GC 04b

Risk Management Process

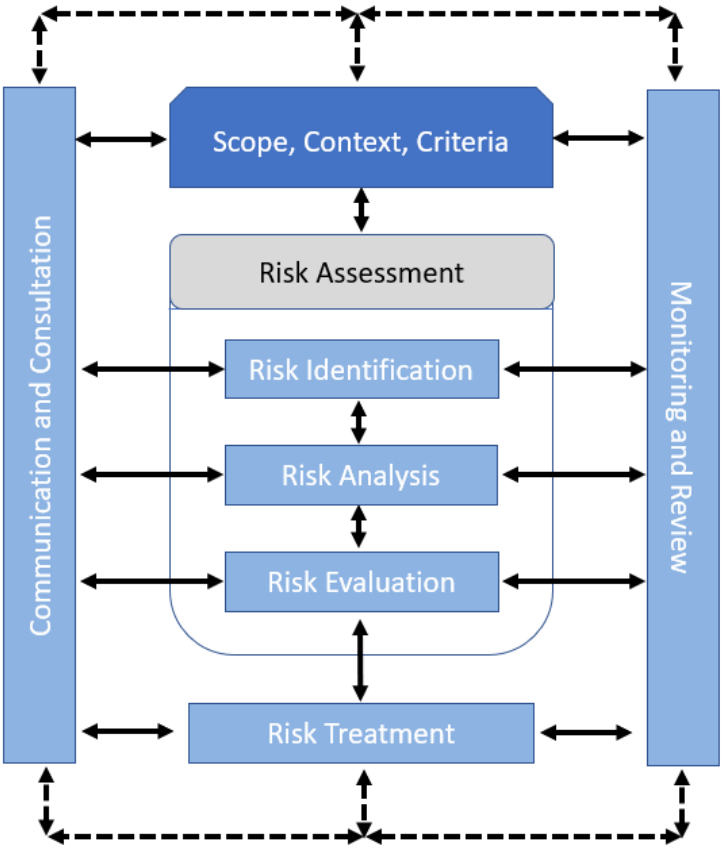
Executive Sponsor:	Director of Corporate Governance
Document Author:	Director of Corporate Governance
Approved by:	Trust Board
Approval Date:	24 September 2020
Review Date:	September 2021
Version:	1.0

Table of contents

1. Introduction

To ensure consistency across the organisation, an iterative process for managing risk has been adopted based on the ISO 31000 (2018) Risk Management - Guidelines. This process provides a logical and systematic method of identifying, analysing, evaluating, mitigating and monitoring risks in a way that will allow Velindre University NHS Trust (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) and 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. Section 7 aims to expand on the process depicted below and use it as the base of the risk management process at VUNHST.

Figure 1: ISO 31000 (2018) Influenced Risk Management Process



1.1 Scope, Context and Criteria

The purpose of establishing the scope, context and criteria is to make the risk management process work for you, enabling effective risk assessment and appropriate risk treatment. It involves defining the scope, the internal and external context, and the risk criteria (such as risk appetite/tolerance and scoring criteria to be used).

1.2 Defining the Scope

As the risk management process may be applied at different levels (i.e. strategic, operational, programme, project or other activities) it is important to be clear about the scope under consideration, the relevant objectives to be considered and their alignment with wider corporate commitments. Considerations include:

Determining the scope of your risk review enables you to focus on identifying the correct risks. For example, are you looking at strategic risks to your organisational objectives? Do you want to identify cross-cutting operational risks that may affect achievement of local objectives or business as usual tasks (e.g. Clinical and non-clinical)? Or do you want to ascertain the potential delivery risks associated with a particular project?

1.3 Defining the Internal and External Context

The internal and external environment in which Velindre University NHS Trust seek to define and achieve their objectives should be considered as it can be a source of risk.

