Gloucestershire Hospitals NHS Foundation Trust

Risk Management Framework

Table of Contents

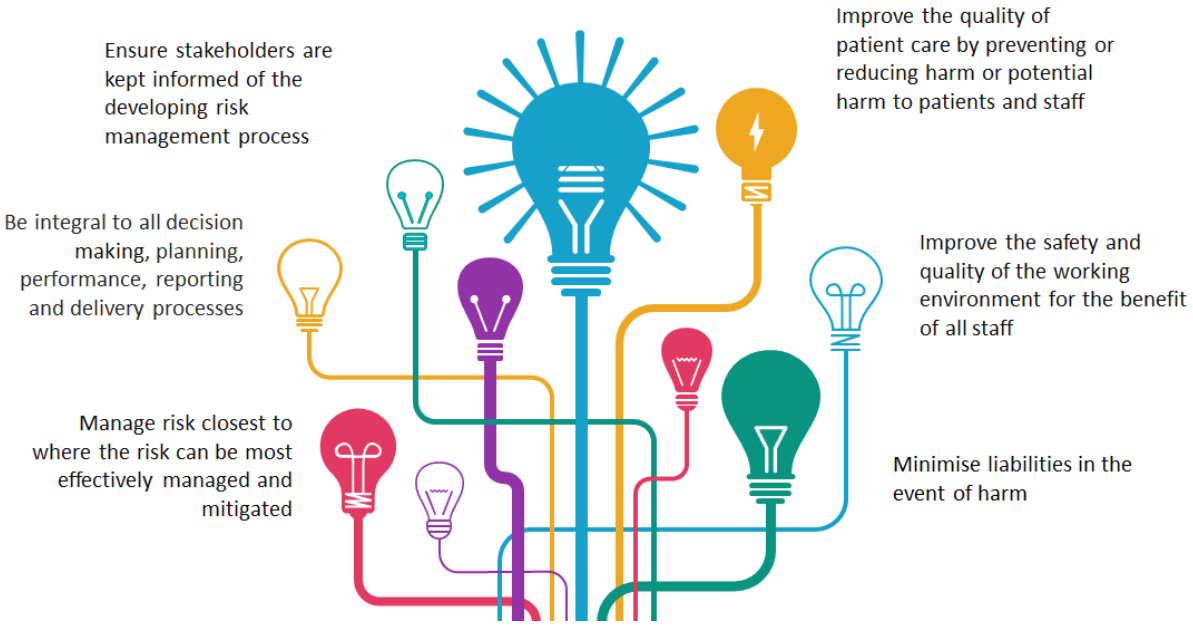
INTRODUCTION

Risk can be defined as the combination of the probability of an event and its consequences. In any type of undertaking there is the potential for events or a set of circumstances to constitute an opportunity for benefit (upside) or a threat to success (downside). Risk Management is recognised as being concerned with both positive and negative aspects of risk. Our risk management framework is designed to provide a structured approach to risk so that we can realise the opportunities and respond to the threats.

OUR VISION

The Trust's goal is to make effective risk management an integral part of everyday practice. This is achieved by having a comprehensive and cohesive risk management system underpinned by clear arrangements for responsibility and accountability throughout the organisational structure of the Trust. These arrangements are set out in more detail in the Trust's Standing Financial Instructions, Scheme of Delegation and Trust-wide policies and procedures and in the relevant section below.

The principle objective of risk management is to create an environment of 'no surprises' where the Trust understands the risks it's facing and eliminates or controls them to an acceptable level. This is achieved by creating a culture founded upon assessment, mitigation and prevention of risk. To realise this goal, this framework seeks to achieve the effective management of risk through a common set of principles:



