South East Coast Ambulance Service
NHS Foundation Trust

Risk Management Policy

Contents

1 Statement of Aims and Objectives

1.1. Risk Management is both a statutory requirement and a key element of effective management. Research shows that organisations which manage risks effectively keep patients and colleagues safer. A comprehensive approach to Risk Management ensures that services are delivered safely, sustainably, and that the Trust achieves its objectives.

1.2. Risk Management is everyone's responsibility.

1.3. Risk is inherent to the work of South East Coast Ambulance Service NHS Foundation Trust (the Trust). However, risks must be mitigated, eliminated, or managed to a tolerable level as far as possible.

1.4. Effective risk management supports decision making at all levels of the organisation. It enables the Board to determine the extent of risk exposure it currently faces, and is willing to accept, to achieve its objectives.

1.5. This policy applies all employees and workers at the Trust, including secondees into and out of the organisation, volunteers, trainees, contractors, and temporary workers, and those working on a bank or agency contract. For ease of reference, all employees and workers who fall under these groups will be uniformly referred to as 'colleagues' in this document.

1.6. This policy defines the approach taken by the Trust to establish a culture of effective risk management and to apply risk management to decision making at all levels. It sets out the roles and responsibilities of individuals and groups in ensuring the Trust is managing risk effectively and risk is supporting effective decision making.

2 Principles

Strategic context

2.1. SECAmb's strategy sets out our vision to transform patient care by delivering prompt, standardised emergency responses while enhancing care navigation with seamless, accessibly virtual services for non-emergency patients. This vision aligns to our three strategic aims:
2.1.1. We deliver high quality patient care.
2.1.2. Our people enjoy working at SECAmb.
2.1.3. We are a sustainable partner as part of an integrated NHS.

2.2. Failing to effectively manage and control risks may mean that the organisation is not able to achieve its strategic aims or enact its vision.

Approach

2.3. The key principle that the Trust follows is that risk should inform decision making at all levels. This requires the active engagement of all our people in risk management activities and the integration of risk management across our governance. All decision making should consider the risks being mitigated, alongside an appreciation of the risks associated with new decisions.

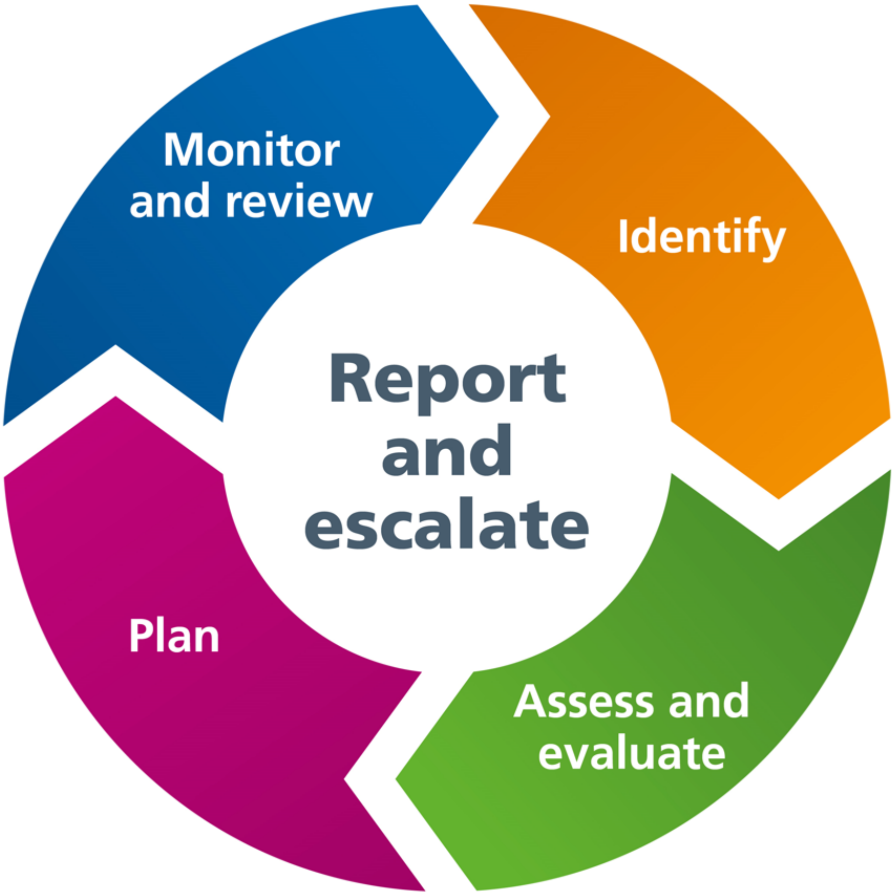
2.4. This policy applies to all categories of risk including but not limited to strategic, people, operational, information, technology, financial, legal, security, project/programme, property, governance, and reputational risks.

