Risk Management Framework

Policy Number: 608  
Supersedes: N/A  
Classification: Corporate

Version No | Date of EqLA | Approved by | Date of Approval | Date made Active | Review Date
---|---|---|---|---|---
V1 | 21/08/17 | Board | 28/09/2017 | 06/10/2017 | 28/09/2020

Brief 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.

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 the development of a risk aware culture within the UHB.

To be read in conjunction with: 156 – Risk Management Strategy and Policy

Owning Committee: Board

Executive Director: Sarah Jennings  
Job Title: Director of Governance, Communications & Engagement
Glossary of terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>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. (ISO Guide 73, 2009)</td>
</tr>
<tr>
<td>Risk management</td>
<td>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)</td>
</tr>
<tr>
<td>Risk management framework</td>
<td>Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout the organization. (ISO Guide 73, 2009)</td>
</tr>
<tr>
<td>Risk appetite</td>
<td>The amount of risk that an organisation is willing to pursue or retain (ISO Guide 73, 2009)</td>
</tr>
<tr>
<td>Risk tolerance</td>
<td>The organisation’s readiness to bear a risk after risk treatment in order to achieve its objectives. (ISO Guide 73, 2009)</td>
</tr>
<tr>
<td>Risk owner</td>
<td>The person with the authority and accountability to make the decision to treat, or not to treat, the risk. (ISO Guide 73, 2009)</td>
</tr>
<tr>
<td>ISO 31000, 2009</td>
<td>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</td>
</tr>
<tr>
<td>ISO Guide 73, 2009</td>
<td>Provides the definitions of generic terms related to risk management.</td>
</tr>
</tbody>
</table>

Keywords | risk, risk management, RM, risk management framework
HYWEL DDA UNIVERSITY HEALTH BOARD

CONTENTS

1. Introduction......................................................................................................................5
2. Scope ...............................................................................................................................5
3. Aim ...................................................................................................................................5
4. Risk Management Framework..........................................................................................5
5. Risk Management Process...............................................................................................7
6. Risk Registers..................................................................................................................7
   6.1. Board Assurance Framework (BAF) ..............................................................................8
   6.2. Corporate Risk Register (CRR) ..................................................................................8
   6.3. Project Risk Registers ..............................................................................................9
7. Risk Architecture..............................................................................................................9
   7.1. The Three Lines of Defence Model ..........................................................................9
   7.2. Individual Responsibilities.......................................................................................10
      7.2.1. Chief Executive Officer ..................................................................................10
      7.2.2. Director of Governance, Communications and Engagement ..........................10
      7.2.3. Board Secretary ..............................................................................................10
      7.2.4. Head of Assurance & Risk .............................................................................10
      7.2.5. Executive Directors .......................................................................................11
      7.2.6. Managers ......................................................................................................11
      7.2.7. Staff ..............................................................................................................12
      7.2.8. Specialist Risk Management Functions ..........................................................12
      7.2.9. Independent Members ...................................................................................12
      7.2.10. Internal Audit ...............................................................................................12
   7.3. Committee Duties & Responsibilities ......................................................................13
      7.3.1. The Board ..................................................................................................13
      7.3.2. The Audit and Risk Assurance Committee .....................................................13
      7.3.3. Business Planning & Performance Assurance Committee ...............................14
      7.3.4. Quality, Safety & Experience Assurance Committee .....................................14
      7.3.5. Mental Health Legislative Assurance Committee .........................................15
      7.3.6. University Partnership Board ........................................................................15
      7.3.7. Charitable Funds Committee ..........................................................................15
      7.3.8. Executive Team ...........................................................................................15
      7.3.9. Directorate Risk Management Arrangements ..................................................16
8. Risk Strategy .................................................................................................................16
9. Risk Protocols .................................................................................................................16
10. Training .........................................................................................................................17
11. Monitoring and Review of the effectiveness of the Risk Management Framework .......17
1. 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 and increasing stakeholder expectations. 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 initiative (and framework) should be:

- Proportionate to the level of risk within the organisation;
- Aligned to other business activities;
- Comprehensive, systematic and structured;
- Embedded within business procedures and protocols;
- Dynamic, iterative and responsive to change.

