NHS Derby and Derbyshire Integrated Care Board

NHS Lincolnshire Integrated Care Board

NHS Nottingham and Nottinghamshire Integrated Care Board

Risk Management Policy

November 2025 – November 2028

Policy purpose and key messages
The purpose of this policy is to set out how NHS Derby and Derbyshire Integrated Care Board, NHS Lincolnshire Integrated Care Board and NHS Nottingham and Nottinghamshire Integrated Care Board (ICBs) will manage both strategic and operational risks. It seeks to ensure alignment of working practices during the ICB transition programme, in accordance with the NHS 10-year plan. This policy aims to ensure that risk management is viewed as an essential process within the ICBs and provides assurance to the public, patients, and partner organisations that risks are being managed appropriately. It sets out the risk architecture of the ICBs (roles, responsibilities, communication and reporting arrangements) and describes how risk management is integrated into governance arrangements, key business activities and culture.

CONTROL RECORD	
Title	Risk Management Policy
Reference number	DLN-GOV-001
Version	1.2
Status	Final
Author	ICB Risk Management Leads
Sponsor	Amanda Sullivan, Chief Executive
Team	Corporate Governance and Assurance
Amendments	Definitions for Sovereign ICB and joint risks have been introduced, together with amendments to the risk reporting process, Senior Leadership Team risk responsibilities and updates to the risk log process.
Superseded documents	DLN-GOV-001 Risk Management Policy v1.1
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	Not applicable
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	20 November 2025
Date of issue	March 2026
Review date	November 2028
Policy retention period	Life of organisation plus 6 years
This is a controlled document and whilst this policy may be printed, the electronic version available on the ICB's 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

1.1 This policy is applicable to NHS Derby and Derbyshire Integrated Care Board, NHS Lincolnshire Integrated Care Board and NHS Nottingham and Nottinghamshire Integrated Care Board, collectively referred to in this policy as 'the ICBs.'

1.2 The ICBs are statutory organisations which form part of the wider Derby and Derbyshire, Lincolnshire and Nottingham and Nottinghamshire Integrated Care Systems (ICS). While this policy specifies risk management arrangements for the statutory ICBs, it is essential that these arrangements operate collaboratively with other key components of the respective ICS families.

Figure 1 – Key parts of the Integrated Care System (ICS)

1.3 The management of risk across organisational boundaries is complex. Governance models should allow sovereign organisations to manage their own risks independently, whilst enabling a strong and holistic partnership approach to risk management to support the delivery of system priorities.

1.4 A sovereign ICB risk is one that impacts one ICB or affects the ICBs differently, meaning the cause, score, and required management may vary across Nottingham and Nottinghamshire, Derby and Derbyshire, and Lincolnshire. These risks do not require uniform treatment or a single shared risk rating. By contrast, a joint risk is shared equally by all three ICBs, with the same cause, event, effect, management expectations, and risk score.

1.5 The ICBs recognise that risk management is an essential business activity that underpins the achievement of an organisation's objectives. A proactive and robust approach to risk management can:

- Reduce risk exposure through the development of a 'lessons learnt' environment and more effective targeting of resources.

- Support informed decision-making to allow for innovation and opportunity.
- Enhance compliance with applicable laws, regulations and national guidance.
- Increase stakeholder confidence in corporate governance and ability to deliver.

1.6 Risk is accepted as an inherent part of health care. Likewise, uncertainty and change in the evolving healthcare landscape may require innovative approaches that bring with them more risk. Therefore, it is not practical to aim for a risk-free or risk-averse environment; rather one where risks are considered as a matter of course and identified and managed appropriately.

1.7 This policy has been developed to ensure that risk management is fundamental to all activities of the ICBs and is understood as the business of everyone. The policy has adopted the following principles of risk management as set out in the ISO 31000: 2018 standard[1].

Principle	Description
Integrated	Risk management is an integral part of all organisational activities.
Inclusive	Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.
Structured and comprehensive	A structured and comprehensive approach to risk management contributes to consistent and comparable results.
Customised	The risk management framework and process are customised and proportionate to the organisation's external and internal context related to its objectives.
Dynamic	Risks can emerge, change or disappear as an organisation's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.
Best available information	The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly considers any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.

[1] ISO 31000 helps organisations develop a risk management approach to effectively identify and mitigate risks, thereby enhancing the likelihood of achieving their objectives and increasing the protection of their assets. https://www.iso.org/iso-31000-risk-management.html

Principle	Description
Human and cultural factors	Human behaviour and culture significantly influence all aspects of risk management.
Continual improvement	Risk management is continually improved through learning and experience.

Table 1 – ISO 31000 principles of risk management

1.8 This policy demonstrates the commitment of the ICBs to a total risk management function. It sets out the risk architecture of the ICBs (roles, responsibilities, communication and reporting arrangements) and describes how risk management is integrated into governance arrangements, key business activities and culture.

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:

- Outline the benefits of risk management.
- Explain the risk appetite and approach to tolerance within the ICBs.
- Set out the ambition of the ICBs to continuously improve risk management arrangements.
- Outline the approach to implementation and monitoring.
- Describe the relevant compliance and assurance arrangements regarding risk management within the ICBs.
- 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 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.

4.2 The diagram below summarises the differences between strategic and operational risks. Further detail is provided at Appendix B.

Figure 2 – The two types of risks

5. Roles and Responsibilities

5.1 Key responsibilities for specific roles and staff groups are described in the table below:

Role / Forums	Responsibilities
Integrated Care Boards	The Boards have overall accountability for risk management and, as such, need to be satisfied that appropriate arrangements are in place and that internal control systems are functioning effectively. The Boards determine the ICBs' joint risk appetite and risk tolerance levels and are also responsible for establishing the joint risk culture.
Audit Committees	The Audit and Risk Committees provide the Boards with assurance on the effectiveness of the Board Assurance Framework and the robustness of the ICBs' operational risk management processes. The role is not to 'manage risks' but to ensure that the approach to risks is effective and meaningful. In particular, the Committees support the Boards by obtaining assurances that controls are working as they should, seeking assurance about the underlying data upon which assurances are based and challenging

Role / Forums	Responsibilities
	relevant managers when controls are not working, or data is unreliable.
ICB Committees	Committees are responsible for monitoring operational risks related to their delegated duties* 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.
Operational groups with oversight of Information Governance	Data protection and information security risks identified through operational activities, DPIAs, or the DSPT are recorded in a combined IG, IT, and cyber risk log. This log includes tailored mitigations for each risk and is regularly updated and reviewed to ensure all risks are current and effectively managed.
Executive Management Team	The Executive Management Team (EMT) provides oversight of the organisations' approach to risk management. It ensures risks are appropriately owned, assessed, and mitigated, and that controls are effective. The EMT reviews escalated risks, determines whether further action or escalation to the Boards is required, and monitors trends to support proactive risk management and continuous improvement.
Individuals	
Chief Executive	The Chief Executive has responsibility for maintaining a sound system of internal control that supports the achievement of the ICB's policies, aims and objectives, whilst safeguarding public funds and assets. As part of the BAF, the Chief Executive on behalf of the Boards, will publish statements on internal control known as the Annual Governance Statements. These will give stakeholders confidence that the ICBs can demonstrate they are adequately informed about the totality of their risks.
ICB Non-Executive and Partner Members	As members of the Boards and committees, Non-Executive Members will ensure an impartial approach to risk management activities and should satisfy themselves that systems of risk management are robust and defensible.