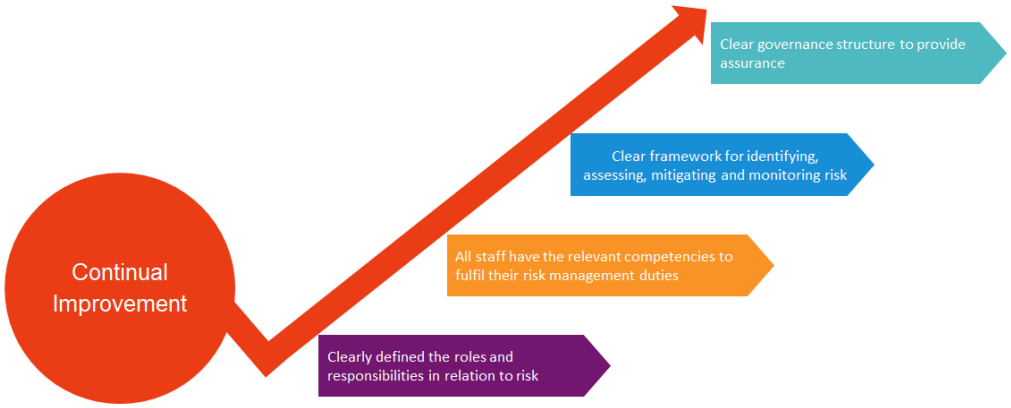
Risk Management empowers the organisation to make better decisions

RISK MANAGEMENT FRAMEWORK

This framework sets out the process whereby the Trust methodically addresses the risks surrounding our past, present and future activities. This will increase the probability of success in achieving our strategic objectives and reduce both the probability of failure and uncertainty.

Risk Management Objectives

Our risk management is objective is to ensure the continuous improvement of standards, supported by a clear governance process embedded into the culture of the organisation from staff to Board level.



Responsibilities

Clear individual and collective responsibilities and accountability are in place to facilitate enhanced oversight of risk and support decision-making:

The Board

Will oversee risk management across the Trust through a high-quality risk assurance process.

Chief Executive Officer

Is accountable for the implementation of this Framework, effective governance and achieving the performance goals that may be affected by risk and risk management activities.

Director for People and OD
Will Chair of the Risk Management Group and is accountable to the Audit & Assurance Committee.

Executive Directors
Are responsible for the oversight of risk-based decisions and effective risk management within their delegated area(s) of responsibility. Executive Directors are accountable to the Chief Executive Officer and the Board.

Director of Finance
Holds accountability for financial risk management.

Director of Quality Improvement & Safety
Has delegated responsibility for co-ordinating the Risk Management Framework and the Trust Risk Register.

Head of Corporate Risk, Health & Safety
Has delegated responsibility for developing, implementing and monitoring performance against the Framework. Will provide risk assurance reports to the Risk Management Group (RMG) and Audit & Assurance Committee.

Divisional Chief of Service / Divisional Risk Lead
Responsible for monitoring compliance with the Framework within their division and proactively intervening where non-compliance is identified. Will oversee the escalation of risks as per the criteria and undertake an annual compliance audit, the results of which will be presented to the Risk Management Group.

Divisional Quality Board
Will maintain a divisional risk register in accordance with the Framework and will monitor divisional compliance with the Key Performance Indicators (KPIs) for risks and incidents. Will ensure risks are escalated in a timely manner to the RMG.

Specialty Boards
Will maintain a specialty risk register in accordance with the Framework and will monitor specialty compliance with the KPIs. Will ensure risks are escalated in a timely manner to divisional board.

Risk Management Group (RMG)
Will monitor Trust-wide compliance with the Framework and KPIs. Will provide assurance to the Audit and Assurance Committee and Board. RMG is responsible for decisions in relation to

escalated Corporate Divisional or Trust Risk Register risks. RMG must act in accordance with its Terms of Reference.

Individual Risk Owners

Must ensure that each risk held on DATIX is fully complete, that scores are in line with our score definition and the risk is well-evidenced. Will have relevant actions in place to actively reduce the risk; unless it is deemed tolerable. Must review risks as per this Framework and ensure that progress notes contain a relevant audit trail.

Risk Management Cycle

The diagram below shows the stages within our risk management framework:

Each stage of the framework is described below in more detail.

Trust Risk Appetite

After identifying the Trust Objectives and goals through the Strategic Plan for 2019/2024, the next step is to articulate the amount of risk the organisation is willing to take to achieve those objectives.

Some objectives may require the Trust to be boldly innovative with limited resources, while others may require the Trust to be cautiously conservative when managing a potential risk. One method to identify the correct level of risk an organisation is willing to take is to agree a risk appetite on which we can build a uniform consensus on the level of risk the organisation is willing to take.