Objectives

2.5. The objectives of risk management across the Trust are to:
2.5.1. Minimise the potential for harm to patients, staff, volunteers and visitors, reducing this to levels that are as low as is reasonably practicable.
2.5.2. Protect everything of value to the Trust, such as high-quality patient care, staff and patient safety, reputation and influence, physical and intellectual assets, current and future income streams, information systems and data.
2.5.3. Enable the Trust to anticipate, respond to, and remain resilient in changing strategic and operational circumstances.
2.5.4. Maximise opportunities for Trust development, innovation and improvement of services and functions in a safe, considered, and controlled manner.
2.5.5. Ensure that the Trust achieves and sustains compliance with statutory, policy, regulatory and legal frameworks, and other similar requirements.
2.5.6. Inform the Trust's strategies, policies and operational decisions by identifying risks and their likely impact, by developing actions and controls to manage these risks and by capturing and applying learning from previous risk and control issues.
2.5.7. Provide standard documentation, training and systems which support consistent risk management practice across all functions and at all levels of the Trust.
2.5.8. Manage risks, incidents, and issues effectively, using distinct processes.

3 Process

3.1. The risk management process involves the identification, assessment, treatment and monitoring of risks.



3.2. The risk management process aims to limit the exposure of patients, staff and the organisation to unnecessary risks. It aims to quantify as best as possible uncertain future events and to put actions in place to minimise how likely they are to occur and/or how bad the consequence could be if it did.

Risk Assessment

3.3. Risk Assessment is a process which uses available data to establish the current level of risk. Wherever possible, this should be objective (using the risk domains at **Appendix A** of this policy) to consider consequence and likelihood. It may be necessary to use subjectivity too.

3.4. To assess risks accurately, it is critical to distinguish between risks, issues and incidents. Definitions are provided in section 5 of this policy. Fundamentally, risks are distinct from issues and incidents in that they are future events, i.e.: they have not yet happened.

3.5. Risk assessments must be documented on Datix Cloud IQ (DCIQ), the Trust’s risk management software.

Articulating risks

3.6. To aid understanding and a consistent approach to assessing and mitigating risks, they should be described in the same way across the trust. This description should follow the following format:

There is a risk that <EVENT> occurs leading to <OUTCOME> that causes <IMPACT>.

Identifying risks

3.7. New and emerging risks can be identified by anyone, of any seniority within the organisation. In the first instance, all employees should discuss the identified risk with their line manager (or another manager) to consider whether immediate mitigation is required.

3.8. Risks can be identified through almost any activity – including day-to-day working practices. The following sources of risk identification should be considered a non-exhaustive list:

- Risk Assessment
- Triangulation of information
- Policy development and review
- Quality Assurance and Engagement Visits
- Performance data
- Management reviews
- Compliance monitoring
- Workplans
- Project management processes
- Statutory or regulatory frameworks (CQC, HSE, NHSE, Counter Fraud Authority)
- Internal and external audit data
- Incidents, inquiries, complaints and claims data including coronial investigations.
- Quality Impact Assessments
- Safety alerts
- Horizon scanning
- Recommendations following Business Continuity incidents

Risk Analysis

3.9. The purpose of analysing and scoring a risk is to make a qualitative estimate of the level of exposure which will then inform how the risk should be managed.

