CONTROLLED DOCUMENT

University Hospitals Birmingham NHS Foundation Trust

Risk Management Policy

CATEGORY:	Policy
CLASSIFICATION:	Governance
PURPOSE	To detail the framework and standards required for the management of Risk
Controlled Document Number:	120
Version Number:	6
Controlled Document Sponsor:	Chief Legal Officer
Controlled Document Lead:	Corporate Risk Lead
Approved By:	Board of Directors
On:	28th April 2022
Review Date:	28th April 2025
Distribution: • **Essential Reading for:** • **Information for:**	Executive Directors, Divisional, Specialty and Department Managers, Risk Leads All staff

Contents

1. Policy Statement 3
2. Scope 3
3. Framework 3
4. Types of Risk 3
5 Risk Management Process 5
6 Identifying the Risk 5
7 Assessing the Risk 5
8 Managing the Risk 5
9 Reviewing the Risk 6
10 Risk Escalation 6
11 Risk Reporting 6
12 Risk Assurance 7
13 Risk Appetite 7
14 Roles and Responsibilities 8
15 Implementation and Monitoring 11
16 References 12
17 Associated Policy and Procedural Documentation 12
Appendix A - Monitoring Matrix 13
Appendix B – Risk Assessment Matrix 15
Appendix C – Sources of Risk 19
Appendix D - Risk Reporting, Escalation and Assurance 20
Appendix E - Glossary of Terms 21

Version Control

Version	Title	Issue Date
1	Risk Management Strategy	Nov 2008
2	Risk Management Policy	27/11/2008
3	Risk Management Policy	31/01/2012
4	Risk Management Strategy and Policy	22/08/2013
4.1	Risk Management Strategy and Policy	31/01/2018
5	Risk Management Policy	31/10/2018
5.1	Risk Management Policy	03/04/2019
5.2	Risk Management Policy	08/11/2019
6	Risk Management Policy	05/05/2022

1. Policy Statement

1.1. University Hospitals Birmingham NHS Foundation Trust (the Trust) is committed to developing and implementing Risk management processes which will identify, assess, manage and review Risks that may threaten the delivery of key priorities, objectives or values.

1.2. The purpose of this Policy and its associated procedure is to set clear standards and accountabilities for the management of Risk within the Trust to ensure that:

1.2.1. The highest possible quality of care is delivered;

1.2.2. Statutory, regulatory and legal obligations are met;

1.2.3. Patients, staff, the public, assets and the reputation of the Trust are protected;

1.2.4. Standardised tools for the management of Risk are provided. This includes the use of Datix® as the Trust's Risk Management system;

1.2.5. Training and support for staff in the management of Risk is available; and

1.2.6. Assurance can be provided to the Board of Directors regarding the effective implementation of this Policy.

2. Scope

This Policy applies to all areas and activities of the Trust and to all individuals employed by the Trust including contractors, volunteers, students, locum and agency staff and staff employed on honorary contracts.

3. Framework

3.1. The framework for Risk Management provides a defined approach that will be implemented across the Trust. Detailed instructions are provided in the associated Risk Management Procedure.

3.2. The Chief Legal Officer shall approve all procedural documents associated with this Policy and any amendments to such documents, and is responsible for ensuring that such documents are compliant with this Policy.

4. Types of Risk

There are three types of Risk that the Trust expects to be identified and managed; they are related to objectives at a strategic, project and operational level.

4.1. Strategic Risks

Strategic Risks relate to the strategic objectives of the Trust, these are identified by the Executive Team, recorded on the Strategic Risk Register and reported in the Board Assurance Framework (BAF)

4.2. Project Risks

4.2.1. Project Risks relate to a project's objectives and are generally expressed in terms of anything that may impact on cost, time or quality.

4.2.2. Project Risks are managed in the same way as other Risks within the Trust in that Risk registers will be maintained, reporting schedules and escalation thresholds to appropriate stakeholders will be defined, and the route of assurance is made clear.

4.3. Operational Risks

Operational Risks relate to the day to day activity of the Trust and may be anything that could impact on the achievement of objectives at an operational level. Operational Risks are recorded on Datix. The subject of Operational Risks (the consequence if the Risk occurs) identified at Specialty, Department and Divisional level will be classified as:

4.3.1. **Quality** – Risks that may impact on the safety of patients (i.e. resulting in harm), effectiveness (e.g. clinical audit, outcomes, delays, cancellations, operational performance), experience for patients and the ability to manage quality (e.g. complaints, audit, surveys, clinical governance and internal systems).

