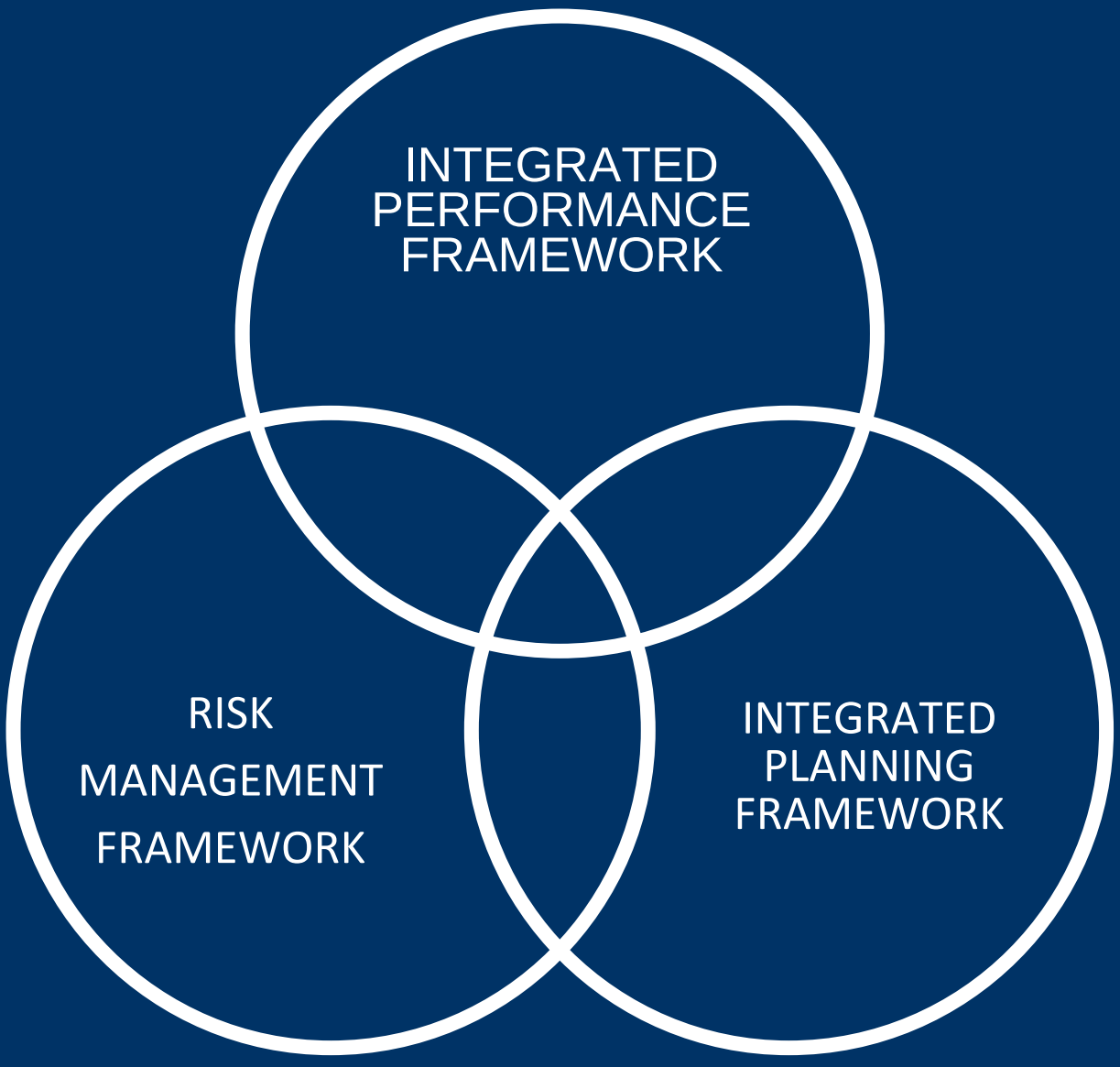
GIG CYMRU NHS WALES

Bwrdd Iechyd Prifysgol
Betsi Cadwaladr
University Health Board

RISK MANAGEMENT FRAMEWORK

2025-28



Author & Title	Director of Corporate Governance Head of Risk Management		
Responsible Department / Director:	Corporate Governance > Risk Management Chief Executive		
Approved by:	Health Board – 27 November 2025 Audit Committee (AC) – 21 October 2025 Executive Committee 17 September 2025		
Date approved:	27 November 2025		
Date activated (live):	7 January 2026		
Documents to be read alongside this document:	Risk Management Procedures (RM02) Risk Management Training Procedures (RM03) Terms of Reference Risk Scrutiny Group BCUHB Integrated Performance Framework BCUHB Integrated Planning Framework Health and Safety Policy (HS01) Risk Assessment Guidance (HS03) Concerns Policy and Procedure (PTR01 and PTR01A) Information Governance Policy Health and Safety Policy		
Date of next review:	28 September 2028		
Date EqIA completed:	December 2025 (Original 2016)		
Date IAST completed:	December 2025		
First Operational:	28 Sept 2023		
Previously reviewed:	Sept 2023	Health Board - 25 July 2024 Audit Committee (AC) - 18 July 2024 Executive Team 26 June 2024	Sept 2025
Changes made yes/no:	Yes - 28 Sept 2023 Approved at Board Major revisions made	Yes - Intermediate updates; as approved at: 18/07/2024 Audit Committee and 25/07/2024 Health Board Meeting– Formalisation of the Risk Scrutiny Group, and key updates to the Risk Framework and Procedures.	Yes - Intermediate updates- Escalation route

CONTENTS

GLOSSARY OF TERMS

Risk: A risk is the uncertainty that something could or may happen that will have an impact on the achievement of the Health Board's objectives and priority areas. Risk is expressed in terms of likelihood (probability of the risk occurring) and consequence (impact if the risks were to occur).

Distinguishing between a risk and an issue: A risk is an event that might occur and that could have an effect (can be positive but usually negative) upon the organisation and/or its stakeholders. A risk is characterised by uncertainty. An issue is something that has already happened or will definitely happen. An issue is a certainty. For example, 'we are short staffed' or 'lack funding to deliver a service', are issues (as these are already happening) and the risk will be the implications of staff shortage or the lack of funding to the successful delivery of our operational and strategic objectives. What these uncertainties (doubt) may cause, is what will constitute (give rise) to risks in both cases.

Assurance: This is a process to provide evidence that the controls in place are effective and working and that the Health Board is doing its best to appropriately reduce and manage risks to the achievement of its operational and strategic objectives.