Role / Forums	Responsibilities
Senior Leadership Team member with oversight of risk management *(including Directors)* *(supported by the Risk Management Team)*	This individual leads on the implementation of corporate governance and risk and assurance systems across the ICBs. This includes the development, implementation and co-ordination of the risk management activities and provision of training and advice in relation to all aspects of this policy. 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; and Staff are suitably trained in relation to risk management.
Risk Management Team	The Risk Management Team is responsible for consolidating, reviewing, and reporting risk management information, and for providing guidance and support to ensure the Risk Management Policy is applied consistently across the ICBs. This includes supporting the implementation of risk management arrangements, maintaining the operational risk register and Board Assurance Framework, providing guidance and training to staff on risk management processes, and monitoring the application of the policy in practice to ensure operational and strategic risks are appropriately identified, assessed, mitigated, and escalated. The Risk Management Team work with subject matter experts to identify risks and articulate control and mitigation strategies.
Executive Directors	Executive Directors are responsible for ensuring effective systems of risk management are in place, and commensurate with this policy, within their respective Directorates. This includes promoting the risk culture and ensuring all senior leaders, within their respective Directorates, have a robust understanding of risk management arrangements.

Role / Forums	Responsibilities
Senior Information Risk Owner (SIRO)	The SIRO takes ownership of the ICBs' information risks. The SIRO operates at Board level and is responsible for ensuring that organisational information risk is properly identified and managed, and that appropriate assurance mechanisms exist to support effective information risk management.
Risk Owners	Risk owners are responsible for the effective management of the risks assigned to them. This includes ensuring that appropriate mitigating actions are identified, implemented, and monitored to reduce the risk to an acceptable level. Risk owners of risks on the Operational Risk Register and Board Assurance Framework are also responsible for providing timely and accurate updates on their risks as part of the regular risk review process coordinated by the Risk Management Team.
Information Asset Owners (IAOs) ***(Executive / Senior Leadership Team Level)***	Information Asset Owners (IAOs) are responsible for ensuring risks relating to information assets under their control are managed securely, in compliance with data protection and information governance policies. They oversee the use, protection and retention of data, ensuring that risks are mitigated, and access is appropriately controlled. This role is supported by the Information Asset Managers, see the Information Governance Management Framework for further detail.
Individuals	All individuals are required to comply with this policy and are expected to consider risks in all activities, including business planning, procurement, and project delivery. This includes identifying risks at the outset of projects or activities, conducting risk assessments where necessary, and continuously reviewing risks throughout the lifecycle. Individuals must integrate risk considerations into planning, procurement, and operational decisions, and ensure that any operational risks they identify are appropriately recorded on local risk logs or the ICB's Operational Risk Register in line with the assessed risk score.

Table 2 – Roles and responsibilities

6. Risk Appetite

6.1 Good risk management is not about being risk averse, it is also about recognising the potential for events and outcomes that may result in opportunities for improvement, as well as threats to success.

6.2 A 'risk aware' organisation encourages innovation to achieve its objectives and exploit opportunities and can do so in confidence that risks are being identified and controlled by senior managers.

6.3 The sovereign ICB Boards have previously approved individual risk appetites, which have now been aligned to create a joint risk appetite statement as follows:

Joint Risk Appetite Statement
The Boards of NHS Derby and Derbyshire, NHS Lincolnshire, and NHS Nottingham and Nottinghamshire Integrated Care Boards (ICBs) recognise that achieving long-term sustainability and improving health outcomes for their populations requires a balanced and considered approach to risk-taking. The ICBs are committed to adopting a **mature** approach to risk, where potential long-term benefits justify short-term risks, provided that appropriate and robust controls are in place. The ICBs seek to **minimise** risks that could negatively affect patient safety, health outcomes, legal and statutory obligations, or the organisations' ability to demonstrate high standards of probity and accountability. While calculated risks may be accepted to achieve strategic objectives, particularly where innovation or improvement may be realised, such risks will only be taken when the level of control is sufficient to manage potential impacts effectively. Reputational risks are approached with caution, favouring delivery options that are more predictable and likely to achieve successful outcomes while safeguarding the ICBs' reputation for providing high-quality, cost-effective services. The ICBs' risk appetite is not static and will be reviewed regularly to ensure it remains appropriate to the changing environment and aligned with the strategic objectives of the organisations. This approach ensures a consistent, transparent, and accountable framework for decision-making across all areas of risk. 1 Good Governance Institute Risk Appetite for NHS Organisations – definition of '**mature**' is confident in setting high levels of risk appetite because controls, forward scanning and responsiveness systems are robust. 2 Good Governance Institute Risk Appetite for NHS Organisations – definition of '**minimal'** is preference for ultra-safe delivery options that have a low degree of inherent risk.

6.4 The statement is further supplemented with a risk appetite matrix, which will describe the organisation's approach to risk taking across five levels, from

averse (taking little or no risk) to significant (taking higher levels of risk). *NB: The development and implementation of the risk appetite narrative and matrix will be undertaken, in line with the clustering of ICBs and associated management of change processes.*

7. Risk Tolerance

7.1 Whilst risk appetite is about the pursuit of risk, risk tolerance is concerned with the level of risk that can be accepted (e.g. it is the minimum and maximum level of risk the ICBs are willing to accept reflective of the risk appetite statement above).

7.2 A target risk score range is applied to each of the ten risk domains: the target risk score being the acceptable level of risk able to be tolerated by the ICBs. A target risk score will be agreed for each risk and mitigating actions identified as appropriate. *NB: The development and implementation of a target risk score range, and the associated risk appetite matrix, will be deferred until late 2025/26, as highlighted at 6.4 above.*

7.3 It is recognised that some risks are unavoidable and will be out of the ability of the ICBs to mitigate to a tolerable level. Where this is the case, the focus will move to the controls in place to manage the risks and the contingencies planned should the risks materialise.