3.10. To analyse a risk, first consider the consequence:

Score	Consequence Descriptor	Definition
1	Insignificant	See **appendix A** about how to assess the consequence score.
2	Minor	
3	Moderate	
4	Major	
5	Catastrophic	

3.11. Secondly, consider how likely it would be that this consequence would occur:

Score	Likelihood Descriptor	Likelihood frequency	Likelihood probability
1	Rare	Not expected to occur in years	May only occur in exceptional circumstances
2	Unlikely	Expected to occur at least annually	Unlikely to occur
3	Possible	Expected to occur at least monthly	Reasonable chance of occurring
4	Likely	Expected to occur at least weekly	Likely to occur
5	Almost certain	Expected to occur at least daily	More likely to occur

3.12. Lastly, to calculate the risk score, multiply the consequence score and the likelihood score.

Consequence x Likelihood = Risk Score

		Consequence				
		1 Insignificant	2 Minor	3 Moderate	4 Major	5 Catastrophic
Likelihood	5 Almost certain	5	10	15	20	25
	4 Likely	4	8	12	16	20
	3 Possible	3	6	9	12	15
	2 Unlikely	2	4	6	8	10
	1 Rare	1	2	3	4	5

Risk Evaluation

3.13. Once risk analysis has been completed, the risk will have a score which enables the Trust to assess the level of exposure and identify appropriate actions and management plans.

Level of risk	
1-5	Low
6-12	Moderate
15-25	High

3.14. Each risk is assigned three scores:

3.15. The **Initial risk score –** this is when the risk is first identified this is a consideration of the risk without any controls or mitigation actions in place. It will not change for the lifetime of the risk.

3.16. The **current risk score** – this evaluation should consider the level of risks on the day you are updating the risk. it should be a realistic measure of consequence and likelihood, considering controls and mitigation actions and their effectiveness on mitigating the risk.

3.17. The **target risk score** – this is the score you are aiming to manage the risk down to, considering possible mitigations and actions.

Risk Treatment

3.18. Risk treatment is the process of implementing measures to treat the risk. there are a number of options to treat risks.

Terminate	Suspend the risk situation / activity. Avoid or eliminate the event or set of events which create the risk. The risk simply cannot happen anymore because circumstances will not allow it.
Tolerate	Accept the risk as it is i.e.: with the current controls in place.
Transfer	Pass responsibility for the risk to someone else to handle.
Treat	Reduce the risk. This could be for example that you substitute a new of different practice that mitigates the risk, contain the hazard, safeguard the person involved or control the way the work is done.

Controls, gaps in control and risk actions

3.19. Controls are arrangements already in place to mitigate or manage the risk. They will differ depending on the nature of the risk identified, but could be policies, procedures or ways of working. For a control to be effective, it must make the risk less likely to occur, or less severe if it did.

3.20. Gaps are the issues which need to be addressed to control the risk. This could be where there are no controls in place or there is an existing control, but it is not fully effective.

3.21. Risk actions should become controls once fully implemented. They will address the gaps to reduce identified risks.

Assurance

3.22. Assurance against a risk is evidence that the risk is being effectively managed.

Adding a risk to the risk register

3.23. Anyone who has undertaken the appropriate training and has access to the Trust's risk register can add a risk. Line managers should always be notified when a risk is added to the risk register. Where a high risk is added, the relevant Executive Director should be notified.

3.24. Directorate SLTs must review their risk registers monthly to ensure that risks are appropriate, scored correctly and reflect the current position with controls and assurances.

Risk and action owners

3.25. Each risk will have a risk owner. This is a person who is responsible for the management and control for all aspects of an individual risk. The risk owner should be able to influence actions to control the risk.

3.26. The risk owner and the action owner can be the same individual. They can also be different individuals and located in different services or directorates.

3.27. Risk and action owners must always be consulted before being assigned risks or actions. This is a matter of professional courtesy in line with the Trust’s values.

Risk review

3.28. The review process should provide assurance that the risk is up-to-date, i.e.: is scored appropriately, has controls and mitigating actions in place. The frequency of review depends on the severity of the risk