4.3.2. **Compliance and Regulatory** – Risks that may impact on legal/regulatory requirements (e.g. Information Commissioner, CQC, Health & Safety (H&S), Professional Standards, external certifications); and national guidance and best practice (e.g. National Institute for health and Care Excellence).

4.3.3. **Financial** – Risks that may impact on income, expenditure, procurement, business continuity, value for money and protection of assets.

4.3.4. **Reputation** – Risk that may impact on the day to day activity of the Trust (e.g. standards of conduct, ethics and professionalism); reputation of the service; or Trust derived from internal or external issues.

4.3.5. **Resources and People** – Risks that may impact on staff recruitment, staff in work, staff retention, security and welfare of people.

4.3.6. **Information and Communication Technology (ICT)** – Risks that may impact on IT security (e.g. access and permissions); controls of assets (e.g. purchasing, movement and disposal of equipment); business continuity (e.g. cyber-attack, network maintenance); data (e.g. integrity of data, availability, confidentiality); innovation infrastructure (maintenance and security); and systems and resources and their ability to support the Trust in pursuit of its objectives.

4.3.7. **Health and Safety** – Risks related to the assessments of hazards under the associated Health and Safety Policy. Records of hazards and their assessment form a part of the day to day activities of the Trust and will be available to all staff members.

5. Risk Management Process

5.1. While this Policy provides standards to support managers in minimising the negative aspects of uncertainty, the management of Risk can have a negative or positive outcome. Opportunities for improvement, usually through innovation, exist in parallel and should be considered by managers as the positive side of Risk management.

5.2. The Risk Management process must not delay appropriate action being taken. Where a Risk is identified that may have an impact on patient safety then the first priority must be to make the situation safe. Where this is not possible then the Risk must be referred to an appropriate line manager at the earliest opportunity

5.3. The process for Risk Management consists of 4 steps to identify, assess, manage and review Risks. These are described in greater detail in the associated Risk Management Procedure. Standards that apply to each step are:

5.3.1. Identifying the Risk

a. All staff have a role to play in identifying Risk which may arise from a wide range of internal and external sources including, but not limited to, those outlined at Appendix C.

b. Strategic Risks are identified and owned by a member of the Executive Team. The details of these Risks are reported to the Board of Directors through consideration and approval of the Board Assurance Framework. This will include an appropriate target score that is agreed for each individual strategic Risk.

c. At an operational level all Specialties and Departments will have a nominated Risk Lead who will ensure a register of the Risks which may impact on the achievement of objectives is maintained.

5.3.2. Assessing the Risk

a. All staff must follow the standardised approach to Risk assessment outlined in the associated Risk Management Procedure. The use of a consistent vocabulary facilitates the effective management of Risk and helps to standardise an approach. To support staff in this a glossary of terms is included in Appendix E to this Policy.

b. All Risks will be scored and graded according to likelihood and consequence using the Trust's Risk Assessment Matrix at Appendix B.

5.3.3. Managing the Risk

a. Once a Risk has been assessed the Risk Owner will need to decide how best to respond based on the Trust Risk Appetite and the resources available.

b. Risk Management responses can be a mix of four main actions;

Transfer, Tolerate, Treat, or Terminate. These options are described in greater detail in the associated Risk Management Procedure.

c. New Operational Risks with a Current Score of 15 or above (Red) will be presented to the appropriate Executive or Divisional Management Team for approval within 1 month (a maximum of 30 days) of being reported on Datix®.

d. New Operational Risks with a Current Score of 12 or below (Amber or Green) will be approved onto the Risk register within 3 months (a maximum of 90 days) of being reported on Datix®.

