation, poor productivity, inefficiencies, commissioning decisions or inability to meet financial duties.	Open	8-15
Partnerships and Social Value: Risks arising from ineffective leadership, collaboration or stakeholder engagement, leading to reduced system effectiveness, failure to deliver shared objectives, loss of confidence, reputational damage, or reduced social value.	Open	8-15
Planning and Transformation: Risks that the ICBs are unable to effectively plan, design and deliver services, programmes and transformation required to meet current and future population needs, including implementation of new care models, service redesign, strategic planning and major change initiatives.	Eager	15-20

- 6.8 It is recognised that some risks may not be capable of being reduced to the target risk score range. In these circumstances, the focus should be on ensuring that all reasonably practicable controls are in place, that the reasons for the residual exposure are clearly understood, and that appropriate contingency arrangements and governance oversight are maintained.

- 6.9 The risk appetite framework is reviewed periodically by the Boards to ensure that it remains appropriate to the operating environment, strategic priorities and the needs of the populations served.

7. Strategic risk management

- 7.1 Strategic risks are high-level risks that are pro-actively identified and threaten the achievement of the ICB's strategic objectives and key statutory duties. Strategic risks, which are explicitly linked to one or more Board-approved strategic objective, are owned by members of the Executive Management Team and outlined within the Board Assurance Framework (BAF) of the ICBs.
- 7.2 The BAF provides the Boards with confidence that strategic risks have been identified and there are robust systems, policies and processes in place (*controls*) that are effective and driving the delivery of their objectives. It provides confidence and evidence to demonstrate that what needs to be happening is actually happening in practice (*assurances*).
- 7.3 The BAF aligns with the three lines of defence model, where operational management (first line) manages risks day-to-day, oversight functions such as risk and governance teams (second line) provide monitoring and challenge, and internal audit (third line) provides independent assurance. This alignment ensures clear accountability and supports the Boards in making informed decisions on the management of strategic risks.



- 7.4 The BAF plays a key role in informing the production of the ICBs' annual Governance Statements and is the main tool that the Boards should use in discharging overall responsibility for ensuring that an effective system of internal control is in place.
- 7.5 Assurance provides evidence that risks to objectives are being appropriately managed and controlled. Its purpose is to give confidence that risks are effectively mitigated, with higher levels of assurance reflecting greater confidence in risk management. Risk owners and leads achieve this by conducting in-depth assessments of the evidence supporting risk controls. While it is not possible to provide complete or absolute assurance, the concept of positive and negative assurance is applied: positive assurance indicates that controls are effective and risks are being managed as intended, whereas negative assurance indicates that controls are not effective, and risks may not be adequately mitigated.

8. Operational risk management

- 8.1 Operational risks are risks arising from day-to-day activities that may adversely affect the delivery of organisational priorities, statutory duties or operational objectives.
- 8.2 Operational risk management relies upon reactive identification of risks, which are 'dynamic' in nature. Operational risks are managed via additional mitigations and are captured on the Operational Risk Register.
- 8.3 The Operational Risk Register is the central repository for the three ICBs' operational risks. Whilst risks will feature across several processes, it is important that these are captured centrally to provide a comprehensive log of prioritised risks that accurately reflect the risk profiles of the ICBs.
- 8.4 The Operational Risk Register contains details of the risk, the current controls in place and an overview of the actions required to mitigate the risk to the desired level. A named individual (risk owner) is given responsibility for ensuring that mitigating actions are completed by the specified due dates.

9. Risk logs

- 9.1 Risk logs are used to record operational risks at individual team, directorate and programme/project-level.
- 9.2 Oversight of risk logs is the responsibility of the relevant senior manager, who may choose to review them within project or team meetings. Risks that could impact the achievement of ICB priorities must be escalated to the Operational Risk Register. As risk logs are maintained at team or project level, a risk reaching a medium or high score should prompt review and discussion but will

not necessarily result in automatic escalation. This reflects the distinction between risks assessed against team-level objectives and those affecting ICB-wide objectives recorded on the Operational Risk Register. An optional risk log template and guidance, and support on risk logs and escalation, are available from the Risk Management Team.

