Bwrdd Iechyd Prifysgol Hywel Dda University Health Board

CYFARFOD BWRDD PRIFYSGOL IECHYD
UNIVERSITY HEALTH BOARD MEETING

DYDDIAD Y CYFARFOD: **DATE OF MEETING:**	28 July 2022
TEITL YR ADRODDIAD: **TITLE OF REPORT:**	Risk Management Framework
CYFARWYDDWR ARWEINIOL: **LEAD DIRECTOR:**	Joanne Wilson, Board Secretary
SWYDDOG ADRODD: **REPORTING OFFICER:**	Charlotte Beare, Assistant Director of Assurance and Risk

Pwrpas yr Adroddiad (dewiswch fel yn addas) **Purpose of the Report** (select as appropriate)
Ar Gyfer Penderfyniad/For Decision

ADRODDIAD SCAA
SBAR REPORT

Sefyllfa / Situation

The Board is asked to approve the revised Risk Management Framework, which aims to clearly set out the components that provide the foundation and organisational arrangements for supporting risk management processes in Hywel Dda UHB,

This framework was developed following recent consultation and was presented to and supported by the Audit and Risk Assurance Committee on 21st June 2022.

Cefndir / Background

Risk Management is 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 (Institute of Risk Management). It forms part of the overall governance framework of the organisation.

The scope of a framework is the risk architecture, strategy and protocols. The risk architecture sets out the roles and responsibilities of the individuals and committees that support the risk management process. The risk strategy should set out the objectives that risk management activities are seeking to achieve, and the risk protocols describe the procedures by which the strategy will be implemented and risks are managed. This is built around and supports the risk management process.

This is consistent with the concept of the risk management framework described in ISO 31000. (ISO 31000, which is a generic risk management standard, provides principles, framework and a process for managing risk, and can be used by any organisation, regardless of size, activity or sector).

The Framework will help provide the mandate for embedding risk reporting in the Health Board by clearly setting out roles and responsibilities of both individuals and committees in one document

Asesiad / Assessment

The review of the Risk Management Framework had been previously delayed due a number of reasons, including changes to governance arrangements during the COVID-19 pandemic, changes to the Committee structure and changes to the Board Assurance Framework and Corporate Risk Register, which also needed to bed in. These changes, as well as comments from the recent global consultation, are now reflected in the revised Risk Management Framework, attached at Appendix 1.

As part of the recent global consultation, the Risk Management Framework has been shared with Executive Directors and Senior Management/Risk Leads within the organisation.

The Risk Management Framework does not replace the current Risk Management Strategy (which will be reviewed later this year) as the latter is a separate but essential component of the Framework. This document primarily focuses on the risk architecture, the roles, responsibilities, communication and risk reporting arrangements that support the risk management process, by clearly setting out roles and responsibilities of both individuals and committees in one document. The Framework also includes the suggested process for escalation of risk, and acceptance of risks above UHB tolerance.

The revised Risk Management Framework, appended, reflects the current arrangements in place to facilitate and maintain a risk-aware culture across the UHB. However, it is anticipated that this may require further updating when the Once for Wales (OfW) system is implemented.

Argymhelliad / Recommendation

The Board is asked to **APPROVE** the Risk Management Framework.

Amcanion: (rhaid cwblhau) **Objectives: (must be completed)**	
Cyfeirnod Cofrestr Risg Datix a Sgôr Cyfredol: Datix Risk Register Reference and Score:	Not applicable

Safon(au) Gofal ac Iechyd: Health and Care Standard(s):	Governance, Leadership and Accountability
Amcanion Strategol y BIP: UHB Strategic Objectives:	All Strategic Objectives are applicable
Amcanion Cynllunio Planning Objectives	All Planning Objectives Apply
Amcanion Llesiant BIP: UHB Well-being Objectives: Hyperlink to HDdUHB Well-being Objectives Annual Report 2018-2019	10. Not Applicable

Gwybodaeth Ychwanegol: Further Information:	
Ar sail tystiolaeth: Evidence Base:	Legislation and national policy. ISO 31000, 2018 ISO Guide 73, 2009
Rhestr Termau: Glossary of Terms:	Explanation of terms is included within the body of the policy.
Partïon / Pwyllgorau â ymgynhorwyd ymlaen llaw y Cyfarfod Bwrdd Iechyd Prifysgol: Parties / Committees consulted prior to University Health Board:	As detailed in the assessment

Effaith: (rhaid cwblhau) Impact: (must be completed)	
Ariannol / Gwerth am Arian: Financial / Service:	Not applicable
Ansawdd / Gofal Claf: Quality / Patient Care:	Staff accessing written control documentation which is out of date, no longer relevant or contradicts current guidance may have a negative effect on the quality, safety and experience of care. It may also lead to unwarranted variation in care delivery
Gweithlu: Workforce:	Not applicable
Risg: Risk:	The presence of written control documentation on the intranet, outside of the Policies, Procedures and other Written Control Documentation intranet webpage, may result in staff accessing documents which are out of date, no longer relevant, or contradicting current guidance.
Cyfreithiol: Legal:	It is essential that the HDdUHB has up to date policies and procedures in place.

Enw Da: **Reputational:**	Not applicable
Gyfrinachedd: **Privacy:**	Not applicable
Cydraddoldeb: **Equality:**	An equality impact assessment has been undertaken for the policy.

Risk Management Framework

Policy information

Policy number: 608

Classification:
Corporate

Supersedes:
Previous versions

Local Safety Standard for Invasive Procedures (LOCSSIP) reference:
N/A

National Safety Standards for Invasive Procedures (NatSSIPs) standards:
N/A

Version number:
2.0

Date of Equality Impact Assessment:
18/05/2022

Approval information

Board
Complete

Date of approval:
Enter approval date

Date made active:
Enter date made active (completion by policy team)

Review date:
Enter review date (normally three years from approval date)

Summary of document:
This document aims to set out the components that provide the foundation and organisational arrangements for supporting risk management processes in Hywel Dda UHB.

Scope:
This framework applies to all UHB staff, contractors and other third parties working within the UHB. Managers at all levels within the UHB must take an active lead to ensure that risks are managed effectively and that a risk aware culture across the UHB is facilitated / maintained.