Considerations for examining VUNHST's external context may include, but is not limited to:

- The social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, whether international, national, regional or local
- Key drivers and trends affecting the organisations' objectives
- Patients and other external stakeholders' relationships, perceptions, values, needs and expectations
- Contractual relationships and commitments
- The complexity of networks and dependencies.

Examining VUNHST's internal context may include, but is not limited to:

- Vision, mission and values
- Governance, organisational structure, roles and accountabilities
- Strategy, objectives and policies
- Culture
- Standards, guidelines and models adopted by the organisation
- Capabilities, understood in terms of resources and knowledge (such as capital, time, people, intellectual property, processes, systems and technologies)
- Data, information systems and information flows
- Availability of adequate funds to fulfil corporate commitments and meet/address anticipated liabilities
- Business continuity plans in place to ensure continuity of activities following disruption

- Relationships with internal stakeholders, taking into account their perceptions and values
- Contractual relationships and commitments
- Interdependencies and interconnections.

2. Risk Assessment

Risk assessment is made up of three processes: risk identification, risk analysis and risk evaluation.

Risk assessment is an iterative and collaborative process which draws on the knowledge and view of stakeholders. It should use the best available information, supplemented by further enquiry as necessary and attempt to answer the following questions:

- What may help or prevent us from achieving our organisational objectives?
- Which of those things are most significant and therefore require the most focus?

Note: When assessing risk, consideration should be given to the category of risk as per the risk management framework. We identify risks by considering the key dependencies of the organisation, the corporate objectives, stakeholder expectations, as well as by analysis of our core processes (which may be strategic, tactical, operational or compliance related). Emphasis should therefore be placed on risks that fall within our full and/or partial control.

2.1 Risk Identification

Risk identification involves identifying the whole range of possible risks and the likelihood of losses occurring as a result of these risks. It finds possible sources of risk as well as events and circumstances that could affect the achievement of the organisation's objectives. The process also involves identifying possible causes and potential consequences such that it allows an entire picture to be formed with regards to any given risk. This can be helped by answering the following questions:

- Causation - what has to happen for the risk to occur?
- Outcome - what are the consequences and the impact on objectives should the risk materialise.

When it comes to an organisations risk portfolio, a balanced approach must be taken, and 3 key questions need to be considered:

- What could go wrong?
- What must go right?
- What may surprise you?

Disruption brings new challenges and an added level of complexity which many organisations have never experienced. In order to deliver value, leadership must focus on understanding the risk portfolio and seize disruption with confidence. The process of risk management is no longer solely focused on risk avoidance and mitigation but has now moved forward into embracing disruption in order to achieve ever greater business outcomes through embracing upside opportunities:

Upside Risk- *Risks that offer benefits. Risks significant to the organization's ability to execute its business strategy and achieve its objectives.*

Outside Risk- *Risks that offer negative or positive benefits beyond the organization's control*

Downside Risk- *Offer a negative impact which an organization is focused on eliminating, avoiding, mitigating or transferring in a cost-effective manner*

There are a variety of techniques for identifying uncertainties that may affect one or more objectives, each of which has strengths and weaknesses, so more than one approach should be used to identify risks. Appendix A provides an overview of common risk assessment techniques. Drawing on experience, examining core assumptions and biases and considering changes in the internal and external environment are all relevant factors to consider when identifying risk. Others are:

- 'Tangible' sources of risk (e.g., schedule slippages, personnel unavailability and budget shortfalls)
- 'Intangible' sources of risk (something which cannot be reasonably predicted or quantified, e.g., reputational harm caused by a tweet or computer hack, or damage or theft resulting from a cyberattack)
- Threats (i.e., chemical, biological, ergonomic, physiological, materials, equipment, environment and people
- Opportunities
- vulnerabilities and capabilities
- indicators of emerging risks
- the nature and value of assets and resources
- limitations of knowledge and reliability of information
- time-related factors (i.e., risk proximity).

