Hertfordshire and West Essex Integrated Care System

NHS
Hertfordshire and West Essex
Integrated Care Board

Risk Management Policy

Version 2.1

DOCUMENT CONTROL

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the website.

Do you really need to print this document?
Please consider the environment before you print this document and where copies should be printed double-sided. Please also consider setting the Page Range in the Print properties, when relevant to do so, to avoid printing the policy in its entirety.

Document Owner:	Michael Watson, Chief of Staff
Document Author(s):	Governance Manager - Risk
Version:	2.1
Approved By:	Executive Team
Date of Approval:	**8th February 2024**
Date of Review:	**February 2025**
Link to Strategic Objective(s):	• Increase life expectancy and reduce inequality • Give every child the best start in life • Improve access to health and care services • Increase the number of citizens taking steps to improve their wellbeing • Achieve a balanced position annually

Change History:

Version	Date	Reviewer(s)	Revision Description
1.0 Draft	1 July 2022	Katy Patrick, Head of Governance	Initial draft document prepared based on and to supersede existing HWECCG's Risk Management Strategies, Policies and Procedures
1.1 Draft	25 July 2022	Leon Adeleye, Corporate Governance Manager	Presented and discussed at the Executive Team: • Removed duplications, added page number to the document and formatting • Replaced the table of content to capture headings and page numbers • Updated various sections, including the terms and definitions – vocabularies in line with ISO31000:2009/18, risk appetite table, consequence table • Replaced process diagrams including the assurance process • Removed the Guidance for Datix Risk Register from the Appendices and provided on a separate document for regular revision Added the Data Protection Impact Assessment (DPIA) Screening Tool to the Appendices

1.2 Draft	18 August 2022	Leon Adeleye, Corporate Governance Manager	Further updates: • Full revision of the structure, content and format. • Added the Risk Management Implementation Plan for 2022/23 • More emphasis on leadership and culture, objectives, ownership risk appetite and revised the assurance • Revised the responsibilities sections, reporting arrangement table and process diagrams. Enhanced the risk matrix and the action trigger table for risk assessment across the ICB. Including risk appetite, and threshold for reportable incidents to ICO.
1.3 Draft	05 September 2022	Leon Adeleye, Corporate Governance Manager	Presented and Discussed at the Audit and Risk Committee: • Revised the risk matrix with minor changes • Added the EqIA to Appendix 4
1.4	November 2022	Leon Adeleye Governance Manager – Risk	Submitted for the Executive Team's final approval.
1.5	June 2023	Leon Adeleye, Governance Manager – Risk	Full annual review and updated with • 2022/27 ICB Strategic Objectives • ICB Risk Appetite Statements • Risk Management Implementation plans for 2023/24 • Rearticulation of various sections, including introduction, statement of commitment, roles and responsibilities, risk management principles, risk appetite, objectives, risk direction, risk scoring • Improved illustrations, appendices updates, Definition of terms moved to appendices
1.6	July 2023	Redouane Serroukh – Head of Information Governance and Risk	Executive Team feedback incorporated.
2.1	December 2023	Leon Adeleye Governance Manager – Risk / Redouane Serroukh – Head of IG and Risk	Full review of the Risk Management Policy using the new HWE ICB policy template. Rearticulation of some sections and a focus on more concise information for staff.
2.1	8th February 2024	Executive Committee	Approved
2.1		Executive Committee	Approved extension of this policy until September 2025

CONTENTS

1 Introduction

1.1 NHS Hertfordshire and West Essex Integrated Care Board (HWE ICB) is dedicated to building a future-ready health and care system with integrated services centred around the needs of individuals. The ICB's objectives guide its plans and decisions, ensuring stakeholders have confidence in its internal control systems.

1.2 The identification, assessment and management of risks against the ICB achieving its objectives plays a crucial role in the ICB's success. This policy outlines the ICB's commitment to fostering a culture where risk management is central and effective at both strategic and operational levels. The aim is to enhance value creation and protection within the organisation.

1.3 The ICB will seek to align risks to its strategic objectives, found under section 9.1.3.

2 Purpose

2.1 The purpose of this policy is to:

(a) Ensure all staff are aware of their responsibilities in relation to effective risk management within HWE ICB.

(b) To provide a firm commitment that HWE ICB acknowledges the importance of effective risk management in fulfilling its obligations and ensuring the achievement of its vision and purpose. The ICB adopts the framework and best practices outlined in this risk management policy. By doing so, the ICB ensures that all identified risks are adequately managed and that opportunities are also identified, evaluated, and controlled consistently.

The ICB will identify and manage risks to achieving its strategic objectives and actively discuss and mitigate against those risks so that their likelihood of materialising is continuously diminished.

3 Scope

3.1 This policy applies to all ICB staff members, including the Board and those involved in achieving the ICB strategic objectives, whether permanent, temporary or contracted-in (either as an individual or through a third-party supplier).

4 Definitions

4.1 The following definitions apply in the context of this policy:

Term	Definition
Risk	The "effect of uncertainty on objectives" (ISO, 2018). To simplify this definition, a risk is defined as a chance or possibility of loss, damage, injury, or failure to achieve objectives caused by an unwanted or uncertain action or event.
Risk identification	The process of finding, recognising, and describing risks • Risk identification involves the identification of risk sources, events, and their causes as well as their potential consequences. • Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder needs.
Risk Management Framework	According to ISO31000:2009, is a set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. The foundations include the policy, objectives, mandate, and commitment to manage risk. The organisational arrangements include plans, relationships, accountabilities, resources, processes, and activities. The risk management framework is embedded within the organisation's overall strategic and operational policies and practices.
Risk source	Element which alone or in combination has the intrinsic potential to give rise to risk.
Event	An occurrence or change of a particular set of circumstances. • An event can have one or more occurrences and can have several causes and consequences. • An event that can be expected but may not happen, or something unexpected and does • An event can be a risk.
Consequence	The outcome of an event, affecting objectives. • A consequence can be certain or uncertain and can have positive or negative, direct, or indirect, effects on objectives. • Consequences can be expressed qualitatively or quantitatively. • Any consequence can escalate through cascading and cumulative effects.
Likelihood	The chance of an event occurring, whether defined, measured, or determined objectively or subjectively, qualitatively or quantitatively, and in general or mathematical terms. • The equivalent of the term "probability."

