University Hospitals Bristol and Weston NHS Foundation Trust

Risk Management Policy

Document Data			
Document Type:	Policy		
Document Reference	15615		
Document Status:	Approved		
Document Owner:	Head of Risk Management		
Executive Lead:	Chief Executive		
Approval Authority:	Senior Leadership Team		
Review Cycle:	36 Months		
Date Version Effective From:	11/01/2022	**Date Version Effective To:**	10/01/2025

What is in this policy?

This **policy** describes the sources of University Hospitals Bristol and Weston NHS Foundation Trust's (the Trust's) risks and its approach to the identification, assessment, management and escalation of risk within the organisation and is predicated on the belief that risk management is an important activity and should be an inclusive and integrative process covering all risks, set against a common set of principles, and a major corporate responsibility which requires strong leadership and regular review.

This policy sets out:

- The framework that supports the maintenance and development of a risk-aware culture where the right people do the right thing at the right time.
- The outline of the processes to be used for the management of all Trust risks.
- Definitions of risk types.
- Escalation processes to ensure oversight of risks from ward to Trust Board.
- The roles of all staff in relation to risk identification, management, and review.

Document Change Control				
Date of Version	**Version Number**	**Lead for Revisions**	**Type of Revision**	**Description of Revision**
September 2012	1.0	Head of Quality (Patient Safety)	Major	New policy following decision to separate out policy requirements from the previous Risk Management Strategy.
May 2013	1.1	Trust Risk Manager	Major	Comprehensive review following approval of the revised Risk Management Strategy.
August 2013	2.0	Trust Risk Manager	Minor	Policy approved at RMG 07/08/2013.
August 2016	3.3	Head of Risk Management	Major	Inclusion of Standards and update to the development of the risk management framework.
August 2016	3.4	Head of Risk Management	Minor	Amendment to 6.14.
June 2017	3.5	Head of Risk Management	Minor	Terminology improved. Addition of project risk guidance and updated in line with Trust risk management framework. Approved at SLT 19/07/17.
January 2020	3.6	Head of Risk Management	Minor	Policy reviewed in preparation of Organisation merger. Inclusion of risk tolerance section. Update of Job titles and changes to roles undertaking SIRO and Caldicott Guardian responsibilities. Removal of reference to H&S workspace RA repository. Inclusion of People Committee, Strategic Risk Register and Counter Fraud.
January 2022	3.7	Head of Risk Management	Minor	Inclusion of risk appetite statement and clarification of points highlighted from ASW Assurance Report UHBW02/21.

Sign off Process and Dates	
Groups consulted	**Date agreed**
Policy Assurance Group	20/02/2020
Risk Management Group	11/01/2022
Senior Leadership Team	19/01/2022

Do I need to read this Policy?

Table of Contents

1. Introduction

The Trust is faced with several factors that may impact upon its ability to meet its objectives. The effect of uncertainty on those objectives is known as risk.

Risk Management can be defined as the identification, assessment, and prioritisation of risks followed by a coordinated and economical application of resources to minimise, monitor and control the probability and/or impact of unfortunate events. Risks should also be reviewed at regular intervals to ensure they continue to be appropriately mitigated.

It is widely recognised that an effectively planned, organised, and controlled approach to risk management is a cornerstone of sound management practice and is key to ensuring the achievement of objectives. A comprehensive management approach to risk reduces adverse outcomes and can result in benefit from what is often referred to as the 'upside of risk'.

Risk Management is an integral part of good governance, and the Trust has adopted an integrated approach to the overall management of risk irrespective of whether the risks are clinical, organisational or financial.

2. Purpose

The purpose of the policy is to:

- Define the framework and systems the Trust will use to identify, manage and eliminate or reduce to a reasonable level, risks that threaten the Trust's ability to meet its objectives.
- Ensure that all staff are adequately trained and competent to execute their duties in respect of risk management.
- Ensure that risk management issues when writing reports and considering decisions.
- Reinforce the importance of effective risk management as part of the everyday work of all staff employed or engaged by the Trust.
- Maintain comprehensive registers of risks (clinical and non-clinical) and ensuring that these are reviewed on a regular basis.
- Ensure controls are in place to effectively mitigate the risk and are understood by those expected to apply them.
- Ensure processes are in place to identify gaps in controls are identified and can be rectified and that assurances are reviewed and acted upon in a timely manner.
- Ensure that documented procedures of the control of risk and provision of suitable information, training and supervision are maintained.
- Ensure that adequate monitoring arrangements are in place.

The application of this policy will allow the following priorities to be realised:

- Alignment between risk management activities with business cycles of the sub-committees of the Trust Board.
- The implementation of risk treatment sufficient to effectively mitigate the risks identified.
- Improved transparency of risk by adopting a standardised method of risk description, focussing on cause and effect of risks.

- Risk registers maintained at a departmental level are of an acceptable standard and subject to regular review.
- The practice of risk reviews being in alignment with quarterly reporting cycles.
- The processes for approval of risks are clearly defined and assuring that there is a consistent approach across divisions.

3. Scope

The policy applies Trust-wide to all staff and students including contractors and agency staff.

4. Definitions

4.1 *Assurance*

Is the confidence the Trust has, based on sufficient evidence, that controls are in place, operating effectively and its objectives are being achieved.

4.2 *Consequence*

The outcome or potential outcome of an event, sometimes referred to as 'impact' or 'severity'.

4.3 *Control*

A measure in place to mitigate a risk.

4.4 *Current score*

What the risk score is assessed as with current controls in place.

4.5 *Governance*

Is the systems and processes by which the Trust leads, directs and controls its functions in order to achieve its organisational objectives, safety, and quality of services, and in which it relates to the wider community and partner organisations.

4.6 *Inherent score*

An assessment of the risk prior to any mitigation and controls being applied. This is the "unmitigated" risk.

4.7 *Internal controls*

Are Trust policies, procedures, practices, behaviour's or organisational structures to manage risks and achieve objectives.