To be read in conjunction with:
156 - Risk Management Strategy and Policy (opens in a new tab)
674 - Risk Assessment Procedure (opens in a new tab)

Patient information:
Include links to Patient Information Library

Owning group:
Audit and Risk Assurance Committee (ARAC)
Date signed off by owning group

Executive Director job title:
Steve Moore – Chief Executive

Reviews and updates:
1.0 – New Policy
2.0 – Full Review including additional risk escalation process

Keywords
Risk, Risk Management, RM, Risk Management Framework

Glossary of terms
UHB - University Health Board
RASP - Risk Architecture, Strategy and Protocols
BAF - Board Assurance Framework
CRR - Corporate Risk Register
CEO - Chief Executive Officer
ARAC - Audit and Risk Assurance Committee
RM - Risk Management
SRO - Senior Reporting Officer
QSEC - Quality, Safety and Experience Committee

Term	Definition
Risk	The effect of uncertainty on objectives. Note that an effect may be positive, negative, or a deviation from the expected. Also, a risk is often described as an event, a change in circumstance or a consequence. (International Organisation for Standardisation (ISO) Guide 73, 2009)

Risk management	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. (The Institute of Risk Management)
Risk management framework	Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout the organisation. (ISO Guide 73, 2009)
Risk appetite	The amount and type of risk that an organisation is willing to pursue or retain (ISO Guide 73, 2009)
Risk tolerance	The organisation's readiness to bear a risk after risk treatment in order to achieve its objectives. (ISO Guide 73, 2009)
Risk owner	The person with the authority and accountability to manage the risk. (ISO Guide 73, 2009)
Risk exposure	The level of risk that the organisation is exposed, either in regard to an individual risk or the cumulative exposure to the risks faced by the organisation
ISO 31000, 2018	Generic risk management standard, which provides principles, framework and a process for managing risk, which can be used by any organisation, regardless of size, activity or sector
ISO Guide 73, 2009	Provides the definitions of generic terms related to risk management.
Hazard risks	"Pure" risks facing the organisation, which result in negative outcomes and disrupt normal operations / service delivery
Opportunity risks	Risk that is associated with the benefit of speculative opportunities

Contents

Introduction

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'. Risk management has become increasingly more important in recent times because of high profile corporate failures, increasing stakeholder expectations and the impact of global events such as COVID-19. As well as supporting better decision making and improved efficiency, risk management can also provide greater assurance to stakeholders.

Any risk management initiative must add value to the organisation. In short, risk management activities should be designed to achieve the best possible outcomes and reduce uncertainty of outcomes. A successful risk management process (and framework) should be:

- **P**roportionate to the level of risk within the organisation;
- **A**ligned to other business activities, e.g. planning;
- **C**omprehensive, systematic and structured;
- **E**mbedded within business procedures and protocols;
- **D**ynamic, iterative and responsive to change.

Risk management should be embedded into the University Health Board's (UHB) business and strategic planning, change management processes, day to day operations and compliance activities. If used successfully, 'risk management enhances strategic planning and prioritisation, assists in achieving objectives and strengthens the ability to be agile to respond to the challenges faced.' (The Orange Book, 2020).

Policy statement

This policy aims to set out the components that provide the foundation and organisational arrangements for supporting risk management processes in Hywel Dda UHB.

Scope

This framework applies to all UHB staff and Independent Members, contractors, other third parties working within the UHB and those who work in partnership with the UHB. All managers, (working in clinical as well as non-clinical/corporate functions/services within the UHB) must take an active lead to ensure that risks are managed effectively and drive the development of a risk aware culture within the UHB.

Aim

The aim of this document is to:

- set out the components that provide the foundation and organisational arrangements for supporting risk management processes in Hywel Dda UHB.

The overall aim of risk management is to:

- Ensure conformity with applicable rules, regulations and mandatory obligations;
- Provide assurance to the Board and the Audit and Risk Assurance Committee (ARAC) that risk management and internal control activities are proportionate, aligned, comprehensive, embedded and dynamic;
- Support decision-making through risk based information; and

- Provide effective and efficient strategy, operations and compliance activities.

Objectives

The aim of this document will be achieved by the following objectives:

- Managers and staff to be aware of this policy and its implications, and adhere to its principles in carrying out their duties.

Risk Management Framework

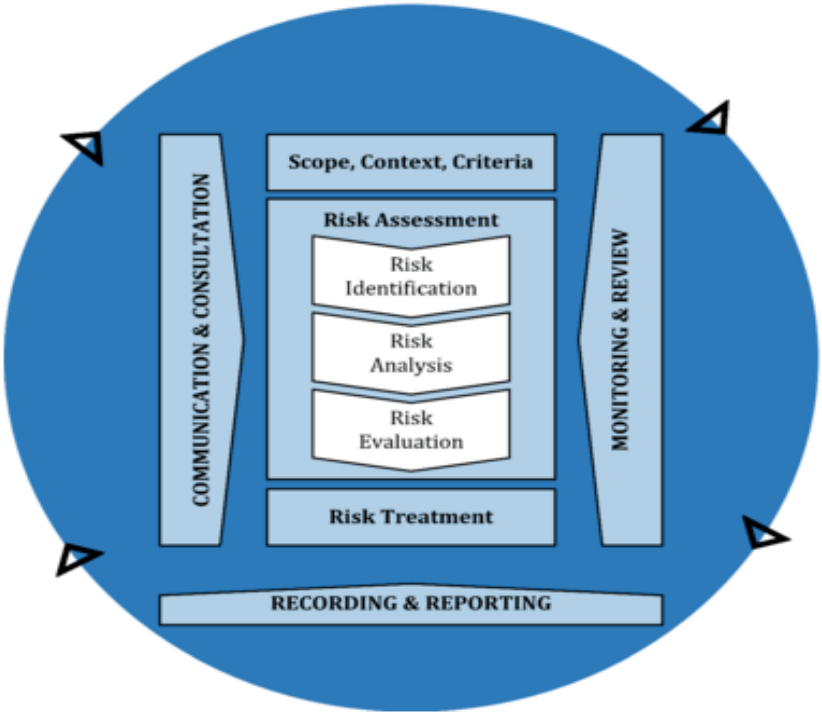
An organisation will describe its framework for supporting risk management by way of the risk architecture, strategy and protocols (RASP) that it is built around and supports the risk management process. It sets out the roles and responsibilities of the individuals and committees that support the risk management process. The risk strategy should set out the objectives that risk management activities are seeking to achieve, and the risk protocols describe the procedures by which the strategy will be implemented and risks are managed.

Fundamentals of Risk Management (2020)

Risk Management Process

Risk management should be a continuous process that supports the development and implementation of the strategy of the UHB. It should methodically address all the risks associated with all the activities of the UHB (including the influence of external factors (e.g. third party partnerships)), such as strategy, operational activities and compliance with legislation/standards. This will include identifying the potential for events that constitute threats to success, opportunities for benefit or an increased degree of uncertainty.

The risk management process can be presented as a list of coordinated activities as illustrated below:



(ISO 31000, 2018)

The primary reason for undertaking risk assessments is to ensure that current controls can be validated and the need for further actions (risk treatment) to improve control of the risk can be identified. Controls are things that the organisation has in place which makes a risk less likely to occur, or to mitigate the risk if it does materialise, i.e. people, processes, systems, policies, etc.