Risk matrix	Tool for ranking and displaying risks by defining ranges for consequence and likelihood
Risk Score	Risk Score (RS) is the result of multiplying the consequence rating by Likelihood rating (i.e., C x L = RS) on the risk matrix table. This provides you with a 'level of risk'.
Risk owner	Person or entity with the accountability and authority to manage a risk. Risk owners have designated responsibilities for each reported risk, therefore they must: • Ensure compliance to the policy in respect of owned risks and the escalation of risks where required. • Ensure the risk owned is effectively always mitigated and kept up to date. • Oversee the delivery of key action plans agreed with action owners. • Monitor the status of owned risks with a particular focus on monitoring circumstances that may alter the severity of risks.
Risk lead	Risk leads have delegated responsibilities including: • Taking a lead role in embedding risk management processes in their directorates and teams. • Taking a lead role in the maintenance of risk registers via the online risk management tool (Datix, at the time of this policy review) and ensuring risks that rate a current risk score of 12 or higher are escalated and managed on the Corporate Risk Register. • Providing assurance of risk management activity through the relevant committees and the Risk Review Group.
Risk appetite	Amount and type of risk that an organisation is willing to pursue or retain i.e., the amount and type of risk that the ICB is willing to take in pursuit of its strategic objectives as determined by the Board.
Control	Measure that maintains and/or modifies risk. • Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk. • Controls may not always exert the intended or assumed modifying effect.
Risk Register	Record of information about identified risks. • The set of risks can contain those that relate to the whole organisation, part of the organisation, or as otherwise defined. • It is presented as a list containing all identified risks faced by an organisation; controls; assurance; and mitigating actions to strengthen the controls and assurance.
Residual risk	Risk remaining after risk treatment. • Residual risk can contain unidentified risk. • Residual risk can also be known as "retained risk".
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation. It is a systematic method of identifying and prioritising risks and then determining the most appropriate risk response.

Mitigating actions	Plans are agreed in response to formal risk assessments or to strengthen existing controls where gaps are identified. Action articulation should follow best practice models, for example: 'SMART' (Specific, Measurable, Achievable, Realistic and Timely).
Assurance	A positive declaration that a thing is true or a control is indeed in place. According to the Good Governance Institute, assurance is the information and evidence provided or presented which are intended to induce confidence that a thing is true (Dower & Bullivant, 2014).
Risk Culture	Is the set of encouraged and acceptable behaviours, discussions, decisions, and attitudes toward taking and managing risk within an organisation[1]. A risk-management-friendly culture promotes open and upward communication, best practices and knowledge sharing, continuous improvement, and a strong commitment to ethical and responsible corporate behaviour. Effective risk management does not exist in a vacuum and is able to succeed with effective leadership.

5 Roles and Responsibilities

Role	Responsibilities
Board	The Board holds the ultimate responsibility for determining the level and nature of risks acceptable in pursuit of its objectives, as well as the required level of assurance for confidence. Executive members of the Board have particular responsibilities for their respective 'areas' where risk management processes, updates and accountability for risk owners are concerned. Non-executive members have particular responsibility for scrutinising and if required challenging the soundness of risk management systems and processes. Collectively, the board will fulfil its responsibility by undertaking the following: • Establish clear and measurable objectives (strategic, corporate, and operational) throughout the ICB to identify risks and obtain necessary assurance. • Scrutinise the significant risks associated with strategic objectives and ensure management has implemented effective controls to achieve those objectives. • Establish and maintain a robust and consistent risk management structure that aligns with the organisation's risk appetite, risk tolerance, and the cumulative impact and likelihood of risks on objectives. • Collaborate with the Audit and Risk Committee, to determine the need for updates or revisions to the risk management policy as part of its on-going oversight role. Review and approve the level of risk the ICB is willing to take.

[1] Risk Culture: From Theory to Evolving Practice

	• Obtain assurance that key and emerging risks within the ICB and the system are adequately identified and appropriately managed through the risk register. • Adhere to the UK Corporate Governance Code, which emphasises establishing procedures to manage risk, overseeing the internal control framework, and determining the principal risks the company is willing to accept for long-term strategic objectives. • Review risk reporting through the assurance framework and monitor 'primary risks' from the corporate risk register. • Review an annual report from the Chair of the Audit and Risk Committee on the adequacy and effectiveness of risk management within the ICB, as well as associated system risks. By fulfilling these responsibilities, the Board strengthens risk oversight, internal controls, and assurance processes, thereby ensuring effective risk management and governance throughout the organisation and with system partners.
Chief Executive	The Chief Executive ("Accountable Officer") has the overall responsibility for risk management within the ICB. As part of the assurance framework, the Accountable Officer, on behalf of the Board, prepares and publishes an Annual Governance Statement. This statement provides stakeholders with confidence that the ICB is adequately informed about its overall risks. Therefore, the Accountable Officer, with the support of the Board, assumes the following responsibilities: • Ensuring the implementation of the ICB's Risk Management Policy, throughout all areas of the organisation, fostering robust governance, risk management and internal control arrangements. • Fostering a culture of open discussion and debate, emphasising accountability among risk owners, and promoting a risk-aware culture. • Ensuring the Executive Team members' personal objectives have an appropriate focus on risk and risk management. • Setting risk appetite and tolerance levels: The Accountable Officer should work with the Board to define the organisation's risk appetite and tolerance levels. • Encouraging continuous improvement in risk management by promoting feedback, lessons learned, and sharing of best practices across the organisation.
Executive Team	The Executive Team is responsible for overseeing the implementation of the ICB's Risk Management Policy, including defining, sponsoring, supporting, debating and challenging key risk and risk management activity across the ICB. The Executive Team will review and monitor progress against the policy and play a key role in providing assurance to the Board and Audit Committee on the effectiveness of the policy, its application, and the management of key risk areas. The Executive Team will:

	• Ensure that key and emerging strategic risks are identified, assessed and managed by undertaking on-going analysis of risk information to assess risk criticality, common themes and trends; and identify areas of emerging risk requiring further quantification or scenario analysis. • Ensure that there is an appropriate reporting structure in place to support the delivery and execution of the ICB's Risk Management Policy. • Executive Team members should establish and lead the appropriate risk management processes in their respective directorates which is to include, at minimum, a monthly discussion with appropriate risk leads to monitor and review risks within their remit. • Promote a risk-aware culture and an environment that creates positive risk-taking behaviour and clear accountability.
Chief of Staff	The Chief of Staff plays a critical role in providing strategic counsel to the Accountable Officer regarding risks across the ICB. To effectively implement the requirements of the risk management policy, the Chief of Staff, with the support of the governance team, will: • Hold departments and teams within the ICB organisation accountable for the implementation of the risk management policy. • Ensure real risk are captured and have adequate oversight. • Prioritise risk as a standing agenda item for the Executive Team and the Board, ensuring that major areas of activity such as the ICB's culture and uncertainties surrounding partners, stakeholders, and regulatory compliance are not overlooked. • Establish controls, including an organisational or committee structure supported by a Scheme of Delegation and accountability framework, policies, procedures, guidelines, training, and regular management actions, to facilitate the achievement of desired outcomes.
Senior Information Risk Owner	The Chief Finance Officer (CFO) of the ICB serves as the designated "Senior Information Risk Owner" (SIRO), specifically responsible for information risk management. The SIRO is accountable for information risks and is concerned with the management of all information assets. The SIRO has responsibility for: • Taking overall ownership and accountability for information risk management within the organisation. • Establishing and maintaining an effective information risk management framework • Reviewing and agreeing actions to address identified information risks • Establishing and maintaining robust Counter Fraud arrangements. • Promoting a culture of risk awareness and information security throughout the organisation.