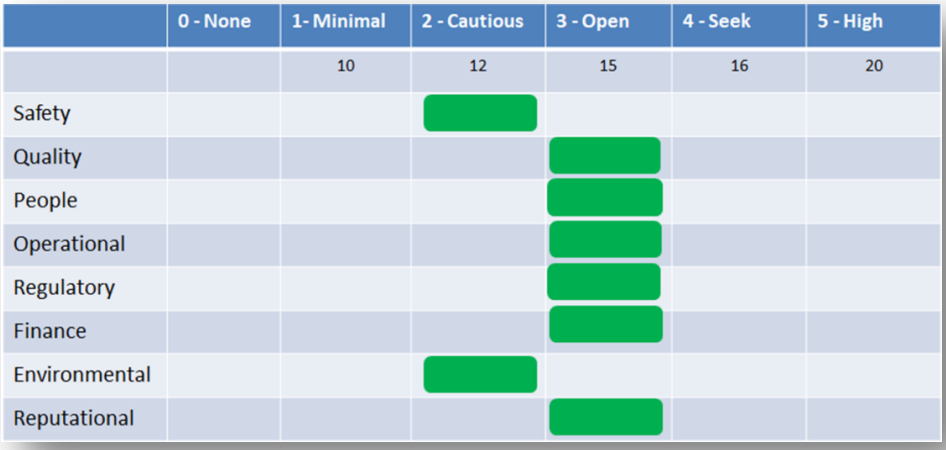
The Trust has a defined risk appetite which denotes when we are willing to seek or tolerate risk and when we will adopt a more cautious risk-adverse approach. Risk appetite defines the level of risk that the Trust actively wishes to engage with in the broader types or categories of risk such as safety, quality or operational risks. Our current Risk Appetite Statement can be found at the end of this Framework and definitions can be found in RD2 – Trust Risk Appetite.

Risk Tolerance

Risk tolerance is the level of risk that an organisation can agree per individual risk. It's related to the acceptance of the outcomes of a risk should it occur, and having the right resources and controls in place to absorb or tolerate the given risk. Risk tolerances have naturally developed from the RD2 Trust's Risk Appetite, and are aligned with our organisational goals. Risk tolerances are the boundaries of risk taking outside of which the organisation is not prepared to venture in the pursuit of its long term objectives.

Awareness of residual risk and operating within a risk tolerance provides the Trust greater assurance that it is operating within acceptable boundaries. A low risk tolerance, leads to more conservative business decisions, whereas a high risk tolerance allows more aggressive decisions in which there is a higher likelihood of a risk occurring or there are more serious consequences at stake.

The Trust categorises and scores its risks according to the broad area of impact; known as domains. For example, risks that impact on safety will have a safety domain score, risks that impact on cost will have a finance domain score and so on. Most risks will impact on more than one domain. However, it is the highest scoring domain that is used to establish whether the risk meets our defined risk tolerances as shown below:



	0 - None	1- Minimal	2 - Cautious	3 - Open	4 - Seek	5 - High
		10	12	15	16	20
Safety						
Quality						
People						
Operational						
Regulatory						
Finance						
Environmental						
Reputational						

As shown above, each domain has a defined risk tolerance score. As an example, if a risk scores 12 or more for safety this has reached the tolerance the Trust has for safety risks and must be escalated.

Where domains score equally high, the highest domain shall be recorded as the Safety domain above all others, followed by Environment and Regulatory. Quality, Finance and People will take precedent over operational (business) and reputational scores.

Risk Identification

Risk identification is the starting point for identifying the Trust's exposure to uncertainty. This requires an intimate knowledge of the internal organisational activities, the external environment in which the Trust operates and the legal, social, political and cultural environment in which it exists. This, coupled with a sound understanding of our strategic and operational objectives, will help pinpoint threats.