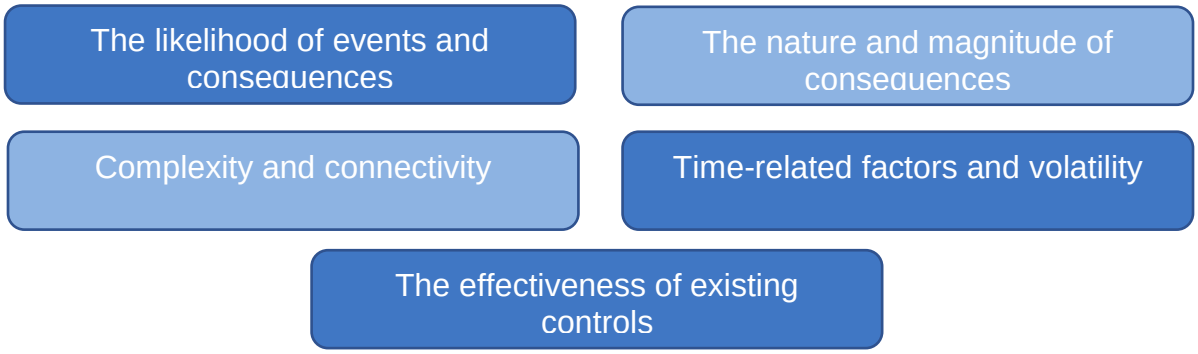
The overarching key point, however, is to ensure that risks relate to an objective or set of objectives. A specific risk owner should be identified for each risk. Ideally the risk owner will also own the related objective or significantly influence its achievement. Ownership of a risk usually results in a greater understanding of said risk, greater emphasis in monitoring the risk, and the implementation of appropriate/ effective controls.

Once identified, the risk needs to be described clearly to ensure that there is a common understanding by stakeholders of the risk. It is important that risks are described in a succinct and

clear way.

2.2 Risk Analysis

Risk analysis determines a risk's significance by considering its potential likelihood in occurring and quantifies the resultant impact if it were to occur and therefore yields the gross risk value. Risks should be assessed in an objective and consistent manner if they are to be managed robustly; risk analysis should therefore consider factors such as:



Assessing likelihood and impact together produces a gross risk rating, known as a RAG (red-amber-green) rating. Appendix B provides VUNHST's risk heatmap criterion which is used to rate risks.

Each risk event on our risk registers has an inherent score (i.e. the exposure before any action has been taken to manage it or if existing controls failed entirely); a residual score (i.e. the threat that remains after all existing controls have been applied); and where risks are outside acceptable levels of tolerance, a target risk score should be agreed (i.e. the level that future mitigation should aim to achieve or better; this will vary over time and should be set and revised by the executive director). All scores should be recorded in the relevant risk register.

Human and cultural factors (risk perception and the social amplification of risk)

Human behavior and culture significantly influence all aspects of risk management at each stage. One of the most perplexing problems in risk analysis is why some relatively minor risks or risk events often elicit strong public concerns and result in substantially higher impacts than anticipated, or higher than our technical risk assessment predicts. This is because risks interact with psychological, sociological, and cultural perceptions and what constitutes 'risky' behavior, which can amplify public responses to the risk or risk event.

2.3 Risk Evaluation

Not all risks are equally important, so we need to filter and prioritise them to find the most potent threats (and the greatest opportunities). The purpose of risk evaluation is to support decisions. The process involves comparing the results of the risk analysis with the established risk criteria to prioritise significant risks and identify where additional action is required. This can lead to a decision to:

Decisions should take account of the wider context and the actual and perceived consequences to external and internal stakeholders.

