GIG CYMRU
NHS WALES

Ymddiriedolaeth
GIG Felindre
Velindre NHS Trust

Velindre University NHS Trust Risk Management Framework

Executive Sponsor: Lauren Fear, Director of Corporate Governance

Document Author: Lauren Fear, Director of Corporate Governance

Approved by: Trust Board

Approval Date: 24 September 2020

Review Date: September 2021

Version: Final Draft

Contents

1. Statement of Commitment

Velindre University NHS Trust (VUNHST) has built a strong reputation for safe, high quality care since its establishment in 1994. We are one of the leading providers of specialist cancer, blood and transplantation services together with the provision of first-class research, development and innovation that has local, national and global impact.

Made up of our **Corporate Services** (including our Workforce & Organisational Development; Finance; Quality & Safety; Governance & Communications; Planning, Performance & Estates; and Research & Innovation departments); **Velindre Cancer Centre** and the **Welsh Blood Service**; and a number of **Hosted Units**, including NHS Wales Informatics Service (NWIS), Health Technology Wales, and NHS Wales Shared Services Partnerships (NWSSP). We also work with other organisations and partners across health, local authorities, emergency services and the voluntary/charity sector; including Macmillan; Cancer Research Wales; Tenovus; and Maggie's Centre. Together we are bound by moral and legal obligations to improve the safety, quality and experience of our services for patients and donors. We are also obliged to protect our employees, volunteers and visitors/members of the public; as well as to protect our material assets and minimise any losses and liabilities as good stewards of public money.

We will not be able to meet the ambitions set out in our Five Strategic Pillars, including our Integrated Medium-Term Plan (IMTP) if we do not take risks. It is only by being innovative that we will meet the challenges for the future, and by continually looking for new and innovative ways of working, in the full knowledge of the potential risks involved.

As such, VUNHST acknowledge that some inherent risk will always exist, and that residual risk will never be fully eliminated. We are therefore committed to adopting best practice in the identification, evaluation and cost-effective control of risks to ensure that they are reduced to an acceptable level or eliminated where reasonably practicable; and that all opportunities to achieve our objectives, are maximised.

Risk management within VUNHST is a long-term commitment and an inherent part of good management and governance practices. To succeed, our strategy for risk must have the **full support of Board members** and be supported by the **active participation of the Trust Executive** and senior management, thereby improving our ability to deliver our priorities and improve outcomes.

With this in mind **all employees** must understand the nature of the risks they face and accept responsibility for risks associated within their area of work. In doing this they will receive the necessary support, assistance and commitment from senior management and Board Members.

Chief Executive Officer
Mr Steve Ham

Chair
Professor. Donna Mead. OBE

2. Background

2.1 Purpose and context

The provision of healthcare is by its nature, a high-risk activity and the process of risk management is an essential control mechanism. To ensure that the care provided at VUNHST is safe, effective, caring, responsive to patient and donor needs and well-led, the VUNHST Board must be founded on and supported by a strong governance structure. Effective risk management processes are central to providing the Board with assurance on potential risk exposure and the appropriateness of governance arrangements. Failure to implement effective risk management processes could severely impact VUNHST's ability to deliver its objectives, affecting its reputation, resulting in serious consequences – both financial and non-financial.

VUNHST aim to make risk management integral to our culture. This Risk Management Framework (RMF) describes how we plan to do that and forms part of our internal control and governance arrangements. It defines the strategy, principles and mandatory requirements for how risks are consistently managed and embedded at all levels 'from Ward to Board', highlights key aspects of the risk management process, and identifies the main reporting and escalation procedures.

The underlying risk principles applied throughout this framework are consistent with the overarching principles of *HM Treasury's Orange Book 'Management of Risk – Principles and Concepts', 2020*; and ISO 31000: 2018 *'Risk Management – Guidelines'*. The framework also supports the UK Corporate Governance Code 2018 and the Financial Reporting Council's *'Guidance on Risk Management, Internal Control and Related Financial and Business Reporting'*.

This document should be read in conjunction with our Risk Appetite Strategy, Trust Assurance Framework (TAF), Risk Management Process (Procedures Manual) and other associated risk management guidance.

2.2 Definitions

Risk can be defined as the "effect of uncertainty on objectives". This definition recognises that we operate in an uncertain world and that potential threats, actions or events may occur (internally or externally) which could adversely or beneficially affect our ability to deliver our strategic priorities, legislative responsibilities, major programmes and business plan objectives.

To ensure consistency of understanding across our Corporate service teams, Divisions and Hosted Units, we have compiled a comprehensive list of risk management terms and definitions.

These are intended as key references for those involved in risk management and are largely based on the definitions in the Risk Management Dictionary to ISO 31000: 2018, *Risk Management – Guidelines*.

Key definitions are highlighted below:

Term	Definition
Risk	'effect of uncertainty on objectives'
Risk management	'co-ordinated activities to direct and control an organisation with regard to risk'
Risk management framework	'set of activities / arrangements for designing, implementing, monitoring, reviewing and continually improving risk management'
Key Control (also referred to as 'internal controls' or mitigating actions')	'measure that maintains and/or modifies risk' / measure, currently in place, that maintains and/or modifies a risk's likelihood and/or impact'
Impact (also referred to as 'consequence')	'outcome of an event affecting objectives' i.e., the effect (i.e., on the organisations finances, infrastructure, and/or reputation etc.) when a risk materialises.
Likelihood (also referred to as 'probability' or 'frequency')	'chance of something happening' i.e., valuation or judgement regarding the chances of a risk materialising.
Risk Register / Trust Risk Register (TRR)	'a log of all the risks that may threaten the success of the Trust in achieving its declared aims and objectives". It will operate at both a local (Department/Division) and organisational (Trust) level and will include Board Assurance Framework managed risks. The TRR is the principle tool that the Trust will use for managing its risk assessment systems and processes.
Trust Assurance Framework (TAF)	'a high level management assessment process and record of the principal risks relating to the delivery of strategic objectives and the strength of internal control to prevent risks occurring. It identifies sources of control and assurance and evaluates them for suitability. By receiving and reviewing actual assurances and using findings, the adequacy of internal control can be confirmed or modified.'
Issue	'an event which has happened and is currently having a negative impact. Issues require immediate attention and action in real-time and may be a result of risks identified or they may have come from an unseen area.'
Inherent risk (also known as the gross risk)	'exposure arising from a specific risk before any action has been taken to manage it (or the risk that would crystallise if

	controls failed in their entirety).' Note: inherent risk rating does not take account of any mitigating actions VUNHST may wish to or plan to implement to further reduce the level of severity for that particular risk.
Residual risk (sometimes referred to as net risk, managed risk or current risk)	'existing level of risk taking into account the current controls in place.'
Actions	'planned / future controls not yet implemented.'
Target risk	ultimate level of risk that is desired by executive and within resource envelope when planned additional actions and controls have been implemented' i.e., the position taking into account successful delivery of all mitigating actions and controls.