5.3.4. Reviewing the Risk

a. All Strategic Risks will be reviewed each quarter by the appropriate member of the Executive Team or Director and the updated Risk will be recorded on the BAF.

b. Operational Risks with a Current Score of 15 (Red) or above must be reviewed each month (a minimum of once every 30 days).

c. Operational Risks with a Current Score of 12 or below (Amber and Green) will be reviewed at least every 3 months (a minimum of once every 90 days).

d. The review of operational Risks will be recorded on Datix® by the Risk Owner, supported by the Risk Lead, and must ensure that the Risk assessment represents the current situation taking into account any changes to the context, effectiveness of Controls, implementation of actions or change in Risk Appetite.

e. When the Current Score of a Risk reaches the Target Score it will be reviewed by the Risk Owner with a view to accepting the Risk.

5.4. Risk Escalation

5.4.1. An integral part of effective Risk Management is ensuring that, when necessary, Risks are escalated to a higher level of management so that appropriate action and prioritisation of resources can take place. Risks are escalated according to the progress in reaching the Target Score (further details can be found in the Risk Management Procedure). Where a Risk cannot be managed to an acceptable Risk Level within the available resource or in an agreed timescale then the Risk must be escalated.

5.4.2. For Operational Risks, the maximum time a Risk will be ‘Treated’ by a Specialty Risk Owner before it is escalated is 24 months. At this time any Risk that has not reached an acceptable Risk Level must be escalated to a Divisional Management Team or member of the Executive Team to determine the most appropriate course of action. This could be additional oversight at Specialty level or a change in ownership to the Divisional/Executive’s risk register.

5.5. Risk Reporting

The data recorded on Datix® will be used to produce reports to facilitate scrutiny and provide assurance regarding the implementation of this Policy. These reports may be adapted at any time to suit the requirements of a particular committee or group however some reports are scheduled as detailed below.

Table 1: Scheduled Risk Reports

Report	Schedule	Content
Corporate Risk Register	Monthly	Approved Operational Risk with a Current Score of 15 or above (Red).
Strategic Risk Report (Public Board of Directors)	Quarterly	Strategic Risks reported to Board of Directors via the BAF for their approval.
Operational Risk Report (Private Board of Directors)	Quarterly	The management (on track/off track) of Approved Operational Risk with a Current Score of 15 or above (Red).

5.6. Risk Assurance

5.6.1. The Board of Directors needs to be aware of the current state of progress with regard to its strategic objectives including threats to achievement (Risk), Controls that have been put in place and actions that are planned.

5.6.2. The resource of the Board of Directors is finite, members cannot be present at every meeting to oversee every transaction and therefore the responsibility for carrying out operational activity falls to the Trust's management. As a result, the Board of Directors requires regular assurance that the Trust is working to achieve strategic objectives in the expected way with the expected outcomes.

5.6.3. The Board of Directors will decide upon the most appropriate source of assurance dependent upon the importance of the subject in question and their Risk Appetite in relation to it. Assurance should enable the Board to have a greater degree of confidence about the likely achievement of strategic objectives and provide a sound basis for decision-making.

5.6.4. The sum of assurances received by the Board of Directors constitutes the BAF. Appendix D to this Policy shows how this process is enacted within the Trust.

5.7. Risk Appetite

5.7.1. Risk Appetite identifies the level of Risk the Board of Directors is willing to accept in pursuit of its objectives. The Board of Directors will agree a statement against each category of operational Risk which

sets out their Risk Appetite and quantifies the level of tolerance it is prepared to accept. Risk Appetite statements and tolerance limits must be used to derive acceptable Target Scores for Operational Risk. The current Board of Directors Risk Appetite Statement is found on the Trust's Intranet site.

5.7.2. The Board of Directors Risk Appetite Statement will be reviewed on an annual basis.

5.7.3. The risk appetite relating to strategic risks will be considered by the Board of Directors on a case by case basis.

6. Roles and Responsibilities

The Board of Directors has overall responsibility for Risk Management within the Trust. Certain aspects of this are delegated to committees and individuals as detailed below.

6.1. Audit Committee

In relation to the management of Risk the Audit Committee will:

6.1.1. Ensure that an annual review of the Risk Management process is undertaken by the internal audit function and provide assurance to the Board of Directors based on outcome; and

6.1.2. Seek further assurance on the management of specific areas of Risk as required by the Board of Directors.

6.2. Chief Executive

6.2.1. The Chief Executive as the Accountable Officer is accountable for the Trust's Risk Management Framework and ensuring that this operates effectively.

6.2.2. The Chief Executive will seek assurance from the systems and processes for Risk Management and ensure these meet regulatory, statutory and legal requirements. The Chief Executive delegates operational responsibility for Risk Management to the Chief Legal Officer.