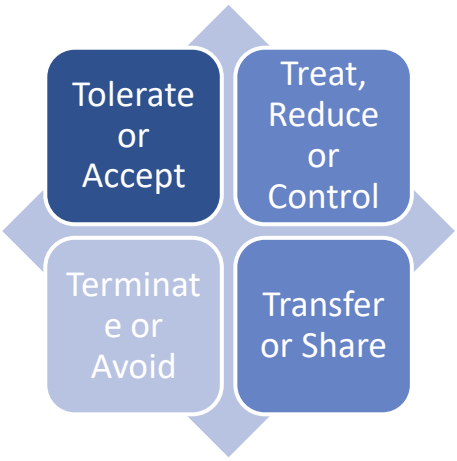
3. Risk Treatment and Response

Once a risk has been recorded, the risk owner needs to consider how each risk will be treated. In this step existing controls are improved, or new controls are developed and implemented. A risk action plan (also referred to as a risk treatment plan) should be put in place, which involves selecting and implementing one or more treatment options. Note: Once a treatment has been implemented, it becomes a control, or it modifies existing controls.

There are many treatment options. You can avoid the risk, you can reduce the risk, you can remove the source of the risk, you can modify the consequences, you can change the probabilities, you can share the risk with others, you can simply retain or accept the risk, you can insure against the residual risk (though this only mitigates financial impact) or you can even increase the risk to pursue an opportunity. The level and type of treatment will vary depending on the level of residual risk that has been determined and the tolerance for managing risk to within its risk appetite.

3.1 4 T's Model

To help guide response, the 4 T's Model (which depicts the 4 primary responses to hazard risk) of risk mitigation (illustrated below) will be utilised at Velindre University NHS Trust:



Terminate or Avoid- *By deciding not to engage in an activity, that gives rise to a risk, the organisation will not be exposed to the risk itself and therefore the consequences. However, it will be very difficult to use this approach in the public sector.*

Transfer or Share- *By 'outsourcing' an activity to transfer the responsibility of the risk to another party, or through buying insurance. Again, it is rare that this option is available, and it is unlikely to remove reputational risks to a great extent.*

***Treat*, Control or Reduce** – *By implementing action to constrain the risk to an acceptable level. This can include implementing controls to help ensure that the possible negative impact of a risk does not increase (managing threats) and can include actions to minimise any impact should the risk occur (such as identifying contingent actions). It can also be implementing actions to help ensure a risk does occur (managing opportunities).*

Tolerate or Accept- *By informed decision a risk owner may feel that:*

- *The level of risk is acceptable, and no further actions are required/ possible*
- *The risk is sufficiently low that treatment is not considered cost effective.*
- *A sufficient opportunity exists that outweighs the perceived* level of threat

Additional considerations

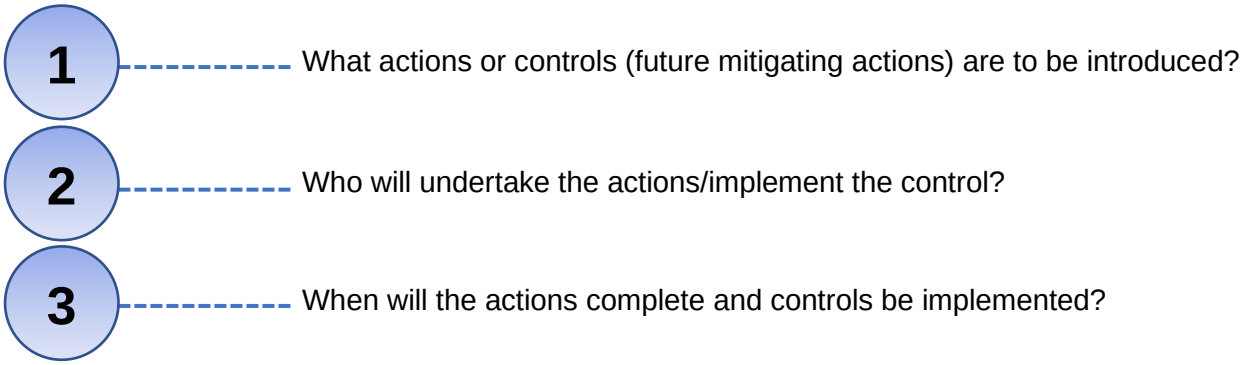
It is not always possible to identify and then fully implement actions to eliminate or minimise a risk. Risk treatments might not produce the expected outcomes and/or could produce unintended consequences. Where this is the case, it is essential that the significance of the risk that remains is understood in the organisation and that, in accordance with risk management governance, the relevant committee confirms it is prepared to accept that level of risk.

