NHS
Nottingham and Nottinghamshire
Integrated Care Board

Risk Management Policy

May 2024 – September 2026

CONTROL RECORD	
Title	Risk Management Policy
Reference Number	GOV-001
Version	2.3
Status	Final
Author	Director of Corporate Affairs Head of Corporate Assurance
Sponsor	Director of Nursing
Team	Corporate Assurance
Amendments	Update to the definition of a system risk - updates to section 4 and addition of paragraph 13.4
Purpose	The purpose of this policy is to ensure that robust arrangements for risk management are embedded across the ICB and to ensure an agreed risk appetite and approach to risk tolerance.
Superseded Documents	Risk Management Policy v2.2
Audience	All employees and appointees of the Nottingham and Nottinghamshire ICB and any individuals working within the ICB in a temporary capacity.
Consulted with	None
Equality Impact Assessment	Complete (see Appendix F)
Approving Body	Audit and Risk Committee
Date approved	May 2024
Date of Issue	May 2024
Review Date	September 2026

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. NHS Nottingham and Nottinghamshire Integrated Care Board (ICB)'s policies can be made available on request in a range of languages, large print, Braille, audio, electronic and other accessible formats from the Communications Team at nnicb-nn.comms@nhs.net

Contents

1	Introduction	Page 4
2	Purpose	Page 6
3	Scope	Page 6
4	Definition of Risk Management Terms	Page 6
5	Roles and Responsibilities	Page 10
6	Risk Appetite	Page 12
7	Risk Tolerance	Page 13
8	Strategic Risk Management	Page 15
9	Operational Risk Management	Page 15
10	Risk Logs	Page 16
11	Risk Management Processes	Page 17
12	Performance Risks	Page 20
13	Interface with ICS Partner Risks (System Risk Management)	Page 20
14	Management of Issues	Page 21
15	Fraud Risk Assessment	Page 22
16	Confidentiality	Page 22
17	Equality and Diversity Statement	Page 22
18	Communication, Monitoring and Review	Page 23
19	Staff Training	Page 23
20	References	Page 24

	Appendix A: Characteristics of Strategic and Operational Risks	Page 25
	Appendix B: Risk Identification Guidance	Page 26
	Appendix C: Risk Scoring Matrix	Page 27
	Appendix D: Risk Review Checklist	Page 34
	Appendix E: Three Lines of Defence Model	Page 35
	Appendix F: Equality Impact Assessment	Page 38

1. Introduction

1.1. This policy applies to NHS Nottingham and Nottinghamshire Integrated Care Board, hereafter referred to as 'the ICB.'

1.2. The ICB is a statutory organisation which forms part of the wider Nottingham and Nottinghamshire Integrated Care System (ICS). Whilst this policy outlines risk management arrangements for the statutory ICB, it is important that these arrangements work in partnership with other key parts of the ICS family.

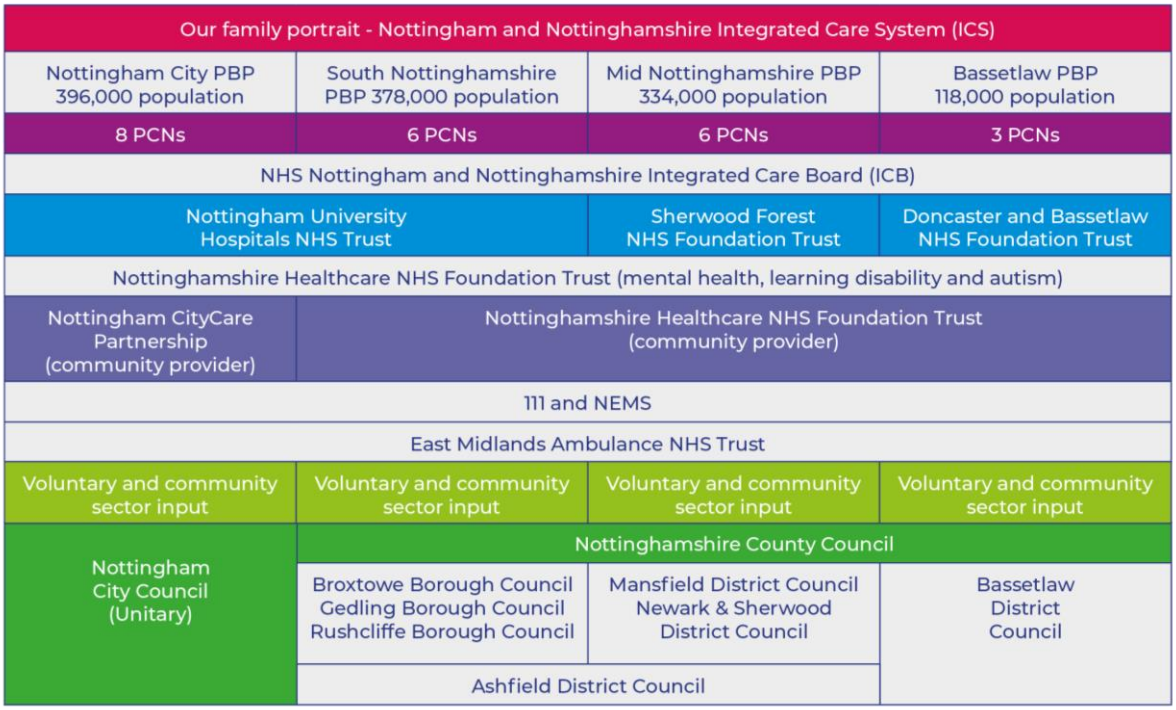


Figure 1 – Key parts of the Integrated Care System (ICS)

1.3. The management of risk across organisational boundaries, e.g. system risk management, 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. Risk should be an important feature within the different parts of the system architecture e.g. Place Based Partnerships (PBPs), Provider Collaboratives and health and care providers. Partnership working can often lead to potential issues regarding risk ownership and accountability. As such, it is important that there are clear inter-relationships regarding the management and ownership of risks between these different elements.

1.5. The ICB recognises that risk management is an essential business activity that underpins the achievement of its 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 ICB's activities and 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.
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] ISO 31000 helps organisations develop a risk management strategy 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

1.8. This policy demonstrates the ICB's commitment to its total risk management function. It sets out the ICB's risk architecture (roles, responsibilities, communication and reporting arrangements) and describes how risk management is integrated into governance arrangements, key business activities and culture, both internally within the ICB and with health and care system partners.

2. Purpose

2.1. This policy describes the ICB's approach to the management of strategic and operational risks across the statutory organisation. It also references how risk arrangements within the ICB will interface with key elements of the Integrated Care System (ICS) and ICS system partners (e.g. system risk management arrangements).