In particular, risk management should be embedded into the University Health Board’s (UHB) business and strategic planning and review, change management processes, day to day operations and compliance activities.

2. Scope
This framework applies to all UHB staff, contractors, other third parties working within the UHB and those who work in partnership with the UHB. Managers at all levels 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.

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

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 that risk management and internal control activities are proportionate, aligned, comprehensive, embedded and dynamic;
- Support decision-making through risk based information;
- Provide effective and efficient strategy, operations and compliance activities.

4. Risk Management Framework
ISO 31000 describes a framework for ‘implementing’ risk management, rather than a framework to 'support' the risk management process. The relationship between the principles (reasons) for managing risk, the framework in which it occurs and the risk management process are shown below:
An organisation will describe its framework for supporting risk management by way of the risk architecture, strategy and protocols (RASP). This 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.

Risk architecture
Roles, responsibilities, communication and risk reporting structure

Risk strategy
Risk strategy, appetite, attitudes and philosophy are defined in the risk management policy

Risk management process

Risk protocols
Risk guidelines for the organisation and include the rules and procedures, as well as the risk management methodologies, tools and techniques that should be used

ISO 31000 (2009)
5. 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. 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, 2009)

The primary reason for undertaking risk assessment is to ensure that current controls can be validated and the need for further actions 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, ie, people, processes, systems, policies, etc.

The aim of risk management is not 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 (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).

6. Risk Registers
The risk management process is recorded via a risk register. A risk register will provide an agreed record 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. It will also provide a record of the additional actions that are proposed to improve control of particular risks, including responsibility and timescales for the implementation of those intended controls.

A well-constructed and dynamic risk register is at the heart of a successful risk management initiative. 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’.
HYWEL DDA UNIVERSITY HEALTH BOARD

Risks can be recorded on 3 different risk registers depending on the type of risk (shown in Appendix 1).

6.1. Board Assurance Framework (BAF)

The BAF provides a mechanism for managing strategic (principal) risks. The BAF sets out strategic objectives, identifies risks in relation to each strategic objective and maps out both the key controls that should be in place to manage those objectives and the sources of assurance (evidence) that these controls are operating effectively. The BAF confirms that agreed actions are in place to address identified gaps in control or assurance. Additionally, the BAF is cross-referenced with operational risks. The BAF should drive the board agenda.

The Executive Team has responsibility to discuss 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 for approval. This will include:

1. Review the updates to the existing principal risks since it was last approved by the Board.
2. Consider de-escalation of any principal risks to operational risk registers and make this recommendation to the Board.
3. Agree the submission of any new principal risks to the Board for approval.

Although each strategic objective has a lead Executive Director, it is in the interests of the Executive Team to work collectively to manage these principal risks to ensure that the strategic objectives delivered within the agreed timescale, thus increasing the UHB’s probability of success and reducing likelihood of failure.

6.2. Corporate Risk Register (CRR)

The CRR is a log of significant risks that emanate from directorate risk registers which could affect the day to day operations of the UHB. Appendix 1 shows how operational risks are included on service and directorate risk registers and the relationship that exists between these. If operational risks materialise, their impacts tend to have an immediate effect and generally result in negative outcomes. The management of these risks usually involves putting in place measures to reduce the likelihood of the risk materialising and/or mitigating any potential impact, if the risk does materialise.

Operational risks should meet the following criteria for inclusion onto the CRR:

1. The risk exceeds tolerance level (risk score of 15 or more for 6 months or more) and
   a) Risk control is not within the directorate’s influence. This could be for a variety of reasons such as the risk requiring an enterprise-wide approach in its management (i.e. the involvement of other directorates) or it is beyond its resources to manage, or
   b) Risk control is not within the UHB’s influence (ie the UHB does not have direct control over the management of the cause of the risk but will be affected by its impact if the risk does materialise).

In addition, the Executive Team agreed that the Board should be advised of any significant new/emerging risks, which it considers is outside of the influence of an individual directorate or the UHB to manage.
The CRR is reviewed monthly by the Executive Team, who has 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 their role to agree that a risk has been 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, 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 3.