Additionally, risks cannot be addressed in isolation from each other; the management of one risk may have an impact on another, or management actions which are effective in controlling more than one risk simultaneously may be achievable.

3.2 Preparing and Implementing Risk Treatment/ Action Plans

The purpose of risk treatment/action plans is to specify how the chosen treatment options will be implemented, so that arrangements are understood by those involved, and progress against the plan can be monitored. The risk owner must appoint an action owner, to be responsible for the day-to-day management and mitigation activity allocated to them. This must be a named individual who has the relevant authority and resources to undertake the task. There may be several action owners from more than one team or business area who will be responsible for managing and mitigating the risk.

When developing a risk action plan, you need to agree:



Risk owners must also ensure that the actions/controls to be introduced offer value for money in relation to the risk, for example is the cost of mitigating the risk in proportion to the cost of the risk materializing?

4. Risk Recording and Reporting

The risk management process and its outcomes should be documented in a live risk register and reported through appropriate risk governance mechanisms. Recording and reporting aims to:

- Communicate risk management activities and outcomes across Velindre University NHS Trust
- Provide information for decision-making
- Improve risk management activities
- Assist interaction with stakeholders, including those with responsibility and accountability for risk management activities

4.1 Risk Register

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.

For Velindre University NHS Trust, once the risk has been identified and analysed the next stage is to ensure the risk is recorded in Datix Web Risk Register Module which will form the Unit's Risk Register. The register allows for corporate teams, departments and divisions throughout the Trust to capture all the information needed to manage risk appropriately and determine whether any risks should be escalated through our governance structure. The risk register should be kept up to date and reviewed regularly. New risks should be added as they are discovered.

The Corporate Governance Team provides a standard risk register template that should be used to capture risks at strategic and operational level. An exception would be if alternative, robust programme or project management arrangements were in place. Note: The Corporate Governance Team must agree all exceptions. NOTE: The intention is for all risk register to be transferred to the Datix system in 2020/21

4.2 Risk Reporting

To ensure Ward to Board connection / connectivity of the Trust Board to actual service delivery, each department maintains their own risk register which ultimately feeds the TAF to triangulate the messages contained in board papers with observations and interactions with patients, staff and stakeholders.

Departments/Divisions regularly monitor and report risks affecting their activities – and the effectiveness of control measures for managing them – to senior managers or executive 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 risk reporting and escalation routes are stated below

→ 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 (will 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 Executive Director, and not wait for the reporting cycle above. The executive 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.

Additional guidance on risk reporting can be found in the VUNHST Risk Management Framework

5. Risk Monitoring and Review

The monitoring of risks forms an essential part of the risk management process. This is due to the ever-changing nature of risk profiles, and to ensure controls are still operating effectively. Risk owners should monitor their risks regularly to:

- Confirm that action plans to address risks are being undertaken and completed
- Report any change in assessment of the impact and likelihood of the risk
- Confirm the risks are still relevant in the changing environment
- Escalate if necessary, including if the risk cannot be managed at the current level.

The review process should fulfil the following requirements:

- Monitor whether controls remain aligned to risks in their area of responsibility
- Monitor whether key risks are being managed within the risk appetite in their area of responsibility
- Monitor the risk profile and key risks identified by the process and how they are changing over time
- Monitor the progress of actions to treat key risks and the operation of key controls
- Escalate risks
- Re-prioritise resources
- Make better informed decisions.