2.2. The purpose of this guidance is to encourage a culture where risk management is viewed as an essential process of the ICB's activities. It provides assurance to the public, patients and partner organisations that the ICB is committed to managing risk appropriately.

3. Scope

3.1 This policy applies to all employees and appointees of the ICB and any individuals working within the ICB in a temporary capacity (hereafter referred to as 'individuals').

4. Definition of Risk Management Terms

4.1 The following terms are used throughout this document:

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 the organisation's strategic objectives to risk, controls and assurances and the main tool a Board should use in discharging its responsibility for internal control.[2]
Controls	The measures in place to control risks and reduce the impact or likelihood of them occurring.

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

Term	Definition
Integrated Care Board (ICB)	The ICB is the statutory NHS organisation within the ICS which holds responsibility for NHS functions and budgets.
Integrated Care Partnership (ICP)	The ICP is a statutory committee which brings together all ICS system partners to produce a health and care strategy.
Integrated Care System (ICS)	The 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.
Initial risk score	The numerical assessment of the risk (impact vs. likelihood) prior to considering any additional mitigating controls and/or actions.
Corporate risks	Operational risks which relate to the delivery of the ICB's statutory duties, functions and/or objectives.
Current (or Residual) risk score	The numerical assessment of the risk (impact vs. likelihood) after taking into consideration any mitigating controls and/or actions.
Operational Risk Register (ORR)	A tool for recording identified 'live' operational risks and monitoring actions against them. The ORR captures both ICB 'corporate' operational risks and system operational risks.
Operational risk management	Risk management processes which focus on 'live' operational risks which the 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 potential to impact negatively on the organisation and its objectives. Operational risks include corporate risks (those which directly relate to the ICB's objectives/duties) and system risks (those which relate to the delivery of system priorities).
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.

Term	Definition
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 (the ICB) 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; transformation programme risk logs.
Risk management	The arrangements and activities in place that direct and control the organisation regarding risk.
Risk mitigation	How risks are going to be controlled to reduce the impact on the 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.
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 the ICB'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.

Term	Definition
System risk management	The collective identification, assessment and mitigation of operational risks where improved outcomes can be achieved by system partners working together through shared accountability arrangements. System risk management does not replace risk management infrastructures in place within each ICS system partner; system risk management arrangements complement organisational risk management arrangements; they do not replace them.
System risks	The ICS Risk Management Network has determined that a system risk should meet one (or more) of the following criteria: • An operational risk that originates from sources that involve multiple partners in the system. • An operational risk that leads to a single event / series of events that may compromise the achievement of system aims and objectives. • An operational risk that, if it occurred, would have medium or high impact consequences on multiple partners within the system. • An operational risk that, if it occurred, would require more than one system partner to manage.
Target risk score	The numerical level of risk exposure that the ICB 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. Individuals in the first line own and manage risk directly. See Appendix E.

Table 2 – Key definitions

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

Figure 2 – The two types of risks

5. Roles and Responsibilities

Roles	Responsibilities
Forums	
Integrated Care Board	The Board has overall accountability for risk management and, as such, needs to be satisfied that appropriate arrangements are in place and that internal control systems are functioning effectively. The Board determines the ICB's risk appetite and risk tolerance levels and is also responsible for establishing the risk culture.
Audit and Risk Committee	The Audit and Risk Committee provides the Board with assurance on the effectiveness of the Board Assurance Framework and the robustness of the ICB's operational risk management processes. The Committee's role is not to 'manage risks' but to ensure that the approach to risks is effective and meaningful. In particular, the Committee supports the Board by obtaining assurances that controls are working as they should, seeking assurance about the underlying data upon which assurances are based and challenging 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.
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.
Director of Nursing	The Director of Nursing is the executive lead for corporate governance and risk and assurance systems across the ICB. This includes promoting the ICB's risk culture within the Executive Team, wider directorates and across system partners.
ICB Non-Executive and Partner Members	As members of the Board and committees, Non-Executive Members will ensure an impartial approach to the ICB's risk management activities and should satisfy themselves that systems of risk management are robust and defensible.

Roles	Responsibilities
Director of Corporate Affairs (supported by the Corporate Assurance Team)	The Director of Corporate Affairs leads on the implementation of corporate governance and risk and assurance systems across the ICB. This includes the development, implementation and co-ordination of the ICB's risk management activities and provision of training and advice in relation to all aspects of this policy.
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 ICB's risk culture and ensuring all senior leaders, within their respective Directorates, have a robust understanding of the organisation's risk management arrangements.
Senior Leadership Team (including Associate/Deputy Directors)	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 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 ICB's risk appetite statement; and • Staff are suitably trained in relation to risk management.
Senior Information Risk Owner (SIRO)	The SIRO takes ownership of the ICB's information risks and acts as advocate for information risk on the Integrated Care Board.
Risk Owners	Risk owners are responsible for ensuring robust mitigating actions are identified and implemented for their assigned risks. In relation to system risks, risk 'owners' are responsible for co-ordinating mitigating actions across relevant system partners.
Individuals	All individuals are responsible for complying with the arrangements set out within this policy and are expected to: • Routinely consider risks when developing business cases, commencing procurements or any other activity which could be impacted by unexpected events (undertaking specific risk assessments as necessary). • Ensure that any operational risks they are aware of are captured on the Operational Risk Register or Directorate/Team Risk Logs as appropriate.

Table 3 – Roles and responsibilities

***** Risks cannot always be addressed in isolation from each other. Risks may have different facets (e.g. finance and quality) and management actions may impact on different areas of the ICB. Where this is the case, a pragmatic approach will be taken, and risks may be scrutinised by more than one committee.

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 ICB Board has agreed to the following narrative risk appetite statement:

Nottingham and Nottinghamshire ICB's Risk Appetite Statement
The Board of NHS Nottingham and Nottinghamshire Integrated Care Board (ICB) recognises that long-term sustainability and the ability to improve quality and health outcomes for our population, depends on the achievement of our strategic objectives and that this will involve a willingness to take and accept risks. It may also involve taking risks with our strategic partners in order to ensure successful integration and better health services for the people of Nottingham and Nottinghamshire. The ICB will endeavour to adopt a **mature** approach to risk-taking where the long-term benefits could outweigh any short-term losses, in particular when working with strategic partners across the Nottingham and Nottinghamshire system. However, such risks will be considered in the context of the current environment in line with the ICB's risk tolerance and where assurance is provided that appropriate controls are in place, and these are robust and defensible. The ICB will seek to **minimise** risks that could impact negatively on the health outcomes and safety of patients or in meeting the legal requirements and statutory obligations of the ICB. We will also seek to **minimise** any risks that may impact on our ability to demonstrate high standards of probity and accountability. In view of the changing landscape, the ICB's risk appetite will not necessarily remain static. The ICB's Board will have the freedom to vary the amount of risk it is prepared to take, depending on the circumstances at the time. It is expected that the levels of risk the ICB is willing to accept are subject to regular review. 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.