	• Collaborating with relevant stakeholders, such as IT teams and senior management, to address information risks effectively. • Monitoring and reviewing the effectiveness of information risk management practices and making necessary improvements. • Reporting on information risk management activities and outcomes to senior management or the board of directors • Ensuring compliance with applicable laws, regulations, and industry standards related to information security and risk management. • Participating in relevant forums or committees related to information risk management.
Managers	• Coordinate the use of resources to reduce, manage, and control the possibility and/or effect of recognised risks in their respective fields of expertise. • Identify, manage and report risks appropriately ensuring the necessary actions are taken on risks within their sphere of influence. • Implement agreed actions to manage risks. • Report activities or circumstances that may give rise to new or changed risks.
Project Manager	• Capture risks that could potentially impact the project's delivery in Project Initiation Documents. • Include project risks in the Project Highlight Report updates and review them with each stakeholder group and lead Director. • Escalate any project risks that cannot be managed at the project team level to the relevant director for inclusion in the corporate risk register.
Governance Team	• Consolidate, challenge, and report all risk management information. • Facilitate risk management activities, including identification and assessment across the ICB. • Proactively raise risk and risk management awareness and understanding at all levels. • Provide regular and ad-hoc reporting on key business risks, control strength, risk environment, progress of critical actions, and risk process effectiveness. • Attend the Executive Team meetings to provide an ongoing view of risk management performance. • Provide ongoing risk management advice and training to all parts of the organisation. • Develop, implement, maintain, and evolve the policy, considering evolving good industry/regulatory practice. • Monitor the overall level of risk assumed by the ICB and the strength of the control environment.
All staff	All staff must comply with this Risk Management Policy and assisting in the risk management process by:

	• Proactively and promptly identifying risks within their area of work and at meetings and adding risks to the relevant Risk Registers on the ICB's web-based risk management system – Datix (at the time of policy review), • ensuring that identified risks have been assigned to an agreed risk owner and risk lead, to estimate the severity of the risk with regards to the likelihood and impact on objectives at any level. • participating in reviewing existing controls and where there is a gap, agreeing on planned actions to strengthen the controls. • describing risks relating to their work using the best practice provided in this risk management policy. • attending required risk management training and development events to ensure a full understanding of their risk management responsibilities and expectations.
Audit and Risk Committee	The Committee's core responsibilities in relation to risk management involves overseeing strategic and system risks related to achieving the ICB's objectives, scrutinising assurances on the adequacy of risk management and internal control, identifying weaknesses, and seeking reports to assess integrated governance effectiveness. The Audit and Risk Committee plays a crucial role in overseeing the effectiveness of internal and external auditors concerning risk management. The Committee: • Ensures qualified individuals are appointed as auditors, regularly evaluating their performance to uphold effective risk assessment. • Assesses audit findings and recommendations, ensuring adequacy of risk mitigation measures and overseeing necessary improvements. • Ensures auditors maintain independence and objectivity, reviewing potential conflicts of interest and ensuring unrestricted access to relevant information. • Encourages a culture of continuous improvement in risk management practices, providing guidance to auditors for enhanced effectiveness and staying current with emerging risks and best practices.
Risk Review Group	As a subcommittee to the Audit and Risk Committee, the Risk Review Group plays a crucial role in evaluating and monitoring the effectiveness of risk management practices, identifying potential areas of concern, and providing regular reports and recommendations to the Audit and Risk Committee to improve risk management processes. The Risk Review Group provides assurance to the Audit and Risk Committee by fulfilling the following responsibilities: • Reviewing and assessing the organisation's internal risk management framework and policies and ensuring they embed mechanisms to drive risk culture, and the use of risk appetite statement and tolerance in decision-making. • Challenging risk management practises to enhance the quality of Board discussions on significant risks to strategic objectives and escalated risks.

	• Monitoring and reviewing the implementation of risk mitigation strategies and evaluating the effectiveness of our processes. • Conducting regular assessments of emerging risks and changes in the business environment to ensure ongoing risk management relevance.

6 Implementation

6.1 This policy will be made available via the HWE ICB intranet.

6.2 The Risk Management Policy will be implemented primarily through the Executive Team and the Governance Team, however, a number of other roles also hold responsibilities for implementation, as outlined in the roles and responsibilities section above.

6.3 The Governance Team will arrange periodic training on risk management to all staff involved in HWE ICB's risk management processes.

7 Monitoring compliance with this policy

7.1 The Governance Team and the Audit and Risk Committee will take an active approach to monitor compliance with this policy through regular reporting and highlighting of areas of improvement.

7.2 Internal and external auditors also play a role in supporting the ICB to monitor the effective compliance of this policy. They support the ICB by independently providing assurance of compliance with the policy (and wider risk management framework), making recommendations as is appropriate to further improve compliance levels.

8 Risk Management Policy Statement

8.1 Risk management is a fundamental part of governance and leadership at all levels and is driven by identification and assessment of risks. All staff must consider risk and accept responsibility for risks associated with their area of authority.

8.2 Risk management should be integrated into the organisation's overall governance, planning, decision-making, and operational processes. It should be embedded in the ICB's culture and become an integral part of day-to-day activities. The Board Directors and senior leadership of the ICB are required to actively identify risks to achieving the ICB objectives and ensure adequate resources to manage risks are in place.

8.3 To assist with the fulfilment of the above point, Risk Owners are expected to meet at least monthly with the Risk leads and appropriate managers to review current risks and receive updates on further actions as and when they arise.

8.4 Risk management processes should be conducted objectively, without bias or personal interests. Information regarding risks, their assessment, and management should be transparently communicated to relevant stakeholders to facilitate informed decision-making.

8.5 Effective risk management involves engaging all relevant stakeholders, including employees, management, customers, suppliers, and regulators. Different perspectives and expertise contribute to a more comprehensive understanding of risks and better risk response strategies.

8.6 Risk management should result in the implementation of appropriate risk response measures within an appropriate timeframe. Decisions and actions should be based on a thorough analysis of risks and their potential impacts.

8.7 All significant risks to the ICB's strategic objectives and their associated controls and assurances must be added to the Risk Register.