4.8 *Likelihood*

Is the probability that the consequence will actually happen.

4.9 *Operational risks*

Are by-products of the day-to-day running of the Trust and include a broad spectrum of risks including clinical risk, financial risk (including fraud), legal risks (arising from employment law or health and safety regulation), regulatory risk, risk of loss or damage to assets or system failures etc. Operational risks can be managed by the Division which is responsible for delivering services.

4.10 *Project risks*

Are risks relating specifically to the delivery of a particular project. They are often run alongside project 'issue' logs (issues being events that are currently occurring).

4.11 *Risk*

Is the threat or possibility that an action or event will adversely or beneficially affect the Trust's ability to achieve its objectives. It is measured in terms of likelihood and consequence. An 'affect' may be positive, negative or a deviation from the expected position.

4.12 *Risk Appetite*

The amount of risk exposure an organisation is willing to seek or accept in the pursuit of its objectives.

4.13 *Risk Assessor*

Is the person who conducts the risk assessment.

4.14 *Risk Assessment*

Is a systematic process of assessing the likelihood of something happening (Frequency or probability) and the consequence if the risk actually happens (impact or consequence).

4.15 *Risk Management*

Is about the Trust's culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse events. The risk management process covers all processes involved in identifying, assessing and judging risks, assigning ownership, taking action to mitigate or anticipate them, and monitoring and reviewing progress.

4.16 *Risk Owner*

The person responsible for ensuring the risk is adequately managed.

4.17 *Risk Tolerance (or Capacity)*

The boundaries of risk taking outside of which the organisation is not prepared to venture in pursuit of its objectives (see section 7).

4.18 *Strategic risks*

Are those that represent a threat to achieving the Trust's strategic objectives or to its continued existence. They also include risks that are widespread beyond the local area and risks for which the cost of control is significantly beyond the scope of the local budget holder. Strategic risks must

be reported to the Board of the Directors and should be managed at executive level, directly or by close supervision.

4.19 *Strategic Objectives*

Are the objectives set by the Board of Directors in the annual planning process specify the standards, outcomes, achievements and targets for various areas of the Trust's operations.

4.20 *Risk Registers*

Are repositories for electronically recording and dynamically managing risks that have been appropriately assessed. Risk registers are available at different organisational levels across the Trust.

4.21 *Target Score*

An assessment of anticipated risk after the planned actions and mitigations have been applied.

5. Duties, Roles and Responsibilities

5.1 *Trust Board of Directors*

The executive and non-executive directors have a collective responsibility as a Trust Board to ensure that the risk management processes are providing them with adequate and appropriate information and assurances relating to risks against the Trust's objectives. The executive and non-executive directors are responsible for ensuring that they are adequately equipped with the knowledge and skills to fulfil this role.

The Board is also responsible for reviewing the effectiveness of its internal control systems and is required to ensure that the Trust's risk management arrangements are sound and protects patients, staff, the public, and other stakeholders against risks of all kinds.

5.2 *Executive Directors*

Executive directors are responsible for managing risk as delegated by the Chief Executive and set out in the risk management policy and the Terms of Reference of the Risk Management Group. Executive directors are also responsible for risks allocated to them on the corporate risk register and Trust Services risk register.

The diagrams below show the principal bodies responsible for the governance and oversight of risk within the Trust and the reporting hierarchy. It details committees and groups which have some responsibility for risk and report directly to the Board of Directors. This provides assurance to the Board that risk management processes are in place and remain effective.

5.3 *Chief Executive*

The Chief Executive is accountable to the Chairman and the Board and, as the accountable officer, has overall responsibility for ensuring that the Trust operates effective risk management processes in order to protect all persons who may be affected by the Trust's business. The Chief Executive is required to sign annually on behalf of the Board, an Annual Governance Statement, in which the Board acknowledges and accepts its responsibility for maintaining and reviewing the effectiveness of a sound system of internal control, including risk management.

5.4 *Medical Director*

Accountable to the Chief Executive and the Board, the Medical Director has joint lead responsibility for healthcare governance with the chief nurse. This includes; lead responsibility for clinical performance of the medical workforce: clinical audit: medical innovation: research governance: medical education; the role of Caldicott Guardian; and will report key clinical risks to the Board on a routine basis.

5.5 *Chief Nurse*

The Chief Nurse has joint lead responsibility for healthcare governance with the Medical Director and is accountable to the Chief Executive and the Board for the delivery of the Trust's patient safety and quality initiatives. The post-holder will also be responsible and accountable for the operational management of the nursing teams and allied healthcare professionals and will lead.

5.6 *Deputy Chief Executive/Chief Operating Officer*

The Deputy Chief Executive/Chief Operating Officer is accountable to the Chief Executive and the Board for overall management of operational risks and corporate services including; corporate governance, risk management, communications, and legal services. The post-holder will ensure that risks in relation to this portfolio are managed in line with the Trust's risk management systems and processes. The post is also responsible for the operational management of divisional teams, supporting the Trust's risk management systems and processes.

5.7 *Director of Strategy and Transformation*

The Director of Strategy and Transformation is accountable to the Chief Executive and the Board leading the development of local health and social care services, strategic development, business planning and service transformation in the Trust. The post-holder will ensure that all risks in relation to this portfolio will be managed in line with the Trust's risk management systems and processes.

5.8 *Director of Finance and Information*

The Director of Finance and Information is accountable to Chief Executive and the Board for the management of financial governance, including advising on financial/business risk, audit and assurance. The Director of Finance and Information also holds the role of Senior Information Risk Owner (SIRO).

5.9 *Director of People*

The Director of People is accountable to the Chief Executive and the Board for the management of all human resources and associated workforce risks, including those relating to training and organisational development.

5.10 *Senior Information Risk Officer (SIRO)*

The Director of Finance and Information shall also fulfil the role and function of the SIRO and is accountable to the Chief Executive for the management of information risks.