- 9.3 Directorates may maintain their risk logs using local formats that meet their operational needs. However, all risk logs must apply the ICBs' 5x5 risk scoring matrix, as set out in this policy, to ensure consistency in the identification, assessment, and reporting of risks across the organisations. Risk scores must be derived using the standard definitions of likelihood and impact, enabling comparability and appropriate escalation of risks to the Operational Risk Register where required.

10. Risk management lifecycle

- 10.1 The risk management lifecycle applies to both strategic and operational risks. Whilst the underlying principles remain consistent, strategic risks are managed through the Board Assurance Framework and focus on risks to the achievement of strategic objectives and statutory duties. Operational risks are managed through the Operational Risk Register and Risk Logs and focus on risks arising from day-to-day delivery of services, programmes, and organisational functions.
- 10.2 The main elements of the risk management lifecycle are described below.

Objectives and context

- 10.3 Risks must be identified, assessed and managed in the context of clearly defined objectives. Each risk should be linked to a strategic, operational or local objective to ensure that the potential impact of the risk can be properly understood and managed.
- 10.4 The table below sets out the relationship between organisational objectives, governance arrangements and risk recording mechanisms.

Objective	Oversight	Recording	Risk management role
Strategic	Boards	Board Assurance Framework	Risks are linked to the agreed strategic objectives of the ICBs relating to their role as a strategic commissioner. Updates and assurance are provided by executives to the Boards to support oversight and decision-making.
Operational	Committees of the Boards	Operational Risk Register	Co-ordinated through the Risk Management Team, operational risks relate to high-level corporate priorities

Objective	Oversight	Recording	Risk management role
			and statutory functions. Risk owners provide updates and assurance on mitigation and control measures. Risks can be joint or sovereign ICB risks.
Local	Directorate/ Programme	Risk Log	Managed locally within teams in line with their directorate, team, or programme objectives. Teams identify and monitor risks to achieving these priorities/objectives. Risks may be escalated to the Operational Risk Register through review discussions with the Risk Management Team and relevant senior managers.

Risk identification

- 10.5 Strategic risks are identified proactively by the Boards through consideration of strategic planning processes, environmental scanning, transformation activity, performance and assurance reporting, and consideration of risks to the achievement of strategic objectives and statutory duties. Strategic risks are recorded within the Board Assurance Framework.
- 10.6 Operational risks are identified through day-to-day management activities, including risk assessments, audit findings, incidents, complaints, project delivery, performance monitoring and horizon scanning. Operational risks are recorded within the Operational Risk Register and Risk Logs, as appropriate.
- 10.7 Risks should be identified as early as possible and reviewed regularly to ensure that emerging threats or opportunities are recognised and managed appropriately.
- 10.8 The Boards, their committees, and management teams should consider new and emerging risks as part of their routine business as appropriate.

Risk articulation

- 10.9 Risks should be described clearly and consistently using the cause-event-effect model shown below.

Risk element	Question	Consideration	Wording
Cause	What will cause the risk to occur?	Risks may arise from strategic uncertainties, external factors, operational activities or specific events that could affect the achievement of objectives.	Where the cause is known, use: “As a result of...” . If the cause is uncertain, hypothetical, or conditional, it

Risk element	Question	Consideration	Wording
			may be appropriate to use: "If...".
Event	What can go wrong?	The risk event is the specific thing that could go wrong, potentially disrupting operations or objectives.	There is a risk
Effect	What will be the consequence/ effect if the risk were to materialise?	Risks may negatively impact the organisation and its ability to achieve objectives. The specific objective at risk should be reflected in the wording.	Which may lead to

Risk assessment

- 10.10 Risks should be assessed using the ICBs' 5x5 risk scoring matrix (shown in Appendix C), considering both impact and likelihood.
- 10.11 Impact should be assessed against the relevant objective affected by the risk, while likelihood should be assessed against the probability of the risk materialising within the next 12 to 18 months.
- 10.12 Strategic risks should additionally be assessed with reference to the effectiveness of existing controls, available assurances, and any identified gaps in control or assurance. Operational risks should be assessed with reference to current controls, mitigating actions and residual risk exposure.
- 10.13 Risk scores should be reviewed periodically to ensure that they remain accurate and proportionate. Where appropriate, risk scores may be challenged through management review, governance processes or committee oversight.