2.3 Scope

VUNHST's risk management framework is a corporate document and represent compulsory minimum standards. Activities and functions in and out of scope are outlined below.

In scope

All members of staff from *'Ward to Board'*

This RMF represents compulsory minimum standards in risk management. It applies organisation wide to all members of staff, those seconded to work in the organisation, and contractors engaged by us in every aspect of their work including all programmes and projects.

All activities, services and new initiatives (projects) across VUNHST's managed Departments and Divisions, including the Velindre University NHS Trust Charity

All activities of VUNHST are in scope of the RMF. This includes assessing risks attached to our key dependencies, core processes, stakeholder expectations, and/or risks to the achievement of our Mission, Vision and Goals as set out within our Five Strategic Pillars/Goals **To Note – these are draft and not yet formally approved:*

1. Goal 1: Be recognised as pioneer in blood and transplantation services across Europe

2. Goal 2: Be a recognised leader in specialist cancer service in Europe

3. Goal 3: Be recognised as a leader in stated priority areas of research, development and innovation

4. Goal 4: An established ‘University’ Trust which provides highly valued knowledge and learning for all

5. Goal 5: An exemplar of sustainability that supports global well-being and social value

Hosted Units

VUNHST is ‘Host’ to a number of external organisations:

The Directors sign an annual Governance Compliance Statement to support the Trust Chief Executive in signing the VUNHST Trust Annual Governance Statement.

Each hosted organisation has its own risk register. Risks are only be escalated to the VUNHST risk register where matters directly affecting the Trust are apparent. Matters relating to service delivery and performance are a matter for the hosted organisation to receive, manage, and escalate as necessary to the relevant sponsor body.

All domains/categories and levels of risk (STOC)

VUNHST view risk as the effect of uncertainty on objectives, measured through a combination of the likelihood of an event happening and the impact of its consequences should it occur. We face numerous levels of risk in delivering on objectives; these can relate to strategic challenges, our tactics/programmes, clinical and operational issues, compliance with laws, statutory duties and reporting obligations. This is often summarised as **STOC** (Strategy, Tactics, Operations and Compliance).

In addition, VUNHST categorise risks across nine key domains. The nine domains are: quality, safety, compliance, research and development, reputation, performance and service sustainability, financial sustainability, workforce, and partnerships. All types of risk are in scope.

Outside, Downside and Upside Risks

Actions or events leading to risk may be internally or externally driven (**outside risks**) and may relate to negative threats (**downside risks**) requiring mitigation or positive opportunities (**upside risks**) to be exploited. Risks may be fully, partially or outside the direct control or influence of VUNHST. All such risks should be considered by VUNHST.

Out of scope

Issue management, Incident Reporting and Investigations

To avoid duplication of the same ‘concern’ as both an issue and a risk, issues will be managed and reported on separately. This will either be through programme/project management reporting, or through existing local management reporting. This ensures that the risk management process is focused and is not overwhelmed by the demands of issue management.

Incidents are considered out of scope and should be escalated and actioned immediately. The aim is to learn lessons from our experiences and ensure that practice is immediately altered to improve the way services are delivered and the environment in which they are provided. For complete details of the incident reporting and investigation process, please refer to VUNHST’s Incident Reporting and Investigation Policy (including Serious Incidents) and any supplementary guidance in this area.

N.B., Materialised risks (i.e., pre-identified risks that later become issues) will continue be tracked via the risk reporting process to ensure adequate visibility and provide assurance that they are being controlled, however they may be managed separately. Note: issues that may impact existing risks should be considered when undertaking risk review exercises.

3. Aims & objectives

The primary objectives of this framework are to identify and manage the risks that may prevent the achievement of the Trust's objectives. The RMF aims to deliver a pragmatic and effective multidisciplinary approach to risk management which is underpinned by a clear accountability structure from Board to Ward. It recognises the need for robust systems and processes to support the continuous and ever-changing nature of risk. The RMF enables individuals throughout VUNHST to embed risk management in the day to day activities and support better decision making through a deeper understanding and insight into risks and their impact.

The RMF is a key component in VUNHST's risk management strategy. As such it:

- promotes consistency and transparency by articulating a single methodology for managing risk, establishing a common risk language across VUNHST;
- provides a governance model for the execution of risk management, establishing authorities for governance committees and defining risk management roles and responsibilities for individuals and teams within VUNHST;
- promotes an 'enterprise-wide' approach by integrating risk management processes with strategy/business planning, programme/project management, and operational process and decision-making, ensuring that risk management processes support and align with the overarching corporate vision and strategy for VUNHST;
- recognises that timely and accurate monitoring, review, communication and reporting of risk are critical to providing:
  - early warning mechanisms for the effective management of risk occurrences
  - assurance to management, the Boards and our partners/stakeholders
  - a sound platform for organisational resilience
- enables the design and implementation of controls that:
  - are structured to promote effective realisation of objectives
  - provide appropriate assurance
  - are cost effective.
- supports decision-making through risk based information;
- helps develop a culture where risk management is integrated into all Trust business;
- Create a system which is user-friendly and allows for the prompt assessment and mitigation of risk;
- Clearly describe the risk appetite of the organisation;
- Reduce risks to patients, carers, staff, members of the public, visitors, etc., to an acceptable level; maximise resources available for patient services and care; and minimise financial liability;

Effective risk management supports better planning and enables the Trust and its senior managers to take risks with increasing confidence. With the result that:

- Adverse (damaging) events are less likely;
- Capital and resources are utilised more efficiently and adverse (damaging) events are less likely;
- Costly re-work and firefighting is reduced;
- Achievement of objectives is more likely;
- Quality of service is improved;
- Compliance with statutory legislation;
- All sources and consequences of risk are identified;
- Risks are assessed and either eliminated or minimised;
- Information concerning risk is shared with staff across VUNHST;
- Lessons are learnt from incidents, complaints and claims in order to share best practice and prevent reoccurrence.

VUNHST will ensure that all employees have the necessary support and assistance to undertake effective risk management. Where appropriate this will tie in with induction/training provided. Our organisation will also be dynamic, iterative and responsive in its approach to change.

4. Risk strategy

The management of risk is a key factor in the provision of high-quality care to our patients, donors and service users. Of equal importance is the legal duty of the Trust to control any potential risk to staff and the general public, as well as safeguarding the assets of the Trust. It is the responsibility of all staff to be involved in the identification and reduction of risks.

VUNHST's risk management strategy does not focus on total risk avoidance but on identifying and managing an acceptable level of risk. We do not want to adopt unnecessary internal controls and management procedures, or introduce bureaucratic processes, but to use risk management to evaluate the impact on our objectives of decisions, actions or uncertainties.