Actions: Actions are the subsequent steps required following the application of controls to address or further mitigate residual (current) risk to as low as reasonably possible (target) level.

Board Assurance Framework: comprises of strategic risks developed by Board members from the Strategic Plans and Objectives that could prevent the Health Board's from fulfilling its strategic objectives/priorities.

Business Continuity: Business continuity is the capability of the Health Board to continue the delivery of products and services within acceptable timeframes at predefined capacity during a disruption. Business continuity is a temporary and alternative measure initiated during a disruption that ensures continuity of service provision whilst a permanent solution is found, or usual services/operations are resumed. The holistic process of business continuity management is an essential tool in ensuring an organisation's resilience.

Controls: These are measures or interventions implemented by the Health Board that reduce the likelihood of a risk and/or the impact/severity of a risk. The types of controls used in reducing risks include preventive, corrective, detective and directive controls. Gaps in control describe the weaknesses identified having put mitigation controls in place.

Corporate Risk Register: A corporate risk register is a repository used to record significant risks that could impact the strategic objectives and operations of the Health Board. Developed by services, corporate functions and members of the Executive Committee, the register provides a comprehensive overview of the key risks facing the organisation. It is a pivotal tool to help proactively strengthen risk oversight and management.

Risk Assessment: This is the overall process of risk identification, analysis and risk evaluation. This is achieved by identifying risks, examining the characteristics of each risk and comparing individual risks against the Health Board's risk appetite. Risk assessment techniques include questionnaires and checklists, workshops and brain storming sessions, and inspections and audits.

Risk Appetite: The amount and type of risk that an organisation is willing to seek or retain in its pursuit of its objectives.

Risk Framework: Set of activities that support the risk management process, i.e., the risk architecture, strategy and protocols.

Risk Management: Coordinated activities to direct or control risks within an organisation. These are management activities that deliver the most favourable outcome and reduce the volatility and variability of that outcome.

Risk Mitigation: This refers to the process of reducing risk exposure through minimising its likelihood and/or lessening the severity of its impact were it to materialise. Types of risk mitigations include the 5Ts (treat, tolerate, terminate, transfer or take opportunity).

Senior Information Responsible Risk Officer (SIRO): This may include the Director responsible for the Directorate or Executive Director or Deputy Executive Director or nominated Executive Sponsor.

Take Opportunity: The type of risk with potential to enhance the achievement of the organisation's objectives. Opportunity risk management is the approach that seeks to maximise on benefits of taking risks i.e., innovation, new systems, processes and procedures, services etc.

Terminate: Risk response that is appropriate when certain activities that give rise to risks are not necessary or worth doing and should be stopped. Also known as avoidance or elimination.

Tolerating: The decision to accept the risk and the impact should the following risk occur without taking any further steps to mitigate it. This is often to avoid significant investment or resources as the response would be disproportionate to the potential harm or gain. Also referred to acceptance or retention. Decision to tolerate any risks that are outside the risk appetite threshold for a particular domain of risk should be made at senior level proportionate to the level of risk.

Transfer: Risk response for risks outside the Health Board's appetite that the organisation wishes to transfer or share with other providers by way of contracts (outsourcing), insurance, joint venture etc. This option is particularly suited to mitigating financial risks or risks to assets.

Treat: Risk response by way of introducing cost effective controls to alter or reduce risk.

Target Risk: Ultimate level of risk that is desired by the Health Board when planned additional controls (see actions) have been implemented to address residual risk to as low as reasonably possible and/or within the Health Board's risk appetite.

RISK MANAGEMENT FRAMEWORK

- The Health Board endeavours to establish a positive risk and safety culture in the organisation, where unsafe practice (clinical, managerial, etc.) is not tolerated and where every member of staff is committed and empowered to identify/correct/escalate system weaknesses.
- The Health Board is committed to ensuring a robust infrastructure to manage risks ensuring an integrated approach, and where risks crystallise, to evidence improvement.
- The Health Board's intention is to ***minimise*** the risk to the delivery of quality services in the Health Board's accountability and compliance frameworks, ***maximise*** performance and is ***open*** to opportunity with considered risk taking.
- To deliver ***safe, quality*** services, the Health Board will encourage staff to work in collaborative partnership with each other and service users and carers to ***minimise*** risk to the greatest extent possible and promote patient well-being as a duty of care to the population.

The Board intends to demonstrate an ongoing commitment to improving the management of risk throughout the organisation by:

• Ensuring a dynamic approach to strategic risk management to support achievement of the Health Board's vision, aims, and strategic objectives;

• Promoting considered risk taking, within authorised and defined limits in-line with the Board's appetite for risk (see Appendix 1-Risk Appetite Statement);

• Adopting an integrated approach to risk management in order to facilitate a cross-functional collaboration of system-wide risks that includes risks related to: clinical care, health and safety, staff wellbeing, financial and business planning, workforce planning, corporate and information governance, performance management, project / programme management, research and development;

• Embedding effective risk management systems and processes within the organisation and promoting the ethos that risk management is everyone's business, with clearly defined roles and responsibilities;

• Creating an environment that is as safe as is reasonably practicable, by ensuring that risks are continuously identified, assessed and well managed, i.e. where possible eliminate, transfer or treat risks to an acceptable level;

• Fostering an organisational culture of openness and willingness to report risks, incidents and near misses to ensure organisation wide learning;

• Establishing clear and effective communication mechanisms that enable a comprehensive understanding of risks at all levels of the organisation by the use of directorate, specialist and organisational-wide risk registers; and

•Providing appropriate training to staff to ensure effective implementation of risk management arrangement

1. PURPOSE OF THIS FRAMEWORK

The Framework seeks to ensure:

- that the Health Board's risks in relation to the delivery of services (provided and commissioned) and care to patients are minimised;
- that the wellbeing of patients, staff and visitors is optimised;
- that opportunities are maximised;
- that the assets, business systems and finances of the Health Board are protected; and
- the implementation and ongoing management of a comprehensive, integrated (clinical and non-clinical) approach to the management of risk across the organisation.

2. SCOPE OF THE RISK MANAGEMENT FRAMEWORK

This framework applies to Board members; all staff of the Health Board; agency staff; contractors brought in to undertake work on behalf of the Health Board, for example capital and estates works; students; locums; volunteers; individuals employed on honorary contracts; and, other third parties engaged in Health Board business. It applies to all activities of the Health Board, including those related to the commissioning of services. Managers at all levels within the Health Board must take an active lead to ensure that risks are managed effectively and to support the development of a risk aware culture within the Health Board.