Risk treatment

- 10.14 Risk treatment is the process of determining how a risk will be managed. The ICBs adopt the 4T model of risk treatment (terminate, treat, transfer or tolerate), as set out in the table below.

Treatment	Description
Terminate	Opt not to take the risk by terminating the activities that will cause it (more applicable to project risks).
Treat	Take mitigating actions that will minimise the impact of the risk prior to its occurrence and/or reduce the likelihood of the risk occurring.
Transfer	Transfer the risk, or part of the risk, to a third party.

Treatment	Description
Tolerate	Accept the risk and take no further actions. This may be due to the cost of risk mitigation activity not being cost effective or the impact is so low it is deemed acceptable to the organisation. Risks which are tolerated should continue to be monitored as future changes may make the risk no longer tolerable.

- 10.15 Risk owners should implement appropriate treatment actions to reduce risks to a level consistent with the ICBs' risk appetite and target risk score ranges.
- 10.16 For strategic risks, treatment may include strengthening strategic controls, obtaining additional assurance, implementing transformation programmes, revising strategic plans, or enhancing governance arrangements.
- 10.17 Where a risk cannot reasonably be reduced further, it may be accepted through the appropriate governance process provided that the residual exposure is understood and appropriate oversight arrangements remain in place.

Monitoring and reporting

- 10.18 Monitoring risk is a continuous activity that results in the awareness of what is happening across the organisations. Risks are required to be reviewed regularly to ensure that controls remain effective, mitigating actions are delivered, and risk scores remain accurate.
- 10.19 Medium scoring risks are required to be reviewed at least quarterly, with high scoring risks reviewed at least bi-monthly, and extreme scoring risks reviewed at least monthly.
- 10.20 Strategic risks are monitored through the Board Assurance Framework and operational risks are monitored through the Operational Risk Register and Risk Logs.
- 10.21 The BAF will be reported to the Boards twice yearly. This will be supported by bi-annual reporting of the relevant strategic risks to their lead committees. These reports will facilitate the review of controls, assurances, gaps in control and assurance, progress against actions and changes in risk exposure. The Audit Committees will also have a key role in providing independent oversight of the effectiveness of the ICBs' strategic risk management processes through bi-annual risk management reports.
- 10.22 Operational Risk Register reporting arrangements are set out below:
- The ICBs' Boards will oversee all risks with an overall score of 15 or above at each of its meetings.

- b) Committees of the Boards will oversee all risks relevant to their remit with an overall score of 8 or above at each of their meetings.
- c) The Executive Management Team will receive all risks with an overall score of 8 or above on a quarterly basis to support effective matrix working, cross-portfolio visibility, and collective oversight of emerging themes.
- d) The **Audit Committees** will receive bi-annual risk management updates, which will enable any risk themes and trends to be reviewed. This will support their duty to provide the Boards with assurance on the robustness and effectiveness of the ICB's risk management processes.

Archiving of risks

10.23 Archiving risks within the ICBs is a structured process designed to ensure that the risk register remains current, relevant, and aligned with the evolving operational landscape.

10.24 Risks may be archived where:

- a) The risk no longer exists or is no longer relevant.
- b) The risk has been adequately mitigated.
- c) The risk has reduced to an agreed target risk score.
- d) Responsibility for the risk has transferred.
- e) The risk is better managed through an alternative governance mechanism.

10.25 Strategic risks may also be removed from the Board Assurance Framework where the associated objective has been achieved, the risk no longer threatens achievement of the objective, or the risk is more appropriately managed through operational risk management arrangements.

10.26 The rationale for archiving must be recorded and archived risks must be retained for audit and assurance purposes.

11. Fraud risks

11.1 The Government Functional Standard 013: Counter Fraud "Management of counter fraud, bribery and corruption activity" has applied to NHS organisations since April 2021. The standard is part of a suite of standards that promotes consistent and coherent ways of working across government, and provides a stable basis for assurance, risk management and capability improvement.

- 11.2 The NHS Counter Fraud Authority (NHSCFA) is a health authority charged with identifying, investigating and preventing fraud and other economic crime within the NHS. The NHSCFA requires the organisation to undertake a local risk assessment to identify fraud, bribery and corruption risks and to ensure these are recorded and managed in line with its risk management policy.
- 11.3 A separate joint fraud risk register will be maintained by the ICBs and reported to the Audit Committees once a year (as a minimum), to coincide with the Counter Fraud annual planning process.