5.11 *The Caldicott Guardian*

The Medical Director Team shall nominate an Associate Medical Director to fulfil the role of Caldicott Guardian and will play a key role in helping to ensure that the Trust satisfies the highest practical standards for managing information governance risks. The Caldicott Guardian will act as the conscience of the organisation in this respect, and will actively support work to manage such risks.

5.12 *Director of Corporate Governance*

The Director of Corporate Governance is responsible for ensuring that the Trust Board of Directors is cognisant of its duties towards risk governance and management and for coordinating the annual cycle of Board business to ensure these duties are incorporated on the Board's agenda.

The Director of Corporate Governance is also responsible for the coordination of the Trust's Board Assurance Framework to ensure proactive management to ensure that the Board remains sighted on the key risks facing the Trust.

5.13 *Head of Risk Management*

The Head of Risk Management develops, implements and monitors compliance with the risk management policy and is responsible for maintaining the overall structure for risk management within the Trust. The post-holder facilitates the development of a risk aware culture within the Trust, compiles risk information and prepares reports for the Senior Leadership Team, Risk Management Group and Trust Board of Directors.

5.14 *Wards and department leads*

Each manager is responsible for ensuring risk assessments are completed with implementation of suitable and sufficient control measures and for communicating the risk assessment to those affected.

Line managers must allocate sufficient time for the risk assessor to complete their assessor responsibilities within normal working hours.

5.15 *Project Managers*

Project managers are responsible for communicating and strategic or operational risks that have given rise during the implementation of a project, to the appropriate senior manager. Operational risks must not be held on project risk registers.

5.16 *All staff (including Honorary Contract holders, locum and agency staff and contractors)*

Notwithstanding the identification of the above key personnel, the Trust recognises that organisational risk management is the responsibility of all members of staff. Every member of staff (including clinicians, temporary staff, contractors and volunteers) are responsible for ensuring that their own actions contribute to the wellbeing of patients, staff, visitors and the Trust.

All staff are required to attend and follow individual essential training requirements and not to use equipment, adopt practices or processes which deviate from mandatory or statutory requirements

and procedures for the purposes of health and safety. They are expected to locate, observe and comply with all relevant policies and procedures that have been made available within the Trust.

All staff must contribute to the identification, management, reporting and assessment of risks and to take positive action to manage them appropriately. This is an essential part of managing risks locally and is a statutory requirement.

In addition, staff have a responsibility for taking steps to avoid injuries and risks to patients, staff, and visitors. In fulfilling this role, which may involve raising concerns about standards, staff might consider the need for reporting under the Trust's Freedom to Speak up Policy.

5.17 *Senior Leadership Team*

The Senior Leadership Team (SLT) is responsible for maintaining the Corporate Risk Register. SLT receives risk exception reports from divisions at each business meeting, informing them of any risks with the division that SLT should have sight of. These may be either risks scoring 12 or above, or those with the potential to significantly impact upon corporate or strategic objectives.

5.18 *Risk Management Group*

As a management group established and chaired by the Chief Executive, the Risk Management Group (RMG) has delegated responsibility from the Senior Leadership Team for the management of organisational risk. This includes receiving the corporate risk register and divisional risk registers in full on an annual basis.

5.19 *Audit Committee*

The Audit Committee shall review the establishment and maintenance of an effective system of governance, risk management and internal control across the whole of the organisation's activities.

5.20 *Quality and Outcomes Committee*

The Quality and Outcomes Committee shall receive the corporate & strategic risk registers and review the suitability and implementation of risk mitigation plans with regard to their potential impact on patient outcomes.

5.21 *Finance & Digital Committee*

The Finance Committee is responsible for monitoring financial risk. The Director of Finance and Information is responsible for reporting this to the Risk Management Group.

5.22 *People Committee*

The People Committee shall receive the corporate & strategic risk registers and review the suitability and implementation of risk mitigation plans with regard to their potential impact on the Trusts workforce.

5.23 *Divisional Management Boards*

Divisional Management Boards are responsible for having a planned risk assessment programme in place, comprised of quarterly Divisional Management Board meetings and monthly Divisional

Governance meetings, at which, the implementation of recommendations from risk assessments and action plans with realistic timescales for mitigating risks are reviewed.

Divisional Management Boards shall adopt a standardised approach to the management of risk in accordance with the duties defined in the Risk Management Policy and the Terms of Reference of the Risk Management Group. They are also responsible for reviewing the divisional risk register and considering risks escalated to the management board from their departments for adding to the divisional risk register. They are required to present their divisional risk registers in full to the Risk Management Group on an annual basis.

Divisions are required to report progress of mitigating actions in respect of their key risks in quarterly performance reviews with executive directors, ensuring resource is allocated within their division to assess and manage their risks.

Divisional directors are accountable to the chief operating officer for the implementation of the Risk Management Strategy and Policy locally and for creating associated procedures within their division, ensuring that the divisional risk register is populated with all risks (clinical, non-clinical and financial) and informed by local risk assessments and reviewed in its entirety by the divisional on a quarterly basis. In addition, divisional directors have a duty to ensure that their staff are given the necessary information and training to enable them to work safely.

(a) Trust-wide specialist advisers are responsible for advising anyone about a specific risk assessment issue e.g. Head of Health and Safety.
(b) Specialist patient care risk assessment support is available from relevant specialists e.g. blood transfusion practitioner, dementia and falls lead, tissue viability nurses.

5.24 *Divisional Governance/Quality/Patient Safety Leads*

Divisional leads are responsible for:

(a) Facilitating divisional and departmental risk process' in accordance with this policy and ensure escalation of risks occur in timely manner to the divisional board; and
(b) Facilitating the preparation of monthly exception reports of any divisional risks of 12 or above, to be received by the central risk team no less than 10 days before the meeting of the SLT.