6.3. Project Risk Registers
Every project or programme should have a specific risk register on which risks to that project can be reported and managed. Project risk management is concerned with the risks embedded within delivery of the project or programme, ie, 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.

Significant risks to capital and I&MT projects are reported to the Capital, Estates and I&MT Sub-Committee for assurance to be gained on the management of the risks and the delivery of relevant projects.

7. 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.

7.1. 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:
Risk Management Framework

Please check that this is the most up to date version of this written control document

HYWEL DDA UNIVERSITY HEALTH BOARD

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.

Senior management and the Board collectively have 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 sections 7.2 & 7.3.

7.2. Individual Responsibilities

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

7.2.1. 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 Annual Governance Statement, as well as devolving responsibility for the management of operational risk to relevant Executive Directors in accordance with the scheme of delegation.

7.2.2. Director of Governance, Communications and Engagement

The Director of Governance, Communications and Engagement is the delegated lead for risk management in the UHB and is accountable for leading on the design, development and implementation of the integrated Board Assurance Framework and Risk Management Framework. This includes the following:

- Producing the UHB Annual Governance Statement;
- Ensuring the processes and systems for managing governance and compliance are fully tied to the risk register and Board Assurance Framework;
- Accountable for the Corporate Risk Register, escalation process, tracking of risk tolerance levels and developing the organisation’s risk appetite;
- Leading the embedding of risk management in the UHB.

7.2.3. Board Secretary

The Board Secretary is responsible for ensuring risk management policies and strategies are in place to inform planning and decision-making within the UHB and also to oversee the corporate risk register.

7.2.4. Head of Assurance & Risk

The Head of Assurance & Risk is responsible for the development of an effective risk management process and framework. This includes the following:

- Developing the risk management policy and strategy;
- Facilitating a risk aware culture within Hywel Dda;
- Establishing internal risk procedures and guidelines;
- Co-ordinating risk management activities;
- Compiling the board assurance framework and the corporate risk register for the Board;
HYWEL DDA UNIVERSITY HEALTH BOARD

- Ensuring risks are reported, monitored and scrutinised by the Board, committee and sub-committees;
- Providing training, information and support to staff and managers.

7.2.5. Executive Directors

Executive Directors have responsibility for the ownership and management of principal (strategic) risks and operational risks within their portfolios (appendix 2). These responsibilities include:

- Promoting a risk aware culture within their directorate;
- Signing off risks for inclusion on the corporate risk register;
- Approving risks emerging from services/departments to be included on the directorate risk register;
- Overseeing the co-ordination, updating and validation of risk registers from services/departments within their directorate;
- Establish local arrangements for communicating and monitoring of risks within their directorates;
- 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 this to the Board (See Appendix 3).

Lead Executive Directors of Board level committees, are also required, with the relevant Committee Chair, to provide a bi-annual report to the Audit and Risk Assurance Committee which provides assurance that risks are being managed appropriately and that the risk management framework and process is effective.

7.2.6. Managers

Managers 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 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;
HYWEL DDA UNIVERSITY HEALTH BOARD

- 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;
- Ensuring the adoption and operation of the risk management framework across their work area.

7.2.7. **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;
- Contributing to the management of risks and opportunities within the scope of their activities and environment.

7.2.8. **Specialist Risk Management Functions**

These 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 (compliance, risk management, quality, IT and other control departments). They provide the tools, information, knowledge and support to assist the first line of defence 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, but are not entirely independent from the first line.

7.2.9. **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, should 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 Chairs, with the Lead Executive Director, are also required to provide a bi-annual report to the Audit and Risk Assurance Committee to provide assurance that risks are being managed appropriately by risk owners and that the risk management framework and process remains effective.

7.2.10. **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
Please check that this is the most up to date version of this written control document

HYWEL DDA UNIVERSITY HEALTH BOARD

efficiency and effectiveness. This is undertaken through Internal Audit programme of work. Accordingly, 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 Annual 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;
- 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.