The Board recognise that effective risk management is a key component of corporate and clinical governance and is integral to the delivery of our objectives. VUNHST's risk strategy therefore focuses on deploying a holistic approach to risk management which embraces financial, clinical and non-clinical risks across all parts of the organisation. It seeks to ensure that risks, untoward incidents and mistakes are identified quickly and acted upon in a positive and constructive manner so that any lessons learnt can be shared. This will ensure the continued improvement in the quality of care and the achievement of strategic objectives. The commitment of the Board is therefore to:

- minimise harm to patients, colleagues or visitors to a level as low as reasonably practicable;
- protect organisational value (such as high standards of patient care, reputation, community relations, assets and resources);
- maximise opportunity by adapting and remaining resilient to changing circumstances or events;
- assist with managing and prioritising activities through using risk information to underpin strategy, decision-making and the allocation of resources; and
- to ensure that there is no unlawful or undesirable discrimination, whether direct, indirect or by way of victimisation, against its service users, carers, visitors, existing employees, contractors and partners or those wishing to seek employment, or other association with the organisation.

The rest of this framework details our approach to risk management / sets out the arrangements for managing risk at all levels within the organisation; however, a summary of key risk management obligations is highlighted below:

Risk management obligation	Description
A **risk management framework (RMF)** in place, endorsed by the Board and communicated to all staff	We have created a risk management framework (this document), which is annually endorsed by the Board and made readily available to all staff. We use it alongside other management tools, such as performance and quality dashboards and financial reports, to give the Board a comprehensive picture of the Trust risk profile and internal control environment. It is formally reviewed every year, or upon significant change. Any changes require approval from the Audit Committee and Board. *Outlined in this document*
Clear **roles, responsibilities and accountabilities for risk management** established	We have assigned risk management roles, responsibilities and accountabilities across the organisation, and appointed business leads for risk in each department / division and hosted unit. *Outlined in this document*
Established **Risk governance** arrangements	Our organisational structure helps us manage risk effectively. A 'three lines of defence' model ensures clear accountability and expectation for risk management. This gives departments / divisions and hosted units autonomy for identifying, managing and reporting risk (this is the first line of defence), with our central functions i.e. governance, IT, HR and Legal etc. providing oversight (this forms the second line of defence) and internal/external audit providing independent assurance (the third line of defence). The following is also in place: • Committee structures and terms of references • internal risk reporting requirements, specifically the reporting and escalation of key risk information through the governance structure on a monthly basis • procedures for responding to urgent incidents and external events • external reporting, disclosures and certification *Outlined in this document*
Risk management **embedded within daily operation and decision-making** processes	Risk management is ongoing and embedded in VUNHST's daily operations and decision-making processes, from strategy setting and business planning, through to programme/project management, business-as-usual processes and activities, and partnership working arrangements.

	- The Board systematically discusses the risks to achieving its Vision, Mission and strategic priorities as part of the IMTP planning process. - Assessing risk compared to acceptable levels is not a one-off, quarterly or annual activity but an integral part of everyday decision-making: – New risks (and altered existing risks) identified through decision-making processes and forums, including the Board, Quality & Safety Committee, Information Governance & IM&T Committee, Workforce & Organisational Development Committee, and Planning & Performance Committee etc. are considered for inclusion in the relevant risk register / TAF and reported through the organisation alongside changes to existing risks according to risk governance and urgent escalation arrangements. – Risks and key controls/mitigations will also be assessed and documented by departments/divisions and hosted units as part of the business planning and performance monitoring processes, and during their regular leadership meetings/regional support groups. *Outlined in this document*
High level **risk appetite** statements and risk tolerance limits should be in place for principal risk categories/types. VUNHST manages risk in accordance with those statements and limits	We have a clear approach to risk taking and innovation, outlined within our risk appetite strategy, and we encourage staff to read it. - **Risk appetite statements** align with the organisation's strategic priorities/objectives, and we communicate them according to high level categories of risk/principal risk types. - Where possible, we will use **early warning indicators** to alert our executive and the Board that the risk of planned outcomes/objectives not being met is increasing. - We use our **risk quantification matrix** / heatmap criteria as a guide for setting risk tolerance levels and where they exist, we will use pre-existing key performance indicators, limits or thresholds as key indicators of risk. - Risk appetite considerations are also an intrinsic part of the standing financial instructions (SFIs) / **delegation of authority arrangements** within VUNHST; and **risk/reward trade-offs are included within impact assessments**. *See separate Risk Appetite Strategy*

A detailed **risk management process** available to guide staff in identifying, assessing, treating, reporting and communicating risks	A risk management process / procedures manual is in place for use by all teams to identify, analyse, manage, monitor and report on risks threatening their objectives. This includes guidance on using our risk quantification matrix, which assess the likelihood of risk occurring and its impact if it is not well managed. It also includes details of risk assessment tools and techniques. *See separate risk management process / procedures manual for details.*
Risk registers established at strategic and operational levels	Top down: TRR and TAF principal risks as they relate to the delivery of commitments, and/or which threaten the viability of our organisation. Bottom up: Our departments / divisions and hosted units are each accountable for managing their risks (and opportunities) and maintain a **local register** of these as they relate to their objectives. Major programmes and/or projects will also have risk registers where necessary. *Outlined in this document*
Trust Assurance Framework: Regular evaluation of the nature and extent of principal risks that we are exposed to, the adequacy of key controls, sources of assurance and commentary against any gaps in control or assurance are provided	Our internal controls are designed to provide reasonable assurance that risks to our objectives are at acceptable levels. Departments/divisions and hosted units regularly consider their effectiveness, and our committees and the Board formally examine them monthly and report on them (externally) annually. Where risk management is judged to be weak or limited in effect, we will enhance controls. *See separate TAF Guidance Document and template*
Opportunities for **training** and shared learning on risk management provided	A variety of risk training materials/course(s) tailored to the audience is available. An annual risk review session for a senior audience and ad hoc risk leads forum are also undertaken. *See separate risk management training material*
Risk and control interdependencies	When assessing risks, our departments/divisions, hosted units and programmes/projects identify where multiple risks could compound each other, ensuring that they are not considered in isolation.

	External risk interdependencies i.e. the identification and evaluation of risks associated with partners, contractors and partner organisations, is also undertaken as standard. *Outlined in this document*
We will ensure that robust **business continuity** arrangements are in place	Specific contingency plans for external events/uncertainties may also be developed and maintained e.g. EU Exit contingency planning, COVID-19 recovery and response planning. *See separate business continuity planning (BCP) procedures.*

5. Risk governance

Risk governance and the internal control system

VUNHST recognise that risk governance is a fundamental part of its corporate governance and broader internal control system. Risk governance refers to the architecture within which risk management operates in our organisation and is fundamental to the day-to-day running of the Trust.

The British Standard BS 13500 defines governance as a: ‘system by which the whole organisation is directed, controlled and held accountable to achieve its core purpose over the long term’. Similarly, the UK Corporate Governance Code states that ‘good governance should facilitate efficient, effective and entrepreneurial management that can deliver the long-term success of the company’.