This framework will:

- Outline the risk management philosophy through our risk statement, identifying arrangements for embedding risk management;
- Explain the role, expectations and appetite of the Board in relation to risk and risk management;
- Detail the high-level roles and responsibilities for implementing and complying with this framework;
- Explain the arrangements for complying with all relevant legislation;
- Detail risk priorities for the present year;
- Detail the high-level Committee structure accountability in relation to risk, internal reporting requirements, assurance arrangements and external reporting controls;
- Signpost the specific policies, procedures and terms of reference and which the Health Board will publish to ensure that all staff understand what is required of them.

3. THE BOARD'S APPETITE FOR RISK

The Board recognises that risk is inherent in the provision and commissioning of healthcare services, and therefore a defined approach is necessary to articulate risk context, ensuring that the organisation understands and is aware of the risks it is prepared to accept in the pursuit of its aims and objectives.

Risks throughout the organisation will be managed within the Board's risk appetite, or where this is exceeded, action will be taken to reduce the risk. The Board is prepared to accept some financial risk and regulatory challenges if appropriate controls and defence strategies are in place. The Board support innovation despite potential short-term quality impacts and reputational risks, as long as there is potential for long-term rewards like improved outcomes for stakeholders and opportunities for staff recruitment, retention and development. The Board takes a holistic view of value for money, with price not being the sole determining factor.

The Health Board seeks to be innovative and will challenge current working practices and financial risk in terms of its willingness to take opportunities where positive gains can be anticipated. The Board's annual Risk Appetite, detailing acceptable levels of risk across five risk types (financial, regulatory/compliance, innovation, quality and reputational), is outlined in Appendix 1.

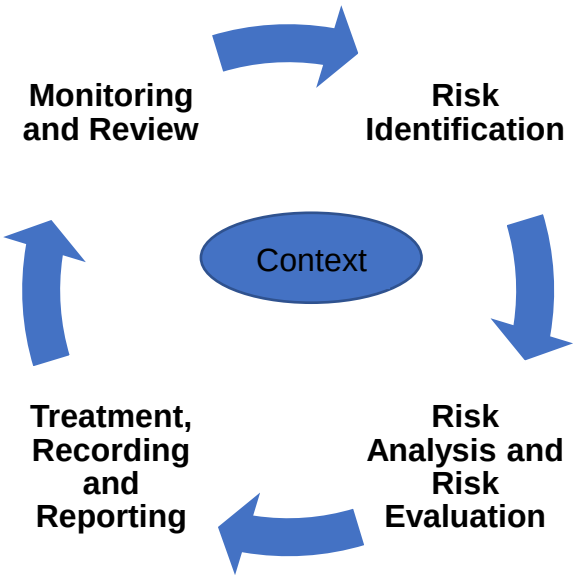
4. RISK MANAGEMENT PROCESS

Risk Management is the systematic application of management policies, practices and procedures to identifying, analysing, assessing, treating and monitoring risk in a way that will enable organisations to minimise losses and maximise opportunities.

The aim of risk management is not to remove risk altogether, but to manage risk to an acceptable level, considering the cost of minimising the risk and reducing risk exposure (the level of risk that the organisation is exposed to, either in regard to an individual risk or the cumulative exposure to the risks faced by the organisation).

The Board has adopted a structured approach to risk management, whereby risks are identified, assessed and controlled, and if appropriate, escalated or de-escalated through the governance mechanisms of the organisation. The process is defined in four key steps:

Figure 1 - Risk Management Process



1. RISK IDENTIFICATION

The Health Board cannot manage risk effectively unless it knows what the risks are. Risk identification is therefore vital to the success of the organisation's risk management process, and ultimately the safe delivery of care. This should be done within context.

2. RISK ANALYSIS AND RISK EVALUATION

Assessment and scoring of risk are used to determine the level of risk, using the Health Board's risk matrix to ensure a consistent approach is adopted across the organisation.

3. TREATMENT, RECORDING AND REPORTING

Treatment is how the risk will be managed, and what the required actions are to achieve an acceptable level of risk. All risks are recorded on a Datix risk register, which is a formal record of all risks raised, which makes up the Operational Risk Register.

4. MONITORING AND REVIEW

Part of managing risk is to continually review and update, and to capture the changes and progress of mitigation.

5. RISK ARCHITECTURE

The current enterprise risk architecture within the Health Board is shown below in a risk management model.

LEVELS OF RISK

The Risk Management Framework defines three levels of risk:

1. Strategic Risks – Risks that represent a threat to achieving the Health Board's strategic objectives or its continued existence. Strategic risks also include risks that are widespread beyond the local area, and risks for which the cost of control is significantly beyond the scope of the local budget holder.

2. Operational Risks – Risks that arise as a result of the day-to-day running of the Health Board and include a broad spectrum of risks comprising clinical risk (e.g., arising from incidents and complaints), financial risk (including fraud); legal risks (e.g., arising from employment law or health and safety regulation); regulatory risk; risk of loss or damage to assets or system failures; etc.

3. Project Risks – Risks that may impact on the delivery of a programme of work or project. All significant projects must be risk assessed before they are progressed, with each project required to have a separate risk register.

RISK REGISTERS

Board Assurance Frameworks, Corporate Risk Registers and Operational Risk Registers can work together in an integrated risk management model:

Board Assurance Framework (BAF)

- Focuses on the top <10 strategic risks that could impact achievement of the Health Boards objectives and priorities.
- Owned by the Board and tied directly to the strategic plan.
- Risks reflect external and internal issues affecting strategy.
- Regularly reviewed by Board and Executive Committee.
- Held by the risk team.

Corporate Risk Register (CRR)

- Consolidates key risks escalated up from the operational level based on the possible impact on Boards objectives and priorities. May include 10-40 major corporate-wide risks.
- Provides Executive Committee with enterprise view of significant operational and strategic risks.
- Enables corporate risk reporting, monitoring and oversight.
- Risk flows to BAF as appropriate.
- Overseen by the corporate risk team, maintained on Datix.

Operational Risk Registers

- Day to day operational risks which impact on service delivery. Includes clinical, financial, compliance, IT risks etc.
- Mandatory for all services to have a register on Datix.
- Service Risk Leads or Risk Champions responsible for maintaining and managing service risk register and escalates higher risks through Senior Responsible Officers and Corporate Risk Team for awareness and where appropriate consideration on the CRR.

Project Risks

- Project lead responsible for ensuring risks are captured and maintained.
- Acceptable for the project risk register to be held locally (not on Datix) but significant risks which could impact on day to day operations or have a wider impact on the Health Board should be escalated to a Datix risk register to allow for overview and consistency of reporting.
- Project team escalate higher risks through Senior Responsible Officers and Risk Scrutiny Group for awareness.