Risk identification is approached in a methodical way to ensure that all significant activities within the organisation have been identified. Risks are identified from both internal and external sources. For example through:

- Barriers to achieving our strategic objectives
- Substandard performance information
- Financial risks (e.g. internal audits, budgetary information, Counter Fraud initiatives)
- External bodies (e.g. Care Quality Commission, National Audit Office, Medical and Healthcare products Regulatory Agency, (MHRA) NHS England / Improvement, NHS Litigation Authority and Health and Safety Executive)
- Quality processes (e.g. claims, complaints, surveys)

- Compliance with contractual arrangements (e.g. SLAs, safety breaches)
- Safety inspections, audits, incident data and assessments
- Risk simulation or table top exercises
- Major project risks

The Trust aims to be as proactive as possible in order to avoid the need to make decisions under unnecessary pressure and without adequate information on the risks involved.

The Trust has a range of risk assessment tools to help identify actual and potential risks associated with its activities. Examples include risk assessments (clinical and non-clinical), peer reviews, audit (clinical and non-clinical), impact assessments, CQC inspections and monitoring visits, workplace inspections, complaints and concerns, incidents and SIRIs, etc.

Risk Analysis

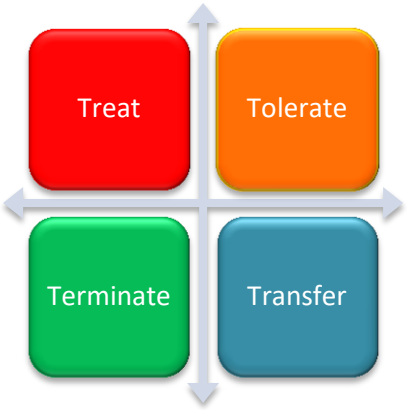
Each risk is scored between 1 and 5 according to the likelihood it will occur and the potential consequence should the risk materialise. The likelihood and consequence are multiplied to give the risk rating score. Score definitions are provided in our RD3 - Domain Risk Score Matrix to support a consistent method of risk rating across all risks. The same score definitions are used for our risk register and our risk assessments.

Risk evaluation and scoring is used to make decisions about the significance of a risk to the organisation or those impacted and whether each specific risk should be accepted or treated (see risk control).

Risk Control

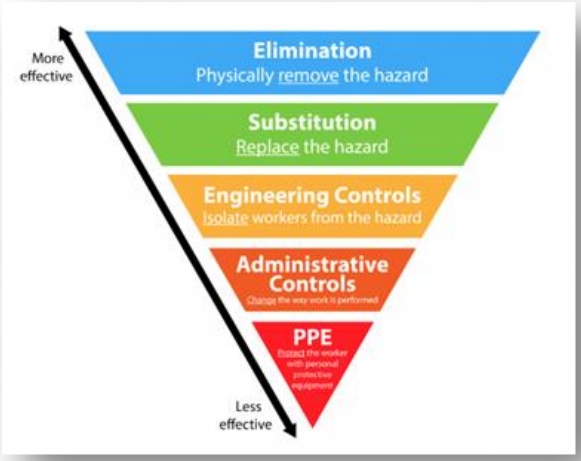
Risk mitigation refers to any steps taken to reduce the likelihood or how serious the consequences (outcome) of a risk would be.

There are four types of risk mitigation strategies, commonly known as the four T's. Risk owners should make clear which mitigation mode is being applied to the risk. These are shown in the diagram below:



- **Treat** – actively working to reduce the risk
- **Tolerate** – no further reasonable actions can be taken so the risk is tolerated at its current level
- **Transfer** – the risk is managed by a third party
- **Terminate** – the risk is eliminated and closed

When **treating** a risk, risk owners should apply the hierarchy of controls, shown below, to ensure the most appropriate actions are taken to reduce the risk.



Where the current controls do not sufficiently reduce the risk and the risk rating remains beyond an acceptable level, risk owners must identify what is missing from the control measures. Each gap in our controls is recorded and should, where reasonably practicable, have a corresponding action or action plan which is designed to mitigate and reduce the residual risk rating.

RD1 contains a step by step guide on how to add gaps in controls and actions to show your risk mitigation over the life of the risk.

Emergency Planning & Resilience

The Trust should be prepared to deal with an emergency and must monitor and have assurance from all service providers that they too are prepared. Plans will be prepared in order to maintain key services when faced with disruption from identified local risks or foreseeable major incidents

such as a severe pandemic, supply shortages or industrial action; this is known as business continuity management.

