Reference Number: UHB 023 **Version Number:** 2.1	**Date of Next Review: 03.02.2029**

Risk Management Policy

Policy Statement

This risk management policy establishes:

- Systems for effective risk management that is integral to the day-to-day operation of the organisation.
- Clear lines of accountability to ensure the management of risk.
- Arrangements to identify the risks that may threaten the achievement of the objectives of the UHB. This will include arrangements for reporting incidents and raising concerns.
- Appropriate action in response to the identification of unacceptable risks.
- Clearly defined structures for providing assurance through the organisational hierarchy up to the Board that risks are being managed.
- Alignment of risk management activity to the corporate aims, objectives and organisational priorities of the UHB, to protect and enhance the reputation and standing of the organisation.
- The embedding of a risk culture where risk analysis forms part of organisational strategic planning, business planning, Quality Management and performance management.

Putting the above arrangements in place will enable the organisation to:

- Become proactive rather than reactive.
- Identify and treat risk throughout the organisation.
- Improve identification of opportunities and threats.
- Comply with relevant legal and regulatory requirements.
- Improve financial reporting and the effective allocation of resources.
- Establish a reliable basis for decision making and planning.
- Improve incident management and prevention.
- Improve organisational learning.
- Improve organisational resilience.

Policy Committment

Cardiff and Vale University Health Board (UHB) is committed to robust, proactive risk management as a core part of good corporate and clinical governance. We aim to identify risks, incidents and mistakes quickly, respond constructively, learn lessons, and prioritise resources to continually improve safety and quality.

We will achieve this by:

- Fostering a culture of openness to reduce and, where possible, eliminate risks.
- Aligning all risk management activities with UHB aims, objectives and priorities to protect and strengthen the organisation's reputation.
- Embedding risk analysis into strategic planning, business planning and project appraisal.
- Implementing routine risk assessment to identify, control and monitor risks that could affect service quality or safety.
- Ensuring clear communication of risk-related issues across the organisation and with stakeholders.
- Maintaining an effective incident reporting system to reduce incidents, claims and complaints.
- Demonstrating to patients, staff and the public that we manage risk to deliver safe, high-quality care at the right time and in the right place.
- Encouraging responsible innovation by supporting calculated, well-managed risk-taking that benefits the organisation.
- Providing a strong foundation for integrated risk management and internal control as part of good governance.
- Monitoring the effectiveness of risk management using performance indicators.

Supporting Policies and Procedures

- UHB 043 Raising Concerns (Policy) to be read alongside the UHB Speaking Up Safely Guidance
- UHB 138 Incident, Hazard and Near Miss Reporting Policy
- UHB 467 Risk Assessment Procedure - Health and Safety
- UHB 470 – BAF AND ASSURANCE

Other supporting documents are:

- Standing Orders
- Standing Financial Instructions
- Scheme of Delegation
- See Risk SharePoint page for further guides and supporting documents

Scope

This Policy is applicable across the whole of the UHB. It should also be referred to when ensuring effective risk management arrangements are in place when working with contractors, partner organisations e.g. Local Authorities and other stakeholders.

Policy Approved by	Audit Committee
Accountable Executive	Director of Corporate Governance
Author	Corporate Archivist and Records Management Manager

Disclaimer

If the review date of this document has passed, please ensure that the version you are using is the most up to date either by contacting the document author or the Governance Directorate.

Summary of reviews/amendments

Version Number	Date Review Approved	Date Published	Summary of Amendments
1.1	25.01.2011	28.01.2011	*New policy to replace and update documents from predecessor organisations*
1.2	09.07.2023	26.11.2023	Change to Statement of Intent, revised management arrangements, changes to executive responsibilities, references to the Annual Governance Statement, minor amendments to Section 12 and amendment of document title regarding incident reporting.
1.3	01.07.2025	01.07.2025	Full review of Policy conducted, transfer to new template, slight updates throughout
2.1	03.02.2026	05.02.2026	Full policy rewrite to reflect the change to using AMAT as a single system for monitoring risk.

Table of contents

Appendices

1. Introduction

The University Health Board (UHB) has moved to a single digital risk management system on AMaT (Audit Management and Audit Tracking). **It is mandatory for all Clinical Boards and Directorates to record their risks on AMaT, ensuring one accurate and accessible risk register for the whole organisation**. This centralised approach strengthens transparency, supports consistent risk management practices, and enables clearer oversight from ward level through to the Board.

Historically, AMAT has been used across the UHB for Clinical, Quality and external Audit management and was considered a tool already well embedded. The risk module can link to these previous services. It also allows related risks to be linked, helping teams understand how a risk in one area may affect others.

For example, if there is a risk with medication, distinct areas or groups, such as the Medicine Safety Group are able to log a risk and communicate it through their stakeholder membership, who in turn will have the awareness to raise the risk and score it reflectively within their own Clinical Boards. This enables each Clinical Board or Service to review and create a risk entry of their own, assessing the level of impact within their respective service. These risks can be cross referenced for increased awareness and transparency allowing for different teams to view the varying impact and proposed controls across the UHB.