Figure 3 – Risk appetite statement

6.4. The above is further supplemented with an ICB risk appetite matrix. This matrix describes five levels of risk appetite the organisation is willing to take; from averse (taking little or no risk) to significant (taking lots of risk).

Risk Appetite Level	Description	Risk Tolerance (i.e. 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 business 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**

Table 4 – Risk appetite levels, description and tolerance

*It should be noted that there is some crossover on the risk tolerance ranges as the scores are dependent on whether the impact or likelihood score is higher (i.e. I1 x L5) is averse vs. (I5 x L1) is cautious.

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 ICB is willing to accept reflective of the risk appetite statement above).

7.2. The below table outlines the target risk score range across eight risk domains; the target risk score being the acceptable level of risk that is able to be tolerated by the ICB. A target risk score will be agreed for each risk and mitigating actions identified as appropriate.

Risk domain	Risk appetite level	Target Risk Score Range	1-5	4-10	8-15	15-20	25
Health Inequalities: Risks that may result in unfair or unavoidable differences in health across different groups within society.	*Cautious*	*4 - 10*		⟷			
Health Outcomes: Risks that may result in poor or worsening health outcomes for individuals or populations.	*Cautious*	*4 - 10*		⟷			
Legal: Risks that may result in successful legal challenge and/or non-compliance with regulatory requirements.	*Averse*	*1 - 5*	⟷				
Patient Safety: Risks that may result in unintended or unexpected harm occurring.	*Averse*	*1 - 5*	⟷				
People: Risks that may result in damage to staff morale, well-being and/or adversely impact workforce collaboration and integration.	*Cautious*	*4 - 10*		⟷			
Reputation: Risks that may result in damage to reputation, poor experience and/or destruction of trust and relations.	*Cautious*	*4 - 10*		⟷			
Resources (i.e., finance / workforce): Risks that may result in the organisation, or system, operating outside its resource or capital allocations, poor productivity, inefficiencies, or no return on investment.	*Cautious*	*4 - 10*		⟷			
Social and Economic Development: Risks relating to decisions or events which may have favourable social, ethical and/or environmental outcomes.	*Cautious*	*4 - 10*		⟷			
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.	*Open / Eager*	*8 – 15 / 15 – 20*			⟷	⟷	

Table 5 – Risk domains, appetite level and target risk score range

7.3. It is recognised that some risks are unavoidable and will be out of the ICB's ability 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 ICB's **Board Assurance Framework (BAF).** The ICB will work with system partners across the ICS to ensure alignment of strategic risks, where appropriate and/or relevant to do so.

8.2. The Assurance Framework provides the Board with confidence that the ICB has identified its strategic risks and has robust systems, policies and processes in place (*controls*) that are effective and driving the delivery of their objectives (*assurances*). Sources of assurance incorporate the three lines of defence, as referenced in Appendix E. It provides confidence and evidence to management that '*what needs to be happening is actually happening in practice.'*

8.3. The Assurance Framework plays a key role in informing the production of the Annual Governance Statement and is the main tool that the Board should use in discharging overall responsibility for ensuring that an effective system of internal control is in place.

8.4. The Board approves the strategic risks (opening position) during the first quarter of the financial year, following agreement of the strategic objectives. The Board reviews the fully populated Assurance Framework bi-annually to affirm that sufficient levels of controls and assurances are in place in relation to the organisation's strategic risks.

8.5. The Assurance Framework is reviewed and updated by Executive Directors and the Head of Corporate Assurance Team 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.

8.6. The Audit and Risk Committee receives a rolling programme of targeted assurance reports which, over a 12-month period, covers all the ICB's strategic objectives (the full Assurance Framework). This enables a focussed review on specific sections of the Assurance Framework and allows for robust discussions on the actions in place to remedy any identified gaps in controls and assurances.

9. Operational Risk Management

9.1. Operational risks are 'live' risks the organisation is 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 ICB's **Operational Risk Register**.

9.3. The Operational Risk Register is the central repository for all ICB operational risks. Whilst risks will feature across several of the ICB's processes, it is important that these are captured centrally to provide a comprehensive log of prioritised risks that accurately reflects the ICB's risk profile.

9.4. The Operational Risk Register reflects operational risks relevant to the ICB as a corporate body (operational risks associated with delivery of the ICB's statutory duties) and operational risks associated with the delivery of system objectives/priorities (operational risks associated with the delivery of transformation programmes, for example).

9.5. 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 chosen 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 should be used to record operational risks which are not considered significant enough to be captured on the ICB's Operational Risk Register. Such risks are identified in line with the Place/programme/team/Directorate-level objectives which have been set. A Risk Log template is in place and accessible from the Corporate Assurance Team by email: nnicb-nn.corporateassurance2@nhs.net

10.3. Whilst a fundamental part of the ICB's risk management arrangements (ensuring and demonstrating that project-level and/or team-level risks are being actively identified and managed), risk logs do not require the same level of management as the Operational Risk Register or Assurance Framework and, therefore, the oversight and scrutiny for team level risk logs is the responsibility of the relevant senior manager(s) (e.g., member of the Senior Leadership Team) to establish this. It may, for example include routine consideration of Risk Logs at project and/or team meetings.

10.4. When risks are added to a risk log, consideration should be given to the key elements of the risk. The risk review checklist can be used to support this exercise. See Appendix D for details.

10.5. When identified risks are considered to have the potential to directly impact the achievement of ICB objectives, these must be escalated from risk logs and captured on the Operational Risk Register. The Head of Corporate Assurance and Operational Risk Manager can offer support and guidance regarding risk escalation.

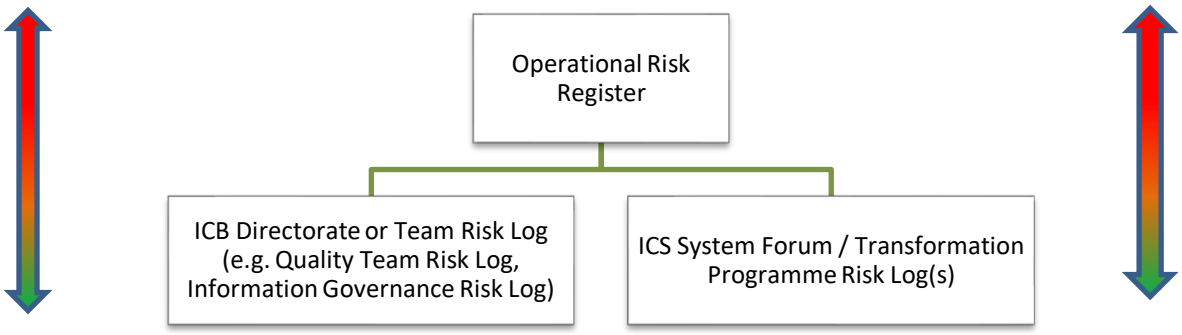


Figure 4 – Risk log and operational risk register process

11. Risk Management Processes

Risk Assessments

11.1. 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 ICB's health and safety policies.