8.8 It is the responsibility of Risk Owners and Risk Leads to ensure that their risk entries on the Risk Register are regularly reviewed and updated in line with the Risk Management Policy

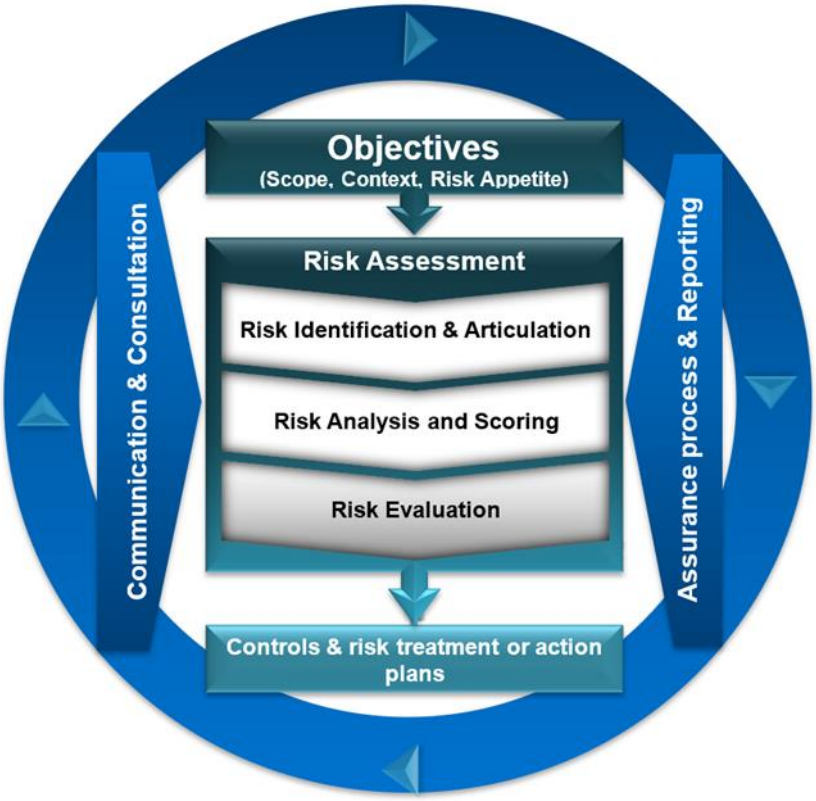
8.9 Primary and principal risks should be reduced to an acceptable level, within an appropriate range in accordance with the ICB's risk appetite statement.

8.10 The risk register produced will include assurance mapping to assist Directors in discussions at the Board, Committees or with their teams to analyse any risks connected to objectives, new projects, or areas of work and to identify any assurance gaps where action is needed to strengthen the existing controls.

8.11 All identified risks must initially be discussed at Team level. After consideration of the nature and scoring of the risk, further discussion and reporting to the Executive Team, Risk Review Group, Committees, and Board meetings should be considered as is appropriate. For proper supervision, risk management should be a standing item on the agenda of each meeting.

8.12 Risk management is a continuous and iterative process, adapting to changes in the ICB's internal and external environments. Regular monitoring, review, and updating of the risk management framework and practices help ensure their relevance and effectiveness over time.

9 Risk Management Process



Source: Adapted from the ISO31000:2018 Risk Management – Guidelines

9.1 Objectives

9.1.1 The process for setting objectives is described on three levels, namely, strategic, corporate, and operational objectives. Objectives set the scope, context, and criteria or risk appetite, against which risks are identified and managed.

9.1.2 Risks should be identified based on a threat to the successful delivery of one or more ICB objective. Therefore, the ICB's objectives provide the landscape and starting point for the assessment of risks.

9.1.3 The ICB has agreed the following strategic objectives for the next 3-5 years:

- Increase healthy life expectancy, and reduce inequality.
- Give every child the best start in life.
- Improve access to health and care services.
- Increase the number of citizens taking steps to improve their wellbeing.
- Achieve a balanced financial position annually.

9.2 Risk Assessment

9.2.1 Risk Identification & Articulation

9.2.1.1 Risk identification involves finding, recognising, and describing risks. It is important to understand the anatomy of risks. As already defined, risk is an uncertainty that something impacting on objectives is likely to happen:

- **NOT** something that *has* happened (incident)
- **NOT** something that *will* happen or is already happening (issue)

9.2.1.2 Risk consists of a combination of three elements, including cause, event, and effect. The risk description should follow the best practice model: **IF** (cause), **THEN** (risk event), and **RESULTING IN** (effect/impact), to help determine risk severity and how risks can best be mitigated.

Cause	**Event**	**Effect**
What might trigger the event to occur e.g., "IF" our financial performance is incomplete	An unplanned/unintended variation from an objective, e.g., "THEN" we may be unable to demonstrate value for money in all areas	How the organisation could be impacted should the event occur, e.g., "RESULTING IN" (1) a threat to future funding and (2) damage to the ICB's reputation

Source: adapted from Amberwing Ltd

9.2.1.3 The above example would therefore be described using this format as:

*"**If** our financial performance is incomplete, **then** we may be unable to demonstrate value for money in all areas **resulting in** (1) a threat to future funding and (2) damage to the ICB's reputation."*

9.2.2 Risk Analysis and Scoring

9.2.2.1 Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, time-related factors and volatility, the effectiveness of existing controls, sensitivity and confidence levels.

9.2.2.2 Risk scoring is a method used in risk assessment to estimate and rank risks based on their likelihood (probability) and consequence (impact). Risk scoring involves assigning numerical values or scores to the likelihood and consequence of a risk, and then combining these scores to determine an overall risk score.

9.2.2.3 Likelihood: refers to the probability or chance of a risk event occurring. It is assessed using the numerical values 1 to 5 provided in the table below. The higher the likelihood, the greater the chance of the risk event occurring.

9.2.2.4 Consequence: represents the potential impact or severity of a risk event if it were to occur. The impact can be assessed based on various factors specific to the risk, such as financial loss, reputation damage, or harm to individuals. Similar to likelihood, consequence is assessed using the numerical values in table below. A more detailed description of each of the scoring categories can be found in *Appendix 1 – Risk matrix descriptors*:

		Consequence (Impact)				
		1. Negligible	2. Minor	3. Moderate	4. Major	5. Catastrophic
Likelihood	5. Almost Certain	5	10	15	20	25
	4. Highly Likely	4	8	12	16	20
	3. Possibly	3	6	9	12	15
	2. Unlikely	2	4	6	8	10
	1. Rare/	1	2	3	4	5

Risk Matrix table

Risk Zones and Descriptors	
Green Zone:	Review – no action required. Risks in this zone should be reviewed every quarter or as required.
Yellow Zone:	Continue to watch. Action is discretionary. Risks in this zone which are scored below 12 should be reviewed quarterly, but if rated above 12 then review monthly.
Amber Zone:	Action should be taken and / or continued monitoring by the ICB. Risks in this zone which are scored below 12 should be review quarterly, but if rated above 12 then review monthly.
Red Zone:	Immediate actions required / or continued monitoring by the ICB; review every month.