8. Strategic Risk Management

8.1 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 are owned by members of the Executive Management Team and are outlined within the **Board Assurance Framework (BAF)** of the ICBs.

8.2 The Assurance Framework provides the Boards with confidence 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 (*assurances*). It provides confidence and evidence to management that 'what needs to be happening is actually happening in practice.

8.3 The Assurance Framework also provides a structured approach for the Boards to gain assurance that key strategic risks are being effectively managed. It 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 Board in making informed decisions on the management of strategic risks (see Figure 3).

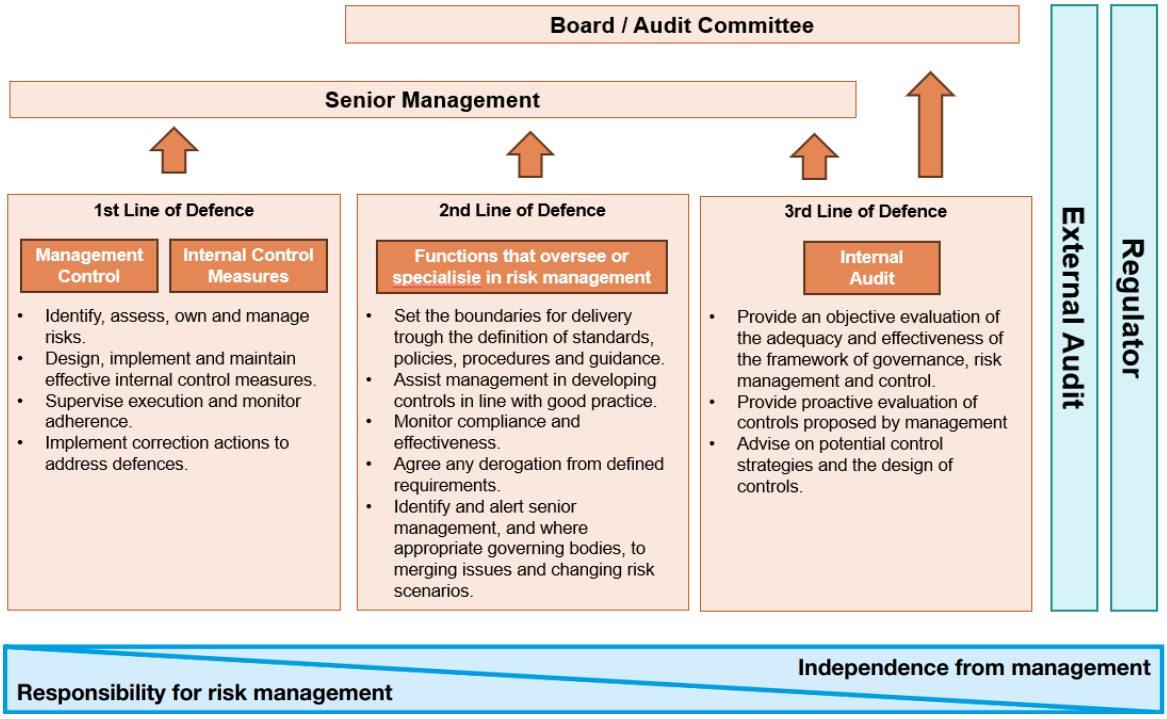


Figure 3 – Three lines of defence model [2]

8.4 The Assurance Framework plays a key role in informing the production of the 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.

8.5 The Assurance Framework 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. The purpose of this reporting is to enable committees to assess whether the assurances provided are robust and sufficient to give confidence that the strategic risks are being effectively managed, and to consider whether any 'gaps' in control or assurance require further action.

8.6 The Audit Committees will also have a key role in providing independent oversight of the effectiveness of the ICBs' strategic risk management processes. In line with the NHS Audit Committee Handbook, the role of the Audit Committees is not to manage the risks themselves, but to review the robustness and effectiveness of the systems and processes that support governance, risk management and internal control. This includes reviewing

[2] Adapted from HM Treasury Orange Book - More information is available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866117/6.6266_HMT_Orange_Book_Update_v6_WEB.PDF

whether the Assurance Framework, and the processes that support its development and maintenance, are robust and 'fit for purpose'.

8.7 The Audit Committees will discharge this responsibility through the bi-annual risk management updates included within their work programme. These updates will include an overview of strategic risk management processes and activity undertaken during the previous six-month period, presentation of the full Assurance Framework, and progress against mitigating action.

8.8 The Assurance Framework is reviewed and updated by Executive Directors throughout the year. This involves a review of the effectiveness of controls and what evidence (internal or external) is available to demonstrate that they are working as they should (assurances). Any gaps in controls or assurances will be highlighted at this point and actions identified.

8.9 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.

9. Operational Risk Register

9.1 Operational risks are 'live' risks the ICBs are currently facing which are by-products of day-to-day business delivery. They arise from definite events or circumstances and have the potential to impact negatively on the organisation and its objectives.

9.2 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**.

9.3 The Operational Risk Register is the central repository for all 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.

9.4 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 the action is completed by the specified due date.

10. Risk Logs

10.1 Risk logs are used to record operational risks at individual team, directorate and programme/project-level.

10.2 Risk logs provide a means to record operational risks at team, directorate, or programme/project level. Risks not significant enough for the Operational Risk Register can be captured in risk logs, aligned with team or programme objectives.

10.3 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. Their use and governance will be reviewed and strengthened once leadership and management arrangements are fully established.

10.4 Directorates may maintain their risk registers 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 organisation. 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.

11. Risk Management Processes

11.1 Risk management is a multi-faceted process of continuous improvement; the main elements are described below.

Risk Assessments

11.2 Risk assessments can be undertaken at the start of any activity and provide a helpful means of anticipating 'what could go wrong' and deciding on preventative actions. For specific risk assessments relating to workplace safety (e.g. use of display screen equipment, lone working, maternity, etc.), please refer to the health and safety policies.

11.3 Risks can be classified as sovereign ICB or joint risks. A sovereign ICB risk is one that impacts one ICB or affects the ICBs differently, meaning the cause, score, and required management may vary across Nottingham and

Nottinghamshire, Derby and Derbyshire, and Lincolnshire. These risks do not require uniform treatment or a single shared risk rating. By contrast, a joint risk is shared equally by all three ICBs, with the same cause, event, effect, management expectations, and risk score.

11.4 When identified risks are considered to have the potential to directly impact the achievement of the ICBs' priorities in their role as a strategic commissioner, these must be captured on the Operational Risk Register. The ICBs' Risk Management Team can offer support and guidance regarding risk escalation.