Risk Identification

11.2. Operational risks (those which require adding to the Operational Risk Register) may be identified through an assortment of means, for example by risk assessments, external assessments, audits, complaints, during meetings and through horizon-scanning. For example, any medium (or higher) risks identified within internal or external audit reports are captured within the Operational Risk Register.

11.3. The ICB, its Committees, and system forums, 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.

11.4. Regular meetings are held with Executive Directors, members of the Senior Leadership Team, as well as operational, clinical and risk leads within ICS system partners, to discuss new or evolving risks within their respective portfolios/teams. This may include corporate or system risks.

Risk Evaluation

11.5. 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.

Figure 5 – 5x5 risk matrix

11.6. Risk Treatment

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 6 – Treatment options

11.7. 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 ICB's risk appetite. 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.

Management and Reporting of Risks

11.8. 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** will oversee all risks with an overall score of 15+ (e.g. any high and/or extreme operational risks from the Operational Risk Register; both ICB and system risks) at each of its meetings.
- **Committees** will oversee all risks relevant to their remit with an overall score of 6+ (e.g. medium rating and upwards; both ICB and system risks) from the Operational Risk Register at each of their meetings.
- **System (ICS) forums** will receive reports relating to system risks that fall within their remit to enable them in their duties to oversee the identification and management of system operational risks at each of their meetings.
- The **Audit and Risk Committee** 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 Board with assurance on the robustness and effectiveness of the ICB's risk management processes.

	Very Low (1-5)	Low (4-10)*	Medium (8-15)*	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 risk could score 8-10 and be 'Low' if the 'Impact' score is low.*	A generally acceptable level of risk but corrective action needs to be taken (e.g. new risk at score 6+ or escalated from Risk Log(s) to ICB Operational Risk Register). **A risk could score 8-10 and be 'Medium' if the 'Impact' score is high.*	An unacceptable level of risk which requires senior management attention and corrective action.	An unacceptable level of risk which requires urgent Executive and senior management attention and immediate corrective action.
Add to ICB 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).

	Very Low (1-5)	Low (4-10)*	Medium (8-15)*	High (15-20)	Extreme (25)
Oversight and scrutiny	Risk Logs to be reviewed in relevant Team/Directorates Meetings or system forum.	Risk Logs to be reviewed in relevant Team/Directorates Meetings or system forum.	ICB Risk Register (full or relevant extracts) to be reviewed by the relevant committee(s) at each meeting. System risks will be reported to the relevant system forum.	ICB Risk Register (full or relevant extracts) to be reviewed by the relevant committee(s) at each meeting. System risks will be reported to the relevant system forum.	All red/high risks on the ICB Operational Risk Register to be highlighted to the ICB Board.

Table 7 – Reporting requirements

12. Performance Risks

12.1. The ICB monitors the system performance against key delivery priorities via a separate, but parallel, process to the ICB's risk management arrangements.

12.2. To minimise duplication, failures to achieve performance standards are not routinely identified as specific risks on the ICB's 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 Statement).

12.3. The consistent non-delivery of performance standards will be assessed to ensure that any specific risks this poses to the ICB's functions and/or system priorities (e.g., a detrimental impact on health outcomes, patient safety or patient experience) are identified and captured on the Operational Risk Register.

13. Interface with ICS Partner Risks (System Risk Management)

13.1. The Integrated Care System has agreed a working definition of system risk management as "the collective identification, assessment and mitigation of risks where improved outcomes can be achieved by system partners working together through shared accountability arrangements".

13.2 System risk management does not replace organisational risk management requirements but is complementary. Organisations are equal partners within the system, so there is no escalation to the system level and there is a collective responsibility on all system partners for managing system risks. System risks are scored in relation to their potential impact on overall system deliverables and priorities, not individual organisations.

13.3 Processes to identify, evaluate, monitor and report operational system risks follow those outlined within section 11 of this Policy; however, the criteria for a system risk, and further detail on system risk management, is outlined in the below paragraphs.

13.4. An operational risk is determined to be a system risk when it meets one of the following criteria:

- An operational risk that originates from sources that involve multiple partners in the system.
- An operational risk that leads to a single event / series of events that may compromise the achievement of system aims and objectives.
- An operational risk that if it occurred would have medium or high impact consequences on multiple partners within the system.
- An operational risk that if it occurred would require more than one system partner to manage.

13.5. System risks can be identified in the following ways:

- Through individual discussions with system partner senior responsible officers, operational leads and clinical colleagues, when updating existing risks or through other general risk awareness raising discussions;
- Through discussions at system forums;
- Through discussions with system partner risk leads at local Risk Management Network meetings; and
- As reported by internal audit, as a result of system-wide audit reviews.

13.6. System risks will be managed by system partners working together through collective accountability arrangements.

13.7. System risks are captured on the ICB's Operational Risk Register. The use of the Operational Risk Register as the source risk register for system risks enables matrix reporting of relevant system risks across ICS oversight and operational groups, as appropriate. System partner representatives are responsible for feeding back on system risk discussions into their respective organisations.

13.8. Ownership of system risks is defined as the individual responsible for co-ordinating and facilitating overall progress against mitigating actions; they are not responsible for delivering all the mitigating actions themselves.

13.9. As system working arrangements mature and embed, it is likely that system risk management processes will evolve.

14. Management of Issues

14.1 Issues are not routinely recorded on the ICB's Operational Risk Register as they are managed via the organisation's performance management framework. However, senior leads/managers may use discretion as to whether local issues are captured on individual risk logs.

14.2 Known issues are an important mechanism to determine if there are any new risks needed to be identified, and captured, within the ICB's risk management arrangements. Head of Corporate Assurance and Operational Risk Manager can provide further support and guidance on the management of issues.

15. Fraud Risk Assessment

15.1. 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.

15.2. 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.

15.3. A separate fraud risk register will be maintained by the ICB and reported to the Audit and Risk Committee once a year (as a minimum), to coincide with the Counter Fraud annual planning process.