Support for using AMAT is available from Corporate Governance via Corporate.Meetingcav@wales.nhs.uk and a range of resources can be found on the Risk SharePoint page. Training is also available through pre-recorded sessions and ad hoc workshops, as described further in Appendix B.

The Institute of Risk Management defines risk management as

'*the process which aims to help organisations understand, evaluate and take action on all their risks with a view to increasing the probability of success and reducing the likelihood of failure*'

As well as supporting better decision making and improved efficiency, risk management can also provide greater assurance to stakeholders that concerns

are being managed and mitigated as effectively as possible. Risk management adds value to the organisation and risk management activities must achieve the best possible outcomes and reduce the uncertainty of these outcomes.

Risk management must be embedded into UHB culture, so people need to be alive to it and talking about risk right across the organisation.

2. Key Points

2.1 Definitions

There are some common definitions that staff need to be aware of when it comes to understanding risk which are set out below:

Risk Management	A systematic process by which potential risks are identified, assessed, managed and monitored in a way that will enable organisations to minimise losses and maximise opportunities
Hazard	Something that may cause harm, damage or loss, e.g. chemicals, manual handling
Risk	The chance of suffering harm caused by a hazard, loss or damage or the possibility that the UHB will not achieve an objective
Risk Assessment	The overall process of identifying risk and evaluating whether acceptable or not taking into account best practice and the appetite of the organisation.
Risk Appetite	The amount of risk that an organisation is prepared to accept, tolerate or be exposed to at any point in time

A full list of definitions can be found at **Appendix E.**

2.2 Organisational Risks

This policy covers the management of risks that impact the organisation. There are many project risks that impact the delivery of more local work, these do not form part of the organisational risk register and should be managed locally outside of this policy.

2.3 Incidents and Risk

Staff must be aware of the difference between what an incident and risk is.

Risk

- A risk is something that might happen in the future and could affect the organisation's ability to achieve its objectives.

- Risk management is proactive, aiming to identify, assess, and mitigate potential threats before they materialise.
- It is characterised by uncertainty and is expressed in terms of likelihood (probability of occurrence) and consequence (impact if it occurs).

Example: *There is a risk that staff shortages could compromise patient safety.*

Incident

- An incident is an event that has already happened or is certain to happen, often resulting in harm or near miss.
- Incident management is reactive, focusing on reporting, investigating, and learning from events to prevent recurrence.

Example: *A patient fall on a ward is an incident that needs to be reported and reviewed.*

For incident management staff must refer to the UHB 138 Incident, Hazard, and Near Miss Policy and support can be provided by the Patient Safety Team.

2.4 Cause v Effect

When recording a risk, staff must be clear whether they are describing the cause of the risk ***or*** the effect it could have.

- Cause based risks focus on what might trigger the problem. The risk owner should be the person responsible for that part of the service.
- Effect based risks focus on the potential impact on patients, services or staff. The risk owner should be the person accountable for managing that impact.

Being clear about the cause or effect helps ensure each risk is owned by the person best placed to control or reduce it.

An example of this would be recording Lifts on a Risk Register

- **Cause-Based** - There is a risk that lift failure or unavailability, caused by mechanical faults or ongoing maintenance could occur, as the ageing lift infrastructure is prone to intermittent malfunction. This risk is owned by Capital, Estates & Facilities because it arises from asset condition and maintenance requirements.
- **Effect-Based -** If lift downtime occurs, patient movement between floors may be delayed, causing potential disruption to clinical pathways,

delayed transfers, and reduced service efficiency. This risk is owned by the affected service area, as they are responsible for managing the operational impact.

3. Risk Architecture

Risk architecture is the organisational arrangements for risk management detailing the responsibilities, system, roles and lines of communication for reporting on risk management.

3.1 Responsibilities

All Staff – risk is everyone's responsibility. All members of staff are accountable for maintaining risk awareness, identifying and reporting risks as appropriate to their line manager

Managers- must take an active lead to ensure that risk management is embedded into the way their service/team/ward operates & their staff understand and implement this Policy, ensuring that staff are provided with the education and training to enable them to do so

Directors/ Clinical Board Directors- are responsible for implementation of the Board Assurance Framework (BAF) and this Risk Management Policy. They must ensure that there is an active risk culture within their area and risks are escalated as appropriate

Executive Directors - are responsible for ensuring their directorates are implementing the Board Assurance Framework (BAF) and this Risk Management Policy and will ensure that the systems, policies and people are in place to manage, eliminate or transfer the key risks related to the health board's strategic objectives

Director of Corporate Governance - works with senior leaders to maintain the Risk Management Policy and Board Assurance Framework, strengthen shared understanding of organisational risks, and promote clear risk awareness. They oversee risk management across the UHB, ensure the BAF is delivered effectively, monitor actions and reporting, and lead the development of the UHB's overall risk management approach

Their team work with Executives and Managers to co-ordinate integrate, oversee and support the risk management agenda, ensuring that risk management principles are embedded across the UHB. The team will also

liaise with Audit Teams regarding Risk Management. The team will download all risks that score 20-25 for inclusion in the Corporate Risk Register for submission to Board from the centralised register (AMaT) and support with co-ordinating Risk Training.