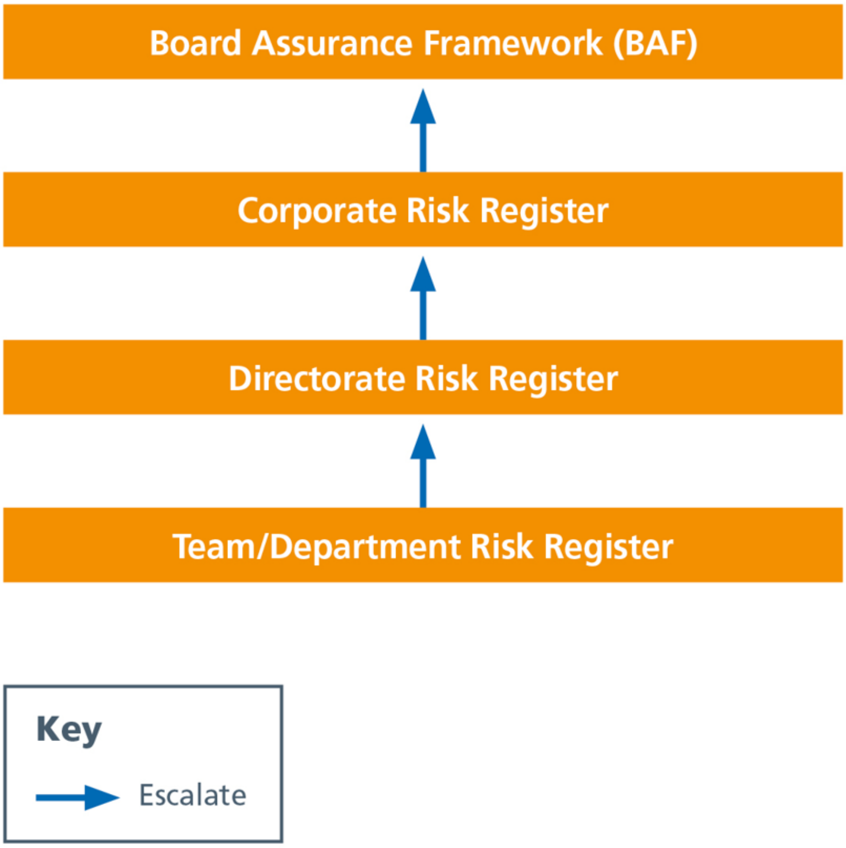
Risk score	Review frequency
Low Risks (1-5)	Every four months
Moderate Risks (6-12)	Every two months
High Risks (15+)	Monthly

Risk Registers

3.29. A risk register is a place where risks are stored, managed and monitored. A risk register should be a live document, and if accurate, will enable staff to have confidence that risks have been identified and managed to support decision making. The Trust uses the Enterprise Risk Management Module (ERM) in Datix Cloud IQ (DCIQ).

3.30. Each Directorate has its own Risk Register which should be reviewed monthly by Directorate SLTs.

3.31. As risks increase in score, they will escalate up through team risk registers, to Directorate registers and then onto the Corporate Risk Register (see diagram below.) Ultimately, risks which are of sufficient strategic importance, irrespective of score, will be captured on the Board Assurance Framework.


Board Assurance Framework (BAF)
Corporate Risk Register
Directorate Risk Register
Team/Department Risk Register
Key
Escalate

Risk Escalation

3.32. Risks may need to be escalated for discussion, action, advice or support. In Directorate risks should be escalated to Directorate Senior Leadership Teams (SLTs), then to Risk Assurance Group (RAG) and then into Executive Management Board (EMB).

Risk closure

3.33. Typically, risks should be closed at the point when the target score is achieved. There may be reasons risks are closed before they reach target, for example where an in-year risk is being closed and a new risk is opened.

3.34. Risks which have been included on the Corporate Risk Register (i.e.: scored above a 12) at any point since opening are required to have their closure approved at Risk Assurance Group.

3.35. Closure of risks below 12 should be approved by the relevant Directorate SLT meeting.

Board Assurance Framework (BAF)

3.36. The BAF is a document used to record and report on the Trust's key strategic objectives, risks, controls and assurances to the Board. It is reviewed by Board bi-monthly.

3.37. Any executive member of staff may propose a risk for inclusion on the BAF. RAG may also chose to escalate to EMB new, emerging or established risks which may present a threat to the organisations strategic objectives for consideration for inclusion on the BAF.

3.38. The Board takes all decisions in relation to accepting, amending, scoring and closing BAF risks.

Organisational Risk Appetite

3.39. Risk appetite provides a framework which enables the Trust to make informed management decisions.

3.40. Any risk appetite framework made by the Trust will sit separately from this policy.

Project Risks

3.41. Project risks will primarily be managed through local project risk registers / RAIDD logs and reviewed for updates/resolution within the frequency set out by the project group.