This model provides top-down and bottom-up connectivity to enable robust risk management at all levels and alignment to strategy.

All staff should be aware of the potential for risks to emerge which may affect the business of the Health Board and all staff should be prepared to identify and report risks as appropriate. When a possible risk is identified, staff should aim to discuss it first with their line manager. This is to avoid duplication of effort, as sometimes risks are identified which are already being managed but have perhaps been articulated differently. Once it is confirmed that a new risk has been identified, the details should be entered onto the Datix system. This will normally be achieved through a service risk lead/champion.

Once correctly identified and assessed, the risk should be logged on a risk register, depending on the seriousness of the risk. Where possible risks should be managed at the lowest level possible, proportionate to the level of exposure to which the risk.

Risks scored ≥15 should be sent to the Senior Information Responsible Risk Officer (SIRO) *(N.B. this may include the Director responsible for the Directorate or Executive Director or Deputy Executive Director or nominated Executive Sponsor)*, for awareness and consideration on the CRR, if critical/strategic in nature. Operational risks scored ≥20 should be sent to the most senior responsible person for management support and advice.

Risks scored 9>12, Risk owners are expected to ensure that there are appropriate processes, systems and governance arrangements in place to regularly review, scrutinise and effectively manage all risks within their areas. They will be required to

periodically present their Divisional risk register reports and assurance of robust risk arrangements to the Risk Scrutiny Group.

Risks scored 1-8 should be regularly reviewed, scrutinised, approved, reduced and managed at the service or departmental levels while those which score above 8 should be escalated in accordance with guidance and the approval of either the relevant quality and safety meeting and/or the triumvirate.

ESCALATION/DE-ESCALATION

Risks should be regularly reviewed and escalated or de-escalated to the appropriate risk register within the Committee or divisional meeting which reviews the risk. Before a risk is presented to a SIRO for approval, it should be quality assured by the Corporate Risk Team and take the assurance that robust action plans are in place.

For escalation of a risk on to the CRR the service risk lead should contact their Executive Director through the appropriate channels and the corporate risk team via their regional risk manager.

Figure 2 - Risk Management Meeting & Escalation/De-escalation

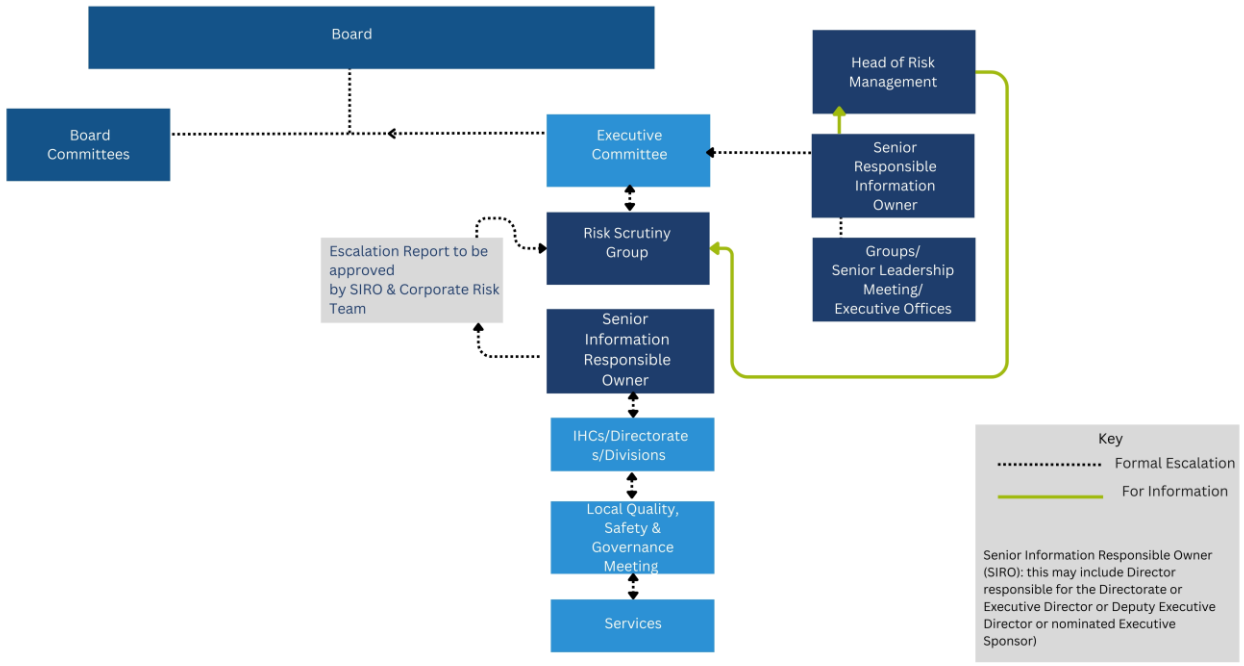
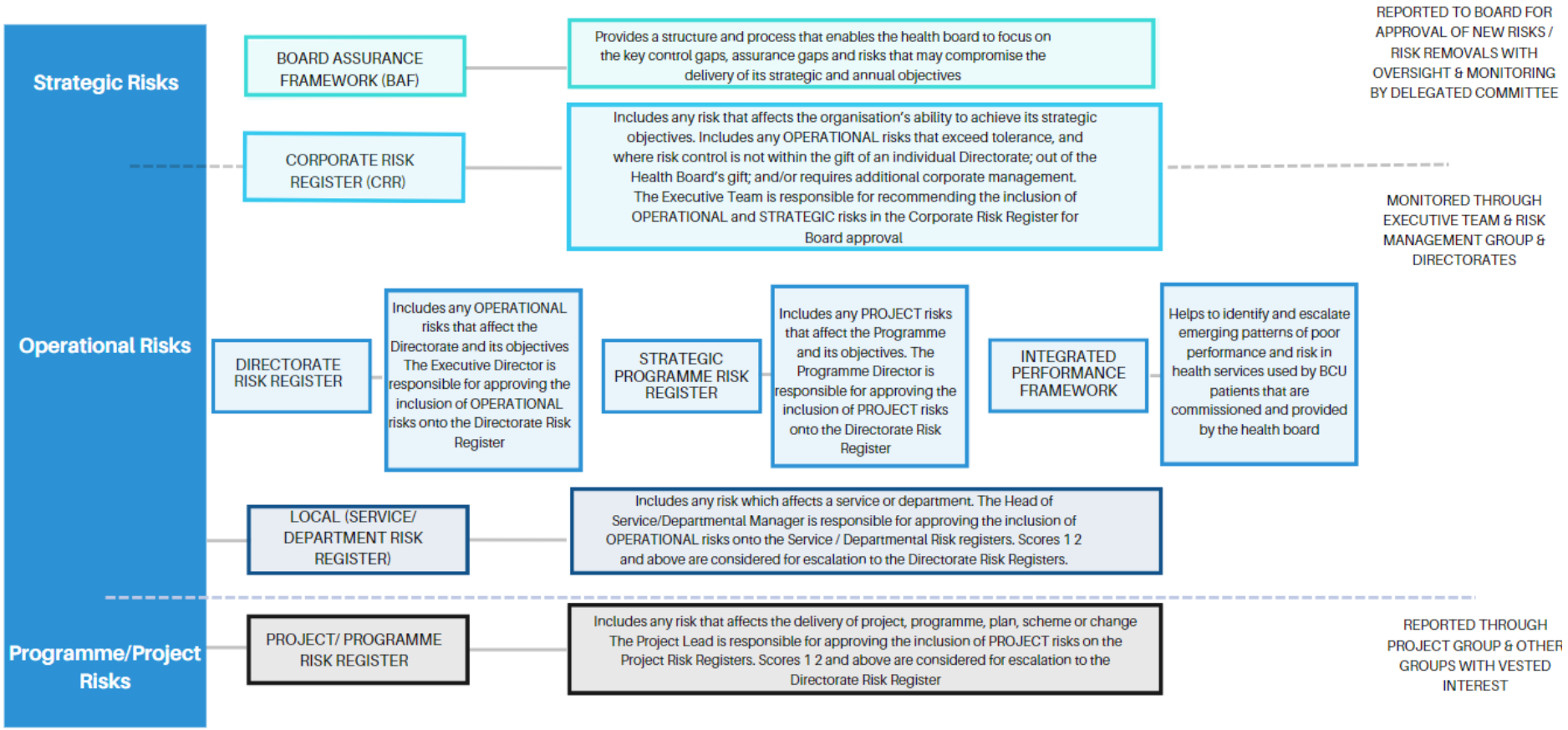