Chief Executive - is the Accountable Officer of the UHB and has overall accountability and responsibility for ensuring it meets its statutory and legal requirements and adheres to guidance issued by the Welsh Government in respect of Governance. This responsibility encompasses risk management, health and safety, financial and organisational controls and governance.

They have overall accountability and responsibility for ensuring that the health board maintains an up-to-date Risk Management Policy and a Board Assurance Framework that is endorsed by the Board.

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

3.2 Risk Register System

The digital risk management system on AMAT (Audit Management and Audit Tracking) provides a live, accurate and accessible risk register for the whole organisation. The system is set up across four levels of the UHB:

AMAT	Local definition	Example
Division	Clinical Board	Medicine CB
Business Unit	Directorate/Department	Integrated Medicine
Speciality	Workstream/Service	Stroke
Ward or Site	Ward or Site	C5 South

Essentially, teams need to set up their risk hierarchy and service structure in the right way that works for them, ensuring that all their different teams, departments and services are assigned to enable risks to be logged in AMaT at the appropriate level of where or who the risk impacts

Contact the Digital Risk Lead, if you need assistance accessing the Risk system or configuration changes to enable your service area . A document containing

the full list of services in AMAT can be found here, this document is updated regularly. This is not fixed and teams must ensure that their departments are adequately configured to ensure effective risk management in their areas.

3.3 Roles

Staff have the ability to view all risks across the organisation provided they have been added to the AMAT system.

Risks are managed on AMAT by the appropriate person from the department depending on the severity of the risk. Generally, risk must be managed at the lowest level possible, proportionate to the level of exposure.

The appropriate access needs to be given to staff who will record risks in AMAT. Those staff will need to be added into the system as **Risk Stakeholders** enabling them to add, approve and edit a risk within a service.

Once a risk is submitted on AMAT, it appears as a draft and must be approved by an **Approver**. This is to ensure the risk entry is acceptable, accurately recorded and proportionate. The Digital Risk lead will work with departments to ensure appropriate approvers are in place.

The ability to edit and manage risks is done in AMAT by the assignment of different roles for users. If you're a ward manager and need to approve, monitor and escalate risks into your Ward meetings, you will need different access to a Nurse who has recorded the risk into the AMAT system. This means teams need to look at their risk hierarchy, in AMAT terms this translates to different levels of Stakeholders. Some staff will only need to work on risks for their area, others will want to review and approve risks right across all departments that sit under them. A Clinical Board Director for example will want to be a Divisional Stakeholder so they have visibility of everything across their Clinical Board. A General Manager will be a Business Unit Stakeholder having access to everything in the department they manage.

*Stakeholders for different Service levels	Example of Service levels	Example of Service levels
Division Stakeholders can view, edit and manage all risks across the Division, Business Unit and all Specialities	Division = Medicine CB Business Unit = Integrate Medicine Speciality = Stroke **Full table of the current Service Areas can be found** here	Division = Corporate Business Unit = People & Culture Speciality = Equity & Inclusion
Business Unit Stakeholders can view, edit and manage all risks across the Business Unit and Specialities - unable to edit Divisional risks		
Speciality Stakeholders can view, edit and manage all risks across a set speciality only - unable to edit Divisional and Business Unit risks including risks from assigned to other specialities		
Approver - ability to review draft risks and approve or reject the risk appearing on the proposed register.		

In the example above Clinical Board representatives who require oversight and the ability to create risks at any level within the clinical board, will be assigned

Divisional Stakeholder access. This level enables full visibility and management capability across the entire Division, including all Business Units and Specialities.

Colleagues who need access across an entire Directorate (Business Unit) will be assigned **Business Unit Stakeholder** access. This allows them to enter and manage risks for the whole Business Unit, including all Specialities within it. When raising a risk, they may set it at the Business Unit level - when the risk affects all linked services or at an individual Speciality level if the risk impacts a single service.

Colleagues working directly within a service will be assigned **Speciality Stakeholder** access, enabling them to enter and manage risks only for that Speciality. They will not be able to edit risks at Business Unit or Divisional level or risks belonging to other specialities.

This can vary from Clinical Board to Clinical Board. An example of a structure is:

Division	Clinical Board Director / Quality & Clinical Governance
Business Unit	General Managers / Directorate Leads
Speciality	Service leads / All users

A Stakeholder and User type guide is available which provides more detail around this.

3.4 Risk Owner

Once a risk has been identified, analysed and evaluated a Risk Owner must be appointed. Risk owners should be the individuals best placed through their authority and influence to take responsibility for mitigation of the risk. The identified risk owner is responsible for:

- Ensuring that the risk is managed appropriately, controls are in place to mitigate the risk and actions are set out on AMAT to address gaps in control measures.
- Reviewing the risk register at appropriate intervals to ensure the descriptor, controls and risk score accurately reflect the level of risk and that progress is being made at sufficient pace to reduce the risk score to the target risk level.
- Communicating with specialist areas to discuss the joint working needed to manage the risk effectively before they are assigned as an Action Owner.

- Assigning action owners within AMAT to ensure they are aware of their responsibilities for delivering actions.
- Reporting on the overall status of the risk, escalating where appropriate in line with the Risk Reporting and Escalation table detailed in section 4.6 of this policy.