7.3. 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 4 sets out the process for monitoring risks through Board & Committee Structure.

7.3.1. 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 associated risks for inclusion 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.
- Reviewing the CRR on a quarterly basis and seek assurance from Executive Directors that 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).

7.3.2. The Audit and Risk Assurance Committee
The Audit & Risk Assurance Committee 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 principal risks (those likely to directly impact on achieving strategic objectives), 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 and overseeing development of the Assurance Framework.

The Audit & Risk Assurance Committee will receive bi-annual reports from Board level committees, which will provide them with assurance that risks are being managed appropriately and that the risk management framework and process is effective.

7.3.3. Business Planning & Performance Assurance Committee
The Business Planning & Performance Assurance Committee is responsible for providing assurance to the Board that risks relating to finance, performance, productivity, access to services, innovation, partnership working and public health are being effectively managed across the whole of the UHB’s activities (including for hosted services and through partnerships and Joint Committees as appropriate).

The Board have agreed that the Business Planning & Performance Assurance Committee will be the ‘Principal Committee’ for responsible for overseeing the management of all risks on the Board Assurance Framework on its behalf. The Business Planning & Performance Assurance Committee will scrutinise and seek assurance on the principal risks on behalf the Board.

Through its sub-committee structure, the Business Planning & Performance Assurance Committee will scrutinise and seek assurance that operational risks relating to the environment and estate infrastructure, information governance, IM&T, health, safety, security and fire and service/business interruption/disruption are being managed. The Sub-Committees will report the discussion on relevant risks and will include risks of over tolerance (risks with a score of 15 and over for 6 months or more) within their update report for the Committee to further scrutinise.

The Business Planning & Performance Assurance Committee will report any areas of significant concern to the Audit & Risk Assurance Committee and/or the Board, as appropriate, and signpost risks to other committees as appropriate.

7.3.4. Quality, Safety & Experience Assurance Committee
The Quality, Safety & Experience Assurance Committee is responsible to the Board for assuring the quality of patient care and service delivery in respect of clinical effectiveness, safety, patient and staff experience.

The Quality, Safety & Experience Assurance Committee may be requested to scrutinise and seek assurance on principal risks within the Board Assurance Framework in relation to quality and safety by the Board or Business Planning & Performance Assurance Committee.

Through its sub-committee structure, the Quality, Safety & Experience Assurance Committee will scrutinise and seek assurance that operational risks relating to quality and safety are being effectively managed. The Sub-Committees will report the discussion on relevant risks and will
include risks over tolerance (risks with a score of 15 and over for 6 months or more) within their update report for the Committee to further scrutinise.

The Quality, Safety & Experience Assurance Committee will report any areas of significant concern to the Audit & Risk Assurance Committee and/or the Board, as appropriate, and signpost risks to other committees as appropriate.

7.3.5. Mental Health Legislative Assurance Committee
The Mental Health Legislative Assurance Committee is responsible for providing assurance to the Board that risks relating to the UHB’s compliance of the Mental Health Act 1983 and Mental Health (Wales) Measure 2010.

The Mental Health Legislative Assurance Committee will review the Mental Health & Learning Disabilities Risk Register bi-annually to ensure that risks relating to compliance with mental health legislation are being appropriately managed by the Mental Health Legislation Scrutiny Sub-Committee. The Sub-Committee will report the discussion on relevant risks and will include risks over tolerance (risks with a score of 15 and over for 6 months or more) within their update report for the Committee to further scrutinise.

The Mental Health Legislative Assurance Committee will report any areas of significant concern to the Audit & Risk Assurance Committee and/or the Board, as appropriate, and signpost risks to other committees as appropriate.

7.3.6. University Partnership Board
The University Partnership Board is responsible for providing assurance to the Board on risks relating to maintaining its university status and any work within its remit.

Through its sub-committee structure, the University Partnership Board will scrutinise and seek assurance that operational risks relating to research and development are being managed. The Research and Development Sub-Committee will report the discussion on relevant risks and will include risks over tolerance (risks with a score of 15 and over for 6 months or more) within their update report for the University Partnership Board to further scrutinise.