Action triggers matrix

9.2.2.5 It is not the intention of this Policy to remove all risks or to manage risks to a low assessment. To be successful, the ICB needs to take informed risks:

9.2.3 Risk Evaluation

9.2.3.1 The purpose of risk evaluation is to support decisions. This compares the results of the risk analysis with the established risk criteria to determine where additional action is required, leading to a decision to:

- do nothing further;

- consider risk treatment options;
- undertake further analysis to better understand the risk;
- maintain existing controls; or
- reconsider objectives.

9.3 Controls and Risk Treatment or Action Plans

9.3.1 Existing controls should be identified and recorded on the Datix Risk Register against each risk. Documenting the current controls ensures that there is a clear indication of what is being relied upon to prevent the risk event from materialising. In addition, the team or individual that provides primary oversight over the control should document the key sources of assurance in relation to the control that are in place.

9.3.2 Risk treatment can be described as the process by which key controls are identified to mitigate a risk. The purpose of risk treatment is to select and implement the best options for addressing the risk.

9.3.3 There are four types of risk response that should be considered in determining the required action:

a) **Terminate.** Terminating or avoiding the activity or circumstance that gives rise to the risk or choosing another approach with a lower risk.

b) **Tolerate.** Accepting the consequences of the risk should it occur. This may be appropriate when the resources required to reduce the risk in other ways exceed the consequences of the risk occurring. If a risk is accepted, a contingency plan will be of increased importance.

c) **Transfer.** Transferring the risk by sharing it with or passing it onto suppliers, customers, or contractors, including the use of insurance and defined liability contracts. In practice, it is more likely that only some elements of a risk can be passed on: financial implications may pass down to a provider, but reputational risk relating to a service is more likely to be retained by the commissioning organisation.

d) **Treat.** Implementing controls and other mitigation actions (including contingency plans) that will reduce the likelihood and consequence of risks identified.

10 Risk Appetite or Tolerance Statement

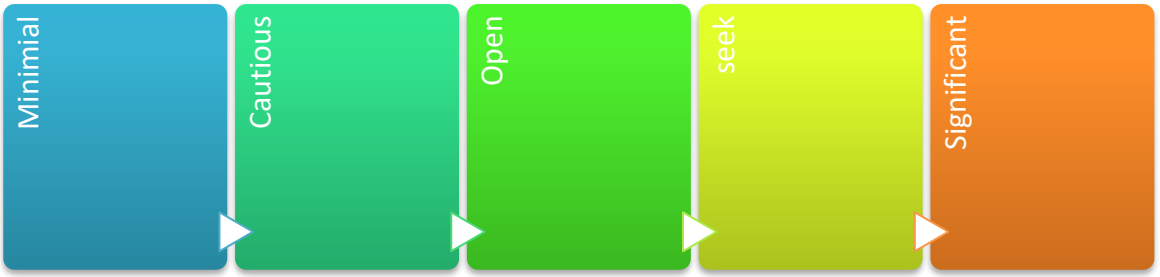
10.1 Risk appetite is the art of taking risks and exercising control while considering differing views at a strategic, tactical, and operational level. It provides consistency in the decision-making process, which will enable the ICB to take well-calculated risks when opportunities arise that will improve delivery, and conversely, to also identify when a more cautious approach should be taken to mitigate a threat.

10.2 Effective risk appetite framework generally includes the following three key principles:

- "Risk appetite should be aligned to the strategic objectives and considered a forward-looking view of an organisation"
- "Board and senior management should be actively involved, and strong accountability structures and clear incentives and constraints should be in place."
- "Risk appetite statements should be operationalised through use of the right level and type of information, fostering strong internal relationships, and establishing risk limits with actionable input for risk and business managers."

10.3 The Board are responsible for making the risk appetite statements for each risk domain, specifying the appetite level the ICB may or may not take, relative to objectives.

10.4 The Board have used the following risk appetite levels to produce the risk appetite statement for each domain. A full description of each risk appetite level for the listed risk domains can be found in *Appendix 2 – Risk Appetite Framework*.



Risk Appetite levels

10.5 The ICB have adopted the risk appetite statements listed in the table below on 24 May 2023. The risk appetite statements outline the level of risk the organisation is willing to accept in each risk domain. These statements enable the ICB to foster innovation and make decisions that may have higher rewards but also carry greater inherent risk compared to other options.

Risk Domains	Risk Appetite	Risk Score Matrix	Appetite statement
FINANCIAL How will we use our resources?	Seek	4	Consistently seek to use available funding to develop and sustain the greatest benefit to health and healthcare for our population and partners, accepting the possibility that not every programme will achieve its desired goals, on the basis that controls are in place.
COMPLIANCE AND REGULATORY How will we be perceived by our regulator?	Open	3	Conform with regulatory expectations but challenge them where we feel that to do so would be to improve outcomes for our residents.
INNOVATIONS, QUALITY AND OUTCOMES	Seek	4	• Pursue innovation and challenge existing working practices, seeking out and adopting new ways of working and new technologies to the benefit of the residents of Hertfordshire and West Essex • Operate with a high level of devolved responsibility • Accept that innovation can be disruptive and to use that as a catalyst to drive positive change
REPUTATION How will we be perceived by the public and our partners?	Seek	4	• We will be willing to take decisions that are likely to bring scrutiny to the organisation but where potential benefits outweigh the risks.

10.6 In recognising the evolving nature of their risk management processes due to the recent establishment of the organisation, the ICB sets an ambition to increase their risk appetite in the future as their control measures, forward scanning, and responsive systems mature.

10.7 The defined risk appetite will provide the Executive Leads (risk owners) and risk leads with relevant information with which they may evaluate significance of risks to ICB objectives and thus support decision-making processes.

11 Recording and Reporting

11.1 The focus of the ICB's Risk Management Policy is continuous proactive engagement on key risk issues as part of everyday business management. One output of this is the on-going process of reporting risks and controls. Reporting of risk and control information is not a one-way process as it promotes oversight, challenge and business engagement that seeks to improve risk and performance.

12 Monitoring and Reviewing of Risks

12.1 The management of risk must be reviewed by the Board, Audit and Risk Committee and Executive Team (in addition to risk owners' with their respective leads) in order to:

- monitor whether the risk profile is changing;
- gain assurance that risk management is effective, or identify that further action is necessary if it is not effective;
- receive assurances available about risk management that deliver an overall opinion about risk management effectiveness; and
- comment on appropriateness of the risk management and assurance processes which are in place.

13 Risk Reporting Arrangements

Risk reporting flow diagram with reporting responsibilities is presented on the next page.