3.5 Action Owner

Action owners have responsibility for the activities needed to address gaps in control measures and the assurance of the effectiveness of existing controls. Action owners are required to report progress to Risk Owners in a timeframe and manner identified by the Risk Owner. Action owners will normally be identified from within the same Clinical Board or Corporate Directorate as the Risk Owner but specialists from other areas of the organisation, such as HR or H&S may also be required to perform as specialist action owners.

3.6 Assurance

The Three Lines of Defence Model

The UHB operates a 'Three Lines' model, with the diagram below outlining the principles for the roles, responsibilities and accountabilities for risk management.

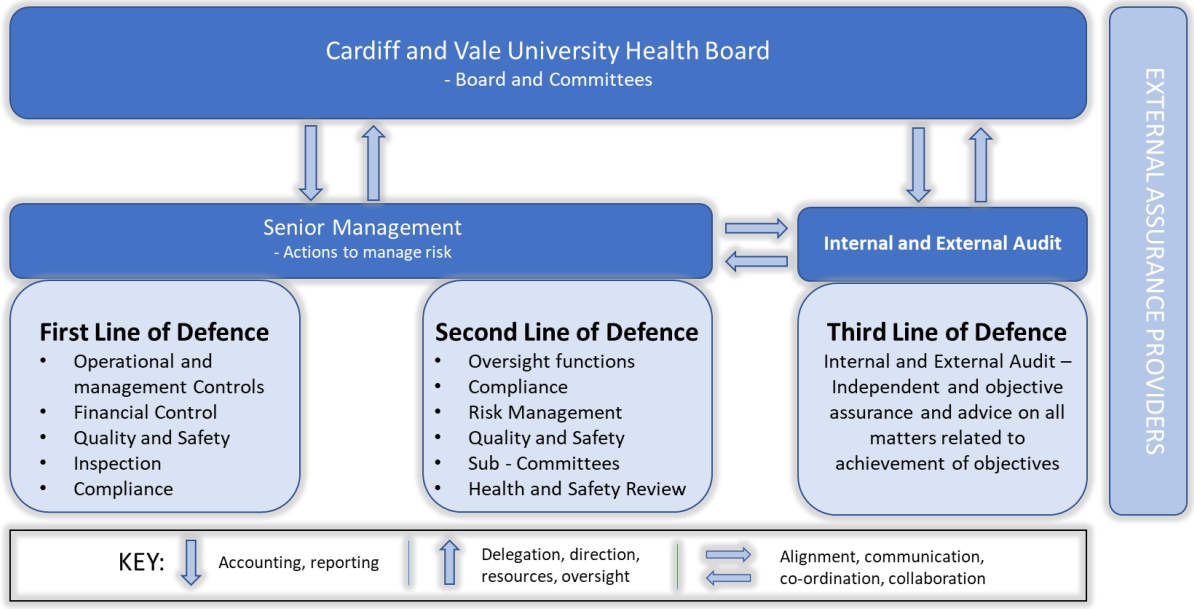


Figure 1 – Three lines of defence Model

In the 'Three Lines of Defence' model, management control is the first line of defence in risk management. The various risk control and compliance oversight functions established by management are the second line of defence, and independent assurance is the third. Each of these three "lines" plays a distinct role within the UHB's wider governance framework. All three lines need to work interdependently to be effective.

The Board has responsibility and accountability for setting the organisation's objectives, defining strategies to achieve those objectives, and establishing governance structures and processes to best manage the risks in accomplishing those objectives.

4. Risk Life Cycle

The cycle of managing risks involves a series of defined steps through which risks are identified, recorded and monitored to ensure they remain within acceptable levels. This systematic approach ensures that risks are managed consistently across the organisation and that issues are escalated or deescalated appropriately through established governance mechanisms. This cycle is set out below in more detail.

4.1 Assessment

If you think you may have an organisational risk, the first step is to undertake a risk assessment.

A suitable and sufficient risk assessment can be undertaken by following the 5 steps detailed below. It is reasonable to review the diagram below and have a discussion with your Line Manager.

Once it is confirmed that a new risk has been identified, the details must be entered onto AMAT the digital risk management platform. All risks regardless of score must be recorded.

Supporting risk documentation must be uploaded to the risk record in AMAT to support the risk and evidence controls and assurances. This is to ensure a contemporaneous record is held and this can be effectively audited. Documentation can include risk assessment forms, evidence of controls which can include but is not limited to policies/procedures/protocols/SOPs etc.

The Health & Safety Executive require all Health & Safety risks to undergo detailed scrutiny, these risks need to be identified through the completion of risk assessments which can be uploaded to the organisational risk register. Health & Safety Risk Assessments must be retained whilst they remain current and for 3 years after they are closed and 40 years for asbestos related documentation as per the Risk Assessment Procedure - Health & Safety.

Undertaking an initial assessment of the activities or objectives to be achieved will help managers to identify those areas that require a more in-depth assessment. Risk assessments should not be undertaken in isolation as a multi-disciplinary approach is encouraged.

4.2 Methods of Managing

Effective risk management aims to anticipate and where possible, avoid risks rather than deal with their consequences. However, this approach is not practicable for all risks. The intention must always be to reduce the risk by all reasonably practicable means. Once it has been reduced to the lowest level possible then it must be carefully managed.