Figure 3 - Risk Management Register



6. RISK STRATEGY

To effectively manage risks, our organisation will take a comprehensive approach across several areas. This will include robust reporting mechanisms to keep leadership and the Board apprised of risks, using systems like risk registers to log and track risks, ensuring staff have adequate training and clear responsibilities, implementing standardised risk management processes, fostering a culture of openness around risks, and continuously monitoring and improving through quality assurance. Together these initiatives across reporting, systems, people, processes, culture and improvement will enable us to better anticipate, manage and mitigate the risks we face in alignment with our values and strategic objectives.

Reporting

- Services to provide their directorates on assurances over the management of the local service risk register.
- Risk Scrutiny Group to oversee risk processes in line with procedures to supports continuous improvement and monitoring of trends in relation to KPIs (outlined in RM02).
- Corporate risk report to Executive Committee and Board Committees on risk actions plans and updates. Terms of reference and cycle of businesses for all support risk as a standing agenda item.
- Board Assurance Framework (BAF) risk report to Board.

Figure 4 – Strategic Register Reporting Cycle

Register /Tier	Review	Formal Review	Approval Escalation/ De-	Committee Oversight	Board
Board Assurance Framework	Reviewed Bi-Monthly	Risk Scrutiny Group	Executive Committee Meeting	Quarterly	Bi-Annually (or any escalations via Audit Committee Chair's report)
Corporate Risk Register				Quarterly	Quarterly

Systems

- Datix to be used to log risks.
- Risk priorities will influence integrated planning.

Processes

- Process in relation to risk management procedures are detailed in RM02 'Risk Management Procedures' and throughout this framework as well as RM03 outlines 'Risk Management Training Procedures' and plans. Risk identification, assessment and treatment processes as detailed in section 4.
- Risk monitoring and review processes, risk reporting and escalation processes.

Culture

- The cultural tone is detailed in the statement and approach to risk as well as supported by the way in which processes are carried out, dynamic and diligence. Risk clearly noted as everyone's business and supported by detailing responsibilities.

People

- Risk management responsibilities are clear for all staff and have been further detailed in section 7.
- The Health Board is committed to continuous learning which applies across risks management. Training as a part of ensuring continuous improvement is crucial. Knowledge of good identification processes and how to manage risk is essential to the successful embedding and maintenance of effective risk management. To support this, a programme of training will be delivered as follows:

Staff Group	Training Need	Frequency
Board Members & Directors & Deputies	Strategic Risk Management Training	Every 2 years
Service managers/Risk owners/Service Risk Leads	Mandatory Operational Risk Management Training	Every 2 years
All staff	Basic awareness on corporate induction as well as a bespoke offer of face to face or virtual risk training	On starting and ad hoc offer as required (Patient safety mandatory module contains risk management awareness for clinical staff)

Strategic (BAF) Risks:

The ‘three lines of assurance’ have been outlined in relation to independent and objective audits and reviews of risk management practices ‘The three lines of assurance’ includes internal/external audit, regulators, professional body reviews and scrutiny. Provides assurance to senior management and Board on effectiveness of risk management.

The three lines of assurance also clarify roles for review and oversight:

First line of assurance: Reviews by operational management

Second line of assurance: Oversight by risk management/compliance functions

Third line of assurance: Independent assurance from audit/regulators

This model structures risk management oversight at the Risk Scrutiny Group Executive Committee, Board Committees and Board levels for the Health Board.

7. ROLES AND RESPONSIBILITIES

Effective risk management requires clear definition of the roles, responsibilities, and accountabilities across the organisation. This section outlines the duties and obligations relating to risk for the Board, relevant Committees, key groups and individuals within the Health Board.

THE BOARD:

The Board (Executives, Directors and Independent Members) being the governing body responsible for strategy, performance, governance, risk management, and ensuring statutory duties are met. The Board is accountable for effective oversight per NHS (Wales) Act and other healthcare regulations.

The cycle of business for the Board is set to receive the CRR and BAF on a quarterly/bi-annual basis. It is the duty of the Board to discuss and advise on the content and progress of action plans in the BAF. It is also the duty of the Board to appropriately monitor BCUHB’s significant risks noted in the CRR, associated controls and assurances outline as well taking a view on the overall decision of tolerating a risk or challenging the possible lack of progression.