The aim of risk management is not necessarily to remove risk altogether but to manage risk to an acceptable level, taking into account the cost of minimising the risk and reducing risk exposure.

Risk Registers

The risk management process is recorded via the Datix Risk Module and reported via a risk register report. A risk register will provide an agreed, standardised approach to recording of the significant risks that have been identified through the risk assessment process, ownership of those risks, and will also serve as a record of the control activities that are currently undertaken to manage or mitigate the risk. It will also provide a record of the additional actions that are proposed to improve 'control' of risks (i.e., to treat the risk further), including responsibility and timescales for implementation. The Datix Risk Module allows us to provide risk registers reporting at different levels (Corporate, Directorate and Service level), as well as reporting of similar types of risks for oversight by specialist areas and functions within the UHB such as Workforce.

All recorded risks on Datix are exported to the UHB Risk Performance Dashboard on a fortnightly basis. The UHB Risk Performance Dashboard offers all managers a more dynamic

and accessible way of reviewing risks, and provides reliable performance data in an easily accessible format using Power Business Intelligence (BI).

A well-constructed and dynamic risk registers at the heart of a successful risk management process. In order for risk management to be effective and make a significant contribution to the organisation, the risk register needs to become a document that drives changes and improvements. Therefore, it can sometimes be better to think of the risk register as a 'risk management action plan'.

As such, risk registers are used to provide assurance that risks are being managed appropriately and effectively. This is undertaken through formal monitoring and scrutiny processes by the UHB's Committee structure who will seek assurance on behalf of the Board (see section 'Committee Duties and Responsibilities (2nd line of defence)'

Risks can be recorded on different levels of risk registers depending on the type and severity of risk, as per the following sections below:

- Board Assurance Framework (BAF)
- Corporate Risk Register (CRR)
- Operational Risk Register (ORR)
  - Directorate Level Risks
  - Service Level Risks
- Project/Programme Risk Registers

Board Assurance Framework (BAF)

The BAF enables the Board to focus on those risks which may compromise the achievement of strategic objectives. The BAF provides a structure and process to enable the organisation to focus on its principal risks. It will also highlight any key controls that have been put in place to manage the risk, sources of evidence or assurance, and any gaps requiring further action. The BAF is more than a risk register as it provides evidence through 'assurance' on the achievement of the UHB's strategic objectives. It should support effective decision-making and inform Board agendas in addition to providing assurance on the system of internal control.

The Executive Team has responsibility to discuss and agree the BAF and any amendments, to ensure there is appropriate scrutiny and challenge of principal risks prior to the BAF being submitted to the Board. This will include:

- Ensuring existing principal risks have been updated by the risk owners and reflect the current position;
- Considering closure or de-escalation of any principal risks to operational risk registers; and
- Agree the submission of any new principal risks.

It is in the interests of the Executive Team to work collectively to manage these principal risks to ensure that the strategic objectives are delivered within the agreed timescales, thus increasing the UHB's probability of success and reducing the likelihood of failure.

Principal risks are closely aligned to the UHB planning process to ensure the Board is aware of the risks to achieving objectives when approving its plan.

The Board has delegated some of its role of scrutiny of the assurances on the BAF to its Committees to make the most appropriate and efficient use of expertise. Therefore, these Committees must also ensure that assurance reports relevant to the principal risks are received and scrutinised, and an assessment made as to the level of assurance it provides, taking into account the validity and reliability (i.e. source, timeliness, methodology behind its generation and its compatibility with other assurances). This enables the Board to place greater reliance on assurances if they are confident that they have been robustly scrutinised by one of its Committees. It also provides Board with greater confidence about the likely achievement of strategic objectives, as well as providing a sound basis for decision-making. It is the role of Committees to challenge where assurances, in respect of any component, are missing or inadequate. Any gaps are escalated to the Board.

Corporate Risk Register (CRR)

The CRR is a log of significant risks that have been identified from a top down and bottom up approach. These are significant risks that affects the organisation's ability to achieve its planning objectives (linked to directorate objectives), and significant operational risks affecting the delivery healthcare services in the 'here and now'. The Executive Team is responsible for approving the escalation of operational risks on the CRR, and subsequent de-escalation/closure of risks on the CRR (see appendix 1 and appendix 2).

Whilst each Director will be responsible for the ownership of risk(s) and identifying current controls and developing action plans, it will be the role of Executive Team, at its formal monthly Executive Risk Group meeting, to review controls and ensure appropriate action plans are in place, which might include the development and agreement of corporate risk management strategies to manage risk(s). It will also be the role of the Executive Team to recommend to the Board the 'acceptance' of those risks that cannot be brought within the Board's risk appetite through the CRR report and/or Committee update reports to Board. The Board must be provided with assurance that everything that can be done, has been done to reduce the risk and that there are effective plans and controls in place to manage the situation should the risk materialise. This will help limit damage, control loss and contain costs for the UHB. Whilst a risk may be accepted by the Board, the risk owner must ensure that the current control measures will be regularly reviewed to ensure they remain effective. This process is outlined in appendix 4.

The Executive Team should also use risk information, including discussions from Committees, to inform prioritisation of resources and decision-making, i.e. by ensuring risk information is fed into different business processes within the UHB such as capital planning, budget planning, workforce planning, etc.

Each risk on the CRR has been mapped to a Board level Committee to ensure that risks on the CRR are managed appropriately, taking account of gaps, planned actions and tolerances, and provide assurance to the Board through their update report to the Board on the management of these risks. The Executive Risk Owner is responsible for discussing acceptance of risk above UHB tolerance level with the Executive Team, before being presented to the relevant Board/Committee for approval.

Operational Risk Registers (ORR)

The operational risk registers should include operational risks associated with:

- the achievement of directorate or service objectives;
- the day to day operation of the directorate or service, i.e., delivering a safe and sustainable service for patients; and
- any legislation or standards that the directorate or service should be compliant with.

Operational risks are mostly identified by a bottom up approach. In the UHB there are two risk register levels (service and directorate level). The majority of operational risks are identified initially at service level and escalated to directorate level when affecting directorate objectives and delivery, or risk treatments are outside the delegation of the service.

Service Level Risks

- Service level risks are risks which affect a service;
- The Head of Service/Departmental Manager is responsible for approving the inclusion and closure of operational risks on to the service risk register, as well as highlighting risks to the relevant Executive Director (or Director/General Manager for the Operations Directorate) for possible escalation or request for acceptance of risk above UHB tolerance (see appendix 2);
- The relevant Executive Director (or Director/General Manager for the Operations Directorate) is responsible for approving service level risks being escalated to directorate level (see appendix 2);
- The Executive Risk Owner is responsible for agreeing acceptance of service level risks above UHB tolerance and reporting this decision to the Executive Team, as well as presenting any service level risks to the Executive Team for approval for inclusion on to the CRR (see appendix 1).