The University Partnership Board will report any areas of significant concern to the Audit & Risk Assurance Committee and/or the Board, as appropriate, and signpost risks to other committees as appropriate.

7.3.7. Charitable Funds Committee
The Charitable Funds Committee is responsible for providing assurance to the Board on risks relating to the relating to control and management of the UHB’s charitable funds.

The Charitable Funds Committee will report any areas of significant concern to the Audit & Risk Assurance Committee and/or the Board, as appropriate, and signpost risks to other committees as appropriate.

7.3.8. Executive Team
The Executive Team collectively share responsibility for risk management and have responsibility for agreeing the risks on the CRR and the BAF prior to sign off by the Board.

The Executive Team has the responsibility to discuss the BAF and any amendments, 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, prior to the BAF being submitted to the Board for approval.

The CRR is reviewed and agreed monthly by the Executive Team, who has 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. This process is outlined in Appendix 3.

7.3.9. Directorate Risk Management Arrangements
All directorates must have the necessary arrangements in place for good governance, quality, safety and risk management.

Directorates, through management, have responsibility for risks to their services and for putting in place appropriate arrangements for the identification, assessment and management of risks. Directorates are also responsible for developing local arrangements for monitoring risk registers and communicating risk information.

8. 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 strategy was approved by the Board in November 2015 and is available on the UHB website and staff intranet site via the following link:

9. 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
http://howis.wales.nhs.uk/sitesplus/862/page/50619 where the following procedures, guidance, tools and templates can be accessed.

- Risk Scoring Matrix
- Risk Management Process
- Risk Assessment Procedure
- Risk Register Procedure
- Board Assurance Framework Procedure
- Risk Reporting Requirements
- Reviewing Risk Registers Guidance for Committees
- Risk assessment form
10. Training
Knowledge of how to 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.

Managers are required to assess the training needs of their staff annually and specify the level of training staff require. This can be:
- Basic risk management awareness including risk assessment;
- Management of risk for risk owners and/or risk management leads.

11. Monitoring and Review of the effectiveness of the Risk Management Framework
Board level Committee Chairs and executive leads are required to provide half yearly reports to the Audit and Risk Assurance Committee on the effectiveness of the risk management process and management of risks within their remit. Where there are areas of concern, the appropriate Executive Director will be invited to the Audit and Risk Assurance Committee to account for the position.

The UHB also completes the Governance, Leadership and Accountability Module on an annual basis as part of its end of year documentation. This is a self-assessment which forms part of the Health and Care Standards of the UHB’s governance arrangements, of which risk management forms an integral part of the Annual Governance Statement.

The Annual Governance Statement is signed by the CEO and sets out the organisational approach to internal control. This is produced at the end of the financial year and is scrutinised as part of the annual accounts process and presented to the Board with the accounts as part of the Annual Accountability Report.

The Head of Internal audit will also provide an opinion together with the summarised results of the internal audit work performed during the year. The overall opinion has been formed by summarising audit outcomes across eight key assurance domains:
- Financial governance and management;
- Corporate governance, risk management and regulatory compliance;
- Operational services and functional management;
- Clinical governance, quality and safety;
- Information governance and security;
- Workforce management;
- Capital and estates management; and
- Strategic planning, performance management and reporting.

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

12. References


Appendix 1 – Risk Registers

13. Appendix 1 – Risk Registers

- **Strategic (Principal) Risks**
  - Strategic Risk Register/Board Assurance Framework (BAF)
    - Includes any risk that affects the organisation's ability to achieve its strategic objectives.
    - The Executive Team discusses the inclusion of these risks prior to the Board approving their inclusion on the BAF and becoming Principal risks.