16. Confidentiality

16.1. Where risks are not deemed to be in the public interest, they will be clearly marked as confidential on the Operational Risk Register and reported to the ICB during its 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.

17. Equality and Diversity Statement

17.1 NHS Nottingham and Nottinghamshire ICB pays due regard to the requirements of the Public Sector Equality Duty (PSED) of the Equality Act 2010 in policy development and implementation, as a commissioner and provider of services, as well as an employer.

17.2 The ICB is committed to ensuring that, the way we provide services to the public and the experiences of our staff does not discriminate against any individuals or groups based on their age, disability, gender identity (trans, non-binary) marriage or civil partnership status, pregnancy or maternity, race, religion or belief, gender or sexual orientation.

17.3 We are committed to ensuring that our activities also consider the disadvantages that some people in our 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.

17.4 As an employer, we are committed to promoting equality of opportunity in recruitment, training and career progression and to valuing and increasing diversity within our workforce.

17.5 To help ensure that these commitments are embedded in our day-to-day working practices, an Equality Impact Assessment has been completed for, and is attached to, this policy.

18. Communication, Monitoring and Review

18.1. The policy will be published and maintained in line with the ICB's Policy Management Framework.

18.2. The policy will be highlighted to new staff as part of the local induction process and made available to all staff through the ICB's internal communication procedures (and internet/intranet sites).

18.3. The ICB's Audit and Risk Committee will review the effectiveness of this policy, and its implementation, via bi-annual risk management update reports and monthly targeted assurance reports.

18.4. The ICB will review the risk appetite on an annual basis.

18.5. Internal Audit will report on the implementation of this policy as part of the annual Head of Internal Audit Opinion work programme.

19. Staff Training

19.1. The Corporate Assurance Team will proactively raise awareness of the policy across the ICB and provide ongoing support to committees and individuals to enable them to discharge their responsibilities. Members of the Corporate Assurance Team can be contacted for formal training at team meetings (or other forums) by email: nnicb-nn.corporateassurance2@nhs.net

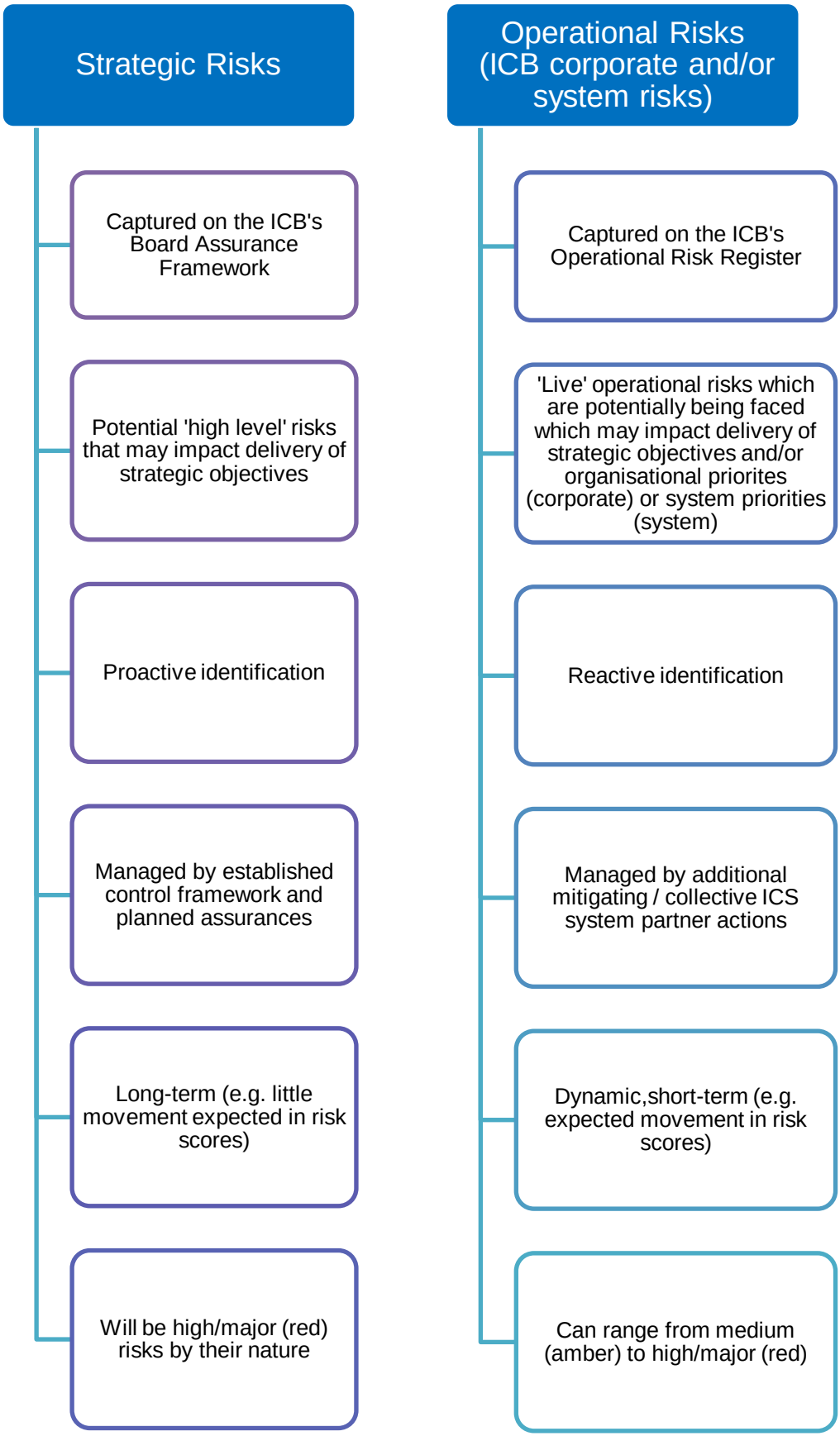
19.2. The Corporate Assurance Team intranet page is under development and will include bite size training on risk management topics. This can be accessed at: https://nhs.sharepoint.com/sites/52R_Intranet/SitePages/Who%27s%20Who/Nursing/Corporate-Assurance-Team.aspx

19.3. Any individual who has queries regarding the content of the policy, or has difficulty understanding how this relates to their role, should contact the ICB's Corporate Assurance Team by email: nnicb-nn.corporateassurance2@nhs.net

20. References

- Assurance Frameworks, (2012). HM Treasury.
- A Risk Practitioners Guide to ISO 31000:2018, (2018). The Institute of Risk Management.
- Board Assurance: A toolkit for health sector organisations, (2015). NHS Providers.
- The Orange Book: Management of Risk – Principles and Concepts, (2020).
- Risk Appetite & Tolerance, (2011). The Institute of Risk Management.
- NHS Audit Committee Handbook, (2018). Healthcare Financial Management Association
- NHS Governance Handbook, (2017). Healthcare Financial Management Association
- Risk Appetite for NHS Organisations: A matrix to support better risk sensitivity in decision taking. (2012). The Good Governance Institute.
- Good Governance Institute (GGI).