Directorate Level Risks

- Directorate level risks are any risks that affect the directorate and its objectives, or risks that have been escalated from service level (see appendix 1);
- The relevant Executive Director (or Director/General Manager for the Operations Directorate) is responsible for approving the inclusion and closure of operational risks onto the directorate risk register, de-escalation to the service level risk register, highlighting risks for possible escalation to CRR or request for acceptance of risk above UHB tolerance (see appendix 2);
- The Executive Risk Owner is responsible for presenting any Directorate level risks to the Executive Team for approval for inclusion on to the CRR;
- The Executive Risk Owner is responsible for agreeing acceptance of directorate level risks above UHB tolerance level and reporting this decision to the Executive Team. The decision will also be reported to the relevant Board/Committee through the operational/corporate risk report.

Risks identified within operational risk registers are aligned by the management leads to a formal Committee or Sub-Committee, which will provide assurance through the parent Committee (e.g., QSEC) to the Board that operational risks are being identified, assessed and

managed effectively. Further details can be found in the section on 'Board Committees' and 'Sub-Committees' below.

Project/Programme Risk Registers

Every project or programme should maintain a risk register. Those projects or programmes managed through the organisational project and programme management tool have risk registers included by default, on which risks to that project or programme can be reported before being transferred or managed. Project risk management is concerned with the risks embedded within delivery of the project or programme (i.e. delivering the project or programme on time, within budget and within specification), and aims to reduce the variance between anticipated outcomes and actual results.

A project risk register should be populated and updated regularly throughout the duration of the project and should help prioritise risk management activity. Project/programme risks are managed/reviewed outside of the Datix system by the relevant Senior Responsible Officer (SRO). Risks are reported through project group risk registers, and other groups with responsibility for project oversight (e.g. Capital Sub Committee), to provide assurance on the management of the risks and the delivery of relevant capital and digital projects funded by discretionary and all Wales capital. Where a project/programme has the ability to impact on operational activity i.e. business continuity, these should be reported within the project risk register for the SRO and transferred to Datix before being recorded as closed, to ensure that all risks are captured and managed appropriately.

Risk Escalation

Risks should be managed by the risk owner, or the person appointed by the risk owner. However there may be circumstances where the ability to manage a risk may exceed the authority of the risk owner. These are some circumstances which may lead to risks being escalated:

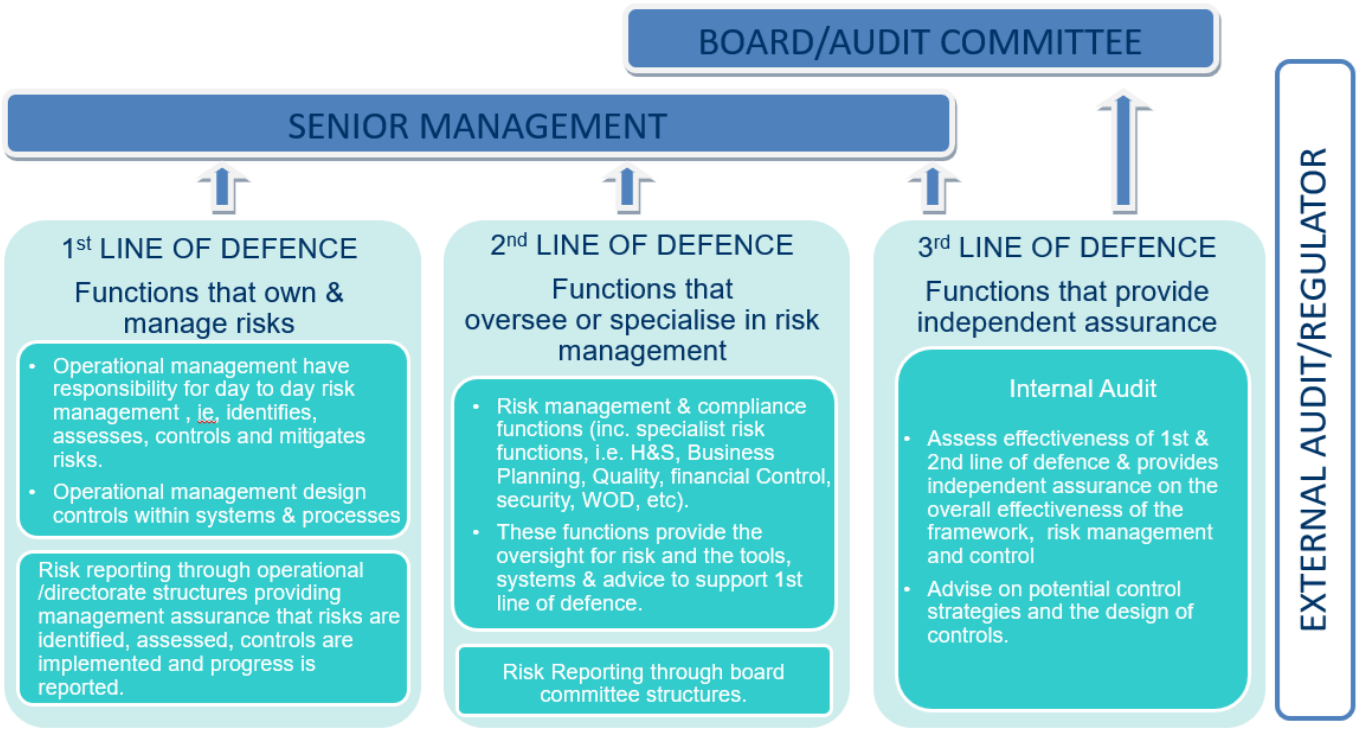
- Risk is above tolerance level and there is nothing that the risk owner can do to reduce it to within tolerance;
- Risk treatments are outside of the delegation of the risk owner; or
- A risk that is shared by other areas of the organisation where risk treatment cannot be agreed.

Where significant risks have been identified which are deemed challenging to manage, consideration should be given for the escalation of these risks to the next level of responsibility for additional risk action e.g. a service level may be considered for escalation to directorate level. This could include decisions for additional resources, increased oversight, review and acceptance of risk. Further guidance on risk escalation, which has been approved by the Executive Team, is outlined in appendix 1 and appendix 2.

Risk Architecture

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

The Three Lines of Defence Model
The UHB operates a 'Three Lines of Defence' model that outlines the principles for the roles, responsibilities and accountabilities for risk management as outlined below:



(based on IIA, 2013)

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.