- **Operational Risks**
  - Corporate Risk Register
    - Includes any operational risks which exceed tolerance and where risk control is not within the gift of an individual Directorate, out of the Health Board's gift and requires additional corporate management.
    - The Executive Team is responsible for approving the inclusion of operational risks on to the Corporate Risk Register.
  - Directorate Risk Register
    - Includes any operational risks that affect the Directorate and its objectives (operational).
    - The Executive Director is responsible for approving the inclusion of operational risks onto the Directorate Risk Register (in the Operations Directorate this is the responsibility of the Directors/General Managers).
  - Local (Service/Department Risk Register)
    - Includes any risk which affects a service or department.
    - The Head of Service/Departmental Manager is responsible for approving the inclusion of operational risks on to Service/Department Risk Registers.

- **Project Risks**
  - Project Risk Register
    - Includes any risk which affects the delivery of project, programme, plan, scheme or change.
    - The Project Lead is responsible for approving the inclusion of project risks on to Project Risk Registers.

**Reported to Board for Approval of New Risks/Risk Removals with Oversight & Monitoring by Business Planning & Performance Assurance Committee**

**Monitored Through Directorate Management Committee Structures and Reported Through Board Committee Structure for Oversight & Scrutiny**

**Reported Through Project Group & Other Groups with Vested Interest (e.g., Capital, Estates, IM&T SUB Committee to Provide Assurance on Capital Projects)**
## 14. Appendix 2 – Executive Risk Ownership

### Deputy Chief Executive/Executive Director of Operations

<table>
<thead>
<tr>
<th>3 Counties inc</th>
<th>Unscheduled Care: Bronlais Hospital Site inc</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Integrated Therapies</td>
<td>- Neurology Pathway</td>
</tr>
<tr>
<td>- Cancer Services</td>
<td>- Gastrology Pathway</td>
</tr>
<tr>
<td>- Central Operations</td>
<td>- Unscheduled Care: Glangwili Hospital Site inc</td>
</tr>
<tr>
<td>- Estates &amp; Facilities</td>
<td>- Pathology</td>
</tr>
<tr>
<td>- Mental Health &amp; Learning Disabilities</td>
<td>- Radiology</td>
</tr>
<tr>
<td>- Scheduled Care</td>
<td>- Unscheduled Care: Prince Philip Hospital Site inc</td>
</tr>
<tr>
<td>- Unscheduled Care</td>
<td>- General Medicine (Diabetes &amp; Respiratory Pathways)</td>
</tr>
<tr>
<td>- Pathology</td>
<td>- Unscheduled Care: Withybush Hospital Site inc</td>
</tr>
<tr>
<td>- Radiology</td>
<td>- Stroke Pathway</td>
</tr>
</tbody>
</table>

### Director of Primary Care, Community & Long Term Care

<table>
<thead>
<tr>
<th>Community &amp; Chronic Conditions</th>
<th>Medicines Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Long Term Care</td>
<td>Primary Care</td>
</tr>
<tr>
<td>Low Vision</td>
<td></td>
</tr>
</tbody>
</table>

### Executive Director of Public Health

<table>
<thead>
<tr>
<th>Public Health</th>
<th>Emergency Planning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Children's Public Health</td>
<td>Substance Misuse</td>
</tr>
</tbody>
</table>

### Executive Director of Finance

| Finance Directorate risks | |
|---------------------------||

### Executive Director of Nursing, Quality and Patient Experience

<table>
<thead>
<tr>
<th>Effective Clinical Practice</th>
<th>Research &amp; Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical Education &amp; Knowledge</td>
<td>Revalidation &amp; Appraisal</td>
</tr>
</tbody>
</table>

### Executive Director of Workforce & OD

| Workforce directorate risks | |
|-----------------------------||

### Executive Director of Therapies & Health Sciences

| Therapies & Health Sciences | |
|-----------------------------||

### Executive Director of Planning, Performance & Commissioning

<table>
<thead>
<tr>
<th>Informatics</th>
<th>Planning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Governance</td>
<td>Commissioning</td>
</tr>
</tbody>
</table>

### Director of Governance, Communications & Engagement

<table>
<thead>
<tr>
<th>Assurance &amp; Risk</th>
<th>Strategic Partnerships</th>
</tr>
</thead>
<tbody>
<tr>
<td>Charitable Funds</td>
<td>Welsh Language</td>
</tr>
<tr>
<td>Equality &amp; Diversity</td>
<td></td>
</tr>
</tbody>
</table>

---

20 of 28 V1.0
15. Appendix 3 – Risk Evaluation

**Risk Decision**

Risk Assessment completed – What are you going to do next?