Discussion Forum:	Reporting requirements:
	Risk Report: • Assurance Framework, • Corporate Risk Register - 'Primary Risks' only (rating 16+).
	Assurance Report: • Assurance Framework, • Corporate Risk Register - 'Principal Risks' only (rating Amber 12+), • Provided summary of decisions made at Executive Meeting (including new risks and mitigated risks). • Risk 'deep dives'
	Reporting updates with regards to: • Assurance Framework, • Corporate Risk Register • Decisions about new risks and closure of mitigated risks.
	Risk Update Report: • Review of strategic and operational risks of the ICB against the risk appetite statement and tolerance levels. • Reviewing development of and compliance with the Risk Policy. • Proposing matters for escalation to the Executive and/or the Audit Committee, including risks from the health and care partnership.
	Identified risks within a Team should be discussed at an appropriate forum within Teams or Directorates monthly for appropriate review. Discussions should focus on: • Any new risks identified and agreement on their articulation and scoring. • Review of existing risks and changes in the mitigations or scoring. • Risks or matters for escalation/discussion the Executive Team or Risk Review Group as is appropriate.
	Risks are identified and reported to the risk owner through the ICB's web-based Risk Management system, currently Datix.
	Risks can be identified by a number of different parties including staff from Teams and Directorates. Risks are entered into the ICB's web-based Risk Management System (currently Datix) for formal reporting through the above chain.

14 Corporate Risk Register

14.1 The Corporate Risk Register contains risks that have a total risk score of 12+. The main aim of the Corporate Risk Register is to ensure that risks are actively and collectively managed by the Executive Team and reported to the Audit and Risk Committee. The objectives of the Corporate Risk Register and its review by the above is to:

- use a systematic approach to provide an overall understanding of the ICB's risk exposure and level of assurance over the effectiveness of the control environment in the ICB's key functions.
- Ensure consistency across the ICB in our risk management approach and provide opportunity for discussion and challenge.
- provide a basis for early warnings; and
- identify actions for improvement (above and beyond those already identified / being pursued).

14.2 This process is reliant upon those who have been assigned ownership of risks acknowledging and taking professional responsibility for the management of those risk. Ensuring that risks are aligned with the ICB's strategic objectives and recognising that one risk may impact on the achievement of several objectives.

15 Directorate Risk Registers

15.1 Each directorate and, where deemed appropriate, distinct functions within a directorate, should maintain and review its own register of risks on Datix with all scoring risks present for review. These risks should be discussed at least monthly at team meetings.

15.2 Risks that have been assessed to have a rating of 12 or above must be reviewed by the Executive Director for the directorate and will be included in the Corporate risk Register for wider awareness and discussion.

16 Risk closure

16.1 Risks can be considered for closure if the risk no longer applies (i.e., the process that gave rise to the risk no longer exists) or the risk has reached its target level and no outstanding actions remain. Risk closure is decided by the Risk Owner (Executive Director) after the appropriate evidence and update is recorded on Datix to ensure an appropriate audit trail is maintained.

16.2 There are two categories for closed risk which determine the level of ongoing review:

- Risk still exists but is within target level. These risks will be reviewed once a year to ensure they remain at the target level.
- Risk no longer applies. These risks will not be subject to further review.

17 Assurance Framework

17.1 Assurance is about providing evidence of adequate levels of confidence that risks to objectives are controlled. However, it is acknowledged that it is never possible to provide complete and absolute assurance, and as such the concept of positive or negative assurance is adopted.

17.2 The assurance framework is an integral part of an ICB's risk management strategy rather than a stand-alone activity and is an integral part of the risk management framework used to effectively achieve the ICB's objectives and outcomes. The Audit and Risk Committee is delegated regular assurance monitoring by the Board.

17.3 A diagram that outlines the ICB's full assurance process can be found in *Appendix 3 - Assurance Process Diagram.*

18 Levels of Assurance

18.1 The aim of obtaining assurance is to ensure sufficient and appropriate evidence, to support confidence that a risk is well mitigated. The higher the level of assurance provided, the greater the confidence in the risk management. The Risk Owners and Leads will achieve this by conducting a more in-depth assessment of the assurance. The following are the two common levels of assurance that can be obtained.

- **Positive assurance (+).** This could mean that either a 'reasonable' or 'substantial' level of assurance is evidenced, not that there is an absolute level of assurance.
- **Negative assurance (-).** This could mean that there is either 'no assurance' or only a 'partial/limited' level of assurance.

18.2 Assurance mapping ensures alignment between assurance activities, controls, and the HWE ICB's objectives and risks. The Risk Lead in Datix maps the sources of assurance within the 'three lines of defence' to the risk controls to rate the levels of assurance. There are four levels, including Substantial, Reasonable, limited and None identified. This structure is already integrated into Datix, with Risk Leads responsible for updating relevant fields when reviewing risks.

19 Three Lines of Defence

19.1 To ensure the effectiveness of the ICB's risk management framework, the board and senior management have adopted the 'Three Lines of Defence' model, which is a way of explaining the relationship between the oversight functions within the assurance process.

19.2 First Line of Defence

The internal control framework that enforces required behaviours and working practices throughout the ICB's day-to-day activities. For example: policies, processes, systems, procedures, protocols, professional standards, codes of conduct, etc. Operational management

has ownership, responsibility, and accountability for assessing, controlling, and mitigating risks together with maintaining effective internal controls.

19.3 Second Line of Defence

Oversight functions that: undertake scrutiny; facilitate and implement effective risk management practices by operational management; assist the risk owners in defining the target risk exposure; and report adequate risk related information through the organisation.

For example: governance, compliance framework, financial control, quality, external performance, and commissioning responsibilities, reported to the board.

19.4 Third Line of Defence

Functions providing independent and objective challenge and assurance with regard to the ICB's governance arrangements. For example, Internal Audit, External and other independent assurance providers and regulators.

20 Training

20.1 Embedding of the Risk Management Policy will be supported by a range of training options for all staff delivered by the Governance team and external consultants.

20.2 It is essential that all staff are aware of the Risk Management Policy and their role in implementing it. Embedding of this Risk Management Policy across the ICB is essential to facilitate delivery of effective governance arrangements.

21 Appendices

Please see next page.