It is necessary to manage risks in the most efficient and effective manner. AMAT is configured to manage Risks in line with the 4 T's format set out below.

Terminate Risk	taking the decision not to take a risk
Treat Risk	by reducing the probability of the risk occurring or by reducing the impact
Tolerate Risk	an informed decision to accept the consequences and the likelihood of a particular risk, for example where the probability or consequence is so low that the cost of managing it would be prohibitive, compared to the benefit or it is not within the remit of the organisation to prevent the risk e.g. emergency situations. For such situations Contingency Plans will need to be developed, e.g. Business Continuity Plans. This will allow the UHB to contain the negative effect of unlikely events that might occur.
Transfer Risk	Risk managed/mitigated by another organisation, for example insurance or contracting out (although still need to have regard of legal responsibilities which cannot be transferred

4.3 Factors

There are a number of factors to determine the nature and the level of impact each risk might present to the organisation. In order to help people score risks consistently a Risk Factors Score Guide found at Appendix D has been developed to provide clear, consistent definitions for staff to rate the severity of their risk. This ensures that risks are assessed systematically, understood across the organisation, and escalated appropriately.

4.4 Scoring

The UHB has a 3-part risk scoring process which is set out below and mirrored on the digital risk management system.

Initial Risk Rating (inherent)	The risk score (Impact x likelihood) assessed before the application of risk treatments/controls
Current Risk Rating	The risk score (Impact x likelihood) assessed at a specific period of time. The current risk rating will usually be lower than the initial rating but higher than the target risk rating
Target Risk Score	The estimated achievable risk score when all risk treatments and mitigations are in place and operating at maximum effectiveness.

The score of a particular current risk rating will determine at what level decisions on acceptability of the risk are to be made and where it needs to be reported.

The UHB operates a 1-25 risk scoring system which is set out below and mirrored on the digital risk management system.

Risk Level	Risk Score	Action
Extreme Risk	20 - 25	Immediately report the risk to the relevant Executive Director or Clinical Board Director.
High Risk	8 - 16	Report to Clinical Board (or for Corporate Directorates to the Executive Director).
Moderate Risk	4 - 6	Report to Heads of Service with proposed treatment/action plans, for particular monitoring.
Low Risk	1 - 3	Report to local manager for local action to reduce risk

4.5 Review & Update

All risks must have a review date, which must be entered manually by the user into AMaT. Once added, the review date appears in AMaT reports and data downloads, allowing teams to track when reviews are due. The risk register can also be filtered by these dates, helping users easily identify upcoming or overdue reviews and maintain timely oversight. In addition, approaching and overdue review dates will automatically notify the stakeholders that reviews are required.

The timescale for this will be influenced by the risk rating and the ability of the organisation to introduce control measures. As control measures are introduced the assessment must be reviewed as a series of incremental actions will gradually reduce the risk rating.

4.6 Escalation

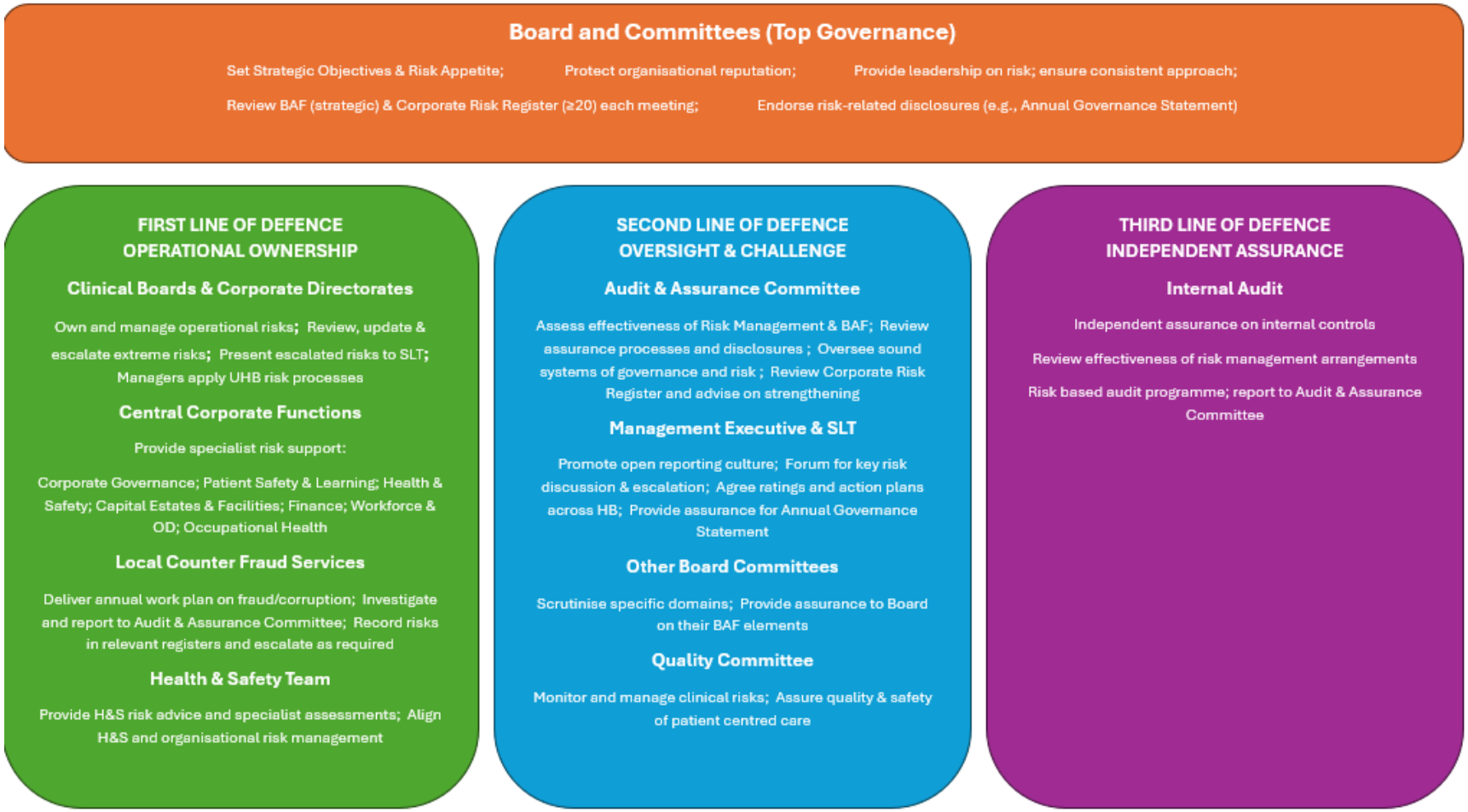
Staff are expected to use their professional judgement and apply common sense when escalating risks. Not every issue will require escalation, but where a risk cannot be managed safely or effectively at a local level—or where the potential impact is significant—it must be escalated to the appropriate level of the organisation in a timely and proportionate way.