Good risk governance should therefore:

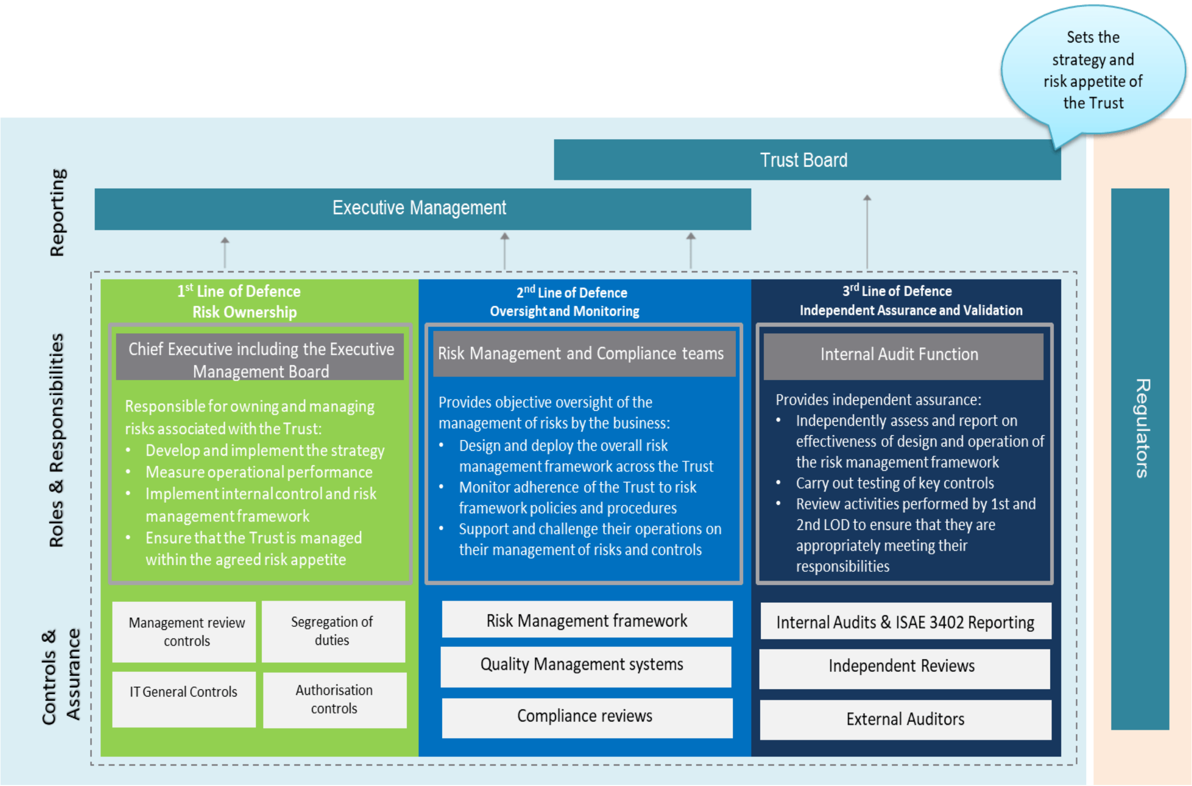
- put in place a structure of risk responsibility throughout the organisation so that everybody is aware of their own risk responsibilities and accountabilities and those of others with whom they work
- establish clear and effective lines of communication up and down the organisation and a culture in which good and bad news travel freely
- result in risk being accepted and managed within known and agreed risk appetites.

Three lines of defence risk governance model

VUNHST operates the three lines of defence model - a leading practice in risk governance - that help ensures segregation between direct accountability for risk decisions, oversight and assurance. This allows us to assure ourselves and those to whom we are accountable that we are managing the organisation well. It gives departments, divisions and hosted units autonomy for identifying, managing and reporting risk; with our specialist functions such as the governance, IT, and legal teams providing oversight; and internal/external audit providing independent assurance. We manage risks and report and escalate key risk information through this governance structure.

Figure 2 below illustrates the three lines of defence summarising reporting responsibilities and roles within the Trust.

Figure 2: VUNHST's three lines of defence model



Sets the strategy and risk appetite of the Trust

Trust Board

Executive Management

Regulators

Reporting

Roles & Responsibilities

Controls & Assurance

1st Line of Defence
Risk Ownership

Chief Executive including the Executive Management Board

Responsible for owning and managing risks associated with the Trust:

- Develop and implement the strategy
- Measure operational performance
- Implement internal control and risk management framework
- Ensure that the Trust is managed within the agreed risk appetite

Management review controls

Segregation of duties

IT General Controls

Authorisation controls

2nd Line of Defence
Oversight and Monitoring

Risk Management and Compliance teams

Provides objective oversight of the management of risks by the business:

- Design and deploy the overall risk management framework across the Trust
- Monitor adherence of the Trust to risk framework policies and procedures
- Support and challenge their operations on their management of risks and controls

Risk Management framework

Quality Management systems

Compliance reviews

3rd Line of Defence
Independent Assurance and Validation

Internal Audit Function

Provides independent assurance:

- Independently assess and report on effectiveness of design and operation of the risk management framework
- Carry out testing of key controls
- Review activities performed by 1st and 2nd LOD to ensure that they are appropriately meeting their responsibilities

Internal Audits & ISAE 3402 Reporting

Independent Reviews

External Auditors

The first line of defence

The first line of defence relates to functions that own and manage risk. Staff and managers working in departments and divisions have direct ownership, responsibility and accountability for identifying, managing and controlling risks to their objectives. Assurance is provided through the monitoring and reporting of risk and control activities through senior leadership/management team meetings. This is ongoing.

The second line of defence

The second line of defence relates to functions that oversee or specialise in risk management and compliance. They guide, support and challenge the first line by bringing expertise and subject matter knowledge to help ensure risks and controls are effectively managed and assured. The Corporate Governance Team and other internal oversight teams such as legal, IT, performance/business planning, finance and workforce & organisational development (among others) form the second line of defence and are responsible for co-ordinating, facilitating and overseeing VUNHST's effectiveness and integrity.

The Corporate Governance Team play a crucial role in the provision of support: facilitating identification and evaluation of risks, coaching management in responding to risks, co-ordinating risk management activities, consolidated reporting on risks, maintaining and developing this framework, championing establishment of risk management, and developing the risk management strategy for committee and Board approval. The team monitors and facilitates the implementation of effective risk management practices by departments and divisions and assists risk owners in reporting adequate risk-related information throughout the organisation. Assurance is provided through monthly monitoring and reporting of risk and control activities through our various committees, Audit Committee and Board.

The third line of defence

The third line of defence relates to functions that provide independent assurance, namely audit. It provides assurance to senior management and the Board over both the first- and second-lines' efforts. It is independent of the design, implementation, control and operation of control activities and they are not permitted to perform management or operational functions. This is a crucial part of the model and helps protect objectivity and independence.

Internal audit and external scrutiny through Audit Wales provide independent assurance and challenge concerning the integrity and effectiveness of risk management and internal control. The independent audit team will, through a risk-based approach, provide assurance to the Boards and senior managers. This will include assurance on the effectiveness of the first and second lines of defence. Audit Wales will review and report on internal controls over financial reporting. Assurance is provided through monitoring and reporting of strategic/corporate risk and control activities through the Audit Committee.