These roles and responsibilities are further outlined in section 'Individual Responsibilities (1st line of defence)' to section 'Internal Audit (3rd line of defence)' below.

Responsibilities

Individual Responsibilities
Risk management is the responsibility of all staff. The following sections define the expectations of particular roles.

Chief Executive Officer

The Chief Executive Officer (CEO), as Accountable Officer, is responsible for systems of internal control and implementing the policies set by the Board. The CEO also has overall accountability for risk management within the UHB and as such is responsible for the annual signing of the Accountability Report including the Governance Statement, as well as devolving responsibility for the management of risk to relevant Executive Directors in accordance with the scheme of delegation.

Board Secretary

The Board Secretary is the delegated lead for ensuring that the UHB has an effective risk management framework in place to inform planning and decision-making within the UHB.

Assistant Director of Assurance and Risk

The Assistant Director of Assurance and Risk will support the Board Secretary to ensure that the UHB has an effective risk management framework in place and is responsible for:

- Developing and maintaining the BAF and the CRR for the Board;
- Facilitating a risk-aware culture within Hywel Dda UHB;
- Developing the risk management framework and strategy;
- Developing the risk appetite statement and acceptable risk tolerance levels;
- Undertaking an assessment of the UHB's risk maturity; and
- Ensuring risks are reported, monitored and scrutinised by the Board and its Committee structure.

Head of Assurance and Risk

The Head of Assurance and Risk is responsible for the development of an effective risk management process and framework. The Head of Assurance and Risk will support the Assistant Director of Assurance and Risk with the responsibilities listed in section 'Assistant Director of Assurance and Risk' above, as well as:

- Implementing the risk management framework and strategy, including the risk appetite and tolerance levels across the organisation;
- Establishing and implementing internal risk procedures and guidelines;
- Co-ordinating risk management activities;
- Strengthening operational risk management arrangements; and
- Providing training, information and support to staff and managers.

Executive Directors

Executive Directors have responsibility for the ownership and management of principal (strategic) risks and operational risks within their portfolios. These responsibilities include:

- Promoting a risk-aware culture within their directorate;
- Identifying strategic (principal) risks associated with the delivery of strategic objectives;
- Identifying new and escalating risks for inclusion on the corporate risk register;
- Ensuring there are processes in place within their Directorate to
  - Approve risks emerging from services/departments to be included on the directorate level risk register(s);
  - Oversee the co-ordination, updating and validation of risk registers from services/departments within their directorate;
  - Communicate and monitor risks within their directorates; and

- Ensuring that the directorate risk management processes are managed in accordance with the UHB Framework.

Lead Executive Directors, as risk owners, are responsible for managing risks to an acceptable level and if this is not possible, to report the acceptance of risk above the UHB tolerance level to the Board, or appropriate Board level Committee, depending on the level of the risk (See appendix 1).

Managers

Managers, working in clinical as well as corporate functions/services, take the lead on risk management and set an example through visible leadership of their staff. These responsibilities include:

- Taking responsibility for managing risk;
- Ensuring that risks are assessed that are:
  - Identified within the working activities carried out within their management control;
  - Identified within the environment within their control;
  - Reported from the staff within their management control.
- Identifying and managing risks that cut across delivery areas;
- Discussing risks on a regular basis with staff and through discussions at meetings to help improve knowledge about the risk faced; increasing the visibility of risk management and moving towards an action focussed approach.;
- Ensuring risks are updated regularly and acted upon;
- Communicating downwards what the top risks are;
- Reporting and escalating risks from the front line.
- Linking risk to discussions on finance, and stopping or slowing down non-priority areas or projects to reduce risk as well as staying within budget, demonstrating a real appetite for setting priorities;
- Ensuring staff are suitably trained in risk management;
- Monitoring mitigating actions and ensuring action owners are clear about their roles and what they need to achieve;
- Ensuring that people are not blamed for identifying and escalating risks, and fostering a culture, which encourages them to take responsibility in helping to manage them;
- Ensuring that risk management is included in appraisals and development plans where appropriate; and
- Ensuring the adoption and operation of the risk management framework across their work area.

Staff

All staff are responsible for:

- Identifying and reporting hazards, risks and opportunities they may encounter within the working activities and environment:
  - To their manager if the hazard, risk or opportunity is within their department;
  - To another manager if outside their department.
- Reporting incidents and near misses;
- Ensuring visitors and contractors comply with procedures; and
- Contributing to the management of risks and opportunities within the scope of their activities and environment.

Specialist Risk Management Functions
These functions provide part of the second line of defence in respect of managing risks. The second line of defence consists of activities covered by several components of internal governance and relate to a number of functions within the UHB (health and safety, workforce, finance, risk management, quality, IT and other control departments). They provide the tools, information, knowledge and support to assist the first line of defence (operational management) manage risks.

This line of defence monitors and facilitates the implementation of effective risk management practices by operational management and assists the risk owners in reporting adequate risk related information up and down the organisation. These are usually management functions that may have some degree of objectivity, however are not entirely independent from the first line.

Independent Members
Independent Members have an important role in risk management within the UHB. This role is restricted to seeking assurance on the robustness of processes and the effectiveness of controls through constructive, robust and effective challenge to Executive Directors and senior management. It is not appropriate for Independent Members to be involved in the management of individual risks, but to understand and question risk on an informed and ongoing basis.

Additionally, Independent Members chair Board level committees, and in line with the relevant committee Terms of Reference, which 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.

Committee Duties & Responsibilities
Effective risk management requires a reporting and review structure to ensure that risks are effectively identified and assessed and that appropriate controls and responses are in place. Appendix 3 sets out process for monitoring risks through Board & Committee Structure.

The Board
The Board maintains overall accountability for effective risk management, and will have responsibility for the following key duties:

- Approving the UHB's framework and strategy for risk and assurance;
- Proactively determining and refreshing its risk appetite to underpin strategy, decision making and the allocation of resources, and ensure the right focus on risk management and reporting within the organisation;
- Setting the UHB's tolerance for risk and deciding what level of risk is acceptable;
- Agreeing strategic objectives and seeking assurance on the management of associated risks included in the BAF, reviewing its achievement against these objectives, and using this Framework as a dynamic tool to drive the board agenda;
- Reviewing the principal risks set out in the BAF, and those risks above tolerance in the risk categories for which the Board has agreed the lowest risk tolerance; and
- Regularly receive assurance that principal and corporate risks are being managed effectively.

The behaviour and culture of the Board are key determinants of the Board's performance. Independent Members and Executive Directors must constructively challenge each other in respect of risk to enable the UHB to maximise its opportunities and manage any threats to the achievement of its purpose, aims and objectives. The Board should have it in mind that it is the first line regulator on behalf of the public, and should be confident at all times that they understand and are alerted to any significant failures in controls or gaps in assurance (NHS Confederation, 2009).