12. Information risks

- 12.1 Information risk management is led by the Senior Information Risk Owner (SIRO) who is responsible for ensuring that information risks are effectively identified, assessed, and managed. The SIRO also ensures the organisation maintains compliance with all relevant legislation, including the Data Protection Act 2018, UK General Data Protection Regulation (UK GDPR), the Human Rights Act 1998, and other applicable information security and cybersecurity requirements.
- 12.2 The organisations recognise that information risks can arise from the loss, misuse, unauthorised access, or failure to protect information, whether in digital or physical form. These risks can impact the confidentiality, integrity, and availability of information, and must be managed through appropriate controls. Several arrangements are in place to support, manage and mitigate information risks which include, but are not limited to, the Information Asset and Data Flow Mapping registers, information governance incident management arrangements, and Data Protection Impact Assessments (DPIAs).

13. Performance against key delivery priorities

- 13.1 The ICBs monitor performance against key delivery priorities via a separate, but parallel, process to the risk management arrangements.
- 13.2 To minimise duplication, failures to achieve performance standards are not routinely identified as specific risks on the Operational Risk Register. This should not indicate its absence from the organisations' overall risk profile and poor performance from a risk perspective will be referenced as necessary when reporting externally on risks.
- 13.3 The consistent non-delivery of performance standards will be assessed to ensure that any specific risks this poses to the functions of the ICBs (e.g., a detrimental impact on health outcomes, patient safety or experience) are identified and captured on the Operational Risk Register.

14. Management of issues

- 14.1 An issue is a current problem, concern, or event that has already materialised and is impacting the organisations. Unlike a risk, which refers to a potential future event with uncertain outcomes, an issue represents something that is happening now and requires immediate attention or resolution.
- 14.2 Issues are not routinely recorded on the Operational Risk Register as they are managed via the performance management framework. However, senior leads/managers may use discretion as to whether local issues are captured on individual risk logs.
- 14.3 Known issues are an important mechanism to determine if there are any new risks needed to be identified, and captured, within the risk management arrangements.

15. Equality and diversity statement

- 15.1 The ICBs pay due regard to the requirements of the Public Sector Equality Duty (PSED) of the Equality Act 2010 in policy development and implementation, as commissioners and providers of services, as well as employers.
- 15.2 The ICBs are committed to ensuring that the way services are provided to the public and the experiences of staff does not discriminate against any individuals or groups on the basis of their age, disability, gender identity (trans, non-binary) marriage or civil partnership status, pregnancy or maternity, race, religion or belief, gender or sexual orientation.
- 15.3 The ICBs are committed to ensuring that activities also consider the disadvantages that some people in the diverse population experience when accessing health services. Such disadvantaged groups include people experiencing economic and social deprivation, carers, refugees and asylum seekers, people who are homeless, workers in stigmatised occupations, people who are geographically isolated, Gypsies, Roma, and Travellers.
- 15.4 To help ensure that these commitments are embedded in day-to-day working practices, an Equality Impact Assessment has been completed, and is included within this policy.

16. Communication, monitoring and review

- 16.1 This policy will be published and maintained in line with the ICBs' Policy Management Framework.

- 16.2 The policy will be highlighted to new staff as part of the local induction process and made available to all staff through internal communication procedures (and internet/intranet sites).
- 16.3 The Audit Committees will review the effectiveness of this policy, and its implementation, via bi-annual risk management update reports.
- 16.4 Any individual who has queries regarding the content of this policy or has difficulty understanding how this policy relates to their role, should contact the Risk Management Team.

17. Confidentiality

- 17.1 Risk-related information will be managed in accordance with the ICBs' information governance policies and relevant data protection legislation. Access to confidential information will be restricted to those with a legitimate business need and handled in a manner appropriate to its sensitivity.
- 17.2 All individuals are responsible for maintaining the confidentiality of risk information and ensuring it is recorded, stored and shared appropriately.
- 17.3 Where disclosure of a risk may not be in the public interest, the risk may be managed through confidential governance arrangements. Such arrangements should be applied only where necessary and reviewed periodically to ensure continued appropriateness.