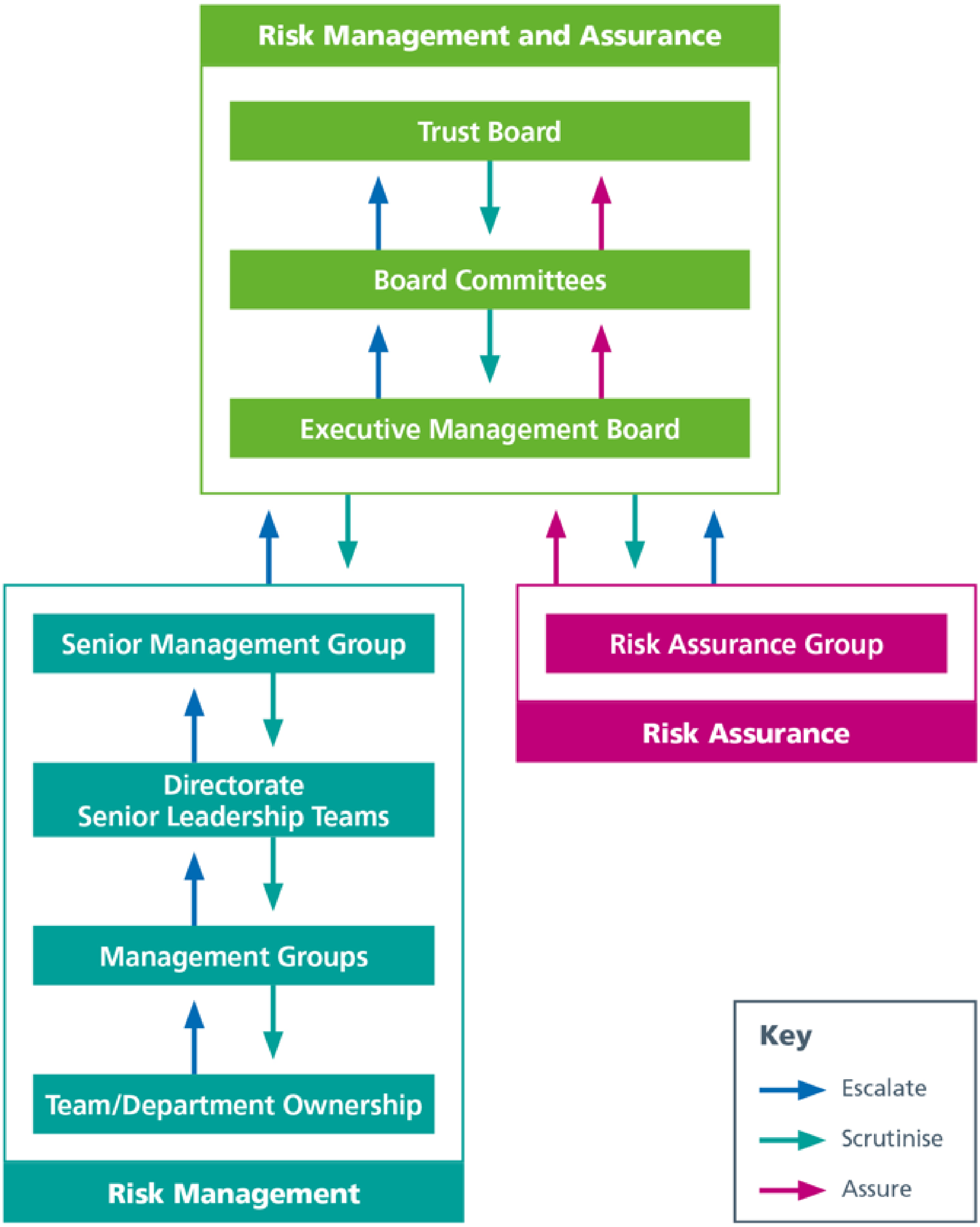
3.42. Overarching programme or project risks and moderate or high risks identified to key projects should be managed using Datix Cloud IQ (DCIQ).

4 Assurance and governance

4.1. The diagram below indicates the flow of risk escalation, assurance and scrutiny throughout the organisation.

Assurance Infrastructure

4.2. Our assurance infrastructure, including the Risk Assurance Group, EMB and other Executive committees and governance, scrutinise key controls and assurances on controls to assess their validity and efficiency.