The Audit and Risk Assurance Committee

The Audit and Risk Assurance Committee (ARAC) is responsible for overseeing risk management processes across the organisation and will have a particular focus on seeking assurance that effective systems are in place to manage risk, that the organisation has an effective framework of internal controls to address risks, and that the effectiveness of that framework is regularly reviewed.

The Committee is responsible for monitoring the assurance environment and challenging the build-up of assurance on the management of key risks across the year, ensuring that the Internal Audit Plan is based on providing assurance that controls are in place and can be relied on and reviewing the internal audit plan in year as the risk profiles change. The Committee will also take on responsibility for considering and recommending to the Board approval of the Risk Management Framework.

The Board will receive annual reports on Committee's activities to provide assurance that Committees have reviewed risks that are aligned to them to ensure that they are being managed appropriately and that the risk management framework and process is effective.

Board Committees

Board Committees are responsible for:

- Seeking assurance on management of corporate risks on CRR and providing assurance to the Board that risks are being managed effectively and report areas of significant concern, e.g., limited assurance, where risk appetite is being exceeded, lack of action;
- Review corporate and directorate-level risks over tolerance and where appropriate recommend the acceptance of risks that cannot be brought within the UHB's risk appetite tolerance;
- Identify through discussions any new/emerging risks and ensure these are assessed by management;
- Signpost any risks out of its remit to the appropriate UHB Committee;
- Use risk registers to inform meeting agendas to seek assurance on management of risks and the systems in place to provide assurance;
- Receive assurance through Sub-Committee Update Reports and other management group reports that risks relating to their areas are being effectively managed; and
- Provide annual reports to ARAC on the effectiveness of management of risks within its remit.

Sub-Committees

Sub-Committees are responsible for:

- Scrutinising appropriate directorate level risks over tolerance within their remit either through standard operational risk reports, through reports from services or assurance reports requested by the Sub-Committee;
- Gaining assurance that the risks are being appropriately managed, effective controls are in place and planned additional controls are being implemented;
- Identifying, through discussions, new risks emerging risks and ensure these are assessed by management;
- Providing assurance to the parent committee that risks are being managed effectively and report risks which have exceeded tolerance through Sub-Committee Update Reports;
- Signposting any risks out of its remit to the appropriate UHB Committee or Sub-Committee; and
- Using risk registers to inform meeting agendas;

Executive Team

The Executive Team collectively share responsibility for agreeing the risks on the CRR and the BAF prior to submission to the Board, to ensure there is appropriate scrutiny and challenge of principal risks, the current controls and assurances and the actions to address any gaps in these. The Executive Team have a pivotal role as a second line of defence, to determine risk management strategies for the more challenging risks that threaten the UHB's operations.

It is also the role of the Executive Team to agree that risks are being managed to an acceptable level, balancing priorities, resources and the risk to the UHB, and recommend this course of action to the Board. The Board must be provided with assurance that everything that can be done, is being done, to reduce the risk, and that there are effective plans and controls in place to manage the situation should the risk materialise. This will help limit damage, control loss and contain costs for the UHB.

Whilst a risk may be accepted by the Board, the risk owner must ensure that the current control measures will be regularly reviewed to ensure they remain effective and efficient. This process is outlined in Appendix 4.

The Executive Team will use risk information to inform prioritisation of resources, improve the decision-making process and feed into different business processes, i.e. IMTP/annual planning, budget planning, capital planning, etc.

Directorate Risk Management Arrangements

All directorates must have the necessary arrangements in place for good governance, quality, safety and risk management. This includes the:

- Identification, assessment and control of risks;
- Preparation and maintenance of an up to date directorate risk register;
- Monitoring and review of directorate risks, including the controls and management action, in line with guidance;
- Communication of risk information to relevant parties, e.g. those who are impacted or those responsible for using the controls; and
- Use of directorate risk registers to inform decision-making and allocation of resources.

Internal Audit

The relationship between risk management and Internal Audit is critically important. Risk management is concerned with the assessment of risk and the identification of existing and

additional controls whereas it is Internal Audit's role to evaluate these controls and test their efficiency and effectiveness. Internal audit are the 3rd line of defence, and should maintain independence from the management of risks. Evaluation of controls is undertaken through the Internal Audit programme of work. The Head of Internal Audit will:

- 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 Governance Statement;
- Focus the internal audit work on the significant risks, as identified by management, and auditing the risk management processes across the organisation;
- Audit of the organisation's risk management, control and governance through operational audit plans in a way which affords suitable priority to the organisation's objectives and risks; and
- 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.

Closing risks

A risk can be closed once it has been successfully managed or mitigated, to within the tolerance level set by the UHB (based on the domain and current risk score), it has been accepted or is within tolerance set by the UHB, or the risk has materialised and therefore has become an issue. Closing a risk is a formal process to which information on the risk being closed is documented.

Risk Strategy

The UHB has a Risk Management Strategy in place that sets out its risk management policy statement, its current risk appetite and objectives in respect of risk management.

The Board is responsible for approving the Risk Management strategy and is available on the UHB website and staff intranet site via the following link:

https://hduhb.nhs.wales/about-us/governance-arrangements/policies-and-written-control-documents/policies/risk-management-strategy-and-policy/ (opens in a new tab)

Risk Protocols

Risk protocols are the means by which the risk management strategy and architecture are delivered in practice and are the operational procedures and practices to put into effect the full range of activities within the risk management framework.

There is an information portal on the staff intranet https://nhswales365.sharepoint.com/sites/HDD_Corporate_Governance/SitePages/Risk.aspx (opens in new tab) where the following procedures, guidance, tools and templates can be accessed.

- Risk Strategy and Policy
- Risk Management Process
- Risk Assessment Procedure and flowchart
- Risk Scoring Matrix

- Risk Assessment Form

Training

Knowledge of how to identify, assess and manage risk is essential to the successful embedding and maintenance of effective risk management.

Specific training is provided to the Board and included as part of the Board's development programme.

Risk management training is provided to staff who are responsible for entering and managing risks on the Datix Risk Module by the Assurance and Risk Team.

Managers are required to assess the training needs of their staff regularly and specify the level of training staff require. This can be:

- Basic risk management awareness including risk assessment; and
- Management of risk for risk owners and/or risk management leads.

Review of the effectiveness of the Risk Management Framework

The UHB's risk management arrangements are reviewed annually as part of the Wales Audit Office's Structured Assessment process.

The UHB will also undertake an assessment of its risk maturity.