18. Staff training

- 18.1 The ICBs are committed to ensuring that individuals have the knowledge and understanding necessary to fulfil their responsibilities under this policy. Appropriate risk management training, guidance and support will be made available to promote the consistent application of risk management principles and processes across the organisations.
- 18.2 Individuals are responsible for familiarising themselves with the requirements of this policy and participating in any training or development activity relevant to their role. Managers should ensure that staff are appropriately supported to discharge their risk management responsibilities.
- 18.3 The effectiveness of risk management training and awareness arrangements will be reviewed periodically as part of the ICBs' broader review of risk management processes and organisational assurance arrangements.

19. Interaction with other policies

- 19.1 This policy should be read alongside the following related ICB policies:
 - a) Standard of Business Conduct Policy.

- b) Health and Safety Policies.
- c) Information Governance Policies.

20. References

20.1 The following references have been used in the formulation of this policy:

- a) HM Treasury. (2012). Assurance Frameworks. London: HM Government.
- b) National Patient Safety Agency (NPSA). (2008). A Risk Matrix for Risk Managers. London: NPSA.
- c) Institute of Risk Management. (2018). A Risk Practitioners Guide to ISO 31000:2018. London: IRM.
- d) NHS Providers. (2015). Board Assurance: A Toolkit for Health Sector Organisations. London: NHS Providers.
- e) HM Treasury. (2020). The Orange Book: Management of Risk – Principles and Concepts. London: HM Government.
- f) NHS England. (2024). Data Security and Protection Toolkit. Retrieved from <https://www.dsptoolkit.nhs.uk>
- g) Institute of Risk Management. (2011). Risk Appetite & Tolerance. London: IRM.
- h) International Organization for Standardization. (2018). ISO 31000:2018 – Risk Management Guidelines. Geneva: ISO.
- i) Healthcare Financial Management Association (HFMA). (2018). NHS Audit Committee Handbook. London: HFMA.
- j) Healthcare Financial Management Association (HFMA). (2017). NHS Governance Handbook. London: HFMA.
- k) Good Governance Institute (GGI). (2012). Risk Appetite for NHS Organisations: A Matrix to Support Better Risk Sensitivity in Decision Taking. London: GGI.
- l) Good Governance Institute (GGI). (n.d.). Risk Appetite. Retrieved from <https://www.good-governance.org.uk>
- m) NHS England. (2025). Risk Management Framework. London: NHS England.
- n) National Quality Board (NQB). (2024). Principles for Assessing and Managing Risks Across Integrated Care Systems. London: NQB.
- o) Financial Reporting Council. (2024). UK Corporate Governance Code. London: FRC.

21. Equality Impact Assessment

Date of assessment:	October 2025			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
Age ¹	There are no actual or expected impacts on the characteristic of age.	Not applicable.	Not applicable.	Not applicable.
Disability (Including: mental, physical, learning, intellectual and neurodivergent) ²	There are no actual or expected impacts on the characteristic of disability.	Not applicable.	Not applicable.	Not applicable.
Gender (including trans, non-binary and gender reassignment) ³	There are no actual or expected impacts on the characteristic of gender.	Not applicable.	Not applicable.	Not applicable.

¹ A person belonging to a particular age (for example 32 year olds) or range of ages (for example 18 to 30 year olds).

² A person has a disability if she or he has a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities.

³ The process of transitioning from one gender to another.

Date of assessment:	October 2025			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
Marriage and civil partnership⁴	There are no actual or expected impacts on the characteristic of marriage and civil partnership	Not applicable.	Not applicable.	Not applicable.
Pregnancy and maternity⁵	There are no actual or expected impacts on the characteristic of pregnancy and maternity Status.	Not applicable.	Not applicable.	Not applicable.
Race⁶	There are no actual or expected impacts on the characteristic of race.	Not applicable.	Not applicable.	Not applicable.

⁴ Marriage is a union between a man and a woman or between a same-sex couple.

Same-sex couples can also have their relationships legally recognised as 'civil partnerships'.

⁵ Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth and is linked to maternity leave in the employment context. In the non-work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman unfavourably because she is breastfeeding.

⁶ Refers to the protected characteristic of race. It refers to a group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins.