Risk Management Governance

4.3. All risks scored 15 and above will be reviewed by the Head of Risk and reported to EMB monthly.

4.4. Each directorate will have a nominated risk champion, who is their designated Directorate Risk Lead. The role of this Risk Lead is to maintain oversight of all risks for their directorate, be the representative for their directorate at Risk and Assurance Group (RAG) and provide updates to RAG on behalf of their service on existing and emerging risks. A description of the role of Directorate Risk Lead is set out at **appendix B.**

Meeting	Type of Risk	Report Frequency
Board	Risks which threaten the delivery of strategic objectives – BAF	Review BAF risks bi-monthly
Board Committees	Risks identified against delivery of strategic objectives relevant to their area of focus	Quarterly basis seek assurance relating to risks within their purview.
EMB	Monthly assurance on the effective management of all BAF risks, high risks (15+) and any escalations from RAG.	Monthly
SMG	Reviews overview of all opening and closing corporate risks (12+) monthly along with all high and BAF risks.	Monthly
RAG	Scrutiny of Directorate and Corporate risk registers (all risks)	Monthly
Directorate Senior Leadership Team meetings	All risks on the Directorate's risk registers (moderate risks), and all relevant risks on the corporate risk register (12+) and issues on its issue log	Monthly
Management and governance groups	Review all risks owned by the management group in line with terms of reference – review existing risks to ensure they are current, consider emerging risks.	Between quarterly and monthly
Team / department meetings	Risks captured on team or department risk registers (low risks)	In line with regularity of meetings

5 Definitions

5.1. Board Assurance Framework (BAF) risks are risks which could impact the delivery of the Board's Strategic objectives.

5.2. Consequence is the outcome of an event affecting objectives.

5.3. Controls are measures that maintains or modified the risk.

5.4. Corporate Risks are any risks which exceed a score of twelve.

5.5. Corporate Risk Register contains all escalated risks from departmental registers scoring above 12.

5.6. Datix Cloud (DCIQ) is the software the Trust uses to manage its risk registers.

5.7. A Directorate risk register contains all a Directorate's risks, save for those captured on the Corporate risk register. Team or departmental risk registers may sit beneath the Directorate risk register.

5.8. An incident, as defined in the Incident Reporting Policy, is "any adverse event or circumstance arising that could have or did lead to unintended or unexpected harm, loss or damage to patients, staff, visitors, carers, members of the public or Trust premises, property, other assets, information, or any other aspect of the organisation. They can involve any number of different factors, e.g. injury, damage, loss, fire, theft, violence, abuse, accidents, ill health, disruption to services etc."

5.9. The initial risk rating is the rating of the risk (consequence X likelihood) before any controls are in place. This is the natural state of the risk.

5.10. An issue is an obstacle or challenge which is already present. It may be a risk which has materialised.

5.11. Likelihood is the chance of something happening.

5.12. An objective is a goal for the organisation at Department, Directorate or Trust level.

5.13. Residual risk rating is the rating of the risk (consequence X likelihood) after current controls have been applied. The current state of the risk.

5.14. A risk is an uncertain future event.

5.15. Risk appetite is the amount and type of risk that an organisation is prepared to pursue, retain or take in pursuit of its strategic objectives.

5.16. Risk Management is a set of co-ordinated activities to direct and control an organisation regarding risk.

5.17. Target risk rating is the rating of the risk (consequence X likelihood) which the Trust will accept.

6 Responsibilities

6.1. The **Trust Board** has accountability for ensuring that there is an effective risk management framework in place across the Trust and providing strategic leadership in relation to risk management through the Trust. This includes:

6.1.1. Maintaining oversight of the strategic risks and opportunities facing the organisation through the Board Assurance Framework (BAF) and to seek assurance that appropriate mitigations are in place or are being actioned.

6.1.2. Leading by example in creating a culture of risk awareness.

6.2. The **Audit and Risk Committee** is responsible for reviewing the system for risk management, integrated governance and internal control environment across all of the Trust's activities. The committee provides assurance to the Trust Board that there are effective systems in place for the management of risk. It must satisfy itself that the processes of populating the BAF are fit-for-purpose.

6.3. Other **Board Committees** – should seek assurance on a quarterly basis that the strategic and relevant operational risks within their purviews are being managed effectively.

6.4. The **Chief Executive Officer** as the Accountable Officer is responsible for ensuring that there is an effective system of control maintained to support the achievement of the Trust's objectives. This includes:

6.4.1. Establishing and maintaining effective corporate governance arrangements, including risk management.

6.4.2. Ensuring the Trust communicates, as appropriate, as openly as possible about its risks internally and externally.

6.4.3. Ensuring the effective implementation and consistent application of this policy throughout the Trust.

6.5. The **Director of Corporate Governance** is accountable to the Trust Board and the Chief Executive for the Trust's governance and risk management activities. They have executive responsibility for governance and risk management and provide (with support from the Head of Risk) the framework for, and assurance on, effective and integrated risk management. This includes the direction, development and implementation of any strategies relating to risk management. They will ensure that risk management forms part of the Board's agenda, and the work of its subcommittees.