The Trust has an Emergency Resilience and Response Policy which outlines how the Trust identifies, assesses, plans for and mitigates emergency or crisis situations.

Risk Review

Risks must be reviewed to ensure control measures are continuously monitored and the risk has not changed. The higher the risk rating, the more frequent a risk will need to be reviewed.

Each risk on the risk register has a single owner, shown as the operational lead on DATIX. This person is responsible for ensuring the risk is regularly reviewed by the review date indicated. The same will apply to risk assessments held in our Risk Assessment Library (SOP B0636).

Each risk owner must review their risks on the **risk register** at a suitable frequency for the level of risk. The minimum review frequency is set out below but where circumstances change or there is an adverse event between review periods, an early review may be necessary.

Risk Register	Minimum Review Frequency
Specialty	Every 4 months
Divisional	Every 3 months
Trust	Every 2 months

Recorded risk information, controls, risk ratings and actions should be reviewed thoroughly by the reviewer to ensure these are adequate, effective and current. It is important that the risk content, progress notes and actions reflect the steps taken over the life of the risk to mitigate the severity of the consequences, the likelihood of it materialising or both.

Risk Culture

Risk culture is a set of beliefs, behaviors, discussions, decisions and attitudes shared by the employees of the organisation toward taking and managing risk.

Through good governance, training, support and shared learning experiences the Trust aims to establish and maintain an effective risk culture that enables and rewards individuals and groups for taking the right risks in an informed manner and escalating those of concern.

Risk Profile – Risk Register

The Risk Register is a core element of our risk management arrangements as it represents an overview and assessment of key risks facing the organisation. Its purpose is to evaluate the level of existing internal control in place and to help prioritise actions, funding or resources and inform decisions.

It is a live document which must be regularly reviewed and updated (see risk review).

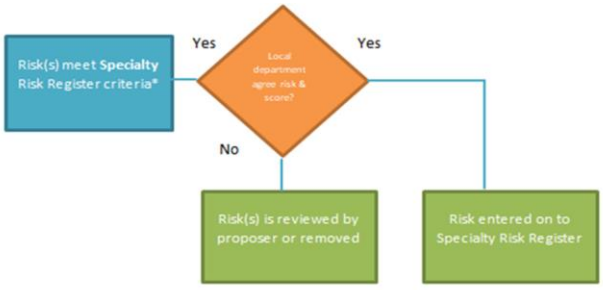
The Trust has a single Risk Register which operates at Specialty (department), Divisional and Trust level. Our Risk Register is held on DATIX.

DATIX has a 'new risk' area where risks can be drafted before being agreed and placed as a live risk on one of the three levels of our Risk Register. RD1 contains a step by step guide on how to add a risk to the new risk area. Risks must not remain at 'new status' for more than 2 months and must be progressed to a live register or closed if no longer relevant.

Specialty / Department Risk Register

All risks must first be agreed by the relevant specialty, department or operational group. This includes agreeing the risk wording and scoring, ensuring all fields on DATIX have been completed and that there is sufficient evidence to support the risk and score. Once agreed, the following action should be taken:

- Where the risk rating score for highest domain is **6 or less** it will be placed on the specialty risk register and will be managed at a local level

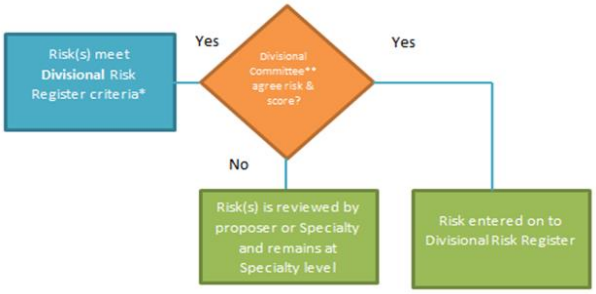


- If a risk **exceeds the specialty risk register criteria** it must still be place on the specialty risk register but escalated to the next divisional risk meeting for approval onto

the divisional risk register. RD1 contains a step by step guide on how to escalate a risk to the division.