Appendix 1 – Risk Matrix Descriptors

Consequence (C) levels descriptors

Risk domains	1. Negligible	2. Minor	3. Moderate	4. Major	5. Catastrophic
Data Protection and Information Security	No adverse effect There is absolute certainty that no adverse effect can arise from the breach	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job	Potentially Some adverse effect An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.	Potentially Pain and suffering/ financial loss There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.	Death/ catastrophic event
Clinical Quality and Patient Safety (Including equipment)	No risk of negative impact to ICB	Small risk of delay in patient receiving the required care Small risk of negative impact to ICB Guidance not regularly reviewed.	High risk of delay in patient receiving the required care High risk of negative impact to ICB, and possibly consequences to commissioned services. Guidance insufficient / poor training.	Serious risk of delay in patient receiving the required care Serious risk of harm to patients due to poor commissioning. Investigation resulting in identification of serious omission on the part of the part of the ICB to consider quality and safety in commissioning decisions.	Potential to cause one or a number of fatalities. Compliance breach, causing serious fine, investigation, legal action.
Strategy, Innovation/ Performance/ Outcomes	Minimal impact upon productivity, costs or quality	Small risk of impact upon productivity, e.g., waiting times, patient outcomes. Small risk of impact upon delivery of QIPP schemes (if applicable)	High risk of impact upon productivity e.g., waiting times, patient outcomes High risk of impact upon delivery of QIPP schemes (if applicable)	Significant risk of impact upon productivity e.g., waiting times, patient outcomes. High risk of impact upon delivery of QIPP schemes (if applicable).	Significant risk of negative impact upon patients, providers and/or the ICB i.e., non- delivery of key objectives; loss of percentage of budget
Reputational	Rumours Potential for public concern	Local media coverage and discussions on social media short- term reduction in public confidence Elements of public expectation not being met	Local negative and critical media coverage and discussions on social media leading to medium-term reduction in public confidence MPs and stakeholders raise concerns with ICB	Sustained negative and critical local media coverage and discussions on social media National negative media coverage for less than 3 days MPs and stakeholders raise concerns with ICB NHS England and Improvement or DHSC raises concerns with ICB.	National negative media coverage for more than 3 days MPs and stakeholders raise concerns in public fora (e.g. questions in the House of Commons or critical media articles) Total loss of public confidence

Risk domains	1. Negligible	2. Minor	3. Moderate	4. Major	5. Catastrophic
Human resources/ organisational development/ staffing/ competence	Short-term low staffing level that temporarily reduces service quality (< 1 day)	Low staffing level that reduces the service quality	Late delivery of key objective/ service due to lack of staff Unsafe staffing level or competence (>1 day) Low staff morale Poor staff attendance for mandatory/key training	Uncertain delivery of key objective/service due to lack of staff Unsafe staffing level or competence (>5 days) Loss of key staff Very low staff morale No staff attending mandatory/ key training	Non-delivery of key objective/service due to lack of staff Ongoing unsafe staffing levels or competence Loss of several key staff No staff attending mandatory training /key training on an ongoing basis
Statutory duty/ inspections / Regulatory Action/Legal	No or minimal impact or Breach of guidance/ statutory duty	Breach of statutory Legislation Reduced performance rating if unresolved	Single breach in statutory duty Challenging external recommendations/ improvement notice	Enforcement action Multiple breaches in statutory duty Improvement notices Low performance rating	Multiple breaches in statutory duty Prosecution Complete systems change required Zero performance rating Severely critical report
Governance/ Business objectives/ projects	Insignificant cost increase/ schedule slippage	<5 per cent over project budget Schedule slippage	5–10 per cent over project budget Schedule slippage	Non-compliance with national 10–25 per cent over project budget Schedule slippage	Incident leading >25 per cent over project budget Schedule slippage Key objectives not met
Finance including claims	Small loss Risk of claim remote	Loss of percentage of budget Claim less than £10,000 Up to 0.05%	Loss of percentage of budget Claim(s) between £10,000 and £100,000 Up to 0.15%	Key objectives not met Uncertain delivery of key objective/Loss of per cent of budget Claim(s) between £100,000 and £1 million Purchasers failing to pay on time Up to 0.5%	Non-delivery of key objective/ Loss of per cent of budget Failure to meet specification/ slippage Loss of contract / payment by results Claim(s) >£1 million Over 0.5%
Health and Safety	Minimal effect on staff	Potential for minor harm or intruding into normal non-working time	Incident requiring hospital treatment for more than one member of staff. Intrusion into normal non-working time	Significant injuries, potential death. Major intrusion into staff's time	Deaths and / or major effect on staff lives
Technology/- Service/ Business interruption/ Environmental impact	Loss/interruption of >1 hour Minimal or no impact on the environment	Loss/interruption of >8 hours Minor impact on environment	Loss/interruption of >1 day Moderate impact on environment	Loss/interruption of >1 week Major impact on environment	Permanent loss of service or facility Catastrophic impact on environment

Likelihood (L) levels descriptors

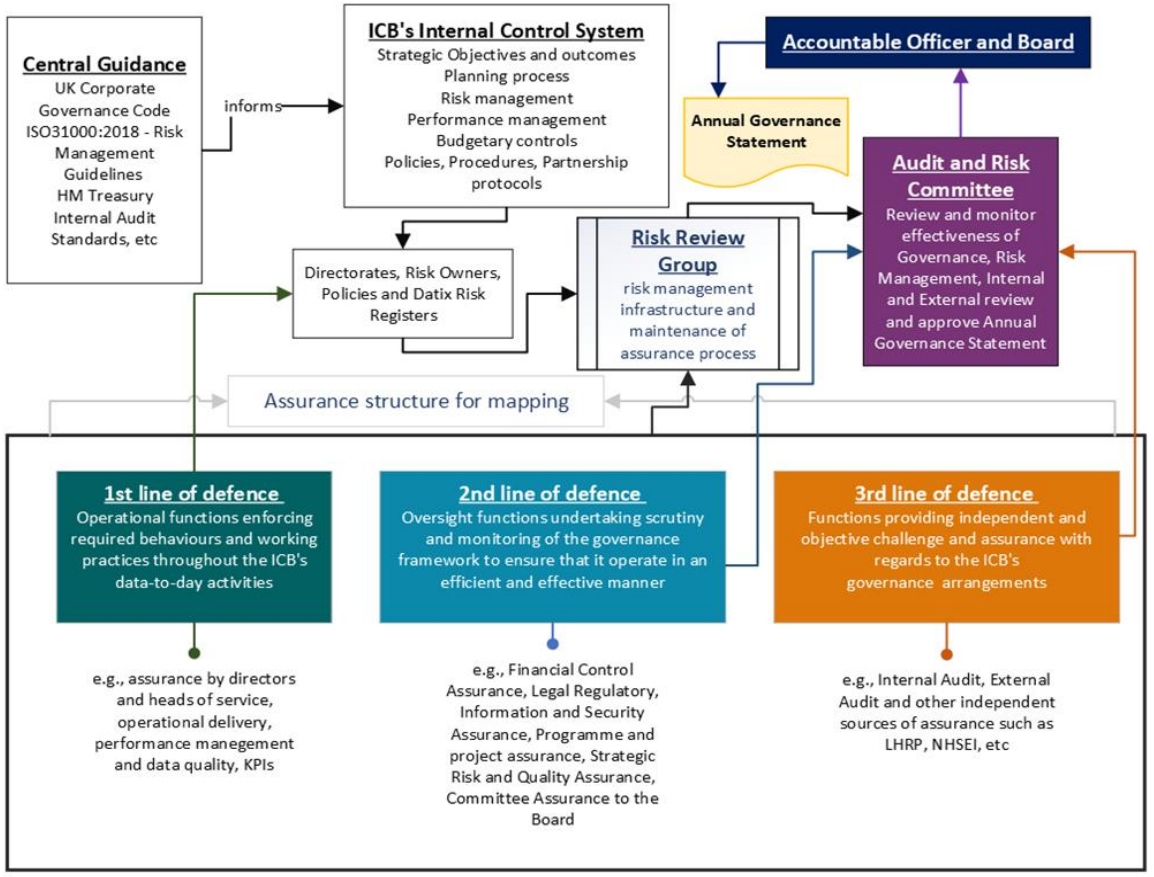
Descriptor	1. Rare	2. Unlikely/	3. Possible	4. Highly Likely	5. Almost certain
Frequency How often might it/does it happen	This will probably never happen/recur or There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence	Do not expect it to happen/recur but it is possible it may do so or In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected	Might happen or recur occasionally or It is likely that there will be an occurrence of an adverse effect arising from the breach	Will probably happen/recur but it is not a persisting issue or There is almost certainty that at some point in the future an adverse effect will happen	Will undoubtedly happen/recur, possibly frequently or There is a reported occurrence of an adverse effect arising from the breach.