Objectives Framework

11.5 Objectives define the scope, context, and criteria or risk appetite that are used to identify and manage risks. If objectives are not established or are unclear, risks cannot be determined. Understanding the context is essential because risk management occurs within the framework of the objectives and activities of the ICBs. Further details are provided in the table below.

Objective	Oversight	Recording	Risk Management Role
Strategic	ICB Board	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 Board to support oversight and decision-making.
Operational	ICB Committees	Operational Risk Register	Managed by the Risk Management Team, operational risks relate to high-level corporate priorities and statutory functions. Risk owners provide updates and assurance on mitigation and control measures. Risks can be joint or sovereign ICB risks
Local	Teams (ICB Directorate / team / 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.

Table 3 – Risk log and operational risk register process

Risk Identification

11.6 Operational risks (those which require adding to the Operational Risk Register) may be identified through an assortment of means, including but not limited to:

- horizon-scanning for external and internal environmental factors that might threaten the achievement of priorities/objectives.
- formal risk assessment exercises.
- lessons learnt following an incident or a complaint.
- discussion at a meeting (e.g. a Board, Committee, Transformation Board or Team meeting).
- completion / review of a project business case or associated Equality Impact Assessment (EQIA).
- discussions with providers.
- external assessments.
- audits (internal / external) - any medium (or higher) risks identified within internal or external audit reports are captured within the Operational Risk Register.

11.7 Factors to be considered when identifying a risk include:

- tangible and intangible sources of risk.
- causes and events, threats and opportunities.
- vulnerabilities and capabilities.
- changes in the external and internal context.
- indicators of merging risks.
- the nature and value of assets and resources.
- consequences and their impact on objectives.
- limitations of knowledge and reliability of information.
- time related factors / likelihood of risk materialising over the next 12 to 18 months.

11.8 The committees of the ICBs all have a key role in the identification of risks in response to information presented to, and discussions held, at each meeting. A standing agenda item is included for every meeting to determine if there are any new risks that need to be considered for the Operational Risk Register.

11.9 Regular meetings are held with Executive Directors and members of the Senior Leadership Team to discuss new or evolving risks within their respective portfolios/teams.

Risk Articulation

11.10 It is good practice to articulate risks using the 'cause, event and effect framework' as outlined in the table below.

Risk element	Question	Consideration	Wording
CAUSE	**What will cause the risk to occur?)**	Operational risks arise from definite events or circumstances linked to the day-to-day running of the organisation.	Where the cause is known, use: "**As a result of**…". If the cause is uncertain, hypothetical, or conditional, it 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 ….**

Table 4 – Cause, event and effect framework

11.11 Training on writing risk statements is available from ICB's Risk Management Team, and you can find guidance documents along with Risk Log templates on the intranet page.

Risk Evaluation

11.12 Risks are evaluated by defining qualitative measures of impact and likelihood, as shown in the risk scoring matrix, shown in Appendix C, to determine the risk's RAG rating. Risk scores can be subjective; therefore, the scores will be subject to review by senior managers and/or the responsible committee.

11.13 When scoring the likelihood of a risk this should be assessed in the context of the likelihood of the risk materialising within the next 12 to 18 months.

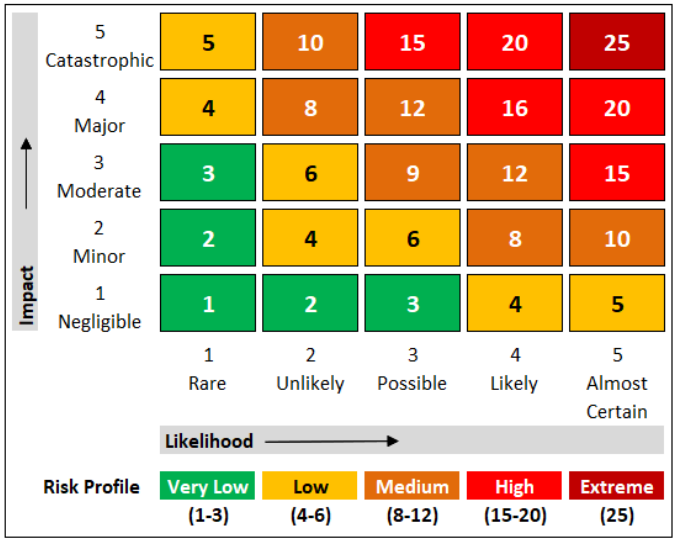


Figure 4 – 5x5 risk matrix

Risk Treatment

11.14 Risk treatment (also known as risk control) is the process of selecting and implementing measures to mitigate the risk to an acceptable level. Once risks have been evaluated, a decision should be made as to whether they need to be mitigated or managed through the application of controls (as described using the 'four T' risk treatment model 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.
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.

Table 5 – The 4T model (Risk treatment options)

11.15 Most operational risks should have the ability to reduce in impact and/or likelihood, and the relevant risk treatment must be performed to mitigate risks to an acceptable level in line with the risk appetite of the ICBs. High and

extreme operational risks (those scoring 15 or above) which are not deemed to be treatable will be highlighted to the Board as part of routine risk reporting.

11.16 For operational risks scored below 12, the responsible committee may agree that they can be tolerated. However, this would be subject to the committee being satisfied that no other actions can be undertaken.

Management and Reporting of Risks

11.17 The reporting of risk is the process of communicating real time risks. Monitoring risk is a continuous activity that results in the awareness of what is happening across the organisation. Reports should help the ICBs to:

- Monitor agreed risk response plans/actions.
- Track key milestones.
- Evaluate the impact of controls and actions on the risk.
- Identify new or unexpected risks.

11.18 Reports should focus on what has changed to allow Executives and other decision makers to make informed decisions.

11.19 Updates to risks are to be obtained via risk review meetings held with Risk Management Team and the risk owner / executive leads. The table below describes the minimum frequency for updates based on the level of risk.

11.20 The following categories of risk grading provide a high-level view of management and reporting requirements. Expected management of risks at each grading has been designed in consideration of the ICB's risk appetite.

- The **ICB Boards** will oversee all risks with an overall score of 15 or above (e.g. any high and/or extreme operational risks from the Operational Risk Register) at each of its meetings.
- **Committees** will oversee all risks relevant to their remit with an overall score of 8 or above (e.g. medium rating and upwards) from the Operational Risk Register at each of their meetings.
- The **Executive Management Team** (EMT) will receive all risks with an overall score of 8 or above (i.e. medium rating and upwards) from the Operational Risk Register on a quarterly basis to support effective matrix working, cross-portfolio visibility, and collective oversight of emerging themes.
- The **Audit Committees** will receive bi-annual risk management updates, including the full Operational Risk Register, which will enable any risk themes and trends to be reviewed; ensuring any multiple, similar risks of a minimal impact and likelihood are not ignored. This will support their duty

to provide the Boards with assurance on the robustness and effectiveness of the ICB's risk management processes.