Divisional risk register

Once a risk has been agreed by the specialty / department / relevant group and placed on the specialty risk register, it must be escalated to the divisional risk register if it has a risk rating score of **8 or more** or a **consequence of 5 and a likelihood of 1 (any domain)**



Risks that are likely to reach this score may include those that:

- affect multiple departments causing an accumulative effect
- give rise to a moderate breach of legislation
- may result in a more serious safety incident
- has the possibility of a moderate financial penalty or loss
- poses a moderate threat to operational stability
- has implications for Fraud, Corruption or Bribery
- where current resources fall below the safe operational threshold
- may affect the achievement of organisational objectives if not reduced

Where the risk score meets the criteria for the divisional risk register and is approved, it will be placed on the divisional risk register and will be monitored at divisional level.

- If a risk exceeds the divisional risk register criteria it must still be place on the divisional risk register (if approved) but must escalated to the next Risk Management Group (RMG) meeting for approval onto the Trust risk register. RD1 contains a step by step guide on how to escalate a risk to the RMG and Trust Risk Register.

Trust Risk Register

A risk must be escalated to the Trust Risk Register (TRR) if it has a risk rating score of:

- **12 or more for safety and environment**; or
- **15 or more for quality, people, operational, regulatory, reputational and finance**; or
- a **consequence of 5 and a likelihood of 2 (any domain)**; and

- it is outside of the control of the divisional leads to reduce the risk to an acceptable level in the immediate future

Risks that are likely to score highly include those that are:

- wholly unacceptable even with current controls
- identified as significant to the whole organisation
- clear evidence of a significant breach of legislation
- credible, serious and/or imminent safety concerns
- high likelihood of a significant financial penalty or loss
- serious reputational damage is very likely
- consistently threatens daily operational stability or likely to trigger a major incident
- has serious potential or evidence of fraud, corruption or bribery
- current resources fall an intolerable level below the safe operational threshold
- highly likely to jeopardise the achievement of organisational objectives / major impact on the Board assurance framework

Risk type	Lead Executive Sponsor
Safety risks	Director of Safety and Medical Director
Quality risks	Director of Quality & Chief Nurse
Finance risks	Finance risks – Director of Finance
People / Workforce risks	Deputy CEO and Director of People & OD
Operational risks	Chief Operating Officer
Strategy & Transformation risks	Director of Strategy and Transformation
Digital risks	Chief Digital and Information Officer

Once the risk has been reviewed and approved by the Divisional Board, an Executive sponsor must be sought before escalating to RMG.

Executive Sponsor:

The **Executive Sponsor** will usually be the Executive responsible for the area of risk and leading domain score.

Once an Executive Sponsor has agreed the risk and scoring, the risk owner should inform the Head of Corporate Risk, Health & Safety or the Risk Coordinator (Safety team) so it can be included in next RMG paper for consideration.

RD1 contains a step by step guide on how to escalate a risk to the RMG and Trust Risk Register.

Risk Management Group

The RMG will review and challenge all risks proposed for escalation to the Trust Risk Register (TRR) to ensure that they meet the relevant criteria and are supported by sufficiently robust evidence. The RMG operates under a defined Terms of Reference.