6. Key accountabilities, roles and responsibilities

Risk management is a core responsibility, and staff at all levels are responsible for being risk aware and for implementing the framework. Key risk management roles, responsibilities and accountabilities are summarised as follows:

Board

The Board has overall responsibility for risk management and will ensure our risk management approach is sufficient by considering whether the Trust Risk Register (TRR) and TAF identifies principal areas of risk against strategic objective and that adequate risk mitigation strategies have been designed and implemented to manage all identified principal risks (bi-monthly) and by endorsing and reviewing the framework's effectiveness (annually) as assured by the Audit Committee. It sets the 'tone at the top' for risk management by setting risk appetite and explicitly considering risk when developing or updating the strategy and business plan, or when considering performance and/or major programmes of change.

Note: in discharging its risk-related responsibility, the Board operates through several key governance forums/committees and will be supported in the discharge of its responsibilities by the Audit Committee.

Audit Committee

The Audit Committee is accountable for overseeing risk management and will support the Board by reviewing the effectiveness of the internal controls system by reviewing the comprehensiveness and reliability of assurances on risk management. Specifically, the Audit Committee monitors that strategic objectives are being achieved and it receives regular reports on risks to the strategic objectives and the processes in place to manage them. It also needs to ensure that:

- the TRR is reviewed, updated and monitored regularly; and
- it is satisfied with the controls in place and progress is being made in completing mitigating actions.

The Audit Committee independently reviews the adequacy and effectiveness of risk management across the Trust. Through a programme of work, it will review and approve compliance monitoring, internal and external audit plans and monitor risk reporting. The Audit Committee plays a key part in supporting the Board in discharging its responsibilities regarding risk management by advising the Board of the outcomes of its work at regular stages throughout the year.

Internal Audit will provide assurance to the Audit Committee on the effectiveness of the Trust's Risk Management Framework and its application across the business. It will also use the outputs from the risk management framework to drive its assurance plan going forward throughout the year.

Directors

Directors will support and promote risk management. They must ensure that risk management is integrated into all activities (i.e. that risk management is not just a checklist feature but embedded), and should demonstrate leadership and commitment by ensuring:

- their portfolios (department/division) implement the framework;
- risk is considered when setting their objectives/drafting their business plan and discussed alongside their performance and in any local management meetings;
- all risks, controls and risk management issues under their control are adequately co-ordinated, managed, monitored, reviewed and reported/escalated in accordance with the requirements of this framework;
- necessary resources are allocated to managing risk/that they identify individuals who have the accountability and authority to manage risk under their control (i.e. risk owners); and
- they raise relevant risks at the appropriate committee or other decision-making forum, where appropriate.

Note: Where principal risks have increased, or risks are outside agreed appetite/tolerance, owning executive directors may be called on to attend the Audit Committee to discuss mitigations.

Executive Lead / Senior Accountable Officer (SRO) for Risk

The Director of Corporate Governance will act as the Senior Responsible Officer (SRO) for risk within VUNHST. The SRO will own this risk management framework and any associated procedures and is accountable for the strategic development and implementation of organisational risk management. Including arrangements for:

→ Maintaining and updating appropriate risk management Policies and procedures;

→ Ensuring there is a clear and dynamic link between the Board Assurance Framework and Corporate Risk Register;

→ Ensuring the Trust has a comprehensive and dynamic Risk Register and working with divisional management teams to ensure that they understand their accountability and responsibilities for managing risks in their areas;

The SRO will also ensure that the overall risk to VUNHST is presented to, and challenged at, the appropriate level in our governance structure.

Risk owners

A risk owner is the person who will be accountable if the risk occurs. They are responsible for monitoring their risks and executing risk responses when appropriate. Risk owners often aid in defining the risk response/treatment plans and in performing qualitative risk analysis and the quantitative risk analysis for their risks. When identifying a suitable risk owner, you should consider if that person has the authority to manage the risk; if they are the person who best understands the causes of the risk, and the impact; if they are willing to monitor the risk and ensure it is mitigated. Note: Members of the Executive Team act as risk owners for corporate-level risks.

Executive Management Team

The Executive Team is responsible for overseeing the implementation of the Trust's risk management framework, including defining, supporting, debating and challenging key risk and risk management activity across the Trust.

Departmental/Divisional Risk leads

Risk leads are embedded personnel who act as the liaison point for risk management in their department or division. They support directors in implementing this framework. This includes developing and maintaining a local risk register and reporting and escalating risks through the governance structure every month, on behalf of their directors. Note: Risk leads will be appointed by their director and it is recommended that as a minimum they operate in a clinical or business manager or equivalent role to ensure consistency of application and adequate focus. They should also be regular attendees at their local management/leadership meetings, have the authority to challenge their peers on risk, and enough capacity to dedicate to managing the risk process on behalf of their areas. Risk leads may be supported by local risk co-ordinators.

Specialist functions, and other executive committees

Specialist functions (including but not limited to: legal, workforce & organisational development, finance, IT, performance, procurement, and business continuity) and other executive committees (including Planning and Performance Committee etc.) in the organisation will be called on to manage, own and/or advise on specific risk exposures as they relate to their sphere of influence.

Corporate Governance Team

The Corporate Governance team are responsible for the maintenance and development of DATIX the Trusts risk management system, maintaining the Trust risk register, supporting the Trust to produce ad-hoc reports outside of those produced routinely by the relevant manager. It will also act as a risk 'think tank' and independent review mechanism for risks and opportunities escalated by teams and programmes/projects.

Service Directors

Service Directors are accountable for ensuring that risk is managed in line with this framework within their service and wider areas of responsibility. They are required to:

- maintain a suitable local forum for the discussion of risks arising, at which the local risk register is reviewed at least monthly;
- ensure that risks raised by staff are fully considered, captured on local risk registers, kept up to date, re-assessed, and re-graded as necessary;
- develop and implement action plans to ensure risks identified are appropriately treated;
- ensure that appropriate and effective risk management processes are in place within their designated area and scope of responsibility and that all staff are made aware of the risks within their work environment and of their personal responsibilities to minimise risk; and
- monitor any risk management control measures implemented within their designated area and scope of responsibility, ensuring that they are appropriate and adequate.

All Managers and Staff

All managers are responsible for the local implementation of this framework and associated policy documents in their departments, wards and/or other clinical and non-clinical areas.

All managers have a 'first line' responsibility for identifying, assessing and managing risk within their own area of responsibility, for implementing agreed actions to manage risk and for reporting activities or circumstance that may give risk to new or changed risk.