5.25 *Trust-wide specialist advisers*

Responsible for advising anyone about a specific risk assessment issue e.g.:

(a) Health and safety advisors
(b) Manual handling and ergonomic advisor
(c) Radiation protection advisor

5.26 *Risk Owners*

Each risk owner is responsible for ensuring:

(a) That risk registers relating to their area of responsibility are managed in accordance with this policy and related procedures;

(b) That risks are reviewed, updated and progress added prior to quarterly review by Risk Management Group or Divisional Boards (annually to governance groups for departmental risks) or when there are any changes which impact on the risk;
(c) The implementation of suitable and sufficient control measures and for communicating the risk assessment to those affected;
(d) Sufficient time to complete assessor responsibilities within normal working hours is available; and
(e) That risk owners and handlers have successfully completed the Trusts Risk Management e-learning.

5.27 *Health & Safety Risk Assessors*

Generic Risk assessor's (GRA's) are responsible for conducting risk assessment on behalf of ward and department managers. They should:

(a) Have attended the Trust's generic risk assessor training, followed by three yearly updates;
(b) Also attend specific training, e.g. Control of Substances Hazardous to Health (COSHH) and manual handing risk assessment (where required);
(c) Ensure essential assessments for their area are completed and re-assessed as necessary;
(d) If the GRA is also a risk handler (responsible for entering details of identified risks onto Datix), they should also successfully complete the Trusts Risk Management e-Learning.

5.28 *Risk Handler*

A member of staff with delegated responsibility from the risk owner for ensuring:

(a) Risks and all associated information is entered onto Datix and maintained in accordance with this policy;
(b) Risk handlers should successfully complete the Trusts Risk Management e-learning.

5.29 *Monitoring Groups*

Monitoring groups are to provide oversight and scrutiny of risks related to their area of work. Monitoring groups are not accountable for risk.

For example:

(a) Trust Health & Safety and Fire Safety Committee will review fire, environmental and health and safety risks;
(b) The Clinical Quality Group will review clinical quality risks and risks to Care Quality Commission compliance;
(c) The People Management Group will review workforce risks;
(d) Information Risk Management Group will review information governance risks;
(e) The Infection Control Group will review infection control risks.

In order to improve the consistency of the quality of record-keeping for the review of risks and risk actions governance groups should:

- Have a structured agenda for all governance meetings involving the review of risks (e.g. risks for closure/ escalated or de-escalated risks/ new risks or risk actions due for review).
- Require that a reason is recorded in the meeting minutes if a risk was not discussed.
- Require that the rationale be recorded in the meeting minutes for any decisions made relating to the closure/ escalation or de-escalation of risks.

6. Policy Statements

6.1 *Statement of Commitment*

The Trust is committed to the proactive management of the risks posed to the achievement of its objectives. In order to do so we will adopt best practice in risk management, employ new technologies to help manage risk and ensure our staff are appropriately trained to do so.

The Trust acknowledges that it is not possible or desirable to eliminate all risks and encourages positive risk-taking in keeping with our statement of risk appetite, where risks may result in positive benefits for our patients, staff and visitors (the 'upside' of risk).

6.2 *Policy Statement*

An effectively planned, organised and controlled approach to risk management is a cornerstone of sound management practice and is key to ensuring the achievement of strategic aims.

The Trust seeks to encourage a risk-aware culture in which the assessment and management of risks is an integral part of decision making, both small and large, and where the right people do the right thing at the right time.

The overriding principle of this policy is that the effort and resources spent on managing risk will be proportionate to the risk. Risks will be evaluated to differentiate those that are unacceptable from those risks which are acceptable (tolerable). This will define the Trust's risk appetite.

Sound risk management can assist in continuous improvement in all its services. Practices will be enacted to ensure that the results of risk assessments are used to improve the Trust's processes and procedures.

It is the intention of the Trust that its management of risk is compliant with all relevant legislation and regulation.

The Risk Management System will be subject to regular comparison against published best practice and will be regularly monitored and assessed to ensure its effectiveness within the context of the Policy.

7. Risk Management

7.1 *Components of the framework*

(a) Risk Management Policy;
(b) Definition of the responsibilities and accountabilities at all levels in the organisation;

(c) Ensuring Risk Management is embedded into all of the Trusts practices and processes;
(d) Ensuring adequate resources and available;
(e) Ensuring staff have the appropriate skills, experience and competence;
(f) Establishing internal reporting processes to encourage accountability for, and ownership of, risk; and
(g) Establishing external communication and reporting mechanisms for all stakeholders

7.2 *Benefits of Risk Management*

The Trust recognises that there are significant benefits to managing risk. They include:

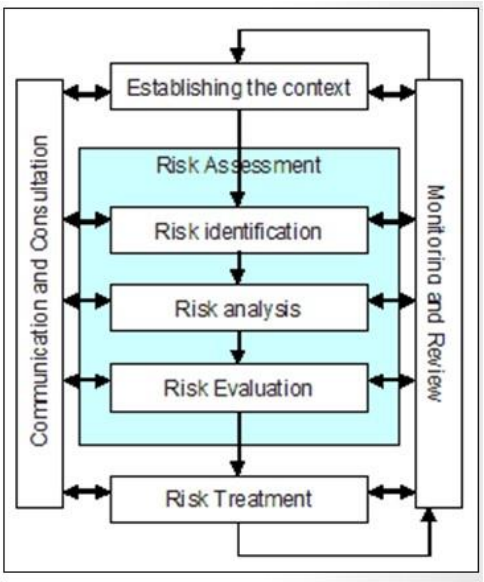
The Trust liaises with the Local Counter Fraud Specialist in relation to all Trust fraud risks any suspected acts of Fraud, Bribery or Corruption which are occurring or have occurred.

The Trust liaises with the Local Counter Fraud Specialist in relation to all Trust fraud risks any suspected acts of Fraud, Bribery or Corruption which are occurring or have occurred.

7.3 *Risk Management Methods*

- **T**reat (Reduce)
- **T**olerate (Accept)
- **T**erminate (Avoid)
- **T**ransfer (Transfer)

7.4 *Risk Management Process*



Establishing the context - Risks have no relevance on their own – they only have meaning in relation to the objectives of the organisation and its stakeholders. Understanding the various environments in which the organisation functions is necessary in order to assess what risks there may be, as well as what effect they could have.