Date of assessment:	October 2025			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
Religion or belief⁷	There are no actual or expected impacts on the characteristic of religion or belief	Not applicable.	Not applicable.	Not applicable.
Sex⁸	There are no actual or expected impacts on the characteristic of sex.	Not applicable.	Not applicable.	Not applicable.
Sexual orientation⁹	There are no actual or expected impacts on the characteristic of sexual orientation.	Not applicable.	Not applicable.	Not applicable.

⁷ Religion refers to any religion, including a lack of religion. Belief refers to any religious or philosophical belief and includes a lack of belief. Generally, a belief should affect your life choices or the way you live for it to be included in the definition.

⁸ A man or a woman.

⁹ Whether a person's sexual attraction is towards their own sex, the opposite sex, to both sexes or none. <https://www.equalityhumanrights.com/en/equality-act/protected-characteristics>

Date of assessment:	October 2025			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
Carers¹⁰	There are no actual or expected impacts on the characteristic of carers.	Not applicable.	Not applicable.	Not applicable.

¹⁰ Individuals within the ICB which may have carer responsibilities.

Appendix A: Definitions and Glossary of Terms

Definitions of key terms referenced in this policy are described in the table below:

Term	Definition
Assurance	Evidence that provides confidence that risks are being effectively managed and that controls are operating as intended.
Board Assurance Framework	A structured framework used by the Boards to identify and manage strategic risks to the achievement of strategic objectives. The BAF records strategic risks, controls, assurances, gaps in control or assurance, and actions required to strengthen risk management and organisational assurance.
Controls	Measures implemented to manage risk by reducing its likelihood, impact or both. Controls may include policies, procedures, systems, behaviours, governance arrangements and oversight mechanisms.
Corporate risks	Operational risks which relate to the delivery of the statutory duties, functions and/or priorities/objectives of an organisation.
Current (or residual) risk score	The numerical assessment of the risk (impact vs. likelihood) after taking into consideration any mitigating controls and/or actions.
Information Asset	An information asset is a body of information, which can be as small as a single document, defined and managed as a single unit so it can be understood, shared, protected, and exploited efficiently. Information assets have recognisable and manageable value, lifecycles, and risks that could impact the confidentiality, integrity and availability of the information.
Initial risk (or inherent) risk score	The numerical assessment of the risk (impact vs. likelihood) prior to considering any additional mitigating controls and/or actions.
Integrated Care Board (ICB)	An ICB is the statutory NHS organisation within the ICS which holds responsibility for NHS functions and budgets.
Joint Risk	A risk that affects more than one ICB and requires coordinated management, oversight or mitigating action across organisations. Joint risks may arise from shared objectives, programmes, partnerships or operational arrangements.

Term	Definition
Operational risk	A risk arising from day-to-day activities that may adversely affect the delivery of organisational priorities, statutory duties or operational objectives.
Operational Risk Register (ORR)	A tool for recording identified 'live' operational risks and monitoring actions to mitigate them.
Operational risk management	Risk management processes which focus on 'live' operational risks which an organisation is potentially facing. It relies upon the identification of risks, which are 'dynamic' in nature and are managed via additional mitigations. Operational risk management processes are centred around the Operational Risk Register.
Risk	There are many definitions of risk, but this policy has adopted the definition set out in ISO 31000 in that a risk is the 'effect of uncertainty on objectives'. The effects can be negative, positive or both. It is measured in terms of impact and likelihood.
Risk appetite	The level and type of risk that an organisation is willing to accept in pursuit of its objectives.
Risk assessment	The process of identifying, analysing and evaluating risks to determine their significance and the need for further action.
Risk culture	The values, beliefs, knowledge and understanding of risk, shared by a group of people with a common intended purpose.
Risk logs	Risk logs are a tool for capturing operational level risks at team/directorate/place/project level which may impact on the delivery of local objectives. Examples of risk logs may include directorate/team specific risk logs, project risk logs and transformation programme risk logs.
Risk management	The arrangements and activities in place that direct and control an organisation regarding risk.
Risk mitigation	Actions or controls implemented to reduce the likelihood or impact of a risk.
Risk owner	The individual accountable for ensuring that a risk is appropriately managed, reviewed and reported. Risk owners are responsible for maintaining risk records, implementing mitigating actions and providing assurance regarding the effectiveness of controls.