All staff should:

- take action to protect themselves and others from risks;
- Identify and report risks to their line manager;
- Ensure incidents and complaints are reported using the appropriate procedures;
- Attend mandatory and statutory training as determined by their Line Manager; and
- Be aware of and comply with Trust's risk management framework

7. Risk domains / categories

Categorising risk for effective risk management

Identifying the cause of risk by type (or root cause) is a useful method for exploring potential risk and risk appetite. Grouping risks this way helps VUNHST understand where the largest risk exposure originates and the effectiveness of its internal controls. In consultation with Executive, Audit Committee and the Board, the following principles were used to guide the selection of key risk types. In summary, risk types should:

- be important to achieving VUNHST's long term strategy and IMTP objectives (as well as to addressing key dependencies on our organisation, and the delivery of our core processes);
- be subject to measurement in a simple, transparent and objective way (where data is relatively frequent, available and complete). Note: This is especially important, so that the Board can see how Trust-wide risks are evolving and moving towards target levels over time;
- allow for risk appetite to be applied and should provide useful direction for management in making trade-off and resource allocation decisions and the primary purpose of setting risk appetite; and
- can be at least partially mitigated by VUNHST and our partners (there is limited value to setting risk appetite if the risk cannot be mitigated and therefore must be accepted)

Using the above principles and with agreement of the relevant Board Committees, nine key risk types / domains were selected. The nine domains are:

1. Quality
2. Safety
3. Compliance
4. Research and development
5. Reputation
6. Performance and service sustainability
7. Financial sustainability
8. Workforce
9. Partnerships.

Interaction between risk categories and types

There may be a degree of overlap between categories. Please see the Risk Appetite Strategy, which is updated from time to time, for final guidance on determining these interactions and how to approach trade-offs between risk categories.

Using risk types to structure risk appetite

VUNHST Board structures its risk appetite around the nine domains or principal risk types. Please see the separate risk appetite strategy document for further details of our risk appetite statements and tolerance limits.

Note: The list of selected risk types is expected to be dynamic and may be changed in consultation with the Committees. If that happens a revised risk appetite proposal will be presented to the Board for approval.

8. Risk and control interdependencies

VUNHST's approach to risk helps us to manage risk opportunities as we work closer with other health and social care providers to find new ways of improving services. It will also enable an integrated approach to risk management as we fulfil our statutory obligations and protect the health and well-being of the people who access our services.

Partnership working / third party risk management / external interdependencies

Risk interdependencies between VUNHST, our Hosted Units and other organisations and partners must be identified, assessed, monitored and tracked. For risk exposure to be understood and managed holistically, it is important for VUNHST to understand where it could cause risk to a partner organisation; where it operates controls that mitigate risk to a partner; where it depends on another body to operate controls on its behalf; or where it is exposed to risk as a result of another organisation.

Our business planning process identifies organisations likely to influence the success of our objectives. Departments/Divisions, programmes/projects identify, and hosted units, assess and communicate risk interdependencies with partner organisations, logging them on their risk register and communicating and escalating them to VUNHST committees and the Boards as required – in accordance with escalations set out in this document.

We jointly identify and assess risks that cut across boundaries or relate to partnership working / shared programmes of work, with responsibility for managing them clearly assigned and understood by all those involved in joint working or partnerships. Such risks are escalated within programme governance structures as well as via arrangements described in this framework. The impact of partnership working / third party risk management on our risk profile forms part of our monthly risk-reporting cycle.

Internal interdependencies

It is important for departments/divisions and hosted units *within* VUNHST to understand where they could cause risk to another part of the Trust; where they operate controls that mitigate risk to another part of the organisation; where they depend on another team to operate controls on their behalf; or where they are exposed to risk because of another part of VUNHST. Such risk should be identified, shared and managed together and raised at relevant committees/Board.

Risk assessment considerations – horizon scanning and emerging risks

VUNHST endeavour to identify risks of the broader risk environment, and periodically undertake horizon scanning of future risk areas to assess emerging areas of risk. Emerging risks are reported through the governance structure alongside other risks.

9. Risk documentation

The purpose of risk management in VUNHST is to challenge the assumptions of management decisions in the areas of strategy setting/business planning, budgeting and performance management. It is therefore an enabling tool for our management teams and staff to respond to opportunities and threats that affect the achievement of objectives, making them aware of the pitfalls of intended actions and providing the ability to change course if necessary.

Good documentation is a prerequisite in the successful implementation of risk management, as it acts both as a delivery and message mechanism. Risk management documentation is used to deliver a consistent message, to speak a common language and to provide clear (risk management) objectives linked to organisational objectives. It is constantly reviewed and evaluated. Documenting VUNHST risk control efforts also provide evidence of our evolution in risk management, may be used for audit purposes to demonstrate that risk management has taken place, and acts to safeguard the organisation against any potential claims.

Risk management document inventory

VUNHST risk management document inventory, which together outlines the Trust’s current exposure, commitment and attitude towards risk, includes the following:

- risk management framework (this document)
- risk appetite strategy (available separately)
- risk management process, and other risk management procedures and methodologies (available separately)
- the risk register (found on Datix)
- Board Assurance Framework (available separately)
- risk reports (available separately)
- risk escalation process (included in this framework)
- risk training material/course(s) (available separately).

Risk registers

A risk register is a live document maintained to monitor potential risks. It also tracks the actions taken to minimise risks and provides contingency plans that should be invoked if a risk does occur.

To ensure consistency, VUNHST provide a standard risk register template (available separately), which allows our departments / divisions to capture all the information needed to manage risk appropriately and determine whether any risks should be escalated through our governance structure. Each area should maintain their own risk register and it should be kept up to date and reviewed regularly. New risks should be added as they are discovered.

Trust Risk Register (TRR)

On the Boards' behalf, the Corporate Governance Team maintains a Trust Risk Register (TRR) of all significant risks that may affect VUNHST's ability to achieve its objectives (and the control measures for dealing with them). They also maintain the TAF.

Trust Assurance Framework (TAF)

The TAF provides a mechanism for managing strategic (principal) risks. It 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 TAF confirms that agreed actions are in place to address identified gaps in control or assurance. Additionally, the TAF is cross-referenced with operational risks. The TAF should drive the board agenda.

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

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

Although each strategic objective has a lead 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 VUNHST's probability of success and reducing likelihood of failure.

Please refer to the separate TAF Guidance document for full details and TAF template.

Local risk registers

Departments / divisions will maintain their own risk registers and escalate risk as appropriate. Major programmes and/or projects will also have risk registers where necessary. Please refer to the VUNHST risk management process / procedures manual for additional risk register guidance.

Risk register

The Corporate Governance Team provides a standard risk register template that should be used to capture risks at strategic and operational level. This will be managed through DATIX.

The standard risk register template allows departments/divisions to capture all information needed to manage risk appropriately and determine whether any risks need to be escalated through our governance structure. This will capture:

Description of risk

A simple phrase that describes the risk: “There is a risk that <risk event> as a result of <cause> which may lead to <impact>.” Departments/Divisions may find it useful to have a shorter ‘risk title’ for use in reports, with a longer and more complete description.