Appendix A: Characteristics of Strategic and Operational Risks



Appendix B

Risk Identification Guidance

The purpose of this guidance is to support staff in identifying operational risks that may require entry on to their local risk logs and/or for escalation to the ICB's Operational Risk Register. Further guidance on identifying risks can be provided by contacting the Corporate Assurance Team by email: nnicb-nn.corporateassurance2@nhs.net

The general definition of a risk is "the effect of uncertainty on objectives" and it is the responsibility of all staff to:

- Identify risks at the conceptual stage of projects, as well as throughout the life of the project.
- Routinely consider risk within any planning, procurement or other ICB business and system activities.
- Ensure that any **operational** risks they become aware of are captured on local risk logs and/or the ICB's Operational Risk Register (dependent on score).

Operational risks are defined as by-products of the day-to-day running of an organisation. They arise from definite events or circumstances and have the potential to impact negatively on the organisation and its objectives. The objective which may not be achieved needs to be considered in the risk wording.

Good practice for articulating risks to use the is as follows:

CAUSE: 'As a result of ….' (what will cause the risk to occur?)
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?)

Training on writing risk statements can be requested from the Head of Corporate Assurance. Guidance documents are also available on the Corporate Assurance Team's Intranet page. Risk Log templates are also available.

Categorise the risk using the categories in one of the nine risk domains (see para 7.2) and use the risk scoring matrix in Appendix C to calculate what the risk is at the moment (before any actions have been implemented). You then need to consider the controls you have in place to manage this (e.g. contract monitoring arrangements) and any additional actions that may be needed to mitigate the risk to an acceptable level.

Appendix C

Risk Scoring Matrix

Table 1A: Impact Score (I) Guidance

Impact Score	1 Minor	2 Moderate	3 Serious	4 Major	5 Catastrophic
Guidance	Minor impact on objective/s. Day to day operational challenges.	Moderate impact on objective/s. Temporary restriction to service delivery with limited impact on stakeholder confidence.	Serious 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 Domains	1 Minor	2 Moderate	3 Serious	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.

Appendix C

Risk Domains	1 Minor	2 Moderate	3 Serious	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.

Appendix C

Risk Domains	1 Minor	2 Moderate	3 Serious	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.

Appendix C

Risk Domains	1 Minor	2 Moderate	3 Serious	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.

Appendix C

Risk Domains	1 Minor	2 Moderate	3 Serious	4 Major	5 Catastrophic
Resources Risks that may result in the organisation, or system, 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.
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	• Day to day operational challenges. • Loss/ interruption of >1 hour. • Insignificant cost increase / schedule slippage. • Key 'political' target is being achieved and	• Temporary restriction to service delivery with limited impact on stakeholder confidence. • Loss/ interruption of >8 hours. • <5 per cent over project budget. • Schedule slippage.	• 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.	• Medium term failure to deliver key objectives with ongoing adverse publicity or negative impact on stakeholder confidence. • Loss/ interruption of >1 week.	• Continued failure to deliver key objectives with long term adverse publicity or fundamental loss of stakeholder confidence. • Permanent loss of service or facility.

Appendix C

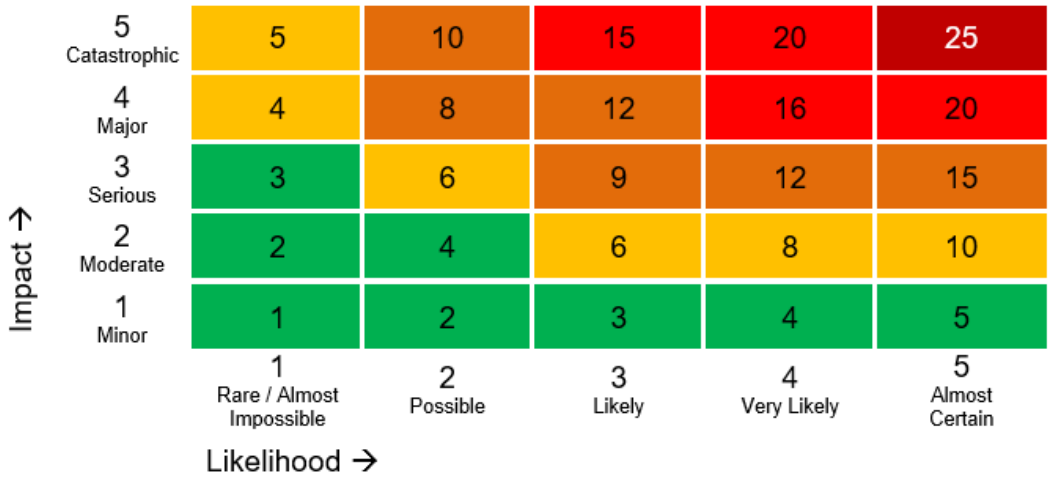
Risk Domains	1 Minor	2 Moderate	3 Serious	4 Major	5 Catastrophic
improvements, opportunities for growth or may contribute positively to the achievement of aims and objectives. [May include, but not limited to, risks linked to capacity, demand, Primary Care, service/ business interruption, digital, projects, planning, delivery, commissioning, partnership working and transformation]	impact prevents improvement.	• 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	• 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.	• 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.	• 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.

Appendix C

Table 2: Likelihood Score (L)

Category	Likelihood Scoring				
Likelihood score	**1**	**2**	**3**	**4**	**5**
Descriptor	**Rare / Almost Impossible**	**Possible**	**Likely**	**Very Likely**	**Almost Certain**
Frequency / How likely is it to happen?	Event very rare, only occur in exceptional circumstances. Less than 20% chance of event happening.	The event may occur at some time. 21% - 40% chance of event happening.	The event is likely to occur at some time. 41% - 60% chance of event happening.	The event will occur in most circumstances. 61% - 80% chance of event happening.	This event is expected to occur in most circumstances. 81% 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?) **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?
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. **PLEASE REMEMBER 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 consequence being realised (see risk description - **EFFECT:** *'Which may lead to ….*') in light of 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?