Term	Definition
Risk profile	The overall nature, extent and combination of risks faced by an organisation at a particular point in time.
Risk treatment	The process of selecting and implementing suitable measures to modify the risk.
Sovereign ICB risk	A risk that principally affects a single ICB and is managed through that organisation's governance and risk management arrangements. The cause, impact, risk score and mitigations may differ across the three ICBs.
Strategic objectives	Strategic objectives describe a set of clear organisational goals that help establish priority areas of focus. Whilst broad and directional in nature, they need to be specific enough that their achievement can be assured, and progress measured. They should have direct alignment with the (Board) Assurance Framework and an organisation's performance management processes.
Strategic risk management	Risk management processes which support the achievement of the organisation's strategic objectives. It focuses on the proactive identification of 'high level' risks which are managed by an established control framework and planned assurances. Strategic risk management processes are centred around the (Board) Assurance Framework.
Strategic risks	A risk that may prevent the achievement of strategic objectives or statutory duties and is managed through the Board Assurance Framework.
Target risk score	The level of residual risk exposure that an organisation aims to achieve through the implementation of appropriate controls and mitigating actions.
Three lines of defence model	A risk governance framework that splits responsibility for operational risk management across three functions, where operational management (first line) manages risks day-to-day, oversight functions such as risk and governance teams (second line) provide monitoring and challenge, and internal audit (third line) provides independent assurance.

Appendix B: Risk Scoring Matrix

Table 1A: Impact Score (I) Guidance

Impact Score	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
Guidance	Negligible impact on objective/s. Day to day operational challenges.	Minor impact on objective/s. Temporary restriction to service delivery with limited impact on stakeholder confidence.	Moderate impact on objective/s. Short term failure to deliver key objectives with temporary adverse local publicity.	Major impact on objective/s. Medium term failure to deliver key objectives with ongoing adverse publicity or negative impact on stakeholder confidence.	Catastrophic impact on objective/s. Continued failure to deliver key objectives with long term adverse publicity or fundamental loss of stakeholder confidence.

Table 1B: Impact Score (I) Further Guidance broken by Risk Domain

The following domain-specific descriptors provide additional guidance to support consistent assessment of impact. They should be applied alongside the general impact score guidance in Table 1A and considered in the context of the objective affected by the risk. Where a risk spans more than one domain, the impact score should reflect the most significant credible consequence.

Risk Domain	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
Quality and Access: Risks that people do not receive safe, effective, high-quality and timely care due to failures in quality oversight, service access, capacity, performance or patient experience.	No, or very limited, impact on patient safety, clinical effectiveness, access or patient experience. Any issue is isolated and	Minor or localised impact on access, quality or experience, with limited disruption and no significant risk of harm.	Noticeable deterioration in quality, access or experience affecting a service, pathway or population group, requiring	Significant deterioration in quality, access or experience, with increased risk of avoidable harm, sustained service	Severe or widespread failure in quality, safety, access or experience, with actual or likely serious harm, loss

Risk Domain	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
	readily managed through routine processes.		management action and oversight.	pressures or formal escalation through governance arrangements.	of confidence, or need for urgent system-level intervention.
Legal and Regulatory Compliance: Risks of non-compliance with legislation, statutory duties, regulatory requirements, or other mandatory obligations, resulting in enforcement action, legal challenge or loss of public confidence.	No breach, or minor technical non-compliance, with no material consequence and readily correctable through routine action.	Isolated or low-level non-compliance with limited impact, requiring local corrective action but unlikely to result in enforcement or formal challenge.	Confirmed non-compliance with statutory, regulatory or mandatory requirements, requiring formal action, reporting or external engagement.	Significant or repeated non-compliance, with risk of enforcement action, legal challenge, regulatory intervention or material loss of confidence.	Severe or systemic non-compliance resulting in, or likely to result in, prosecution, major regulatory action, critical findings or significant loss of public confidence.
Health Outcomes and Inequalities: Risks that the ICBs fail to improve population health outcomes or reduce health inequalities, including failure to target interventions effectively, address unwarranted variation, deliver prevention activity, or achieve improvements in health and wellbeing for the populations served.	No material impact on population health outcomes or inequalities; any effect is limited, short-term and easily addressed.	Minor impact on a small group or locality, with limited effect on access, outcomes or inequalities.	Measurable or noticeable impact on outcomes or inequalities for a defined population, pathway or locality, requiring targeted corrective action.	Significant impact on population outcomes or inequalities, with substantial variation in access, experience or outcomes and risk to delivery of strategic objectives.	Severe or widespread deterioration in outcomes or inequalities, with long-term consequences for population health, major inequity or substantial failure to deliver statutory ambitions.
Workforce and Organisational Capability: Risks that the ICBs lack the workforce	Minimal impact on workforce capacity,	Minor workforce or capability pressure	Sustained workforce,	Significant workforce or	Critical workforce or organisational