The **Risk Reporting Hierarchy** (shown in the diagram below) provides a clear route for proportional escalation from Directorate Risk Registers to Clinical Board and Corporate Risk Registers, and ultimately to the Board Assurance Framework. Risks will move through this structure only as far as necessary to ensure they are owned, understood, and effectively managed.

The table below outlines the UHB's graded approach to risk escalation and oversight.

Score	Level	Action	Review	Oversight
1 - 3	Low Risk	Quick, easy measures implemented immediately, and further action planned for when resources permit	Risk Review meetings – at least 6 monthly	Local service
4 - 10	Moderate Risk	Quick, easy measures implemented immediately, and further action planned for when resources permit	Ward Department Risk Review meetings – at least quarterly.	Local Service Directorate
12 – 16	High Risk	Actions implemented as soon as possible but no later than six months	Directorate Meeting Monthly Clinical Board/QSE Quarterly	Local Service Directorate Clinical Board
20 - 25	Extreme Risk	Requires urgent action. The UHB Board is made aware, and it implements immediate corrective action	SLT – responsible for moderating Executive Clinical Board Reviews Committees Board	Local Service Directorate Clinical Board Executive/Board

Appendix A Lines of Defence in Risk Management – Roles and Responsibilities



Appendix B - Training

Details on risk training options is set out on the Risk Sharepoint Page

AMAT Training & Guidance

Video tutorial on how to add a new risk to AMAT
AMAT Risk Module Guidance

Non-Specific Training and Support- It is recognised that, in addition to the above there may emerge a need for non-specific risk management training and support. Where this is applicable please contact the Digital Risk Lead or the Corporate Governance team to discuss the support and training required