The regular review of risks should be built into the local management reporting and review cycle, supported by relevant risk leads and discussed at relevant management team meetings, programme or project meetings

6. Communication and Consultation

You must continually communicate with and consult internal and external stakeholders, where possible, to gain input and agree ownership of risk assessment results. It is also important to understand stakeholders' objectives, so you can plan their involvement and take their views into account in agreeing whether a specified risk level is acceptable or tolerable.

Discussions could be about the existence of risks, their nature, likelihood, impact and significance, as

well as whether risks are acceptable or should be treated, and what treatment options to consider.

As responsible professionals we should take advantage of our experience to learn lessons and benefit future ventures. This means that we should spend time thinking about what worked well and what needs improvement and recording our conclusions in a way that can be reused by ourselves and others.

Effective internal and external communication is important to ensure that those responsible for implementing risk management, and those with a vested interest understand the basis on which decisions are made and why particular actions are required.

Internal stakeholders can include any managers which the risk identified may impact on their service or staff. External stakeholders will vary depending on the type of risk and the divisional risk lead will need to consider which external stakeholders will need to be notified. All significant risks will be reported to the Welsh Government through the weekly brief from organisations and quarterly performance review meetings.

There will be occasions when a risk is shared with another Health organisation for example in the instance of Service Level agreements for the delivery of services across organisations. In this case VUNHST can share these risks with the relevant health organisations through the risk management database on the request from Units.

Appendix A: Risk Assessment Techniques

Risk assessment is an important step in the risk management process. If you don't identify a risk, you can't manage it. It's also important to scan the environment from time to time to identify new and emerging risks, as our exposure to risk is constantly changing.

Technique	Description	Advantages	Disadvantages
Questionnaires, checklists, surveys and interviews	Use of structured questionnaires and checklists to collect information that will assist with the recognition of the significant risks.	Consistent structure guarantees consistency Greater involvement than in a workshop	Rigid approach may result in some risks being missed Questions will be based on historical knowledge
Workshops and brainstorming To have a structured discussion at a risk assessment workshop, several brainstorming techniques can be used e.g. SWOT analysis (Strength, Weakness, Opportunity Threats); PESTLE analysis (Political, Economic, Sociological, Technological, Legal, Environmental); Hazard and Operability analysis (HAZOP); and Failure Modes Effects Analysis (FMEA).	Collection and sharing of ideas at workshops to discuss the events that could impact the objectives, core processes or key dependencies.	Consolidated opinions from all interested parties Greater interaction produces more ideas	Senior management tends to dominate Issues will be missed if incorrect people involved
Inspections and audits	Physical inspections of premises and activities and audits of compliance with established systems and procedures.	Physical evidence forms the basis of opinion Audit approach results in good structure Inspections are most suitable for hazard risks	Audit approach tends to focus on historical experience
Flow charts and dependency analysis	Analysis of the processes and operations within the organisation to identify critical components that are key to success.	Useful output that may be used elsewhere Analysis produces better understanding of processes	Difficult to use for strategic risks May be very detailed and time-consuming

Appendix B: Additional guidance on controls

Types of controls

There is a fundamental difference in how we respond to the upside and downside of risk. VUNHST naturally try and minimise hazard risks and the potential downside of opportunity risks, subject to it being commercially viable to do so. The upside of opportunity risks, however, is different and in this instance, we look to attach Key Risk Indicators to opportunity risks to monitor them and assess how best we might respond.

There are a range of controls that can be applied to hazard risks. The most convenient classification system is to describe these controls as preventive, corrective, directive and detective (PCDD). This is the risk classification system suggested in the Orange Book.