Cause(s) and consequence(s) / impact

Causes (also referred to as risk drivers or influencing factors), both internal and external, should be explained. Consequences (also referred to as effects, impact or outcomes) should also be explained.

Link to objectives/ business plan priorities

Where possible, risks should be linked to our strategic priorities, legislative duties, major programmes/projects, business plan objectives or business-as-usual activities.

Triggers

Where identified, early warning triggers or indicators should be identified and tracked to signal whether the risk is becoming an issue or has reached a point that requires action.

Existing controls

To aid risk assessment and action planning, the current measures to control the risk – and whether they are considered adequate – are recorded.

Assessment of risk and control

Risk ranking (impact and likelihood): to assist with prioritisation, risks are scored/given a ranking using VUNHST’s impact and likelihood matrix; this enables the ‘most significant’ risks to be identified. Inherent, residual and target risk scores are assigned.

Risk and control owner(s)

Owner (lead person): you need to assign risks and controls to a lead person responsible for ensuring they are adequately controlled and monitored.

Action(s)/treatment plans

Where a plan of action or treatments to address the risk have been agreed, they should form part of the register. Alternatively, include a link to a separate action plan.

Dates

As the register is a ‘living’ document, it is important to record the date that risks are added or modified. If the register includes an action plan, you should provide target and completion dates for actions. To ensure all open risks are reviewed at least annually, you must provide a review date.

Comments / updates

Where separate update/summary reports are not produced, risk registers should include a comments column to allow for useful updates, such as meetings to discuss the risk.

The risk treatment / action plan

Where a risk is outside agreed appetite levels, where controls are deemed inadequate, or where controls are missing, a risk treatment action plan should be in place to document the management controls to be adopted; it should include the following information:

- who has responsibility for the implementation of the plan
- what resources are to be utilised;

- timetable for implementation;
- details of the mechanism and frequency of review.

Please refer to the risk management process and procedures manual for additional guidance on controls/treatment options.

Risk embedded into terms of references

VUNHST’s risk governance structure has been designed to help provide effective stewardship to anticipate and combat threats and to take appropriate opportunities to improve. Risk governance is a fundamental part of corporate governance, and therefore our committee and Board terms of references have a built in risk component / risk discussed as a standing agenda item.

Risk communications, assurance statements and disclosures

The Board has overall responsibility for ensuring that risks are managed. One of the key requirements of the Board is to gain assurance that risk management processes are working effectively and that key risks are being managed to an acceptable level. The starting point and most foundational step in this assurance are the existing documents listed within the risk management document inventory; specifically, live risk registers and regular risk reports.

In addition to these, twice a year all Directors are asked to provide supplementary assurance by certificating that identified risks are being managed and that internal controls are working effectively. These assurances will inform the Annual Governance Statement, which is signed off by the internal audit team and the Chief Executive. All external disclosures are handled by the legal and governance team and any disclosures related to risk management are discussed with the Corporate Governance Team before disclosure. For example, any freedom of information requests in relation to risk management documentation are discussed with the relevant committee and Audit Committee before information is released to the requester.

10. Risk Reporting

Monthly risk reporting cycle

Bottom up: local risk reporting for departments and divisions

Departments/Divisions regularly monitor and report risks affecting their activities – and the effectiveness of control measures for managing them – to senior managers or directors during routine management meetings, committees, groups or panels. Note: each department/division is responsible for defining an internal risk review and reporting process, proportionate to its local needs, however risk registers are formally submitted to the Corporate Governance Team every month for upward reporting; alongside a covering paper articulating changes to risk profile and any risks requiring escalation.

The following considerations for escalating a risk should be followed:

- sufficient capability is not held at the current risk reporting level to manage risk successfully
- risk rating has significantly worsened
- risk is significantly outside appetite
- risk is related to cross-cutting / operational issues and/or has a wider impact than just one department/division.

Top down: corporate risk reporting at Trust Level

The Corporate Governance Team coordinate risk reporting through our governance structure monthly. In addition to managing monthly reporting, they will on a periodic basis (and at least annually) review and challenge risk management procedures and their implementation defined by departments/divisions and programmes in compliance with the risk management framework.

This may take the form of initial self-assessments of risk management activity, subsequent further analysis of these assessments with key risk responsible personnel, monitoring of risk registers/Datix activity by respective areas and/or programmes, and review of escalation processes to ensure:

- sufficient capability is held at the current risk reporting level to manage risks successfully
- risk ratings if worsened are escalated
- risks outside appetite are escalated
- if risks are related to cross-cutting issues and/or has a wider impact than just one department/division they are escalated.

Urgent risk escalation / out of cycle escalations

Risks can be raised at any meeting and at any level in our organisation. Staff must immediately escalate newly emerging, high impact, highly likely risks; risks breaching risk appetite or with a significant or rapid change in severity resulting in a RAG rating of red or amber/red, to their director and business lead for risk, and not wait for the monthly reporting cycle. The Corporate Governance Team should be informed at the same time.

The director affected must decide whether the risk needs to be escalated to the wider executive immediately or at its next available meeting, for consideration and action. Otherwise the risk will form part of the monthly report to the Audit Committee and the Board.

Summary of risk reporting and escalation routes:

- Risks can be raised at any meeting and at any level in VUNHST e.g. any member of staff; local management/team meetings; Executive Committees, or any other specialist/technical committees; at the Board; or from our partners.

- Risks scored **>=15**, and any risks where the impact is scored as 5 regardless of likelihood require confirmed review by the relevant Executive Committee and confirmed review by the Board. It should be escalated according to the RMF and considered for inclusion on the TRR and TAF, monthly.

- Risks scored **>=12**, and any risks where the impact is scored as 5 regardless of likelihood, will require confirmed review by the relevant Executive Committee, depending on source.

- Risks outside Board-specified tolerance ranges: As outlined in the Risk Appetite Strategy, the VUNHST Board has developed indicative tolerance ranges against 9 principal risk categories (or risk domains). In addition to the above-mentioned escalation criteria, any risks outside these ranges will require confirmed review by the relevant Executive Committee i.e., any material Quality, Safety and Reputational risks above a Low rating; any Compliance, Performance and Service Sustainability, or Financial Sustainability risks above a Moderate rating; or any Research and Development, Workforce, or Partnership risks above a High rating should be escalated for discussion.

- Example below (to note exact scoring levels to be finalised when modelling on refreshed risk register is completed):

Risk Appetite Levels	**Escalation level to Trust Board if at risk score at or above:**
0 – Avoid	9
1 – Minimal	12
2 – Cautious	12
3 - Open	12
4 - Seek	15
5 - Mature	15

- Urgent risks: Staff must immediately escalate newly emerging, high impact/highly likely risks; risks breaching VUNHST's risk appetite (see Risk Appetite Strategy) or with a significant or rapid change in severity rating, to their owning Director, and not wait for the reporting cycle above. The director affected must decide whether the risk needs to be escalated to the wider executive immediately or at its next available meeting, for consideration and action. Otherwise the risk will form part of the above reporting to the relevant Executive Committee and/or the Board monthly.