- Yes ➔ Continue to treat the risk to reduce likelihood and mitigate impact to bring it in line with risk appetite
- No ➔ Is the risk within tolerance for this type of risk? *NB Risk tolerance currently risk score of 15 or more for 6 months & over*

  - Yes ➔ Stop the activity
  - No ➔ Can the activity giving rise to the risk be terminated without giving rise to a higher risk?

    - Yes ➔ Stop the activity
    - No ➔ Does the Directorate have the resources (financial, people) to reduce this risk to within risk tolerance/risk appetite?

      - Yes ➔ Invest in putting in place additional controls and align to Directorate priorities
      - No ➔ Lead Executive to prepare paper for Board to ask the Board to accept the risk. Paper must set out current controls and their effectiveness, reasons why no further action can be taken, and assurance that the UHB is prepared if risk materialises.

**Director to add risk to Corporate Risk Register for the Executive Team to discuss and agree additional risk management strategies to reduce likelihood and mitigate impact**

- Yes ➔ Can further action be taken to reduce this risk, ie invest more resources?

  - Yes ➔ Feedback to Directorate Lead to take appropriate actions
  - No ➔ Are there sufficient controls in place to mitigate the risk if it does materialise, ie, have we taken all possible action to reduce the level of loss, limit the damage and contain the costs?

    - Yes ➔ Feedback to Directorate Lead to take the appropriate actions
    - No ➔ No ➔ Can the activity giving rise to the risk be terminated without giving rise to a higher risk?

      - Yes ➔ Stop the activity
      - No ➔ Is the risk within tolerance for this type of risk? *NB Risk tolerance currently risk score of 15 or more for 6 months & over*
16. Appendix 4 – Committee Reporting

**BOARD**
- Overall responsibility for risk management
- Approve framework and strategy for risk
- Determine 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 Health Boards tolerance for risk and deciding what level of risk is acceptable
- Agreeing strategic objectives and associated risks for inclusion in the Board Assurance Framework
- Reviewing the principal risks set out in the Assurance Framework, and those risks above tolerance in the risk categories for which the Board has agreed the lowest risk tolerance

**ARAC**
- Seek assurance on the effectiveness of the risk management processes & framework of internal control
- Recommending Board approval of the Risk Management Framework & Strategy
- Agreeing and internal and external audit plans to gain assurances on the controls in place

**BOARD COMMITTEES (eg BPPAC)**
- Seek assurance on the management of operational risks relating to patient safety & quality exceeding tolerance for over 6 months (reported through Sub-Committee reports)
- Provide assurance to the Board that risks are being managed effectively & report areas of significant concern, ie, where risk appetite is exceeded.
- Provide half yearly reports to ARAC on the effectiveness of the risk management process and management of quality and safety risks
- Identity through discussions any new/emerging risks & ensure these are assessed by management
- Signpost any risks out of its remit to the appropriate UHB Committee

**EXECUTIVE TEAM**
- Agrees risks for inclusion on Corporate Risk Register
- Develop risk management strategies for the more challenging risks that threaten the Health Board’s operations.
- Use corporate risk register to inform meeting agenda

**SUB COMMITTEES**
- Scrutinise risk registers within their remit
- Gain assurance that the risks are being appropriately managed, effective controls are in place and planned additional controls are being implemented
- Identity through discussions new risks emerging risks & ensure these are assessed by management
- Provide assurance to parent Committee that risks are being managed effectively and report risks which have exceeded tolerance

**DIRECTORATE RISK MANAGEMENT**
- Identifies, assesses and controls risks
- Prepares & keeps up to date directorate risk register
- Monitors & reviews directorate risk register, including the controls and management action
- Use directorate risk register to inform decision-making and allocation of resources

Reporting to provide assurance
Monitors actions & scrutinises controls
BUSINESS PLANNING & PERFORMANCE ASSURANCE COMMITTEE