Appendix E

Three Lines of Defence Model

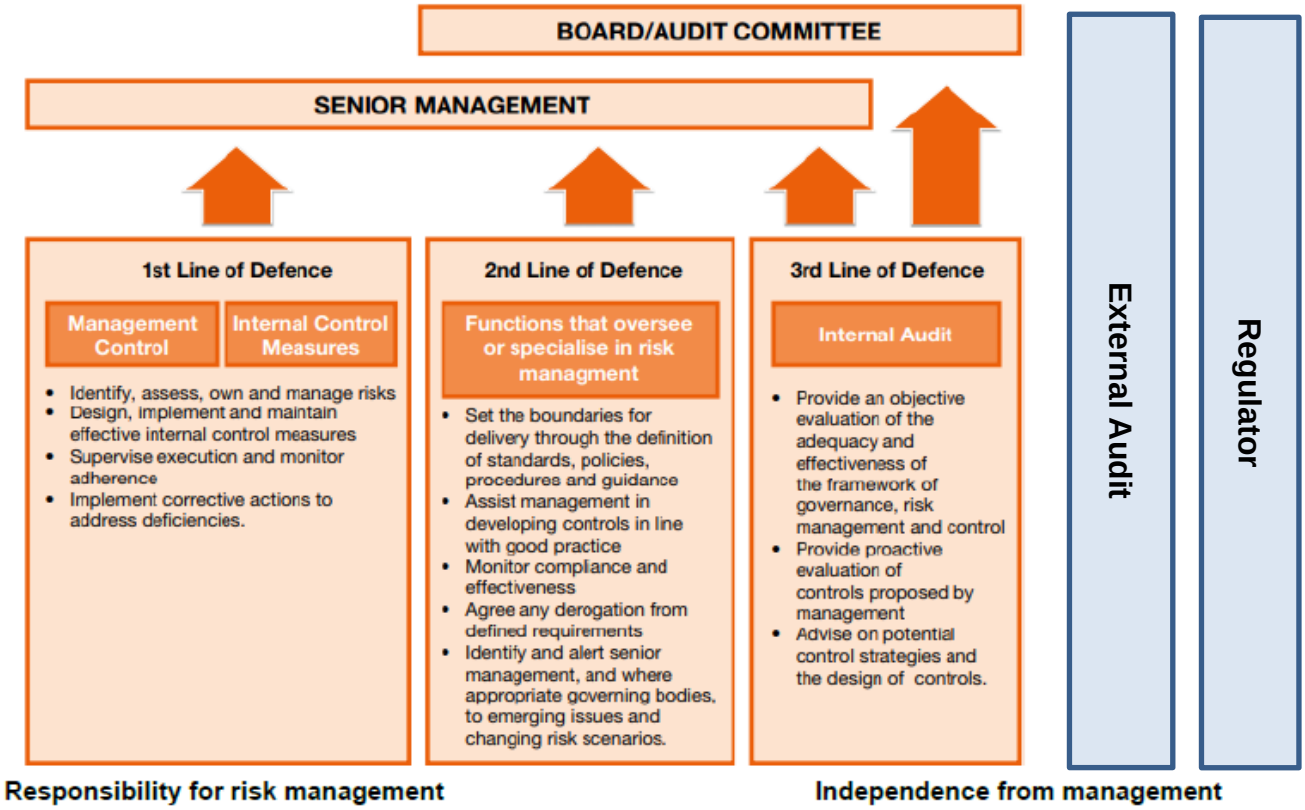


Figure 6 – Three lines of defence model

Everyone in the organisation has some responsibility for risk management. The "three lines of defence" model provides a simple and effective way to help delegate and coordinate risk management roles and responsibilities within and across the organisation.

1. First line of defence

1.2 Under the "first line of defence," management have primary ownership, responsibility and accountability for identifying, assessing and managing risks. Their activities create and/or manage the risks that can facilitate or prevent an organisation's objectives from being achieved.

1.3 The first line 'own' the risks and are responsible for execution of the organisation's response to those risks through executing internal controls on a day-to-day basis and for implementing corrective actions to address deficiencies.

1.4 Through a cascading responsibility structure, managers design, operate and improve processes, policies, procedures, activities, devices, practices, or other conditions and/or actions that maintain and/or modify risks and supervise effective execution.

1.5 There should be adequate managerial and supervisory controls in place to ensure compliance and to highlight control breakdown, variations in or inadequate processes and unexpected events, supported by routine performance and compliance information.

2. Second line of defence

2.1. The second line of defence consists of functions and activities that monitor and facilitate the implementation of effective risk management practices and facilitate the reporting of adequate risk related information up and down the organisation. The second line should support management by bringing expertise, process excellence, and monitoring alongside the first line to help ensure that risks are effectively managed.

2.2. The second line should have a defined and proportionate approach to ensure requirements are applied effectively and appropriately. This would typically include compliance assessments or reviews conducted to determine that standards, expectations, policy and/or regulatory considerations are being met in line with expectations across the organisation.

3. Third line of defence

3.1. Internal audit forms the organisation's "third line of defence." An independent internal audit function will, through a risk-based approach to its work, provide an objective evaluation of how effectively the organisation assesses and manages its risks, including the design and operation of the "first and second lines of defence."

3.2. It should encompass all elements of the risk management framework and should include in its potential scope all risk and control activities.

3.3. Internal audit may also provide assurance over the management of cross organisational risks and support the sharing of good practice between organisations, subject to considering the privacy and confidentiality of information.

4. External / Fourth line of defence

4.1. Sitting outside of the organisation's own risk management framework and the three lines of defence, are a range of other sources of assurance that support an organisation's understanding and assessment of its management of risks and its operation of controls.

4.2. The tend to be external independent bodies such as the external auditors and regulators.

4.3. External bodies may not have the existing familiarity with the organisation that an internal audit function has, but they can bring a new and valuable perspective. Additionally, their outsider status is clearly visible to third parties, so that they can not only be independent but be seen to be independent.