Appendix C – Risk Factors Score Guide

Consequence:	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
Safety & Well-being - Patients/ Staff/Public	Minimal injury requiring no/minimal intervention or treatment. No time off work. Physical injury to self/others that requires no treatment or first aid. Minimum psychological impact requiring no support. Low vulnerability to abuse or exploitation - needs no intervention. Category 1 pressure ulcer.	Minor injury or illness, requiring minor intervention. Requires time off work for >3 days Increased hospital stay 1-3 days. Slight physical injury to self/others that may require first aid. Emotional distress requiring minimal intervention. Increased vulnerability to abuse or exploitation, low level intervention. Category 2 pressure ulcer.	Moderate injury/professional intervention. Requires time off work 4-14 days. Increased hospital stay 4-15 days. RIDDOR/Agency reportable incident. Impacts on a small number of patients. Physical injury to self/others requiring medical treatment. Psychological distress requiring formal intervention by MH professionals. Vulnerability to abuse or exploitation requiring increased intervention. Category 3 pressure ulcer.	Major injury leading to long-term disability. Requires time off work >14 days. Increased hospital stay >15 days. RIDDOR Reportable. Regulation 4 Specified Injuries to Workers. Patient mismanagement, long-term effects. Significant physical harm to self or others. Significant psychological distress needing specialist intervention. Vulnerability to abuse or exploitation requiring high levels of intervention. Category 4 pressure ulcer.	Incident leading to death. RIDDOR Reportable. Multiple permanent injuries or irreversible health effects. An event which impacts on a large number of patients.
Quality/ Complaints/ Assurance/ Patient Outcomes	Peripheral element of treatment or service suboptimal. Informal complaint/inquiry.	Overall treatment/service suboptimal. Formal complaint (Stage 1). Local resolution. Single failure of internal standards. Minor implications for patient safety. Reduced performance.	Treatment/service has significantly reduced effectiveness. Formal complaint (Stage 2). Escalation. Local resolution (poss. independent review). Repeated failure of internal standards. Major patient safety implications.	Non-compliance with national standards with significant risk to patients. Multiple complaints/independent review. Low achievement of performance/delivery requirements. Critical report.	Totally unacceptable level or quality of treatment/service. Gross failure of patient safety. Inquest/ombudsman/inquiry. Gross failure to meet national standards/requirements.
Workforce/ 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 (>1 day)/competence. Low staff morale. Poor staff attendance for mandatory/key professional training.	Uncertain delivery of key objective/ service due to lack/loss of staff. Unsafe staffing level (>5 days)/competence. Very low staff morale. Significant numbers of staff not attending mandatory/key professional training.	Non-delivery of key objective/service due to loss of several key staff. Ongoing unsafe staffing levels or competence/skill mix. No staff attending mandatory/professional training.
Statutory Duty, Regulation, Mandatory Requirements	No or minimal impact or breach of guidance/statutory duty.	Breach of statutory legislation. Reduced performance levels if unresolved.	Single breach in statutory duty. Challenging external recommendations/improvement notice.	Enforcement action. Multiple breaches in statutory duty. Improvement notices. Low achievement of performance/ delivery requirements. Critical report.	Multiple breaches in statutory duty. Zero performance rating. Prosecution. Severely critical report. Total system change needed.
Adverse Publicity or Reputation	Rumours. Low-level negative social media. Potential for public concern.	Local media coverage - short-term reduction in public confidence/trust. Short-term negative social media. Public expectations not met.	Local media coverage - long-term reduction in public confidence & trust. Prolonged negative social media. Reported in local media.	National media coverage <3 days, service well below reasonable public expectation. Prolonged negative social media, reported in national media, long-term reduction in public confidence & trust. Increased scrutiny: inspectorates, regulatory bodies and WG.	National/social media coverage >3 days, service well below reasonable public expectation. Extensive, prolonged social media, MP/MS questions in House/Senedd. Total loss of public confidence/trust. Escalation of scrutiny status by WG.
Business Objectives or 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 targets,10-25 per cent over project budget. Schedule slippage. Key objectives not met.	>25 per cent over project budget. Schedule slippage. Key objectives not met.
Financial Stability & Impact of Litigation	Small loss. Risk of claim remote.	Loss of 0,1–0,25% of budget Claim less than £10,000.	Loss of 0,25–0,5% of budget. Claim(s) between £10,000 and £100,000.	Uncertain delivery of key objective. Loss of 0,5–1,0% of budget. Claim(s) between £100,000 and £1 million. Purchasers failing to pay on time.	Non-delivery of key objective. Loss of >1 per cent of budget. Failure to meet specification. Claim(s) >£1 million. Loss of contract/payment by results.
Service/ Business Interruption	Loss/interruption of >1 hour. Minor disruption.	Loss/interruption of >8 hours. Some disruption manageable by altered operational routine.	Loss/interruption of >1 day. Disruption to a number of operational areas in a location, possible flow to other locations.	Loss/interruption of >1 week. All operational areas of a location compromised, other locations may be affected.	Permanent loss of service or facility. Total shutdown of operations.
Environment/Estate/ Infrastructure	Minimal or no impact on environment/service/property.	Minor impact on environment/ service/property.	Moderate impact on environment/ service/property.	Major impact on environment/ service/property.	Catastrophic impact on environment/service/property.
Health Inequalities/ Equity	Minimal or no impact on attempts to reduce health inequalities/improve health equity.	Minor impact on attempts to reduce health inequalities or lack of clarity on the impact on health equity.	Lack of sufficient information to demonstrate reducing equity gap, no positive impact on health improvement or health equity.	Validated data suggests no improvement in the health of the most disadvantaged, whilst supporting the least disadvantaged, no impact on health improvement and/or equity.	Validated data demonstrates a disproportionate widening of health inequalities, or negative impact on health improvement and/or equity.
Fraud/Bribery	Unlikely to result in material loss or reputational damage. (Little or no loss to the organisation, material loss less than £500)	Material loss or reputational damage likely to be minimal. (Some risk to the organisation, which may result in minor reduction in service capacity or material loss of up to £5000. Reputational damage likely to be within the organisation which may lead to complaint)	Could result in material loss or reputational damage. (Moderate risk to the organisation, which may result in reduction of service. Material loss of up to £10000. Reputational damage across the NHS with a high potential for complain or a low risk of litigation)	Could result in high material loss or reputational damage (may result in temporary loss of service or material loss of up to £50,000. Reputational damage widespread and outside of NHS with a likelihood of litigation.	Could result in significant material loss or reputational damage. (High risk, which may result in, prolonged loss of service or material loss of over £50,000. Nationwide media coverage causes reputational damage, which is likely to lead to criminal prosecution or external investigation.