External: those features, relationships and drivers outside the organisation that can influence its success or failure;

Risk identification defined as the process of finding, recognising and describing risks, it is the part where the organisation's objectives should be considered in the light of any and all events or situations that could affect their achievement, whether positive or negative.

Risk analysis is defined as the process to comprehend the nature of risk and to determine the level of risk. This is the part where an understanding of the risks is developed. Causes are examined, consequences defined and the likelihood of various scenarios considered, taking into account the effectiveness of any controls that are already in place. This is an important step in providing a basis for risk-informed decision making.

Risk evaluation is defined as the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable. The risks that have been identified and analysed can now be compared with the risk criteria developed earlier, ideally in the design of the framework. With this as the basis, the organisation can make rational decisions as to the tolerability of the risks and the need for further risk treatment.

Risk Treatment is defined as the options available to management the risk, decision making of action plan to implementation of new controls. It also includes the decision to take no further action and 'accept' the risk.

Communication and consultation - This is important at all stages of the process but is vital as a first step. All those with a stake in the objectives and activities of the organisation, as well as anyone with useful knowledge, should be included from the outset.

Monitor and Review - The process is continuous from re-establishing the context in line with service changes to regular re-assessment as actions plans are completed.

7.5 *Attributes of effective risk management*

Proportionate - The effort spent managing an individual risk should be proportionate to the level of risk faced.

Aligned - The identification and assessment of risk should be in the context of, and aligned to, the achievement of the organisations objectives.

Comprehensive - The controls and actions put in place to manage risk need to be detailed and specific enough that they fully achieve the desired level of mitigation.

Embedded - Risk management should be imbedded into normal working practices, this requires risk to be integrated into business and operational planning cycles.

Dynamic - Risks can change so controls put in place need to be continually monitored to ensure they are up to date.

7.6 *Risk Review and Reporting Arrangements*

Corporate and Strategic Risks are received by Trust Board on a quarterly basis alongside updates to the achievement of strategic objectives, following review at Risk Management Group, Audit Committee and SLT. Review dates for all corporate risks are set 1 month prior to presentation at RMG.

Divisional Risks should be reviewed by divisional boards in full on a quarterly basis using the standard reporting templates for both coversheet and risk register. Review dates for all divisional risks are set 1 month prior to presentation at Divisional Board. Divisional Risk Leads should ensure that the Escalation/Divisional Review Tab on Datix is updated for all risks meeting the criteria for escalation to allow for accurate reporting.

Local/ Departmental Risks should be reviewed in full on a quarterly basis by divisional risk or governance groups. Review dates for all local risks are set 1 month prior to presentation at governance group.

Exception reporting should take place on a monthly basis to both Divisional Boards and SLT.

7.6.1 Details of the quarterly risk reviews should be entered into the 'Progress Notes' section of Datix.

7.6.2 Any changes to the description of actions, or amendments to the due date of actions should be entered into the progress section of the 'Actions form' in Datix.

8. Risk Appetite

Risk appetite can be defined as 'the amount and type of risk that an organisation is willing to take in order to meet their strategic objectives. Organisations will have different risk appetites depending on their sector, culture and objectives. A range of appetites exist for different risks and these may change over time.

We need to know about risk appetite because:

- If we do not know what our organisation's collective appetite for risk is and the reasons for it, then this may lead to erratic or inopportune risk taking, exposing the organisation to a risk it cannot tolerate; or an overly cautious approach which may stifle growth and development
- If our leaders do not know the levels of risk that are legitimate for them to take, or do not take important opportunities when they arise, then service improvements may be compromised and patient and user outcomes affected.

The Board of Directors have determined the Trusts risk appetite as an 'open' one. In practice this means that a level of risk taking is encouraged in order for the Trust to maintain a progressive approach to the delivery of services, where assurance can be sought that any associated risks can be mitigated to a tolerable level.

9. Risk Appetite Statement

6.1 The UH Bristol Board of Directors is willing to consider all potential delivery options in pursuit of the achievement of organisational objectives, provided that a satisfactory level of reward or value for money can be demonstrated, proportionate to the risk being taken.

Specifically;

6.2 With regard to finance, the Board is prepared to invest but will always seek to minimise the possibility of financial loss by ensuring all associated risks are mitigated to a tolerable level. During decision making, service improvements, benefits and patient outcomes will be considered alongside value for money. Where appropriate the Board will ensure resources are allocated in order to capitalise on potential opportunities.

6.3 With regard to compliance with statue and regulations, the Board will seek assurance that the organisation has high levels of compliance in all areas other than where it has been specifically determined that the efforts required to achieve compliance would outweigh the potential adverse consequences.

6.4 Research and innovation is encouraged at all levels within the organisation, where a commensurate level of improvement can be evidenced and an acceptable level of management control is demonstrated. As a Global Digital Exemplar Organisation the Board of Directors will seek to implement digital systems and support technological developments to optimise operational delivery.

6.5 The Board of Directors accepts that some decisions made in the interest of change may have the potential to expose the organisation to additional public scrutiny or media interest.

Proactive management of Trust communications may be considered to protect the organisation's reputation and maintain public confidence.

10. Risk Tolerance

Whilst risk appetite is about the pursuit of risk to achieve objectives, risk tolerance is about what an organisation can actually cope with and thresholds at which it is willing to 'accept' a specific risk. The following tables define the risk scores, above which risks may not be 'accepted' and must be actively mitigated.