	Very Low (1-3)	Low (4-6)	Medium (8-12)	High (15-20)	Extreme (25)
Level of risk	An acceptable level of risk that can be managed at directorate/ team/project level (recorded in Risk Logs).	An acceptable level of risk that can be managed at directorate/ team/project level (recorded in Risk Logs).	A generally acceptable level of risk. Corrective action needs to be taken.	An unacceptable level of risk which requires senior management attention and immediate corrective action.	An unacceptable level of risk which requires urgent executive and senior management attention and immediate corrective action.
Add to ICBs Operational Risk Register?	No.	No.	Yes, with quarterly progress updates (as a minimum).	Yes, with bi-monthly progress updates (as a minimum).	Yes, with monthly progress updates (as a minimum).
Oversight and scrutiny	Risk Logs to be reviewed in relevant Team/Directorates Meetings.	Risk Logs to be reviewed in relevant Team/Directorates Meetings.	ICB Operational Risk Registers (full or relevant extracts) to be reviewed by the relevant committee(s) at each meeting.	ICB Operational Risk Registers (full or relevant extracts) to be reviewed by the relevant committee(s) at each meeting. Detail of the high risks to be included in main body of risk report.	ICB Operational Risk Registers (full or relevant extracts) to be reviewed by the relevant committee(s) at each meeting. Detail of the extreme risks to be included in main body of risk report.
			All risks scored 8 and above to be shared with Executive Management Team on a quarterly basis.		

Table 6 – Reporting requirements

Archiving of Risks

11.21 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. The decision to archive a risk typically follows a review with the risk owner.

11.22 Risks may be archived when they meet one of the following triggers:

- **Cause updated or no longer valid:** If the original cause of the risk has changed significantly or is no longer applicable, the risk may be archived. This ensures that the register does not retain outdated entries that no longer reflect the current operating environment.
- **Risk no longer reflects current challenge:** Risks that were once relevant but no longer pose a threat due to changes in service delivery, policy, or external conditions are candidates for archiving. This helps maintain a focused and actionable risk profile.
- **Risk fully mitigated, tolerated (at target risk score) or transferred**: Where controls have been successfully implemented and assurance is strong, the risk may be closed and archived. In some cases, risks may be transferred to another team or escalated to a different register (e.g. operational risk register to local risk log when the risk no longer meets the threshold for reporting on the operational risk register).

11.23 The rationale for archiving is documented, including any changes to the cause, context, or objective.

11.24 Updates are reflected in the Operational Risk Register or local risk logs, and archived risks are retained for audit purposes. Archiving is not deletion. Archived risks remain accessible for reference and audit.

12. Fraud Risks

12.1 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.

12.2 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.

12.3 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.

13. Information Risks

13.1 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.

13.2 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, IG incident management arrangements and Data Protection Impact Assessments (DPIAs).

14. Performance Risks

14.1 The ICBs monitor performance against key delivery priorities via a separate, but parallel, process to the risk management arrangements.

14.2 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 organisation's overall risk profile and poor performance from a risk perspective will be referenced as necessary when reporting externally on risks (e.g., in the Annual Governance Statements).

14.3 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.

15. Management of Issues

15.1 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.

15.2 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.

15.3 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. The Risk Management Team can provide further support and guidance on the management of issues.

16. Equality and Diversity Statement

16.1 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.

16.2 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.

16.3 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.

16.4 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.

17. Communication, Monitoring and Review

17.1 The policy will be published and maintained in line with the Policy Management Framework.

17.2 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).

17.3 The Audit Committees will review the effectiveness of this policy, and its implementation, via bi-annual risk management update reports and targeted assurance reports.

17.4 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.

18. Confidentiality

18.1 Confidential information related to risk management will be handled in accordance with the organisation's Information Governance policies and relevant data protection legislation. Access to such information will be restricted to authorised individuals on a need-to-know basis and stored securely using approved systems.

18.2 All staff have a responsibility to maintain the confidentiality of sensitive information, including risk registers, incident reports, and assurance documentation. This responsibility is underpinned by the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Code of Conduct of the organisation.

18.3 Where risk-related information includes personal, clinical, or commercially sensitive data, additional safeguards, such as restricted access permissions, anonymisation, or redaction, will be applied. Any sharing of such information must be justified, proportionate, and documented in line with organisational procedures.

18.4 Where risks score 15 or above, are not deemed to be in the public interest, they will be clearly marked 'confidential' on the Operational Risk Register and reported to the Boards during the closed session. This should be for a time-limited period only and risk owners and committees are responsible for agreeing when confidentiality no longer applies.

19. Staff Training

19.1 The ICBs will proactively raise awareness of the risk management policy and provide ongoing support to committees and individuals to enable them to discharge their responsibilities effectively. Formal training sessions can be arranged through team meetings or other forums by contacting the designated risk management function.

19.2 The intranet will include accessible, bite-sized training materials on key risk management topics to support continuous learning.

19.3 Any individual with queries regarding the content of the policy or its relevance to their role should initially discuss these with their line manager. Further support can be sought from the Risk Management Team.

20. Interaction with other Policies

- Standard of Business Conduct Policy
- Health and Safety Policies

- Information Governance Policies

21. References

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

22. 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[3]	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)[4]	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)[5]	There are no actual or expected impacts on the characteristic of gender.	Not applicable.	Not applicable.	Not applicable.

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

[4] 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.

[5] 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 partnership[6]	There are no actual or expected impacts on the characteristic of marriage and civil partnership	Not applicable.	Not applicable.	Not applicable.
Pregnancy and maternity[7]	There are no actual or expected impacts on the characteristic of pregnancy and maternity Status.	Not applicable.	Not applicable.	Not applicable.
Race[8]	There are no actual or expected impacts on the characteristic of race.	Not applicable.	Not applicable.	Not applicable.

[6] 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'.

[7] 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.

[8] 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 belief[9]	There are no actual or expected impacts on the characteristic of religion or belief	Not applicable.	Not applicable.	Not applicable.
Sex[10]	There are no actual or expected impacts on the characteristic of sex.	Not applicable.	Not applicable.	Not applicable.
Sexual orientation[11]	There are no actual or expected impacts on the characteristic of sexual orientation.	Not applicable.	Not applicable.	Not applicable.

[9] 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.

[10] A man or a woman.