There is a relationship between these four types of controls and the dominant risk response described in the 4Ts of hazard response i.e., you would typically deploy Preventive controls for risks that you wish to terminate, Corrective controls for risks that you choose to treat, Directive controls for risks you wish to transfer, and Detective controls for those risks you agree to tolerate. Further information and examples of the types of hazard controls are provided below:

Control Type	Description	Examples
Preventive (terminate)	These controls are designed to limit the possibility of an undesirable outcome being realized. The more important it is to stop an undesirable outcome, then the more important it is to implement appropriate preventive controls.	• Authorization limits of and separation of duties • Pre-employment screening of potential staff
Corrective (treat)	These controls are designed to limit the scope for loss and reduce any undesirable outcomes that have been realized. They may also provide a route of recourse to achieve some recovery against loss or damage.	• Passwords or other access controls • Staff rotation and regular change of supervisors • Exposure reduction by limitation on hours worked
Directive (transfer)	These controls are designed to ensure that a particular outcome is achieved. They are based on giving directions to people on how to ensure that losses do not occur. They are important, but depend on people following established safe	• Training and supervision to enforce procedures • Personal protective equipment and improved welfare facilities

	systems of work.	• Accessible, detailed, written systems and procedures • Training to ensure understanding of procedures
Detective (tolerate)	These controls are designed to identify occasions when undesirable outcomes have been realized. Their effect is, by definition, 'after the event' so they are only appropriate when it is possible to accept that the loss or damage has occurred.	• Health monitoring to enquire about potential symptoms • Reconciliation, audit and review by internal audit • Whistleblowing policy to report (alleged) fraud

Documenting and reviewing Key Controls

Controls are only good if they are relevant; therefore, departments/divisions need to ensure that they routinely review their controls to see if they are still effective. As things change, you need to think about making changes to your controls as your organisation evolves i.e., assessing whether controls are no longer valid and how new controls may help the organization implement changes.

When identifying / assessing key controls, the first steps are to determine:

- Do Key Controls exist?
- Are those controls working?
- Are those control activities documented and properly performed?
- What mechanisms are there to provide assurance (evidence) on the operation of controls?

Key versus Non-Key Controls

Only Key Controls should be documented within your risk register. A Key Control has the following characteristics:

→ It is required to provide reasonable assurance that material errors will be prevented or timely detected

→ It is the only or one of the only controls that covers a risk of material misstatement (it is indispensable to cover its control objective)

→ If it fails, it is highly improbable that other controls could detect the control absence.

→ It is a control that covers more than one risk or supports a whole process execution

→ It needs to be tested by internal audit to provide assurance over financial assertions

A Non-Key Control has the following characteristics:

- It can fail without affecting a whole process
- It has an indirect effect on the risk of material misstatement
- It is generally not included within internal audit testing

Appendix C: Risk Quantification Matrix

IMPACT Matrix

	Impact, Consequence score (severity levels) and examples				
	1	**2**	**3**	**4**	**5**
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Impact on the safety of patients, staff or public (physical/ psychological harm)	Minimal injury requiring no/ minimal intervention or treatment. No time off work	Minor injury or illness, requiring minor intervention Requiring time off work for >3 days Increase in length of hospital stay by 1-3 days	Moderate injury requiring professional intervention Requiring time off work for 4-14 days Increase in length of hospital stay by 4-15 days RIDDOR/agency reportable incident An event which impacts on a small number of patients	Major injury leading to long-term incapacity /disability Requiring time off work for >14 days Increase in length of hospital stay by >15 days Mismanagement of patient care with long-term effects	Incident leading to death Multiple permanent injuries or irreversible health effects An event which impacts on a large number of patients
Quality/complaints/ audit	Peripheral element of treatment or service suboptimal Informal complaint/ inquiry	Overall treatment or service suboptimal Formal complaint (stage 1) Local resolution Single failure to meet internal standards Minor implications for patient safety if unresolved Reduced performance rating if unresolved	Treatment or service has significantly reduced effectiveness Formal complaint (stage 2) complaint Local resolution (with potential to go to independent review) Repeated failure to meet internal standards Major patient safety implications if findings are not acted on	Non-compliance with national standards with significant risk to patients if unresolved Multiple complaints/ independent review Low performance rating Critical report	Totally unacceptable level or quality of treatment/service Gross failure of patient safety if findings not acted on Inquest/ombudsman inquiry Gross failure to meet national standards
Human resources/ organisational development/staffing/ competence	Short-term low staffing level that temporarily reduces service quality (< 1 day)	Low staffing level that reduces the service quality	Late delivery of key objective/ service due to lack of staff Unsafe staffing level or competence (>1 day) Low staff morale Poor staff attendance for mandatory/key training	Uncertain delivery of key objective/service due to lack of staff Unsafe staffing level or competence (>5 days) Loss of key staff Very low staff morale No staff attending mandatory/ key training	Non-delivery of key objective/service due to lack of staff Ongoing unsafe staffing levels or competence Loss of several key staff No staff attending mandatory training /key training on an ongoing basis