The tolerance level applies to the 'Target' score of 'Action Required' risks and the 'Current' (and Target) score of 'Accepted' risks and is shown on the table and matrices below, by risk domain:

Risk Domain	Definition	Accepted Risk Score	Risk Level
Safety	Impact on the safety of patients, staff or public	1-6	Moderate
Quality	Impact on the quality of our services and patient experience.	1-6	Moderate
Workforce	Impact upon our human resources (not safety), organisational development, staffing levels, competence and training.	1-8	High
Statutory	Impact upon on our statutory obligations, regulatory compliance, assessments and inspections.	1-8	High
Reputation	Impact upon our reputation through adverse publicity.	1-9	High
Business	Impact upon our business and project objectives. Service and business interruption.	1-9	High
Finance	Impact upon our finances.	1-9	High
Environmental	Impact upon our environment, including chemical spills, building on green field sites, our carbon footprint.	1-8	High

Tolerance levels of Safety & Quality risks 1-6 (Below the black line)

Impact	Likelihood				
	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
5 Very Likely	5	10	15	20	25
4 Likely	4	8	12	15	20
3 Possible	3	6	9	12	15
2 Unlikely	2	4	6	8	10
1 Rare	1	2	3	4	5

Tolerance levels of Workforce, Statutory and Environmental 1-8 (Below the black line)

Impact	Likelihood				
	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
5 Very Likely	5	10	15	20	25
4 Likely	4	8	12	15	20
3 Possible	3	6	9	12	15
2 Unlikely	2	4	6	8	10
1 Rare	1	2	3	4	5

Tolerance levels of Reputation, Business & Finance Risks 1-9 (Below the black line)

	Likelihood				
	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
5 Very Likely	5	10	15	20	25
4 Likely	4	8	12	15	20
3 Possible	3	6	9	12	15
2 Unlikely	2	4	6	8	10
1 Rare	1	2	3	4	5

11. Reporting to External Bodies

There are various national external agencies that monitor the Trust on its risk management processes and arrangements and the implementation of these, including but not restricted to:

11.1 *NHS Improvement*

The Trust is required to, on a quarterly basis, submit to NHS Improvement self-declared Financial Risk Rating (based on various financial indicators: EBITDA, I&E) and Governance Risk Rating (based on the achievement of operational targets and the Trust's CQC Compliance status).

11.2 *Care Quality Commission (CQC)*

The CQC will undertake announced and unannounced inspections of the Trust's sites throughout the year. The Trust is required to provide the CQC with information on the steps that have/will have been taken in addressing any risks/compliance concerns arising from these inspections.

11.3 *Health and Safety Executive (HSE)*

The Trust will respond to any visit, either planned or unplanned, by the enforcing authorities e.g., HSE and provide to them, on request, any information they require. In addition, under the Reporting of Injuries, Diseases and Dangerous Occurrence Regulations (RIDDOR) the Trust has an obligation to report categorised incidents types (death and specified injuries that are work related, injuries where an employee is away from work or unable to perform their normal work duties for more than seven consecutive days as the result of an occupational accident or injury, diagnosis of any occupational disease made by a GP or consultant and the member of staff has been carrying out work activities that led to the condition and finally any dangerous occurrences that are certain listed near misses).

11.4 *National Reporting and Learning System (NRLS)*

The Trust reports all patient safety incidents through the NRLS via the online reporting system. Serious incidents are uploaded as soon as classified as such.

11.5 *NHS Central Alerting System (CAS)*

The Trust is obliged to respond to all CAS alerts (i.e., safety alerts, drug alerts, medical device alerts) within timescales dictated by CAS according to the nature and seriousness of each individual alert.

11.6 *Counter Fraud*

The Trust liaises with the Local Counter Fraud Specialist in relation to all Trust fraud risks any suspected acts of Fraud, Bribery or Corruption which are occurring or have occurred.

11.7 *Police*

The Trust liaises with Avon and Somerset Constabulary in relation to any suspected criminal activity either taking or having taken place.

11.8 *Public Health England (PHE)*

The Trust is required on a weekly, monthly and quarterly basis to report on data relating to Clostridium Difficile, E. Coli, Glycopeptide-Resistant Enterococci (GRE), MRSA and MSSA bloodstream infections.

11.9 *Safeguarding*

The Trust will actively work within an inter-agency framework to ensure that the welfare and safety of patients at risk is paramount. This joint working will be under the auspices of the Bristol Safeguarding Adults Board and the Bristol Safeguarding Children Board.

12. Incident Investigations and Root Cause Analysis

Investigations into the circumstances of incidents, accidents, claims and complaints provide an essential source of risk identification. Where a risk is identified through such an investigation, that cannot be immediately addressed, it should be entered onto the appropriate risk register. Further detailed guidance relating to undertaking investigations can be found in the Complaints and Concerns Policy and the Serious Incident Policy.

The Trust adopts a Root Cause Analysis (RCA) methodology when undertaking investigations relating to potentially serious incidents and never events. RCA is a problem solving methodology based on the premise that, once removed from the problem fault sequence, addressing the root cause prevents the final undesirable event from recurring. It is a systems-based approach to analysis rather than focusing on individual actions and has been shown to provide a means to identify effective learning and long term solutions to a range of issues.

13. Risk Registers

13.1 *Types & Frequency of Review*

The minimum requirement for the review of risk registers whether 'action required' or 'accepted':

(a) Corporate & Strategic Risk Register - Quarterly prior to review by Trust Board
(b) Divisional Risk Register - Quarterly prior to review at Divisional Board
(c) Departmental Risk Registers – Quarterly prior to review at appropriate governance group.

All risks regardless of level or status should be review and updated in line with any service changes.

13.2 *The Strategic Risk Register (Board Assurance Framework)*

The Trust's Board Assurance Framework is formed of two elements:

- Part A - Assurance around the achievement of the Trusts strategic objectives
- Part B - Assurance that any risks to the achievement of the strategic objectives are being adequately mitigated or controlled.

The strategic risk register forms part B of the Trust's risk Board Assurance Framework and is the mechanism for reporting on the management and treatment of strategic risks (*risks to the achievement of the Trusts strategic objectives)*.

The strategic risk register is maintained on Datix, by the Head of Risk Management. Risks are approved for entry onto the strategic risk register by the Senior Leadership Team or the Trust Risk Management Group on their behalf.