- The Head of Corporate Governance will compile a Trust Assurance Framework (TAF), for the Board, consisting of the top strategic risks to VUNHST's objectives, including those that meet the above-mentioned escalation criteria and those the Board have requested sight of regardless of score.

What should risk reports contain?

Departments/divisions, and major programmes/projects should submit updated risk registers to the Corporate Governance Team monthly; and should include an overview of significant changes to their risk register since last reporting. This may include:

- new or emerging risks;

- risks breaching the escalation threshold;

- risks outside acceptable appetite / tolerance levels;
- progress on completing action plans for risks;
- Gaps in control / assurance;
- status of performance indicators for risk (where they exist);
- significant incidents or near misses;
- risks requiring upward escalation/central treatment; and
- progress on embedding risk management into the business-as-usual activities of their directorate/region or programme/project.

Corporate risk reporting at a Trust-wide level should provide an aggregate picture of VUNHST's exposure to risk. It will focus on updates to the Trust Risk Register (including any escalated local and/or programme/project risks) since the last reporting cycle. This may include:

- new or emerging strategic or high level operational risks;
- strategic or high level operational risks over the agreed TRR / TAF escalation threshold;
- risks where there is a substantial gap between current and target risk rating or where it is outside agreed appetite/tolerance levels;
- key control gaps / gaps in assurance;
- significant incidents or near misses affecting the strategic risk profile; and
- progress on embedding risk management across VUNHST.

11. Risk management process

The VUNHST risk management process provides the framework against which all categories of risk can be identified and assessed, so that risk-handling activities may be planned and invoked as needed.

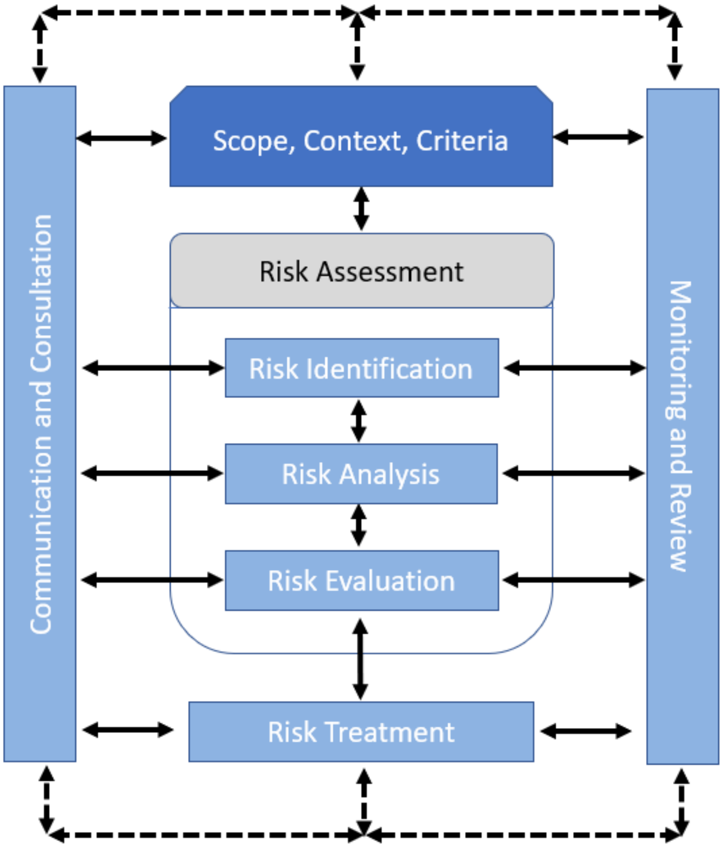
To ensure consistency across the organisation, we have adopted an iterative process for managing risk based on the ISO 31000 Risk Management - Guidelines. It consists of the following activities:

- establish the scope, context and criteria
- risk assessment (risk identification, risk analysis and risk evaluation)
- risk treatment
- recording and reporting
- monitoring and review
- communication and consultation

This process provides a logical and systematic method of identifying, analysing, evaluating, mitigating and monitoring risks in a way that will allow VUNHST to make effective decisions and allow for a timely response to risks and opportunities as they arise.

Figure 1 below demonstrates a high-level view of the risk management process influenced by the ISO 31000 (2018) Risk Management Guidelines. The diagrammatic representation is an update from the previous ISO 31000 (2009) depiction and now includes the additional elements of scope, context, criteria as well as recording and reporting. The aim of this is to build a more holistic, well rounded and interconnected approach to risk management, whereas previously it was more focused on the risk assessment piece itself. Please refer to our Risk Management Process / Procedures manual for full details.

Figure 3: VUNHST Risk Management Process



Please refer to the VUNHST risk management process and procedures manual (available separately) for further details of this process.

12. Implementation, training and support

The policy will be implemented across VUNHST and will be disseminated through the Directors portfolios.

To help implement the framework, an ‘Introduction to risk management’ eLearning module will be available to all staff through the intranet.

A tailored overview of the risk management process and accountabilities will also be built into induction/onboarding packs for staff at all levels, up to and including new directors and Independent Members.

To operationalise risk management, plans are in place to use Datix to log risks, controls and mitigating actions. Datix training will be available and should be taken up wherever possible when new users start to access the system; this can be tailored to the experience of the user(s), and their role in the system.

There will be annual facilitated risk review sessions and/or a stand-alone in-house training exercise for a senior audience (e.g. in the form of an executive or board risk workshop) to ensure risk is treated as a core discipline at senior/executive level.

The Corporate Governance Team will make further guidance and support available on the intranet as required and bespoke risk management training will also be available to departments/divisions, tailored to their specific needs on request. This could include advice and guidance on identifying and managing risk, the co-ordination of peer reviews and/or help with developing risk registers.

Appendix 1: Bibliography

VUNHST's approach to risk management considers HM Treasury guidance on managing risk (The Orange Book), with reference to good practice from the National Audit Office (Managing Risks in Government) and other risk management standards as appropriate. Other reference material used to inform our approach includes:

- Welsh NHS Confederation (2009) The Pocket Guide to Governance in NHS Wales. Good Governance Institute
- Your Risk & Assurance Framework: A structured approach – (Welsh Government, December 2009)
- Risk Essentials – A Risk Management Framework (Welsh Government, Version 2, October 2006)
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management – Integrated Framework, 2017.
- "Fundamentals of Risk Management" by Paul Hopkin
- HM Treasury (2012) Assurance frameworks
- HM Treasury (2005) Principles of managing risks to the public
- HM Treasury (2020) The orange book: management of risk – principles and concepts
- IRM/Alarm/AIRMIC (2002) A risk management standard
- ISO 31000: 2018, Risk management – Guidelines
- "Managing Risks: A New Framework" by Robert S. Kaplan and Anette Mikes
- National Audit Office (2011) Managing risks in government
- OCEG 'Red Book' 2.0 (2009) A governance, risk and compliance capability model
- UK Corporate Governance Code