6.6. Members of **the Executive** are responsible for the consistent application of this policy within their areas of accountability. This includes:

6.6.1. Maintaining an awareness of the risk profile of the organisation and their Directorate.

6.6.2. Ensuring that this policy is implemented within their area of responsibility and that risk management is embedded in governance arrangements.

6.6.3. Management of risks assigned to them in accordance with this policy.

6.6.4. Promoting a risk aware culture within their teams and in the course of their duties.

6.6.5. Reviewing high risks monthly at EMB.

6.6.6. Proposing risks for inclusion on the BAF and scrutinising and challenging the BAF.

6.6.7. Receiving escalations from RAG.

6.7. **Risk Assurance Group** is the governance group responsible for providing assurance to the Executive Team and Audit and Risk Committee on the effectiveness of the Trust's risk management arrangements. It has responsibility for the closure of any risk which was on the Corporate risk register.

6.8. **Directorate Senior Leadership Teams** are responsible for oversight and management of their Directorate's risk registers to ensure they are current and that risks are scored consistently with appropriate controls, actions and assurances. Directorate SLTs should have sight of their Directorate's risks at least monthly.

6.9. **Senior Management Group** reviews opening and closing risks from the Corporate risk register monthly. Members of SMG are responsible for the consistent application of this Policy within their areas of accountability, which includes:

6.9.1. Making active use of the Trust's risk registers to manage risks assigned to them and to consider risks within their area of responsibility.

6.9.2. Following this policy.

6.9.3. Promoting a risk aware culture within their team and in the course of their duties.

6.10. **Management groups** are responsible for ensuring risk management is a regular standing agenda item. They should consider all risks within their purview, including adequacy of actions and controls, risk grading and any emerging risks.

6.11. **The Head of Risk** is responsible for:

6.11.1. The operational implementation of the Risk Management Priorities and policy including monitoring for effectiveness.

6.11.2. Providing specialist advice and training on risk management

6.11.3. Providing support, guidance and training to Risk Leads.

6.11.4. Ensuring Board and Executive Committees are provided with appropriate reports in relation to risk management.

6.11.5. Implementing arrangements to ensure that the Trust Risk Register is maintained as an active document.

6.12. **Risk Owners** are responsible for managing risks assigned to them in line with this policy. In particular, ensuring that risks are up to date, reviewed in line with this policy and have appropriate controls, assurance and actions in place. Risk Owners should escalate increasing risks.

6.13. **Risk Leads** are the nominated leads for each Directorate to support managers, staff, risk and action owners to identify and manage risks. They support Risk Owners to ensure that the Directorate risk registers are kept up to date and risks are reviewed in line with this policy. Further responsibilities are articulated at **Appendix B** of this policy.

6.14. **Managers** are responsible for implementing and monitoring any identified and appropriate risk management control measures within their designated areas and scope of responsibilities.

6.15. **All staff** are responsible for adhering to this policy and identifying and managing risks. This includes:

6.15.1. Maintaining an awareness of the primary risks within their area of work.
6.15.2. Identifying, and where practicable managing, risks they identify in the course of their duties.
6.15.3. Bringing risks to the attention of their line managers.

7 Education and training

7.1. The table below details the training offered for staff in relation to risk management.

Audience	Training Title	Delivery	Required Frequency	Reporting
All Staff	Risk Awareness Training	E-Learning via Discover	3 yearly	Head of Risk reporting into RAG
Band 7 staff members and above and/or staff members who require access to DCIQ	Risk management Training	E-Learning via Discover	Once	Head of Risk reporting into RAG

8 Monitoring compliance

8.1. The Head of Risk will have responsibility for the day-to-day compliance with this policy.

8.2. The Risk Assurance Group is responsible for monitoring compliance regularly with this policy. They will be presented with a monthly report from the Head of Risk.

8.3. If regular non-compliance is identified, RAG will formally escalate into EMB.

Audit and Review (evaluating effectiveness)

8.4. All policies have their effectiveness audited by the responsible Management Group at regular intervals, and initially six months after a new policy is approved and disseminated.

8.5. Effectiveness will be reviewed using the tools set out in the Trust's Policy and Procedure for the Development and Management of Trust Policies and Procedures (also known as the Policy on Policies).