*Responsible for monitoring the following risks*

- All principal risks on Board Assurance Framework
- Operational Risks
  - Finance risk register
  - Public Health risk register
  - Commissioning & performance risk register
  - Private patients risk register
  - Financial long term care risks
  - All operational risks relating to innovation, partnership working, compliance (other).
  - All risks exceeding tolerance levels which are reported to the BPPAC Sub-Committee structure

CAPITAL, ESTATES & IM&T SUB-COMMITTEE

*Responsible for monitoring the following risks*

- Planning Risk Register
- Environment & Estates Infrastructure risks
- IM&T risks

EMERGENCY PLANNING AND HEALTH & SAFETY SUB-COMMITTEE

*Responsible for monitoring the following risks*

- Health, Safety, Security & Fire
- Service/Business interruption

INFORMATION GOVERNANCE SUB-COMMITTEE

*Responsible for monitoring the following risks*

- Information governance
- IT Security
QUALITY, SAFETY & EXPERIENCE ASSURANCE COMMITTEE

Responsible for monitoring the following risks

- Principal risks on the BAF (on request from Board or BPPAC)
- Operational risks
  - All operational risks relating to patient safety & quality exceeding tolerance for over 6 months (included & reported through Sub-Committee reports)

WORKFORCE & OD SUB-COMMITTEE
Responsible for monitoring the following risks

- Workforce & OD Risk Register
- Oversight of all workforce risks
- Risks relating to medical education & revalidations and appraisal exceeding tolerance for over 6 months (included & reported through Sub-Committee reports)

ACUTE QSE SUB-COMMITTEE
Responsible for monitoring the following risks

- Scheduled care risk register
- Unscheduled care Risk Register
- Cancer Services Risk Register
- Women & Children Risk Register
- Central Operations Risk Register (except private patients)

IMPROVING EXPERIENCE SUB-COMMITTEE
Responsible for monitoring the following risks

- Concerns & Incidents Risks
- Welsh Language & Equality risks

MENTAL HEALTH & LD QSE SUB-COMMITTEE
Responsible for monitoring the following risks

- Mental Health & Learning Disabilities Risk Register

STRATEGIC SAFEGUARDING SUB-COMMITTEE
Responsible for monitoring the following risks

- Safeguarding Risks

PRIMARY & COMMUNITY QSE SUB-COMMITTEE
Responsible for monitoring the following risks

- 3 Counties Community Risk Register
- Primary Care Risk Register

EFFECTIVE CLINICAL PRACTICE SUB-COMMITTEE
Responsible for monitoring the following risks

- Clinical Practice risks (inc NICE, clinical audit)
- Risks relating to its TORs exceeding tolerance for over 6 months (included & reported through Sub-Committee reports)

Please check that this is the most up to date version of this written control document
Risk Management Framework

Please check that this is the most up to date version of this written control document
MENTAL HEALTH LEGISLATION ASSURANCE COMMITTEE

Responsible for monitoring the following risks

- Operational risks
  - All operational risks relating to the implementation and operation of the Mental Health Act 1983 and Mental Health (Wales) Measure 2010 exceeding tolerance for over 6 months (included & reported through Sub-Committee reports)

MENTAL HEALTH LEGISLATION SCRUTINY SUB-COMMITTEE

Responsible for monitoring the following risks

- All operational risks relating to the implementation and operation of the Mental Health Act 1983 and Mental Health (Wales) Measure 2010
UNIVERSITY PARTNERSHIP BOARD

Responsible for monitoring the following risks

- Operational risks
  - Relating to it maintaining its university status and any work within its remit
  - All operational risks relating to research and development exceeding tolerance for over 6 months (included & reported through Sub-Committee reports)

RESEARCH & DEVELOPMENT SUB-COMMITTEE

Responsible for monitoring the following risks

- Research & development risks
CHARITABLE FUNDS COMMITTEE

*Responsible for monitoring the following risks*

- Operational risks
  - Relating to the control and management of the UHB’s charitable funds

CHARITABLE FUNDS OPERATIONAL SUB-COMMITTEE