[11] 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.
Carers[12]	There are no actual or expected impacts on the characteristic of carers.	Not applicable.	Not applicable.	Not applicable.

[12] 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 controls are working effectively. Assurance can be internal (e.g. committee oversight) or external (e.g. internal audit reports).
Assurance Framework	A (Board) Assurance Framework is a structured means of identifying and mapping the main sources of assurance in an organisation, and co-ordinating them to best effect. The Assurance Framework document is the key source of evidence that links an organisation's strategic objectives to risk, controls and assurances and the main tool a Board should use in discharging its responsibility for internal control.[13]
Controls	The measures in place to control risks and reduce the impact or likelihood of them occurring. • Internal controls include policies, procedures, practices, behaviours and organisations structures to manage risks and achieve objectives. • External controls may include oversight by regulatory bodies, external audits, independent reviews, or accreditation processes that provide additional assurance beyond the organisation itself.
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.

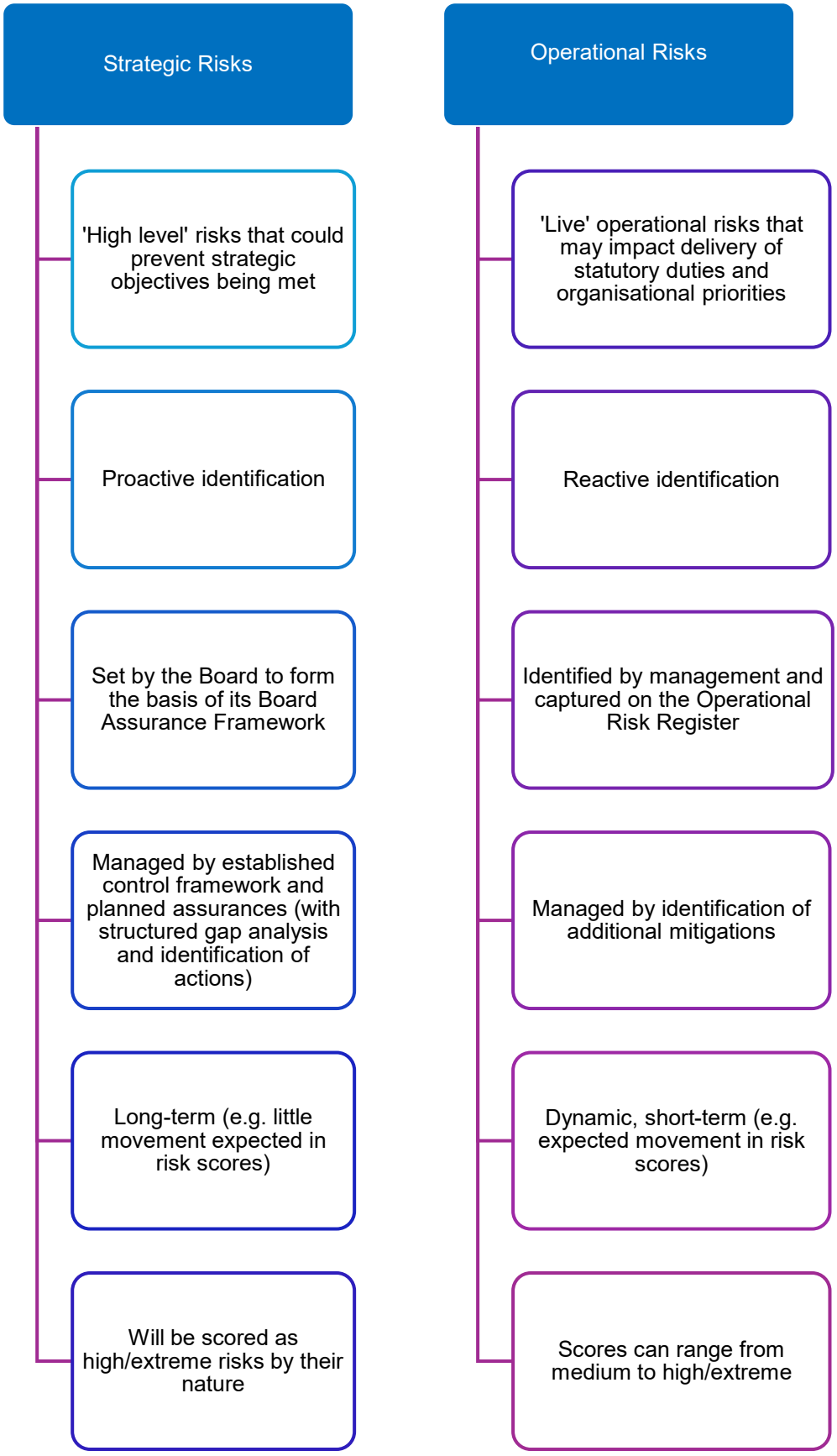
[13] NHS Governance, Fourth Edition 2017 (HfMA)

Term	Definition
Integrated Care Board (ICB)	An ICB is the statutory NHS organisation within the ICS which holds responsibility for NHS functions and budgets.
Integrated Care Partnership (ICP)	An ICP is a statutory committee which brings together all ICS system partners to produce a health and care strategy.
Integrated Care System (ICS)	An ICS is a partnership that brings together providers and commissioners of NHS services across a geographical area with local authorities and other local partners to collectively plan health and care services to meet the needs of the population.
Joint Risk	A **joint risk** is a risk shared equally by all three ICBs, with the same cause, event, effect, management expectations, and risk score. a) *Cause:* The risk originates from a common factor affecting all three statutory ICBs. b) *Event:* The risk occurring would prevent the three ICBs from achieving joint priorities or objectives. c) *Effect:* If the risk materialises, all three ICBs would be affected equitably, with no single ICB disproportionately impacted. d) *Mitigation:* Managing the risk requires coordinated action across all three ICBs. e) *Risk score:* The risk is recorded at the same likelihood and impact across all three ICBs.
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.
Operational risks	These risks are by-products of day-to-day business delivery. They arise from definite events or circumstances and have the

Term	Definition
	potential to impact negatively on an organisation and its priorities/objectives. Operational risks include corporate risks (those which directly relate to the priorities/objectives/duties of an organisation).
Place-Based Partnerships (PBPs)	Place-based partnerships are collaborative arrangements formed by the organisations responsible for arranging and delivering health and care services in a locality or community.
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 total amount and type of risk that an organisation is willing to take to meet its strategic objectives. A range of appetites exist for different risk domains, and these may change over time.
Risk assessment	An examination of the possible risks that could occur during an activity.
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	How risks are going to be controlled to reduce the impact on an organisation and/or likelihood of their occurrence.
Risk profile	The nature and level of the threats faced by an organisation.
Risk treatment	The process of selecting and implementing suitable measures to modify the risk.
Sovereign ICB risk	A sovereign ICB risk is one that impacts one ICB or affects the ICBs differently, meaning the cause, score, and required management may vary across Nottingham and Nottinghamshire, Derby and Derbyshire, and Lincolnshire. These risks do not require uniform treatment or a single shared risk rating.
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