8.6. This document will be reviewed in its entirety every three years or sooner if new legislation, codes of practice or national standards are introduced, or if feedback from employees indicates that the policy is not working effectively.

8.7. All changes made to this policy will go through the governance route for development and approval as set out in the Policy on Policies.

9 Associated Trust Documentation

9.1. Trust Strategy

9.2. Board Assurance Framework

9.3. Health and Safety Policies and Procedures

9.4. Information Security and Governance Policy

9.5. Incident Reporting Policy

9.6. Business Continuity Policy

10 References

10.1. CQC Key Lines of Enquiry, prompts and ratings characteristics for healthcare services (Assessment framework: Healthcare services (cqc.org.uk))

10.2. Good Governance Institute, Board Guidance on Risk Appetite 2020 (GGI-Board-Guidance-on-risk-appetite-2020.pdf)

10.3. UK Government: The Orange Book – Management of Risk – Principles and Concepts 2023 (The Orange Book – Management of Risk – Principles and Concepts (publishing.service.gov.uk))

10.4. HMFA (2014). NHS Audit Committee Handbook. (3rd ed.). England: Healthcare Financial Management

10.5. Health and Social Care Act 2012, Ch 7

10.6. Health and Social Care Act (Safety and Quality) Act 2015, Ch 28

10.7. NHSLA (2013). NHSLA Risk Management Standards 2013-2014. England: NHS Litigation Authority.

11 Financial Checkpoint

11.1. This document has been confirmed by Finance to have no unbudgeted financial implications.

12 Equality Analysis

12.1. The Trust believes in fairness and equality, and values diversity in its role as both a provider of services and as an employer. The Trust aims to provide accessible services that respect the needs of each individual and exclude no-one. It is committed to comply with the Human Rights Act and to meeting the Equality Act 2010, which identifies the following nine protected characteristics: Age, Disability, Race, Religion and Belief, Gender Reassignment, Sexual Orientation, Sex, Marriage and Civil Partnership and Pregnancy and Maternity.

12.2. Compliance with the Public Sector Equality Duty: If a contractor carries out functions of a public nature then for the duration of the contract, the contractor or supplier would itself be considered a public authority and have the duty to comply with the equalities duties when carrying out those functions.

Appendix A: Consequence Domains

	Consequence score (severity levels) and examples of descriptors				
	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/ombud sman inquiry Gross failure to meet national standards

	Consequence score (severity levels) and examples of descriptors				
	1	2	3	4	5
Domains	Negligible	Minor	Moderate	Major	Catastrophic
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	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

	Consequence score (severity levels) and examples of descriptors				
	1	2	3	4	5
Domains	Negligible	Minor	Moderate	Major	Catastrophic
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	Non-delivery of key objective/ Loss of >1 per cent of budget Failure to meet specification/ slippage
Financial (including damage/loss/fraud/ bribery) – escalation to audit/board dependent on limits specified in SFI's	Negligible Organisational / personal financial (loss £<5k)	Minor Organisational / personal financial loss (£5k - £24k)	Significant Organisational / personal financial loss (£25k - £50k)	Major Organisational / personal financial loss (£50k - £1 million)	Severe Organisational / personal financial loss (>£1 million)

Service/business interruption Environmental 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

Appendix B: Role of Directorate Risk Leads

Directorate Risk Lead Responsibilities:

Risk Leads promote and support effective risk management and encourage compliance with the Trust's Risk Management Policy and Procedure.

The Directorate Risk Lead will:

- Support risk register owners, risk owners and action owners in their directorate to identify and manage risks effectively and in accordance with the Risk Management Policy and Procedure.
- Ensure that risk registers within their directorate are maintained, updated, and reviewed in a timely and effective manner.
- Ensure that risks are identified and recorded in a timely and effective manner and in accordance with the Risk Management Policy and Procedure.
- Ensure that their Directorates risks have up-to-date actions, assurances and controls.
- Attend relevant directorate management groups, Trust committees, governance group and forums to discuss and present new/revised risks
- Attend the Risk and Assurance Group monthly to present their Directorates risk profile
- Develop a good level of competence in using the Trust's risk management system, and support staff in their directorate to use the system effectively.
- Support the Head of Risk to develop a Trust-wide professional network relating to risk management and related assurance activities.
- In general, act as a champion and positive role model for risk management