Risk Domain	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
capacity, capability, leadership, culture or organisational resilience required to deliver its objectives and statutory responsibilities effectively.	capability, leadership, culture or resilience; objectives remain deliverable through routine management.	causing limited disruption to delivery, with manageable local action required.	leadership, cultural or capability pressures affecting delivery of objectives, staff experience or organisational effectiveness.	organisational capability failure, including loss of key capacity, leadership instability, poor culture or reduced resilience affecting delivery of statutory responsibilities.	failure resulting in inability to deliver key functions, maintain safe operations or discharge statutory responsibilities effectively.
Financial Sustainability and Resource Allocation: Risks that the ICBs fail to achieve financial sustainability or maximise value from available resources, including ineffective resource allocation, poor productivity, inefficiencies, commissioning decisions or inability to meet financial duties.	No material financial impact, or negligible effect on resource use, productivity, value for money or financial duties.	Minor financial pressure, inefficiency or resource allocation issue, manageable within existing plans and controls.	Material financial pressure, inefficiency or sub-optimal resource allocation affecting delivery of plans, productivity or value for money.	Significant financial risk affecting delivery of statutory duties, financial balance, investment decisions or ability to allocate resources effectively.	Severe financial failure or unsustainable resource position, with inability to meet financial duties, maintain services or support strategic objectives.
Partnerships and Social Value: Risks arising from ineffective leadership, collaboration or stakeholder engagement, leading to reduced system effectiveness, failure to deliver shared objectives, loss of confidence, reputational damage, or reduced social value.	No material impact on partnership relationships, stakeholder confidence, collaboration or social value.	Minor tensions or limited stakeholder concern, with negligible impact on delivery of shared objectives.	Deterioration in relationships, collaboration or stakeholder confidence affecting coordination, delivery or the ability to realise shared benefits.	Significant breakdown in partnership working, stakeholder engagement or collective leadership, with sustained impact on delivery, confidence or social value.	System-wide failure of collaboration or confidence, causing substantial loss of trust, inability to deliver shared objectives or major reputational damage.

Risk Domain	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
Planning and Transformation: Risks that the ICBs are unable to effectively plan, design and deliver services, programmes and transformation required to meet current and future population needs, including implementation of new care models, service redesign, strategic planning and major change initiatives.	No material disruption to planning, programme delivery, transformation or implementation of agreed change.	Minor delay, dependency issue or planning gap, with limited impact on delivery and manageable through routine programme controls.	Noticeable delay, slippage or delivery risk affecting a programme, service redesign or strategic planning objective, requiring formal corrective action.	Significant failure or sustained slippage in planning or transformation, affecting delivery of major change, strategic objectives or expected benefits.	Fundamental failure to plan, deliver or implement major transformation, resulting in long-term inability to meet population needs, deliver strategic objectives or maintain system confidence.

Table 2: Likelihood Score (L)

Likelihood score	1	2	3	4	5
Descriptor	Rare	Unlikely	Possible	Likely	Almost certain
Frequency	Probably never happen / recur only in very exceptional circumstances.	Do not expect it to happen / recur but is possible it may do so.	Might happen / recur occasionally.	Will probably happen / recur but is not a persisting issue.	Will undoubtedly happen / recur, expected to occur in most circumstances.
How likely is it to happen?	Less than 1% chance of event happening.	1% - 30% chance of event happening.	31% - 60% chance of event happening.	61% - 95% chance of event happening.	96% to 99% of chance of this occurring.

Table 3: Impact (I) x Likelihood (L) Risk Matrix

Impact ↑	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
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
		Likelihood →				
Risk Profile		Very Low (1-3)	Low (4-6)	Medium (8-12)	High (15-20)	Extreme (25)