Term	Definition
	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	Potential, significant risks that are pro-actively identified and threaten the achievement of strategic objectives.
Target risk score	The numerical level of risk exposure that an organisation is prepared to tolerate following completion of all the 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: Characteristics of Strategic and Operational Risks



Appendix C: 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

Risk Domain	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
Health Inequalities Risks that may result in unfair or unavoidable differences in health across different groups within society.	• Minor risk to individuals or communities, with limited impact on health inequalities or disparities.	• Moderate risk which may lead to noticeable effects on certain populations, leading to moderate disparities in access to healthcare services or health outcomes across different groups within society.	• Serious risk which may significantly affect certain populations, resulting in substantial disparities in health status, access to care, or health-related quality of life among affected groups.	• Major risk which may have a profound impact on certain populations, exacerbating disparities in morbidity, mortality, and overall well-being, with far-reaching consequences for affected communities.	• Catastrophic threats to individuals or populations, leading to widespread and severe health crises, overwhelming healthcare systems, and causing significant loss of life and societal disruption.

Risk Domain	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
Health Outcomes Risks that may result in poor or worsening health outcomes for individuals or populations.	• Health outcomes for individuals are minimally affected, with only minor variations to care or health status observed.	• Moderate risk which may lead to noticeable effects on health outcomes, leading to moderate disparities in disease management, treatment outcomes, or overall well-being.	• Serious risk which may lead to significant impacts to health outcomes, resulting in disease progression, functional impairment, and health-related quality of life.	• Major risk which may lead to profound impact on health outcomes, exacerbating disparities in morbidity, mortality, and life expectancy, with significant implications for health trajectories and long-term prognoses.	• Catastrophic threats to health outcomes, leading to severe and potentially life-threatening consequences, overwhelming individuals' ability to cope, and causing significant harm to their physical and mental well-being.
Legal Risks that may result in successful legal challenge and/or non-compliance with regulatory requirements. [May include, but not limited to, risks linked to statutory duties, inspections, Information Governance, general governance / probity, compliance, safeguarding and Emergency Preparedness, Resilience and Response (EPRR)]	• No impact 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.

Risk Domain	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
Patient Safety Risks that may result in unintended or unexpected harm occurring. [May include, but not limited to, risks associated with harm, quality, medicines and pharmacy and patient Experience]	• Minor adverse events or safety incidents identified, and appropriate safeguards in place to mitigate any risks. • Peripheral element of treatment or service suboptimal. • Informal complaint/ Inquiry.	• Moderate level of safety incidents or adverse events occurring, but generally manageable with existing protocols and interventions. • 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.	• Serious safety concerns or adverse events occurring sporadically, indicating the need for heightened vigilance and targeted interventions to address underlying factors contributing to patient safety risks. • Treatment or service has significantly reduced effectiveness. • Formal complaint stage 2. • 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.	• Frequent safety incidents or adverse events occurring with major impacts, indicating systemic weaknesses in care delivery and patient safety protocols requiring urgent attention and comprehensive improvement efforts. • Non-compliance with national standards with significant risk to patients if unresolved. • Multiple complaints/ independent review. • Low performance rating. • Critical report.	• The risk of harm to patients is severe, with widespread and persistent safety failures posing a significant threat to patient well-being, necessitating immediate and decisive action to prevent further harm and restore trust in the healthcare system. • 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.

Risk Domain	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
People Risks that may result in damage to staff morale, well-being and/or adversely impact workforce collaboration and integration. [May include, but not limited to, risks linked to human resource issues, organisational development, skills mix and staff experience]	• 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 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 training.	• Non-delivery of key objective / service due to lack of staff. • Ongoing unsafe staffing levels or competence. • Loss of several key staff. • Staff unable to attend mandatory training on ongoing basis.
Reputation Risks that may result in damage to reputation, poor experience and/or destruction of trust and relations. [May include, but not limited to, risks linked to adverse publicity and engagement]	• Rumours. • Potential for public concern.	• Local media coverage – short-term reduction in public confidence. • Elements of public expectation not being met.	• Local media coverage – long-term reduction in public confidence.	• National media coverage with <3 days service well below reasonable public expectation.	• National media coverage with >3 days service well below reasonable public expectation. • MP concerned (questions in the House). • Total loss of public confidence.

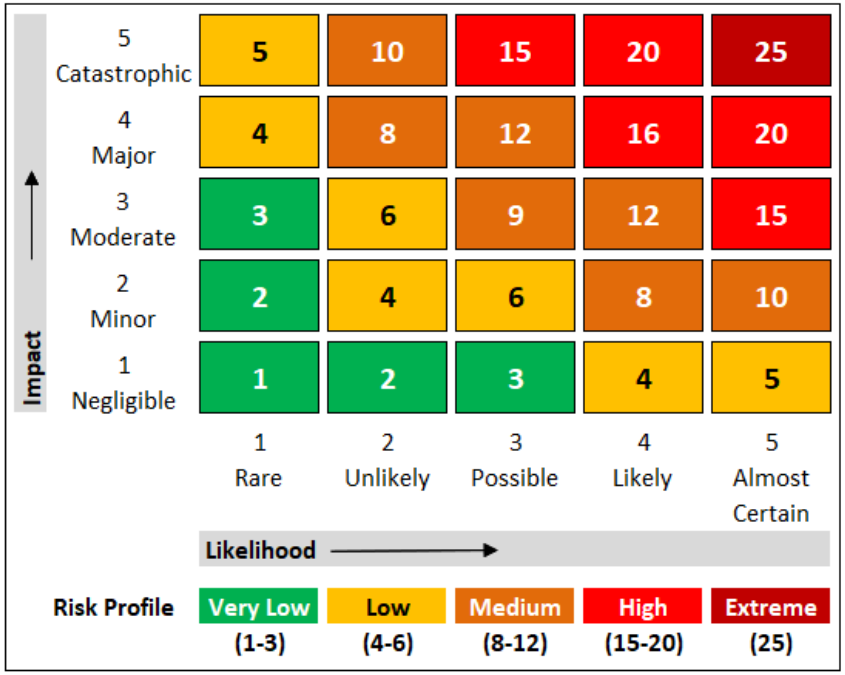
Risk Domain	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
Resources Risks that may result in the organisation operating outside its resource or capital allocations, poor productivity, inefficiencies, or no return on investment. [May include, but not limited to, risks linked to workforce, finance, procurement and claims]	• Small loss. • Risk of claim remote.	• Loss of 0.1–0.25 per cent of budget. • Claim less than £10,000.	• Loss of 0.25–0.5 per cent of budget. • Claim(s) between £10,000 and £100,000.	• Uncertain delivery of key objective. • Loss of 0.5–1.0 per cent of budget. • Purchasers failing to pay on time. • Claim(s) between £100,000 and £1 million.	• Non-delivery of key objective • Loss of >1 per cent of budget. • Failure to meet specification. • Slippage. • Loss of contract/ payment by results. • Claim(s) >£1 million.
Social and Economic Development Risks relating to decisions or events which may have favourable social, ethical and/or environmental outcomes.	• Minimal or no impact on the environment.	• Minor impact on environment.	• Moderate impact on environment.	• Major impact on environment.	• Catastrophic impact on environment.
Strategic Commissioning Risks associated with potential threats or uncertainties that may impact the ICB's ability to plan, procure, and deliver services that meet population needs, improve outcomes, and ensure value for money. Strategic commissioning risks emerge when this process is	• Negligible disruption to commissioning activities with no impact on service delivery or population outcomes. • Temporary delay in pathway design or contract negotiation.	• Minor impact on commissioning capacity or service planning. • Delays in procurement or pathway redesign affecting a small population group.	• Moderate disruption to commissioning functions. • Inability to deliver planned service changes or meet transformation targets.	• Major failure in commissioning processes. • Inability to deliver key services or meet statutory duties. • Major impact on population health outcomes, equity, or	• Catastrophic failure / systemic breakdown in commissioning capability. • Widespread service failure or collapse of strategic programmes. • Catastrophic impact on population health,