References

AcademiWales (2017) The Good Governance Pocket Guide for NHS Wales Boards. Available at: http://www.primarycareone.wales.nhs.uk/sitesplus/documents/1191/Pocket%20Guide%20for%20NHS%20Wales%20Boards%20English.pdf (opens in a new tab)

HM Government (2020) Orange Book: Management of risk - Principles and Concepts. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866117/6.6266_HMT_Orange_Book_Update_v6_WEB.PDF (opens in a new tab)

Hopkin & Thompson (2021) Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Enterprise Risk Management. 6th Ed. London: Kogan Page Ltd.

IIA (2013) The Three Lines of Defence in Effective Risk Management and Control. Altamonte Springs: The Institute of Internal Auditors Inc. Available at: https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf (opens in a new tab)

ISO 31000:2018(en) Risk management. Available at: https://www.iso.org/iso-31000-risk-management.html/ (opens in a new tab)

Welsh NHS Confederation (2009) The Pocket Guide to Governance in NHS Wales. Good Governance Institute. Available at:

http://www.wales.nhs.uk/sitesplus/documents/1064/NHS%20Wales%20Confed%20-%20Governance%20Pocket%20Book%20FINAL%5B1%5D.pdf. (opens in a new tab)

Appendix 1 – Escalation and Acceptance of Risk above UHB Tolerance

The risk management system includes the opportunity for escalation through the levels of risk management. Risks should be managed by the risk owner, or the person appointed by the risk owner. There may however be circumstances where the ability to manage a risk may exceed the authority of the risk owner.

Where significant risks have been identified which are deemed challenging to manage, consideration should be given for the escalation of these risks to the next level of responsibility for additional risk action. These could include decisions for additional resources, increased oversight, review, acceptance of risk), and also allows for it to be considered against other risks at that level in terms of its potential individual and cumulative impact(s) e.g. helicopter perspective across the directorate/corporate/etc. This allows for a higher level of authorisation to sanction the continued tolerance of increasingly higher levels of risk.

Risks which may need to be escalated (not an exhaustive list) – judgement is required:

- Risk is above tolerance level and there is nothing that the risk owner can do to reduce it to within tolerance;
- Risk treatments are outside of the delegation of the risk owner;
- A risk that is shared by other areas of the organisation where risk treatment cannot be agreed.
- Significant threat to achievement of Health Board objectives or targets;
- Assessed to be of significant concern (current risk score may be 'extreme').

It is the responsibility of the management lead to escalate a risk via the appropriate management structure. It will then be the responsibility of the next level of management to make a decision if further risk treatments can be implemented, if escalation is required, or if the risk may be required to be accepted above the UHB tolerance level.

Risks that are escalated to the level above (e.g. a service level risk escalated to directorate level, or a directorate level risk escalated to corporate level) should remain within the risk profile of the level that is responsible for the management of the risk. For example, a service may have a risk profile/register that includes risks at corporate, directorate and service level, and a directorate may have a risk profile/register that includes risks at corporate and directorate level.

Risks can be de-escalated when the higher level is satisfied with the management of the risk, e.g. the risk has been reduced, the risk has been accepted above tolerance level and there is no further benefit of higher-level oversight (see table below).

There may be circumstances where there is no alternative other than to accept a risk above the tolerance level set by the UHB, (for example no further actions can be taken by the UHB to reduce the risk, or it is not proportionate to reduce the risk taking into account current capacity/resources available). It is the responsibility of risk owners to highlight such risks to the Head of Service/ Departmental Manager/Director in order that it is evaluated to determine if it will be formally accepted above UHB tolerance level (see appendix 4). Where a judgement is made to request accepting a risk above UHB tolerance, the relevant Director/General Manager must obtain support by the Executive Risk Owner.

Once the Executive Risk Owner agrees to accept a risk above UHB tolerance level, the risk decision on Datix will be noted as 'Tolerate'. The rationale for tolerating the risk will be added, as well as including the 'Date of Decision' on Datix. The Executive Risk Owner will report the decision to accept the risk above UHB tolerance level to the Executive Team, as well as reported to the appropriate Board/Committee through the operational/corporate risk reports (with the exception of service level risks, see table below). The risk will remain noted as 'Tolerate' on Datix for a maximum of six months (earlier review of the risk may be required if the risk is determined to have worsened during this period), at which point it must be reviewed to establish if risk treatment can now be made, or any further escalation required.

The review and monitoring arrangements for each level of risk are as follows:

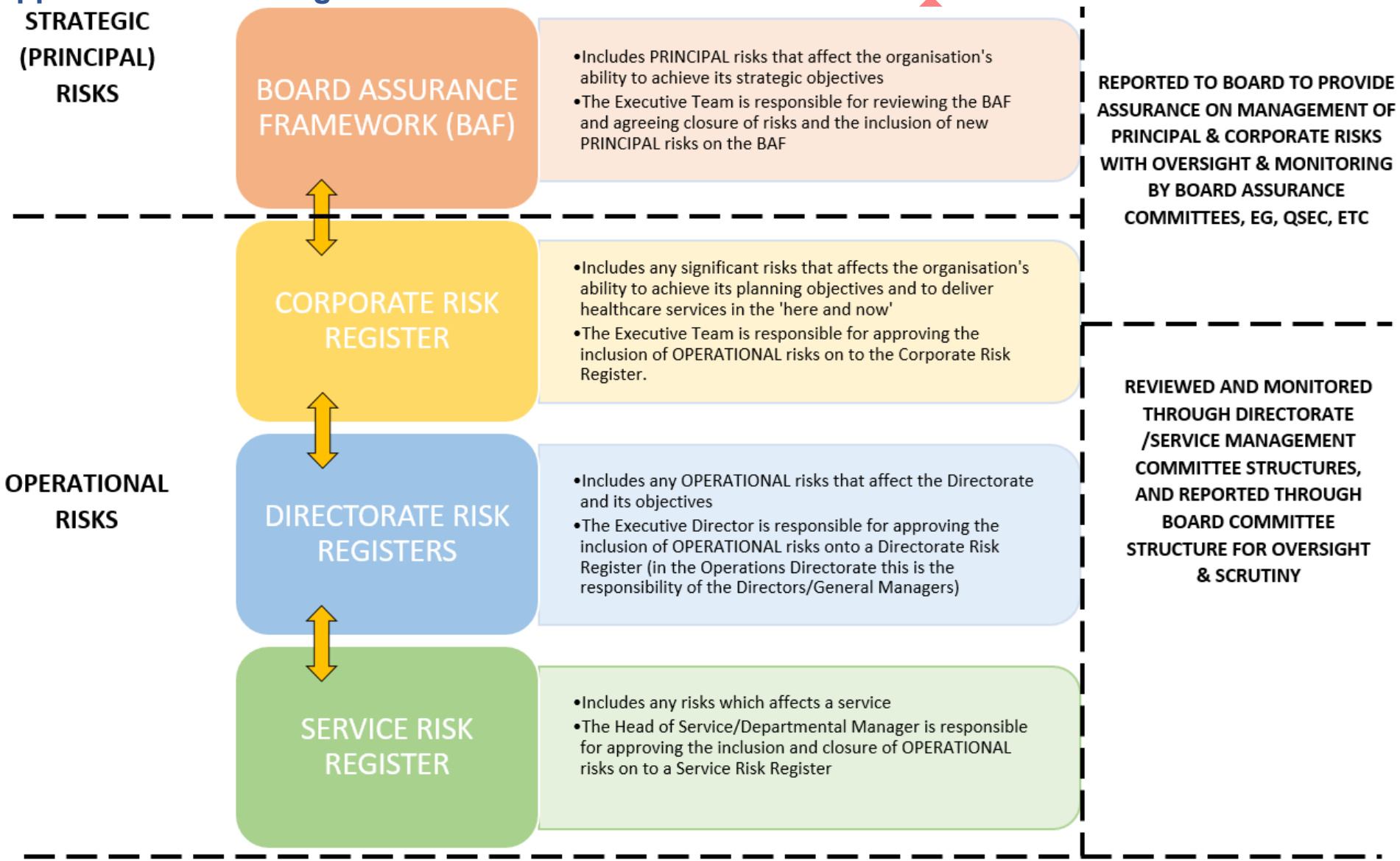
Risks	**Identification, management and review of risks**	**Management Monitoring, Oversight and Review Arrangements**	**Formal Committee Assurance Reporting, Oversight and Scrutiny**	**Acceptance of risks above UHB tolerance**
Principal risks	Executive Risk Owner / Management Lead	Executive Team	Board and Board level Committees	Board**
Corporate risks	Executive Risk Owner / Management Lead	Executive Team	Board and Board level Committees	Board**
Directorate risks	Management Lead	Directorate Lead and/or local Directorate management/ governance meetings *	Board Committees including Quality Governance meetings	Board Committee**
Service Risks	Management Lead	Service/Department Lead and/or local management/ governance meeting *	N/A – only Directorate level risks are reported through Health Board Committee structure	Executive Director