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

Appendix F: Equality Impact Assessment

Overall Impact on: **Equality, Inclusion and Human Rights**	**Neutral**

Name of Policy, Process, Strategy or Service Change	Risk Management Policy
Date of Completion	August 2023, Reviewed May 2024
EIA Responsible Person Include name, job role and contact details.	Sian Gascoigne, Head of Corporate Assurance Email: sian.gascoigne@nhs.net
EIA Group Include the name and position of all members of the EIA Group.	
Wider Consultation Undertaken State who, outside of the project team, has been consulted around the EIA.	None
Summary of Evidence Provide an overview of any evidence (both internal and external) that you utilised to formulate the EIA. E.g., other policies, Acts, patient feedback, etc.	Equality Act 2010

For the policy, process, strategy or service change, and its implementation, please answer the following questions against each of the Protected Characteristics, Human Rights and health groups:	What are **the actual, expected or potential positive impacts** of the policy, process, strategy or service change?	What are the **actual, expected or potential negative impacts** of the policy, process, strategy or service change?	What **actions have been taken** to address the actual or potential **positive and negative impacts** of the policy, process, strategy or service change?	**Impact Score**
Age	There are no actual or expected positive impacts on the characteristic of Age.	There are no actual or expected negative impacts on the characteristic of Age.	None.	3
Disability[1] (Including: mental, physical, learning, intellectual and neurodivergent)	There are no actual or expected positive impacts on the characteristic of Disability.	There are no actual or expected negative impacts on the characteristic of Disability.	Mechanisms are in place via the Communications and Engagement Team to receive the policy in a range of languages, large print, Braille, audio, electronic and other accessible formats.	3
Gender[2] (Including: trans, non-binary and gender reassignment)	There are no actual or expected positive impacts on the characteristic of Gender.	There are no actual or expected negative impacts on the characteristic of Gender.	None.	3
Marriage and Civil Partnership	There are no actual or expected positive impacts on the characteristic of Marriage and Civil Partnership.	There are no actual or expected negative impacts on the characteristic of Marriage and Civil Partnership.	None.	3

Pregnancy and Maternity Status	There are no actual or expected positive impacts on the characteristic of Pregnancy and Maternity Status.	There are no actual or expected negative impacts on the characteristic of Pregnancy and Maternity Status.	None.	3
Race[3]	There are no actual or expected positive impacts on the characteristic of Race.	There are no actual or expected negative impacts on the characteristic of Race.	Mechanisms are in place via the Communications and Engagement Team to receive the policy in a range of languages.	3
Religion and Belief[4]	There are no actual or expected positive impacts on the characteristic of Religion or Belief.	There are no actual or expected negative impacts on the characteristic of Religion or Belief.	None.	3
Sex[5]	There are no actual or expected positive impacts on the characteristic of Sex.	There are no actual or expected negative impacts on the characteristic of Sex.	None.	3
Sexual Orientation[6]	There are no actual or expected positive impacts on the characteristic of Sexual Orientation.	There are no actual or expected negative impacts on the characteristic of Sexual Orientation.	None.	3
Human Rights[7]	There are no actual or expected positive impacts on the characteristic of Human Rights.	There are no actual or expected negative impacts on the characteristic of Human Rights.	None.	3
Community Cohesion and **Social Inclusion**[8]	There are no actual or expected positive impacts on the characteristic of Community Cohesion and Social Inclusion.	There are no actual or expected negative impacts on the characteristic of Community Cohesion and Social Inclusion.	None.	3

Safeguarding[9] (Including: adults, children, Looked After Children and adults at risk or who lack capacity)	There are no actual or expected positive impacts on the characteristic of Safeguarding.	There are no actual or expected negative impacts on the characteristic of Safeguarding.	None.	3
Other Groups at Risk[10] of Stigmatisation, Discrimination or Disadvantage	There are no actual or expected positive impacts on the characteristic of Other Groups at Risk.	There are no actual or expected negative impacts on the characteristic of Other Groups at Risk.	None.	3

Positive Impact	Neutral Impact	Undetermined Impact	Negative Impact	Equality Impact Score Total	39
56 to 46	45 to 33	32 to 20	19 to 13		

Additional Equality Impact Assessment Supporting Information

1. **Disability** refers to anyone who has: "…a physical or mental impairment that has a 'substantial' and 'long-term' negative effect on your ability to do normal daily activities…" (Equality Act 2010 definition). This includes, but is not limited to: mental health conditions, learning disabilities, intellectual disabilities, neurodivergent conditions (such as dyslexia, dyspraxia and dyscalculia), autism, many physical conditions (including HIV, AIDS and cancer), and communication difficulties (including d/Deaf and blind people).

2. **Gender**, in terms of a Protected Characteristic within the Equality Act 2010, refers to: "A person has the protected characteristic of gender reassignment if the person is proposing to undergo, is undergoing or has undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attributes of sex."

3. **Race**, in terms of a Protected Characteristic within the Equality Act 2010, refers to: A person's colour, nationality, or ethnic or national origins. This also includes people whose first spoken language is not English, and/or those who have a limited understanding of written and spoken English due to English not being their first language.

4. **Religion and Belief**, in terms of a Protected Characteristic within the Equality Act 2010, refers to: Religion means any religion and a reference to religion includes a reference to a lack of religion. Belief means any religious or philosophical belief and a reference to belief includes a reference to a lack of belief.

5. **Sex**, in terms of a Protected Characteristic within the Equality Act 2010, refers to: A reference to a person who has a particular protected characteristic and is a reference to a man or to a woman.

6. **Sexual Orientation**, in terms of a Protected Characteristic within the Equality Act 2010, refers to: Sexual orientation means a person's sexual orientation towards persons of the same sex, persons of the opposite sex or persons of either sex.

7. The **Human Rights Act 1998** sets out the fundamental areas that everyone and every organisation must adhere to. In relation to health and care, the most commonly applicable of the Articles within the Human Rights Act 1998 include: Article 2 Right to Life, Article 5 Right to Liberty and Security, Article 8 Right to Respect of Private and Family Life, and Article 9 Freedom of Thought, Conscience and Religion.

8. **Community Cohesion** is having a shared sense of belonging for all groups in society. It relies on criteria such as: the presence of a shared vision, inclusion of those with diverse backgrounds, equal opportunity, and supportive relationships between individuals. **Social Inclusion** is defined as the process of improving the terms of participation in society, particularly for people who are disadvantaged, through enhancing opportunities, access to resources, voice and respect for rights (United Nations definition). For the EQIA process, we should note any positive or negative impacts on certain groups being excluded or not included within a community or societal area. For example, people who are homeless, those from different socioeconomic groups, people of colour or those from certain age groups.

9. **Safeguarding** means: "…protecting a citizen's health, wellbeing and human rights; enabling them to live free from harm, abuse and neglect. It is an integral part of providing high-quality health care. Safeguarding children, young people and adults is a collective responsibility" (NHS England definition). Those most in need of protection are children, looked after children, and adults at risk (such as those receiving care, those under a DoLS or LPS Order, and those with a mental, intellectual or physical disability). In addition to the ten types of abuse set out in the Health and Care Act 2022, this section of the EQIA should also consider PREVENT, radicalisation and counterterrorism.

10. **Other Groups** refers to anyone else that could be positively or negatively impacted by the policy, process, strategy or service change. This could include, but is not limited to: carers, refugees and asylum seekers, people who are homeless, gypsy, Roma and traveller communities, people living with an addiction (e.g., alcohol, drugs or gambling), people experiencing social or economic deprivation, and people in stigmatised occupations (e.g., sex workers).