Appendix D – Risk Scoring

Likelihood score	**1 Rare**	**2 Unlikely**	**3 Possible**	**4 Likely**	**5 Almost certain**
Frequency How often might it/does it happen	This will probably never happen/recur	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it is not a persisting issue	Will undoubtedly happen/recur, possibly frequently

Risk scoring

Impact x Likelihood Risk Grading	1 Rare	Unlikely	Possible	Likely	Almost Certain
Negligible	1	2	3	4	5
Minor	2	4	6	8	10
Moderate	3	6	9	12	15
Major	4	8	12	16	20
Catastrophic	5	10	15	20	25

Appendix E – Definitions

Annual Governance Statement	A document which provides a high level account of the structures in place to support governance and review of their effectiveness. It will be produced at the same time as the annual accounts.
Assurance	Confidence, based on sufficient evidence, that internal controls are in place, operating effectively and objectives are being achieved
Assurance Committee	A board level committee with overarching responsibility for ensuring appropriate assurance is gained on the management of all principal risks. This function will be performed by the Audit Committee
Barriers	Actions, Measures or Processes that prevent mitigating controls being established.
Board Assurance Framework (BAF)	The key source of evidence that links strategic objectives to risk and assurance, and the main tool that the Board will use in discharging its overall responsibility for internal control.
Corporate Risk Register	Candidate risks comprise of all risks with a current risk rating of 20 or above, or those risks with a lower score which in the opinion of the risk owner that require greater visibility within the organisation to manage due to authority/resource, or their complexity or the potential for a health board wide impact.
Controls	Any process, policy, device, practice or other conditions/actions which modify risk. A risk treatment becomes a control once the effectiveness of the treatment has been confirmed through assurance processes
Current Risk Rating	The risk score (Impact x likelihood) assessed at a specific period of time. The current risk rating will usually be lower than the initial rating but higher than the target risk rating
Escalation	The act of advancing a risk to a higher management level for resolution, action or attention
Event	The occurrence or change of a particular set of circumstances. An event can have one or more occurrences and can have several causes and several consequences
Exposure	The consequences, as a combination of impact and likelihood, which may be experienced by the organisation if a specific risk is realised.
Gap in Assurance	Failure to gain sufficient evidence that policies, procedures, practices or organisational structures on which reliance is placed are operating effectively

Gap in Control	Failure to put in place sufficient effective policies, procedures, practices or organisational structures to manage risks and achieve objectives
Hazard	Something that may cause harm, damage or loss, e.g. chemicals, manual handling
Horizon Scanning	Systematic activity designed to identify, as early as possible, indicators of changes in risk.
Impact	The outcome of an event that has affected objectives. Can be certain or uncertain and can have positive, negative, direct or indirect effects on objectives. Can be expressed qualitatively or quantitatively
Initial Risk Rating (inherent)	The risk score (Impact x likelihood) assessed before the application of risk treatments/controls
Likelihood	The chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively, or quantitatively, and described using general terms or mathematically
Operational risks	These are key risks that affect individual Clinical Boards and Corporate Directorates. They are managed within the Clinical Boards and Corporate Directorates and where necessary included in the Corporate Risk Register and potentially BAF
Residual Risk	The exposure arising from a specific risk after action has been taken to manage it and making the assumption that the action is effective
Risk	The effect of uncertainty on objectives. An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities or threats. The chance of suffering harm caused by a hazard, loss or damage or the possibility that the UHB will not achieve an objective
Risk Acceptance	An informed decision to accept (tolerate) the consequences and the likelihood of a particular risk, for example where the probability or consequence is so low that the cost of managing it would be prohibitive compared to the benefit or it is not within the remit of the organisation to prevent the risk e.g. emergency situations.
Risk Appetite	The amount of risk that an organisation is prepared to accept, tolerate or be exposed to at any point in time

Risk Assessment	The overall process of risk identification, risk analysis and risk evaluation. It must be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. It must use the best available information, supplemented by further enquiry as necessary
Risk Avoidance	Taking the decision not to take a risk
Risk Categories	Identify and help classify risks based on potential consequences for example risks impacting on Quality or Infrastructure
Risk Management	A systematic process by which potential risks are identified, assessed, managed and monitored in a way that will enable organisations to minimise losses and maximise opportunities
Risk Reduction	By reducing the probability of the risk occurring or reducing the impact
Risk Register	A register of all risk across the UHB identified within a team, department, speciality, board/directorate or the UHB as a whole.
Risk Terminate	Take a decision to remove the risk by stopping the related activity entirely
Risk Tolerate	A decision is taken to accept the risk if impact is low or manageable.
Risk Transfer	Shift risk to third party, e.g. insurance or contract
Risk Treat & Risk Treatment	Implement controls to reduce likelihood or impact of risk. Any process, policy, device, practice or other conditions/actions with the potential to modify risk in a desired manner. Risk treatments become controls once their effectiveness in modifying the risk is assured.
Strategic risks	These are significant risks that have the potential to impact upon the delivery of Strategic Objectives and therefore need to be raised and monitored by the Executive Team and the Board
Target Risk Score	The estimated achievable risk score when all risk treatments and mitigations are in place and operating at maximum effectiveness.