**Reporting at directorate and service Level on risk is the responsibility of risk owners*

***Executive Risk Owner must agree acceptance of risk above UHB tolerance, and report this decision to the Executive Team. The decision will also be reported to the relevant Board/Committee through the operational/corporate risk report.*

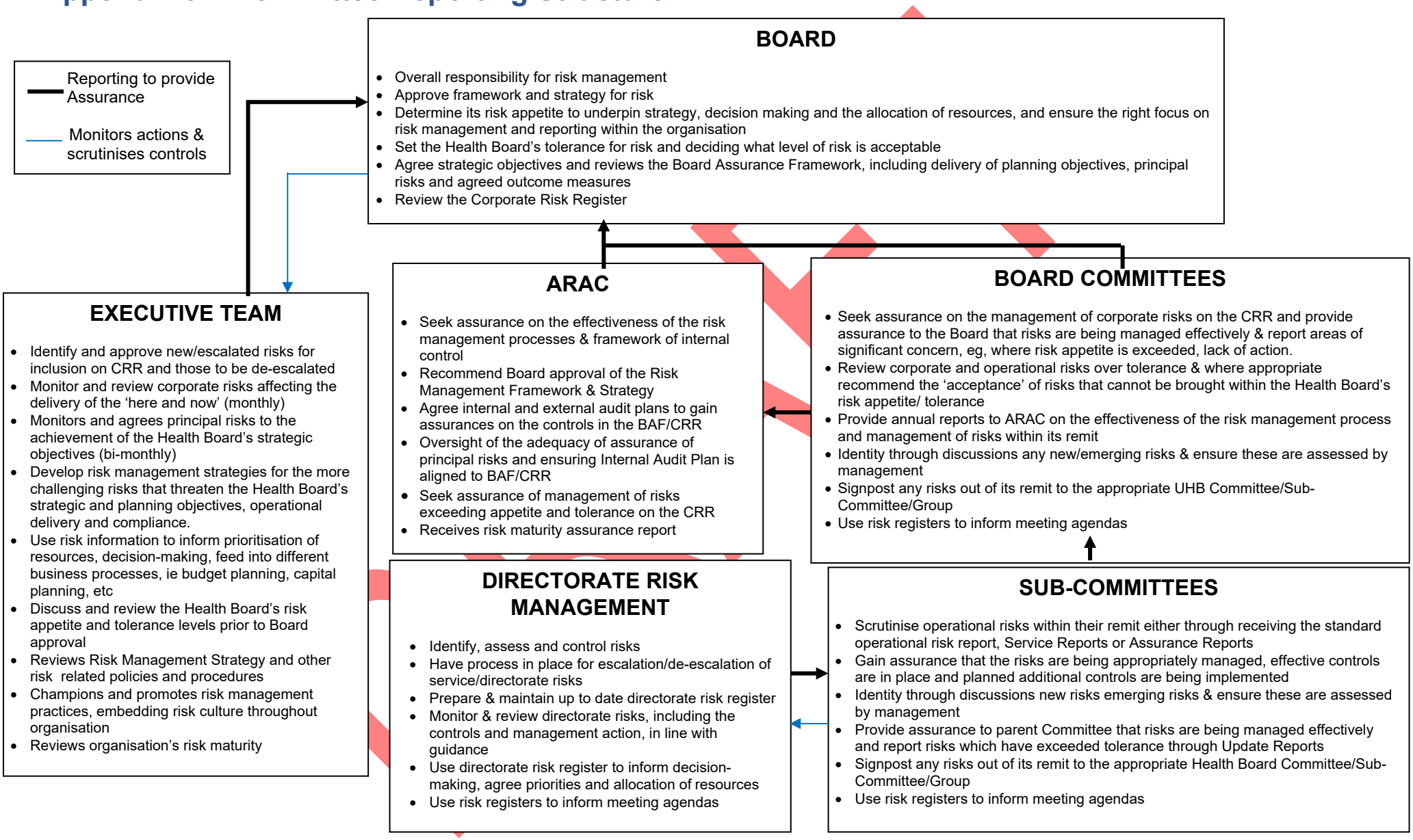
Please note: Project/programme risks are managed/reviewed outside of the Datix system by the relevant Senior Responsible Office (SRO).

Appendix 2 – Risk Registers



Please note: Project/programme risks are managed/reviewed outside of the Datix system by the relevant Senior Responsible Office (SRO), and are reported through project group risk registers and other groups with responsibility for oversight e.g. Capital, Estates, IM&T Sub Committee to provide assurance on capital projects.

Appendix 3 – Committee Reporting Structure



Appendix 4 – Risk Evaluation (accepting a risk)