The Board is responsible for ensuring that the Health Board consistently follows the principles of good governance; ensuring that the systems, policies and people are in place to manage risks and its effectiveness. The Board will be focused on key risks and driving the delivery of the Health Board’s strategic objectives. Gaining assurance demonstrates good oversight of effective risk identification and management; risk architecture as well as due diligence including robust governance. It is a key principle of accountability.

The workplans for the Board and each of its Committees will be aligned to the BAF and CRR, ensuring appropriate focus on areas of risk. In the context of this Framework the Board will:

1. demonstrate its continuing commitment to risk management through the application and interest in the overall compliance with this Framework;
2. ensure, through the Chief Executive, that the responsibilities for risk management outlined in this document are communicated, understood and maintained;
3. take a proactive role in 'horizon scanning' for emerging threats/risks to the delivery of the Health Board's strategic objectives, and ensuring that controls put in place in response, manage risks to an acceptable level;
4. commit financial, managerial, technological and educational resources necessary to adequately control identified risks;
5. ensure that lessons are learned and disseminated into practice from complaints, claims and incidents, and other patient experience data;
6. oversee and participate in the risk assurance process;
7. allocate strategic risks to Committees for oversight;
8. ensure communication with partner organisations on problems of mutual concern including risks;
9. ensure that appropriate structures are in place to implement effective risk management; and
10. receive reports from the Committees of the Board in line with terms of reference and workplans of those committees.

AUDIT COMMITTEE (AC):

Provides assurance on governance, risk management, internal controls, financial reporting and internal/external audits. The Committee is responsible for points 1-5 as noted above.

The cycle of business for the Committee is set to receive the CRR and BAF in its entirety on a bi-monthly basis. The Audit Committee, on behalf of the Board, will be responsible for providing oversight of the adequacy and management of the CRR and BAF arrangements.

PERFORMANCE, FINANCE AND INFORMATION GOVERNANCE COMMITTEE (PFIG):

Oversees financial and operational performance, information governance, and delivery of plans/targets. The Committee is also responsible for points 1-5 as noted above. The cycle of business for the Committee is set to receive the section of the CRR and BAF to which it is accountable for on a bi-monthly basis.

QUALITY SAFETY AND EXPERIENCE COMMITTEE (QSE):

Reviews quality of care, patient safety issues, clinical effectiveness and outcomes, patient experience. The Committee is also responsible for points 1-5 as noted above.

The cycle of business for the Committee is set to receive the section of the CRR and BAF to which it is accountable for on a bi-monthly basis.

RISK SCRUTINY GROUP:

The Risk Scrutiny Group reports to the Executive Committee and advises on any risk management issues, including all significant risks arising from activities within the organisation. The Group is responsible for scrutinising the CRR and BAF ensuring appropriate escalation of operational risks. The Group will report on any weaknesses identified to ensure that the Board has in place effective systems for the reporting of risk, and the management of risk registers (local, directorate and corporate) and the Board's Assurance Framework.

Specifically, the Group is responsible for:

- Operationalising the objectives of the Risk Management Framework through the organisation's directorates, by embedding risk management and establishing local risk reporting procedures to ensure the effective integrated management of risk and assurance;
- Coordinating the escalation of all clinical and non-clinical risks, making recommendations to, and advising the Executive Committee and Board accordingly;
- Reviewing and monitoring the CRR and BAF;
- Advises on any risk documentation ensuring the Framework and any other relevant policies and procedures are in place
- Coordinating the achievement of the objectives of the Risk Management Framework through the organisation's directorates, by embedding risk management and establishing local risk reporting procedures to ensure the effective integrated management of risk and assurance;
- Reviewing high risk recommendations made by the Internal Audit Service, ensuring that where appropriate they are acted upon and recorded through risk registers and the BAF appropriately.

EXECUTIVE COMMITTEE

The Executive Committee holds accountability for individual risks listed on the BAF and CRR and plays a key role in the ongoing review of the risk register. They are responsible for identifying risks that require escalation or de-escalation, and for providing regular updates on the progress of action plans aimed at mitigating and managing the risks under their remit.

7.1 INDIVIDUAL RESPONSIBILITIES

All members of staff, and those working on behalf of the Health Board, have an individual responsibility for managing risk. They must understand and adhere to this Risk Management Framework. The following individuals have specific responsibility, accountability and authority for risk management, as part of their existing roles:

CHIEF EXECUTIVE (CEO)

The Chief Executive Officer (CEO) serves as the Accountable Officer for the Health Board, holding overarching responsibility for ensuring compliance with statutory and legal obligations, as well as adherence to governance guidance issued by the Welsh Government. This accountability extends across key areas including risk management, health and safety, financial and organisational controls, and overall governance. The CEO is ultimately responsible for

▪ ensuring the Health Board maintains an up-to-date Risk Management Framework endorsed by the Board;

▪ promoting a risk management culture throughout the Health Board;

▪ ensuring that there is a framework in place, which provides assurance to the Board in relation to the management of risk and internal control;

▪ ensuring that risk issues are considered at each level of business planning, from the corporate process to the setting of staff objectives;

▪ setting out their commitment to the risk management principles, which is a legal requirement under the Health and Safety at Work Act 1974. The Welsh Government requires the Chief Executive to sign a Governance Statement annually on behalf of the Board. This outlines how risks are identified, evaluated and controlled, together with confirmation that the effectiveness of the system of internal control has been reviewed.

EXECUTIVES & DIRECTORS

Executives and/or Directors have overall responsibility for the operational management of risks within their Directorates and are the named senior responsible officer for individual risks on the CRR and BAF.

They are also responsible for the effective allocation of resources to timely reduce risks within their remit, while ensuring prompt escalation and de-escalation of risks where appropriate. They shall also be responsible for ensuring that senior managers under their portfolio have effective risk management systems and processes in place in their directorates, divisions, sites, and services to demonstrate robust identification, assessment, mitigation and management of all risks.

They are responsible for ensuring that best practice in risk management and a positive risk-aware culture are fully embedded in their portfolio. Executives and Directors will work with the risk management team to ensure the appropriate use of the BAF and CRR.

Executives and Directors play a pivotal role in setting the expected cultural tone, one which is positive and encourages identification, risk is not to be considered as negative or to be avoided. The Executives and Directors will do so by ensuring communication is open, and transparent where all staff have the confidence to raise a risk. Executives and Directors will seek assurances that risk training is well attended for their regions and departments. Good risk awareness, awareness of roles and responsibilities, timely management of action plans, and a sense of accountability. Executives and Directors will seek assurances respective risk registers are maintained regularly, action plans are well managed, well communicated and actions which have blocks are escalated in a timely manner. Registers are expected to be agile and reflective of the service. Executives and Directors will foster a culture of continuous improvement supporting teams to engage with Better by Betsi, a community of continuous improvement, enhancing innovation with risk identification, mitigations strategies for their service. Executives will take a proactive identification approach to counter fraud risks.