Appendix 2 – Risk Appetite Framework

RISK APPETITE LEVEL ▶ / RISK TYPES ▼	0 NONE Avoidance of risk is a key organisational objective.	1 MINIMAL Preference for very safe delivery options that have a low degree of inherent risk and only a limited reward potential.	2 CAUTIOUS Preference for safe delivery options that have a low degree of residual risk and only a limited reward potential.	3 OPEN Willing to consider all potential delivery options and choose while also providing an acceptable level of reward.	4 SEEK Eager to be innovative and to choose options offering higher business rewards (despite greater inherent risk).	5 SIGNIFICANT Confident in setting high levels of risk appetite because controls, forward scanning and responsive systems are robust.
FINANCIAL **How will we use our resources?**	We have no appetite for decisions or actions that may result in financial loss.	We are only willing to accept the possibility of very limited financial risk.	We are prepared to accept the possibility of limited financial risk. However, VFM is our primary concern.	We are prepared to accept some financial risk as long as appropriate controls are in place. We have a holistic understanding of VFM with price not the overriding factor.	We will invest for the best possible return and accept the possibility of increased financial risk.	We will consistently invest for the best possible return for stakeholders, recognising that the potential for substantial gain outweighs inherent risks.
REGULATORY **How will we be perceived by our regulator?**	We have no appetite for decisions that may compromise compliance with statutory, regulatory of policy requirements.	We will avoid any decisions that may result in heightened regulatory challenge unless absolutely essential.	We are prepared to accept the possibility of limited regulatory challenge. We would seek to understand where similar actions had been successful elsewhere before taking any decision.	We are prepared to accept the possibility of some regulatory challenge as long as we can be reasonably confident we would be able to challenge this successfully.	We are willing to take decisions that will likely result in regulatory intervention if we can justify these and where the potential benefits outweigh the risks.	We are comfortable challenging regulatory practice. We have a significant appetite for challenging the status quo in order to improve outcomes for stakeholders.
QUALITY **How will we deliver safe services?**	We have no appetite for decisions that may have an uncertain impact on quality outcomes.	We will avoid anything that may impact on quality outcomes unless absolutely essential. We will avoid innovation unless established and proven to be effective in a variety of settings.	Our preference is for risk avoidance. However, if necessary we will take decisions on quality where there is a low degree of inherent risk and the possibility of improved outcomes, and appropriate controls are in place.	We are prepared to accept the possibility of a short-term impact on quality outcomes with potential for longer-term rewards. We support innovation.	We will pursue innovation wherever appropriate. We are willing to take decisions on quality where there may be higher inherent risks but the potential for significant longer-term gains.	We seek to lead the way and will prioritize new innovations, even in emerging fields. We consistently challenge current working practices in order to drive quality improvement.
REPUTATIONAL **How will we be perceived by the public and our partners?**	We have no appetite for decisions that could lead to additional scrutiny or attention on the organisation.	Our appetite for risk taking is limited to those events where there is no chance of significant repercussions.	We are prepared to accept the possibility of limited reputational risk if appropriate controls are in place to limit any fallout.	We are prepared to accept the possibility of some reputational risk as long as there is the potential for improved outcomes for our stakeholders.	We are willing to take decisions that are likely to bring scrutiny of the organisation. We outwardly promote new ideas and innovations where potential benefits outweigh the risks.	We are comfortable to take decisions that may expose the organisation to significant scrutiny or criticism as long as there is a commensurate opportunity for improved outcomes for our stakeholders.
PEOPLE **How will we be perceived by the public and our partners?**	We have no appetite for decisions that could have a negative impact on our workforce development, recruitment and retention. Sustainability is our primary interest.	We will avoid all risks relating to our workforce unless absolutely essential. Innovative approaches to workforce recruitment and retention are not a priority and will only be adopted if established and proven to be effective elsewhere.	We are prepared to take limited risks with regards to our workforce. Where attempting to innovate, we would seek to understand where similar actions had been successful elsewhere before taking any decision.	We are prepared to accept the possibility of some workforce risk, as a direct result from innovation as long as there is the potential for improved recruitment and retention, and developmental opportunities for staff.	We will pursue workforce innovation. We are willing to take risks which may have implications for our workforce but could improve the skills and capabilities of our staff. We recognize that innovation is likely to be disruptive in the short term but with the possibility of long term gains.	We seek to lead the way in terms of workforce innovation. We accept that innovation can be disruptive and are happy to use it as a catalyst to drive a positive chan.

WWW.GOOD-GOVERNANCE.ORG.UK

Appendix 3 – Assurance Process Diagram



Appendix 4 – Equality and Health Inequalities Analysis

Equality Analysis

Title of policy, service, proposal etc being assessed:
Risk Management Policy

What are the intended outcomes of this work? The Risk Management policy will support the HWEICB's strategic direction and objectives, as well as staff duties and responsibilities in understanding and creating an effective risk profile, management's controls to reduce risks, and the mapping of assurances to ensure the Board is aware of known and new risks.
How will these outcomes be achieved? The Risk Management Policy v1.3 will be published and distributed to all employees. This policy will guide ICB's risk management activities. It will replace version 1.0, adopted on 1 July 2022.
Who will be affected by this work? There is no scope for differential impact based on a person's characteristic.

Evidence
Impact Assessment Not Required This is a risk management policy at the highest level. It has no impact on those who have or share a protected characteristic. It specifies critical and/or priority actions as actions that ensure there is no impact on people.

Having considered the proposal and sufficient evidence to reach a reasonable decision on actual and/or likely current and/or future impact I have decided that a full equality impact assessment is not required.	
Assessor's name and job title Date	Paul Curry, Equality and Diversity Lead 30 November 2022