Statutory duty/ inspections	No or minimal impact or breech of guidance/ statutory duty	Breech of statutory legislation Reduced performance rating if unresolved	Single breech in statutory duty Challenging external recommendations/ improvement notice	Enforcement action Multiple breeches in statutory duty Improvement notices Low performance rating Critical report	Multiple breeches in statutory duty Prosecution Complete systems change required Zero performance rating Severely critical report
Adverse publicity/ reputation	Rumours Potential for public concern	Local media coverage – short-term reduction in public confidence Elements of public expectation not being met	Local media coverage – long-term reduction in public confidence	National media coverage with <3 days service well below reasonable public expectation	National media coverage with >3 days service well below reasonable public expectation. MP concerned (questions in the House) Total loss of public confidence
Business Objectives/ Projects	Insignificant cost increase/ schedule slippage	<5 per cent over project budget Schedule slippage	5-10 per cent over project budget Schedule slippage	Non-compliance with national 10–25 per cent over project budget Schedule slippage Key objectives not met	Incident leading >25 per cent over project budget Schedule slippage Key objectives not met
Finance Including Claims	Small loss risk of claim remote	Loss of 0.1–0.25 per cent of budget Claim less than £10,000	Loss of 0.25–0.5 per cent of budget Claim(s) between £10,000 and £100,000	Uncertain delivery of key objective/Loss of 0.5–1.0 per cent of budget Claim(s) between £100,000 and £1 million Purchasers failing to pay on time	Non-delivery of key objective/ Loss of >1 per cent of budget Failure to meet specification/ slippage Loss of contract / payment by results Claim(s) >£1 million
Service/ business interruption Environ-mental impact	Loss/interruption of >1 hour Minimal or no impact on the environment	Loss/interruption of >8 hours Minor impact on environment	Loss/interruption of >1 day Moderate impact on environment	Loss/interruption of >1 week Major impact on environment	Permanent loss of service or facility Catastrophic impact on environment

Likelihood – MATRIX

LIKELIHOOD (*)					
LIKELIHOOD SCORE	1	2	3	4	5
DESCRIPTOR	RARE	UNLIKELY	POSSIBLE	PROBABLE	EXPECTED
Frequency: How often might it/ does it happen?	Not expected to occur for 10 years	Expected to occur at least annually	Expected to occur at least monthly	Expected to occur at least weekly	Expected to occur at least daily
Probability: Will it happen or not?	Less than 0.1% chance	0.1 - 1% chance	1 - 10% chance	10 - 50% chance	Greater than 50% chance

Risk Rating Matrix- Impact X Likelihood

RISK MATRIX	LIKELIHOOD (*)				
CONSEQUENCE (**)	1 - Rare	2 - Unlikely	3 - Possible	4 - Probable	5 - Expected
1 - Negligible	1	2	3	4	5
2 - Minor	2	4	6	8	10
3 - Moderate	3	6	9	12	15
4 - Major	4	8	12	16	20
5 - Catastrophic	5	10	15	20	25