In addition, Clinical Executive Directors (Executive Medical Director, Executive Director of Nursing & Midwifery, Executive Director of Therapies & Health Sciences, and the Executive Director of Public Health) have collective responsibility for clinical quality governance, which will include patient safety, incident management and patient experience, and will therefore have a responsibility to ensure that clinical risks are appropriately managed in-line with this Framework.

DIRECTOR OF CORPORATE GOVERNANCE

The Director of Corporate Governance is the delegated lead for risk management in the Health Board, and is accountable for leading on the design, development and implementation of the integrated BAF and Risk Management Framework.

The Director of Corporate Governance will:

▪ lead the embedding of an effective risk management culture throughout the Health Board;

▪ work closely with the Chair; Chief Executive; Chair of the Audit Committee; and, Executive Directors, to implement and maintain an appropriate Risk Management Framework and related processes, ensuring that effective governance systems are in place;

▪ develop and communicate the Board’s risk awareness, appetite and tolerance;

▪ lead and participate in risk management oversight at the highest level, covering all risks across the organisation on a Health Board basis;

▪ lead the ongoing development of the Risk Scrutiny Group (established by the Executive Committee).

HEAD OF RISK MANAGEMENT

The Head of Risk Management is accountable to the Director of Corporate Governance, and in relation to risk management will specifically:

▪ provide specialist advice in relation to controls and assurances for a range of functions at all levels in the organisation to support the effective management of clinical and non-clinical risk and governance;

▪ ensure a central system is in place to collate risk registers across the Health Board, which link to the BAF;

▪ support the management and development of the BAF and Risk Management Framework;

▪ work with directorates and Heads of Service to ensure risks are escalated in accordance with the Risk Management Framework;

▪ compile the CRR and BAF, for Board;

▪ support the development and functioning of the Risk Forum and Risk Scrutiny Group; and

▪ provide training, information and advice to operational staff and corporate functions on risk management and risk registers, ensuring linkage to the BAF.

CORPORATE RISK TEAM

The corporate risk management team will facilitate and ensure effective risk management practices are in place throughout the organisation. The team will support the escalation of risks the CRR and BAF. The risk management team will support services by validating risk registers, including the adequacy of the risk descriptions, controls, and assurances and justification of the risk scoring and take a lead on assurances of compliance pan BCU.

They will advise all colleagues including Executives and Directors in managing their risks. The risk team will lead the development of procedures as required under this framework. They will ensure the delivery of training to staff who have responsibilities under this policy. They will be responsible for the overall management of the risk module in Datix.

SENIOR MANAGERS

Senior managers will take the lead on risk management within their divisions, sites and areas and set the example through visible and exemplary leadership.

They are also responsible for supporting the effective allocation of resources in managing, escalating and de-escalating operational and strategic risks within their remit. The risk service lead and risk team will work with senior managers to ensure risks are articulated appropriately and described in line with procedures and will further support organisational wide learning.

The risk management team will provide healthy challenge and support to those risks that do not have adequate actions or action plans and have not progressed in a

timely manner with a route to escalation to SIROs. Senior manager will provide SIROs with regular assurances around effective management of risk registers.

SERVICE RISK LEADS

Services are required to nominate a risk lead/champion on behalf of the service to ensure the risk register is well maintained and risk is championed throughout the service facilitating good identification processes. Service risk leads will support the operational management of their respective service risk register and will liaise with the risk management team around escalation or de-escalations of risks and will work on any feedback around the quality assurance of the risk register. Service managers and service risk leads will be responsible for ensuring activities and action plans within risks are regularly maintained. All leads and champions will have regular risk management training.

ALL STAFF

All staff including, Trade Union colleagues and contractors are required to comply with this Risk Management Framework, raise any issues of concern to the attention of their line manager and to appropriately minimise and manage risks to the best of their knowledge and ability. Controls and actions implemented in mitigating risks must be timely disseminated to all staff involved with the management of the risk. All staff are expected to share intelligence around any potential risks with contractors providing services within and on behalf of the Health Board. Risk is the responsibility of all staff of the Health Board; agency staff; contractors brought in to undertake work on behalf of the Health Board, for example capital and estates works; students; locums; volunteers; individuals employed on honorary contracts; and, other third parties engaged in Health Board business.

INDEPENDENT MEMBERS (IMs)

Independent Members have an important role in risk management in seeking assurance on the robustness of processes and the effectiveness of controls through constructive, robust, positive and effective challenge to the Executives, Directors and senior management. IMs are expected to satisfy themselves that the Health Board`s risk management arrangements are effective, efficient and fit-for-purpose. IMs will provide healthy challenge on those risks that are not treated in a timely manner; the overall decision to tolerate the risk and/or the risks alliance to Health Board objectives.

IMs will challenge overall Board decision-making ensuring this is within the Boards risk appetite. In addition, IMs chair Board Committees and in line with the relevant Committee's terms of reference, should gain and provide assurance to the Board that risks within its remit are being managed effectively by the risk owners and report any areas of concern to the Board. IMs should seek assurance in ensuring a measured risk culture.

INTERNAL AUDIT

The relationship between risk management and Internal Audit is critical. Risk management is concerned with the assessment of risk and the identification of existing and additional controls, whereas Internal Audit's role is to evaluate these controls and test their efficiency and effectiveness. This is undertaken through the Internal Audit programme of work. Accordingly, the Head of Internal Audit will:

a. Provide an overall opinion each year to the Accountable Officer of the organisation's risk management, control and governance; to support the preparation of the Annual Governance Statement;

b. Focus the internal audit work on the significant risks as identified by management, and audit the risk management processes across the organisation;

c. Audit the organisation's risk management, control and governance through operational audit plans, in a way that affords suitable priority to the organisation's objectives and risks;

d. Provide assurance on the management of risk and improvement of the organisation's risk management, control and governance; by providing line management with recommendations arising from audit work.