Approval onto the TRR

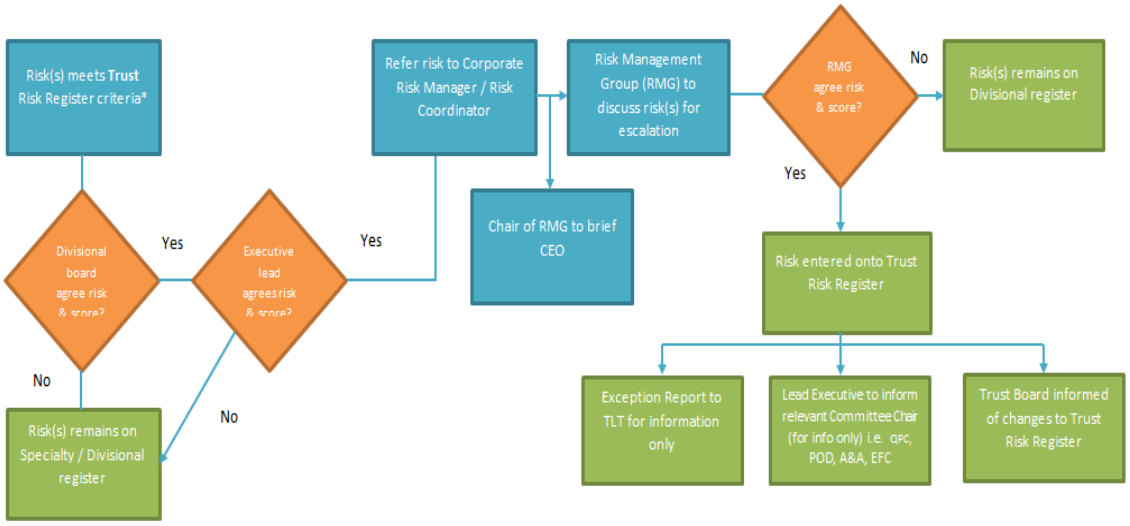
If approved, the risk will be escalated from the divisional risk register to the Trust Risk register. The Head of Corporate Risk, Health & Safety or the Risk Coordinator (Safety team) will notify the Trust Leadership Team (TLT), Audit & Assurance Committee and Board of any risks approved onto the Trust Risk Register by exception.

The Executive Sponsor will notify the Chair of the appropriate assurance committee to which the risk relates of its entry onto the TRR. For example, the Chair of the Quality & Performance Committee will be notified if a quality is risk added to the TRR or the Chair of the People & OD Committee will be modified of a people risk is added to the TRR. The risk owner will notify any sub-committees and the divisional leads.

Not approved onto the TRR

If the risk is not considered to be appropriately defined or scored or there is a lack evidence to support it, the risk will remain on the divisional risk register and be returned to the division for further consideration.

TRR flow diagram:



GOVERNANCE AND ASSURANCE

The Trust takes a proactive stance to risk assurance supported by a strong governance process and assurance cycle.

Assurance and risk management are complementary processes which provide the evidence needed to support:

- management confidence in their assertions;
- assurances to the Board on the state of internal controls; and
- public statements by the board as to the state of internal control.

Demonstrability of core governance is essential for the support of good risk management.

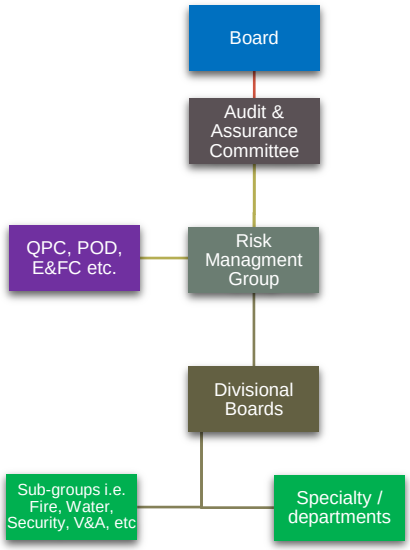
Key decision-makers must be able to answer the questions 'why did you make that decision?', 'what are the risks to its success?' and 'how are you managing that risk?'

Risk Governance Structure

The risk management governance structure is shown below.

Accountability for risk management and assurance flows from specialty / department level up through the Trust to the Board. Accountability exists at each level of the organisation.

Divisional board are accountable to the Risk Management Group and, in turn, the latter is accountable to the Audit and Assurance Committee; the role of which is to provide assurance to Board.



Key Performance Indicators

At the very minimum, risk managers must prove they are meeting the expectations of not only regulators, examiners, and the Board of directors, but also patients, employees, and our communities.

The Trust has a number of risk Key Performance indicators (KPIs) in place which are designed to ensure that our risk management system is functioning effectively. Each indicator is measurable, comparable, and reportable.

*KPIs to be measured from 1 June 2021

*[1]Refer to the Patient Safety Team plan for which **patient safety incidents** can be reviewed and closed without an investigation

Board Assurance Framework

The Board Assurance Framework (BAF) provides the Trust with comprehensive method for the effective and focused management of the principle threats to meeting the Trust's overall strategic objectives.