13.3 *Corporate Risk Register*

The corporate risk register is comprised of risks that have the potential to impact on the Trusts ability to meet its corporate objectives.

Corporate risks:

(a) Assessed as having a current rating of 12 or above
(b) Significant risks to the corporate objectives of the Organisation
(c) Risks scored 12 or above and escalated by divisions.

The corporate risk register is maintained on Datix, by the Head of Risk Management. Risks are approved for entry onto the corporate risk register by the Senior Leadership Team or the Trust Risk Management Group on their behalf.

13.4 *Divisional Risk Register*

Each division has its own risk register which captures in one place how divisional risks are being managed. The Divisional Boards are accountable for the assessment, communication and management of risks within their area of responsibility.

Divisional risks:

(a) Assessed as having a current rating of 12 or above, or;
(b) Affecting more than one department or specialty
(c) Includes risks that score 12 or above escalated from the departmental risk registers

The divisional risk registers are maintained on Datix, by the divisional governance leads. Risks are approved for entry into the divisional risk register by the Divisional Board.

13.5 *Departmental Risk Registers*

In this context, the term 'departments' is defined as wards, departments, services and clinics listed in the 'Department' field on Datix.

Each department will maintain a register of risks to departmental objectives. The departmental risk registers are maintained on Datix, by the department manager or specialty lead. Risks are approved for entry onto the risk register by the department manager or specialty lead.

Health & Safety risk assessment should in the first instance be completed on the template available and uploaded to the health & safety generic risk assessment workspace to determine if an unacceptable element of risk exists.

All risk assessments completed that identify an element of risk outside of acceptable parameters or uncontrolled by standard operating procedures should, following consultation from the ward manager and divisional health & safety advisor, be entered onto the departmental risk register. Where a paper risk assessment has been completed, a copy of the document should be attached to the Datix record for information.

13.6 *Cross-divisional and Trust-wide risks*

To ensure appropriate oversight and scrutiny, all risks must reside on one of the six divisional risk registers. Divisional ownership of a risk will usually be dictated by the division to which the individual risk owner belongs. Where a risk is identified in a division that may also be a risk to another division, it is attendant on the owner of the risk to notify the other division. There is functionality in Datix to communicate and give staff access to a new risk.

A decision will then be made as to whether:

- One division takes a lead on managing the risk, involving the other division as appropriate;

Or:

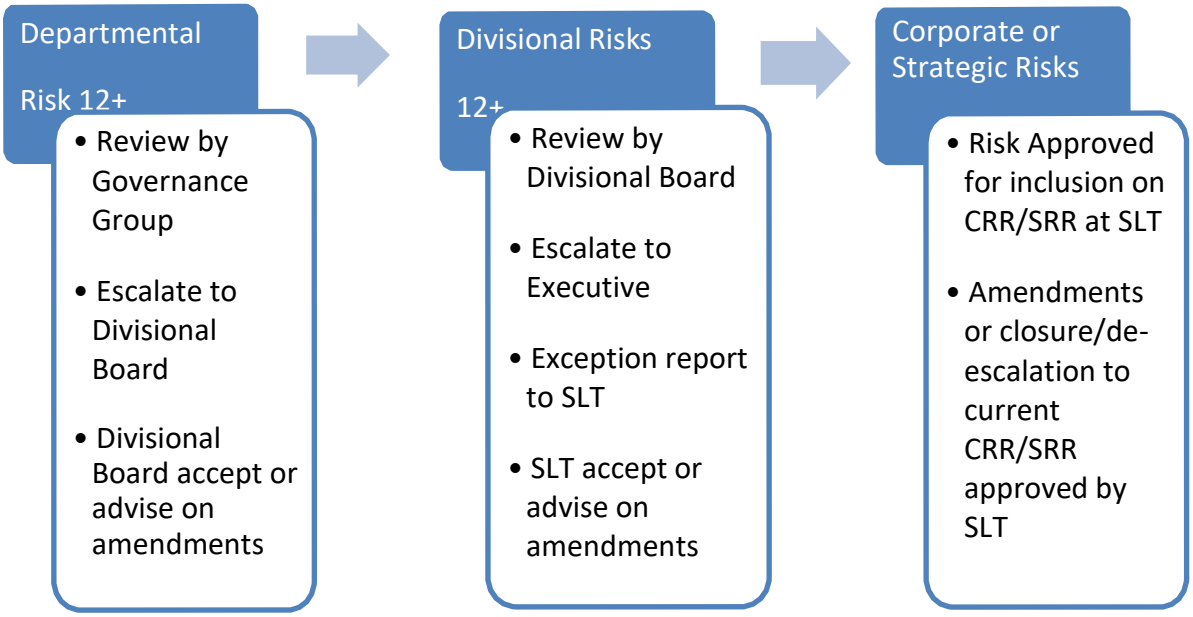
- Both divisions record the risk (e.g. patient falls) in their risk register and each manage their own risk in accordance with the risk management policy; or
- Where the risk is under the control of a specialty that crosses divisions, e.g. pharmacy, the risk may reside in the division in which the specialty is housed, e.g. Diagnostics and Therapies; or
- Where the risk is Trust-wide, agreement can be sought from the relevant executive director for the risk to be added to the Trust Services risk register.
- Risks may be 'owned' by one division, but have actions added against staff in a number of other divisions.

13.7 *Escalation of Risk*

Where a significant departmental risk scoring 12 or above is identified, following appropriate scrutiny from the divisional risk lead or manager, it will be reported into the divisional governance or risk management group. If the risk score is approved the group will then make a recommendation to the divisional board for the risk to be escalated to the divisional risk register. Upon receipt of the recommendation the board will re-assess the risk in the context of the division and either agree to accept the risk onto the divisional risk register or provide advice to the risk owner on the effective management. If the risk remains 12 or above at a divisional level continue to follow the step below:

Where a divisional level risk is assessed as scoring 12 or above the divisional board will first approve the new assessment and request the risk owner to contact the relevant Executive for their assessment from a corporate perspective in the context of the Organisation. This is done by way of an exception report which is produced from the template section of Datix. Upon completion of the executive director assessment the exception report will either be submitted via the risk management team to SLT or advice will be provided by the executive on either the assessment or effective management.