LOCAL COUNTER FRAUD SERVICES

The Health Board's nominated Local Counter Fraud Specialist (LCFS) provides assurance to the Board regarding risks relating to fraud and/or corruption. The Health Board's Annual Counter Fraud Work Plan, as agreed by the Audit Committee identifies the arrangements for managing and mitigating risks as a result of fraud and/or corruption. Where such issues are identified they are investigated by the LCFS, and then reported to the Audit Committee as appropriate. The LCFS works with the Chief Executive, Executive Committee and Director of Corporate Governance to review any fraud or corruption risks. Such risks are referred to the relevant risk register for the Directorate concerned, and are then escalated through the Health Board's escalation process. The Executive Committee recognises that fraud, bribery, and corruption pose significant risks that require proactive management. To protect the interests of our stakeholders, act ethically, and comply with counter fraud laws and regulations, we commit to proactively identify fraud risks and vulnerabilities across the Health Boards operations through audits, reviews of complaints and allegations, and risk assessments. Routinely assess changes that may impact exposure to fraud, bribery and corruption. This also includes effective controls tailored to the highest risk areas identified. This includes clear financial controls, investigation and response diligence, training, and ensuring robust channels for reporting concerns.

SENIOR INFORMATION RISK OFFICER

The Board will nominate an Executive or Director as the Senior Information Risk Officer (SIRO) with delegated responsibility by the Chief Executive for ensuring that information risks are treated as a priority for business outcomes.

8. MONITORING THE EFFECTIVENESS OF THE RISK MANAGEMENT FRAMEWORK

Compliance with this Framework is monitored by the Executive Committee and the Audit Committee. The Annual Governance Statement is signed by the CEO and sets out the organisational approach to internal control. This is produced at the end of the financial year and is scrutinised as part of the annual accounts process and presented to the Board with the accounts, as part of the Annual Accountability Report. The Corporate Risk Team and Risk Scrutiny Group will take a lead on seeking assurances and providing Committees and Board with an overview of the Health Board's effectiveness and compliance. The Head of Internal Audit will also provide an opinion together with the summarised results of the internal audit work performed during the year.

The Health Board's risk management arrangements are also subject to review annually, as part of the Audit Wales Structured Assessment process. The risk management framework draws from best practice standards ISO31000, policy, and legislative instruction such as the National Health Service (Wales) Act 2006, the Health and Safety at Work Act 1974 and the Management of Health and Safety at Work Regulations 1999. The Health Board understands that risk is inherent in every business and is committed to ensuring full compliance.

This document should be read in conjunction with the 'Risk Management Procedures' (RM02) and 'Risk Training Procedures' (RM03) which are supportive of this Framework and outline all the procedural requirements for managing a risk operationally through to escalation.

Appendix 1

RISK APPETITE

The Board set their risk appetite in a developmental session on the 27 August 2025 and is subject to annual review. The appetite session referenced the Good Governance Institute Appetite Risk Matrix for Sensitive Decision Making, for risk types in order to score appetite.

The output of the session detailed appetite across five risk types:

Quality Risk: There was willingness to be 'open' and consider all potential delivery options and choices while also providing an acceptable level of reward (and VfM). We are prepared to accept the possibility of short-term, managed risks to quality or safety where there is strong evidence that the change will deliver long-term improvement in patient outcomes. We will embed investigation and learning into all decisions, ensuring the duty of candour remains central to our approach. **<15**

Financial Risk: There was an agreed consensus on an 'open' appetite and consider all potential delivery options and choose while also providing an acceptable level of reward (and VfM). There was an agreed consensus to invest for return and minimise the possibility of financial loss by managing the risks to a tolerable level. Value and benefits considered (not just cheapest price). Resources allocated in order to capitalise on opportunities. **<15**

Regulatory/Compliance Risk: There was an agreed consensus supporting an 'open' risk appetite to consider all potential delivery options and choose while also providing an acceptable level of reward (and VfM). Challenge would be problematic but we are likely to win it and the gain will outweigh the adverse consequences. **<15**

Reputational Risk: There was an agreed consensus to 'seek' some reputational risks and an eagerness to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk). We are willing to take bold decisions that may attract significant scrutiny if they are in the best interests of patient safety and service improvement. Reputation is actively managed through transparent, values-based communication, and we view public interest as an opportunity to demonstrate leadership. **<20**

Innovation: There was a clear consensus to 'seek' innovation, with eagerness to be forward-thinking and to pursue options offering potentially higher business rewards. We actively pursue innovations that challenge current practice while implementing controls to minimise risks to patient safety, where there is strong potential for substantial improvement in outcomes. Controlled trials, pilot programmes, and transparent stakeholder engagement remain integral to this approach. **<20**

Score tolerances are communicated for each risk domain and risks should be managed throughout the Health Board in line with domain scores.

EQUALITY IMPACT ASSESSMENT

The Health Board has undertaken an Equality Impact Assessment on the implementation of the Risk Management Framework and procedures to ensure that

it is inclusive and does not discriminate against any protected characteristics. The assessment has highlighted an equality impact concern regarding the availability of the documentation in a format to address any visual impairment disabilities. Any RAG ratings in Datix and other documents will have descriptors for those with colour blindness and RM01-03 will be available in Welsh as well as all risk training. Further support to understand the document is also available through bespoke support and training through the corporate risk team. Any other challenges to implement or apply these Risk Management documents can be communicated to the corporate risk team in order to ensure the Health Board to positively meet its responsibilities under the equalities and human rights legislation.

REFERENCES

AS/NZS ISO 31000:2018 (2018) Risk Management Guidelines. BSI Publication.

Bribery Act 2010. (c.23). London: The Stationery Office.

Cabinet Office. (2013). Functional Standard GovS013: Counter Fraud. [online]

Committee of Sponsoring Organizations of Treadway Commission (2017) Guidance on Enterprise Risk Management – Integrating with Strategy and Performance. Available at: https://www.coso.org/enterprise-risk-management

Criminal Finances Act 2017. (c.22). London: The Stationery Office.

Deloitte (2015) Enterprise Risk Management – A 'risk-intelligent' approach. Deloitte Advisory Publication.

Good Governance Institute (2018) Risk Appetite Matrix https://www.good-governance.org.uk/wp-content/uploads/2020/05/GGI_RiskAppetite_CHV19-version3.pdf

Fraud Act 2006. (c.35). London: The Stationery Office.

HM Treasury (2020) The Orange Book: Risk Management – Principles and Concepts.

IRM (2011) Risk Appetite & Tolerance Guidance Paper.

NHS Leadership Academy (2013) The Healthy NHS Board 2013 – Principles for Good Governance. Available at: www.leadershipacademy.nhs.uk

Public Interest Disclosure Act 1998. (c.23). London: The Stationery Office.

WHC (2000)13 – Corporate Governance in the NHS in Wales: risk management and organisational controls.

Included a desktop review of Welsh Health Boards Risk Frameworks