Risk Domain	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
disrupted or compromised. These risks may affect the ICB's ability to ensure person-centred, equitable, and sustainable care.		• Minor misalignment with strategic objectives.	• Moderate impact on access, equity, or quality of care.	financial sustainability.	legal compliance, and organisational viability.
Strategy and Operations Risks associated with identifying and pursuing strategies/plans (including risks associated with the establishment of innovative systems and processes to deliver the strategies/plans), which could lead to improvements, opportunities for growth or may contribute positively to the achievement of aims and objectives. [May include, but not limited to, risks linked to capacity, demand, Primary Care, service/ business interruption, digital, projects, planning, delivery, commissioning, partnership working and transformation]	• Day to day operational challenges. • Loss/ interruption of >1 hour. • Insignificant cost increase / schedule slippage. • Key 'political' target is being achieved and impact prevents improvement.	• Temporary restriction to service delivery with limited impact on stakeholder confidence. • Loss/ interruption of >8 hours. • <5 per cent over project budget. • Schedule slippage. • Key 'political' target is being achieved but impact reduces performance marginally below target in the near future or performance currently on target, but there is no agreed plan to meet	• Short term failure to deliver key objectives with temporary adverse local publicity. • Loss/ interruption of >1 day. • 5–10 per cent over project budget. • Schedule slippage. • Key 'political' goal is marginally below target or is soon projected to deteriorate beyond acceptable limits or there is an agreed plan, but it does not yet meet the rising target.	• Medium term failure to deliver key objectives with ongoing adverse publicity or negative impact on stakeholder confidence. • Loss/ interruption of >1 week. • Non-compliance with national 10–25 per cent over project budget. • Schedule slippage. • Key 'political' target not being achieved, and impact prevents improvement, or substantial decline in performance trend.	• Continued failure to deliver key objectives with long term adverse publicity or fundamental loss of stakeholder confidence. • Permanent loss of service or facility. • Incident leading >25 per cent over project budget. • Schedule slippage. • Key objectives not met. • Key 'political' target is not being achieved and the impact further deteriorates the position.

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



Appendix D: Risk Review Checklist

Element	Guidance	Findings (with prompts)
Risk Description	Think about the reader when formulating the description, a clear and concise description helps the reader to understand what the risk is. A description includes: **CAUSE:** 'As a result of ….' (what will cause the risk to occur?) or if the cause is uncertain, hypothetical, or conditional, it may be appropriate to use: 'If ….' **EVENT: '**There is a risk ….' (what can go wrong?) **EFFECT: '**Which may lead to ….' (what will be the consequence/effect if the risk were to materialise?)	Q: Does the description follow the above format?
Objective	Objectives define the purpose and context within which risks are identified, assessed, and managed. They should be clearly stated and aligned with one of the three recognised levels within the organisation: **strategic**, **corporate (operational)**, or **local**. Each risk must be linked to a relevant priority/objective to ensure it is meaningful and appropriately contextualised. When recording a risk, ensure the associated objective is specific, current, and reflects the organisational level at which the risk is being managed.	Q: Is the priority/objective clearly stated and relevant to the risk? Q: Is the priority/objective aligned with the ICB's statutory functions, team goals, or strategic priorities? Q: Is the priority/objective specific enough to guide the identification and evaluation of the risk?
Controls	A control is a process, policy, device, or action that acts to minimise risk and describes what is in place to reduce or manage the risk. **PLANNED ACTIONS ARE NOT CONTROLS**	Q: Are any controls identified? Q: Are your controls up to date?
Gaps in Control	It is essential you consider what controls may be missing (not recorded) that would help to manage the risk.	Q: For all instances of negative assurance, do you have a corresponding ACTION to close the gap in control.
Actions	An action will exist where you have a gap in control and completion of actions should provide assurance, strengthen existing controls, or add new controls. **All gaps in control and gaps in assurance require an ACTION to close the gap.**	Q: Are you confident the actions will be delivered and on time? Q: Is the action owner the right action owner? Q: Is the action owner aware they have this action assigned to them?

Initial Risk Score	This was the score evaluated when the risk was first recorded.	Q: Are you confident the initial risk score was reflective of the risk when recorded?
Current Risk Score	It is essential to consider the likelihood of the impact being realised (see risk description - **EFFECT:** '*Which may lead to ….*') considering the existing controls and assurances.	Q: Does the current score consider all the controls and assurances? Q: Have you used the risk scoring guidance? Q: Have you evaluated the evidence to quantify the risk?
Likelihood Score	Score your risk on the potential of the risk occurring in the next 12 - 18 months.	Q: Have you assessed the probability of this risk materialising within the next 12-18 months?
Impact Score	Score your risk on the impact the risk materialising would have on the priority/objective the risk is being scored against.	Q: Have you assessed the potential impact on the priority/objective?