Escalation Process



13.8 *Closure of Risks*

Where risks have been sufficiently mitigated they may be closed. This could be due to the root cause being eliminated, or the controls being embedded into business as usual and forming part of the Trusts systems of internal control.

Risks should follow the same process for approval to be closed as they do for escalation, as above and form part of the monthly risk exception report received by the divisional board.

14. References

ISO 31000 - Risk Management

Risk Appetite for NHS Organisations (GGI 2012)

Building the Assurance Framework: A Practical Guide for NHS Boards

Assurance – The Board Agenda (DOH July 2002)

A Practical Guide for NHS Boards (DOH March 2003)

NPSA Guide: A Risk Matrix for Risk Managers

NPSA Guide: Healthcare Risk Assessment Made Easy

15. Associated Documentation

This strategy should also be read in conjunction with the following Risk Management Policies which are all available on the intranet:

Risk Management Strategy

Risk Register Review Procedure

Incident Management Policy

Serious Incidents Policy

Health & Safety Policy

16. Appendix A – Monitoring Table for this Policy

Objective	Evidence	Method	Frequency	Responsible	Committee
Ensure that risks are appropriately escalated to the corporate risk register and managed in accordance with the requirements of this policy.	To include agendas, risk register reports and minutes of: Trust Board. Senior Leadership Team. Risk Management Group.	Internal Audit of Trust's risk management arrangements	Annual	Head of Risk Management	Risk Management Group
That key individuals – Executive Directors, Divisional Directors the Trust Risk Manager are performing their responsibilities under this policy.	Risks presented to Divisional Boards and Governance Groups. Risk Management Group agendas, reports and minutes evidencing Executive Director risk portfolio reports.	Audit of Trust's risk management arrangements	Annual	Head of Risk Management	Risk Management Group
That risk is managed at a divisional level through review of divisional and departmental risk registers at Governance Group and Divisional Boards.	Agendas, risk register reports and minutes of Divisional Boards and Governance Groups. Risk registers reviewed by Divisional Boards.	Audit of Divisions risk management arrangements	Annual	Head of Risk Management	Risk Management Group
Ensure that risk descriptions and assessments of risks are completed in line with Trust guidance.	Quality of risk registers.	Review of divisional risk registers	Annual	Head of Risk Management	Risk Management Group
Ensure that Risks are kept up to date on Datix and that action plans are included where appropriate	Quality of risk registers.	Review of divisional risk registers	Annual	Head of Risk Management	Risk Management Group

17. Appendix B – Dissemination, Implementation and Training Plan

Plan Elements	Plan Details
The Dissemination Lead is:	Head of Risk Management
This document replaces existing documentation:	Yes
This document is to be disseminated to:	Executive Directors, Divisional Board members, Risk Management Group members, Patient Safety Group members, Divisional Health and Safety Leads
Method of dissemination:	Via email to divisional leads, RMG members and routine communication in Newsbeat.
Training is required:	Risk Management ELearning
The Training Lead is:	Head of Risk Management

Additional Comments
The Risk Management Policy & Strategy is made available to staff via the intranet. Generic risk assessor training is available to all divisions through the Health & Safety Department and where request is made to the Risk Management Team to provide such training. General awareness-raising for staff is also undertaken through staff briefings, induction programs and various newsletters. A new e-Learning package on risk and incident management is available via the essential training portal For all other enquiries or for Datix Training contact: Risk Management Team on 23691 Email DatixSupport@UHBW.nhs.uk or visit the Risk Management Pages on Connect.

18. Appendix C – Equality Impact Assessment

Further information and guidance about Equality Impact Assessments is available here:
http://nww.avon.nhs.uk/dms/download.aspx?did=17833

Query	Response
What is the main purpose of the document?	Articulation of the Trusts Risk Management Framework
Who is the target audience of the document? Who is it likely to impact on? (Please tick all that apply.)	Add ☑ or ☒ Staff ☑ Patients ☒ Visitors ☒ Carers ☒ Others (Contractors) ☑

Could the document have a significant negative impact on equality in relation to each of these characteristics?	YES	NO	Please explain why, and what evidence supports this assessment in relation to your response.
Age (including younger and older people)		☒	
Disability (including physical and sensory impairments, learning disabilities, mental health)		☒	
Gender reassignment		☒	
Pregnancy and maternity		☒	
Race (includes ethnicity as well as gypsy travelers)		☒	
Religion and belief (includes non-belief)		☒	
Sex (male and female)		☒	
Sexual Orientation (lesbian, gay, bisexual, other)		☒	
Groups at risk of stigma or social exclusion (e.g. offenders, homeless people)		☒	
Human Rights (particularly rights to privacy, dignity, liberty and non-degrading treatment)		☒	

Could the document have a significant positive impact on inclusion by reducing inequalities?	YES	NO	If yes, please explain why, and what evidence supports this assessment.
Will it promote equal opportunities for people from all groups?		☒	
Will it help to get rid of discrimination?		☒	
Will it help to get rid of harassment?		☒	
Will it promote good relations between people from all groups?		☒	
Will it promote and protect human rights?		☒	

On the basis of the information/evidence so far, do you believe that the document will have a positive or negative impact on equality? (Please rate by circling the level of impact, below.)

Positive impact				Negative Impact		
Significant	Some	Very Little	NONE	Very Little	Some	Significant

Will the document create any problems or barriers to any community or group? YES / **NO**

Will any group be excluded because of this document? YES / **NO**

Will the document result in discrimination against any group? YES / **NO**

If the answer to any of these questions is YES, you must complete a full Equality Impact Assessment.

Is a full equality impact assessment required? YES / **NO**

Date assessment completed: 06/01/2022

Person completing the assessment: Head of Risk Management