Risk owners must identify which of the strategic objectives may be impacted by their risk and log this on DATIX (RD1). The Corporate Governance team will evaluate risks linked to the BAF to determine the overall level of threat to the Trust Objectives.

The BAF is a live document updated by the Executive leads for each of the strategic objectives on a quarterly basis and provides the basis for both the assurances and gaps in controls reported in the Annual Governance Statement.

Internal and External Audit

Internal and external audits may focus on the effectiveness of the risk management framework as a system or on specific risk themes. The Trust will work co-operatively with the auditors and seek opportunities to audit and examine risk management.

TRAINING

Risk Register training is available from the Quality and Safety team. This may be delivered in a

Key Performance Indicators

Risk KPIs

- All new risks entered onto DATIX must be agreed by the Specialty / relevant group or department within two months of opening and be placed on a live risk register
- All risks must be linked to at least one objective in the Board Assurance Framework
- All risks must have relevant controls identified
- All risks must have identified actions
- All risks must be reviewed by the review date

Incident KPIs

- All incidents should be moved to investigation status or reviewed and closed within 7 days*[1]
- All no and minor harm incidents requiring investigation should be completed within 30 days*[1]
- All moderate harm and above incidents should be investigated within 60 days
- All health and safety harm incidents affecting staff should have contributory factors identified on the incident in DATIX
-

Actions KPIs

- All actions must be completed by their due date

one to one or group sessions and will provide the knowledge and skills on how to add, manage, escalate and review a risk on the register.

RD1 also provides a step-by-step guide to using the DATIX risk register.

Risk Appetite Statement

The Trust does not have a single risk appetite, but rather a range of defined appetites across the differing areas of our operations. It is expected that risks will be managed within the defined appetites which have been approved by the executive management and the board of directors. However, where the Trust chooses to accept an increased level of risk it will do so, only after ensuring that the potential benefits and threats are fully understood before actions are authorised, that it has sufficient risk capacity, and that sensible and proportionate measures to mitigate risk are established.

Safety

Our risk approach to safety is a cautious one. We are prepared to take calculated safety risks where there is clear and established evidence of a benefit to life / patient outcome, or where further risk reduction is not practical and/ or the cost is disproportionate to the benefit. E.g. we may risk moderate to major harm where there is a clear favourable longer term outcome *and* the risk of this harm is remote or unlikely. We will not tolerate preventable and unjustified harm to patients, the public and employees.

Quality

Our risk approach to quality is an open one. We are prepared to take risks that could result in more frequent negative patient experiences and/or clinical outcomes in specific areas of the Trust (or in relation to specific clinical activities) where there is no long term impact on the patient(s), staff or service e.g. the risk is considered tolerable given the time, money or effort to resolve the issues is not considered proportionate to the benefit of doing so.

People

We will take a neutral approach to risks relating to our people. We are willing to accept risks in relation to staff recruitment, retention, development, experience, wellbeing, inclusion or morale to achieve other imperatives e.g. cost savings providing they do not jeopardise the delivery of safe care or impact significantly of the wellbeing of our staff.

Operational

Our risk approach to operational is a neutral one. We are willing to accept operational risks where this relates to manageable or tolerable operational issues with no long term impact on the patient(s) or staff and where the time, money and effort to resolve the issues would not be proportionate to the benefit of doing so. We are willing to consider all potential delivery options and may well consider factors such as reward or reputational benefit when weighing up the benefit of taking a risk

Regulatory

We will take a neutral approach to regulatory risk. We are willing to accept regulatory risk/ action which is likely to materialise as long as we can be reasonably confident we would be able to justify and defend this successfully if challenged and such actions are not outside the Trust's values and expected behaviours.

Finance

We will take a neutral approach to finance risks. We are willing to accept financial risks which are likely to materialise if this allows the Trust to support investments for potential greater return. We accept a material level of risk for investments which may further the organisation's strategic objectives providing there is a clear route back to financial balance.

Environmental

We will take a cautious approach to environmental risks. We are prepared to take calculated risks relating to low level environmental damage, accepting that our finite resources and budget will constrain our desire to improve against all aspects of sustainability. However, we will endeavor to ensure that our practices are as sustainable as possible, with the time and resources available to us.