6.3. Executive Team

6.3.1. The Executive Team is responsible for overseeing a programme of Risk Management activities for their Departments and areas of responsibility, in accordance with this Policy.

6.3.2. This will include the provision of assurance to the Executive Team and the Board of Directors on the management of Operational Risk reported on the Corporate Risk Register, approval and review of Operational Risks identified within their Departments, ownership of escalated Risks and consideration of Strategic Risk and assurance for inclusion on the BAF.

6.4. Chief Legal Officer

6.4.1. The Chief Legal Officer (CLO) is responsible to the Board of Directors and Chief Executive in relation to the Risk Management Framework and will provide regular reports to the Board in this regard.

6.4.2. The CLO is also responsible for providing expert advice to the Board of Directors in relation to Risk Management and ensuring the Board of Directors has access to regular and appropriate Risk Management information, advice, support and training where required.

6.4.3. The CLO is designated as the Trust's Senior Information Risk Officer (SIRO), providing assurance to the Board of Directors on the management of information Risk.

6.5. Chief Operating Officer

The Chief Operating Officer (COO) is responsible for providing assurance to the Executive Team and Board of Directors on the management of Operational Risks reported on the Corporate Risk Register. In doing this the COO (or their nominated Deputy) will review Red Risks approved by the clinical Divisional Management Teams to decide whether the management of each Risk is on track to meet the target score in the agreed timeframe.

6.6. Divisional Management Boards

Divisional Management Boards are collectively accountable for the day to day the management of all Risks relating to their Division. They are responsible for:

6.6.1. Ensuring that Risk Management processes are in place and functioning appropriately within the Specialties;

6.6.2. Approving and reviewing Risks owned by Specialties under their management that have a Current Score of more than or equal to 15 (Red Risks);

6.6.3. Monitoring Risks owned by Specialties under their management that have a Current Score of less than 15 (Amber and Green);

6.6.4. Reviewing Risks that are escalated to them to decide upon the most appropriate course of action.

6.6.5. Communicating with other Divisional teams where Risks may impact or require action across these boundaries;

6.6.6. Taking ownership of Risks escalated from their Specialties; and

6.6.7. Escalating Risk to an Executive Director as appropriate.

6.7. Specialty/Department Management Teams

Members of Specialty/Department Management Teams will have day to day responsibility for the identification, management, review and escalation of all Risks that fall within their areas of responsibility. They will have responsibility for:

6.7.1. Ensuring appropriate governance and Risk Management arrangements are in place within their Specialty/Department which enables communication, monitoring and learning from Risks;

6.7.2. Overseeing and monitoring the management of all Risks which fall within their responsibility, escalating Risks where appropriate, authorising the Current Score of Risks under their management.

6.7.3. Ensuring appropriate prioritisation and allocation of resources to most effectively mitigate these Risks.

6.8. Director of Corporate Affairs

The Director of Corporate Affairs (DCA) is responsible for:

6.8.1. Providing oversight and assurance in relation to the Risk Management Framework in non-clinical areas

6.8.2. Providing assurance to the Board of Directors on the management of Operational Risks from the Corporate Divisions reported on the Corporate Risk Register. In doing this the DCA will review Red Risks approved by the Corporate Specialties to decide whether the management of each Risk is on track to meet the target score in the agreed timeframe.

6.8.3. Ensuring the timely submission of the quarterly Risk Report (BAF and Operational Risk) to the Board of Directors.

6.9. Head of Clinical Governance and Patient Safety

The Head of Clinical Governance and Patient Safety is responsible for providing oversight and assurance in relation to the Risk Management Framework in clinical areas.

6.10. Corporate Risk Lead

The Corporate Risk Lead is responsible to the Director of Corporate Affairs for monitoring the Risk Management standards (Appendix A) and managing the implementation of the Risk Management Framework in corporate (non-clinical) areas.

6.11. Clinical Risk Lead

The Clinical Risk Lead is responsible to the Head of Clinical Governance and Patient Safety for the implementation of the Risk Management Framework in clinical areas.

6.12. Risk Lead

Each Specialty/Department/Division will nominate a Risk Lead who is responsible for:

6.12.1. Ensuring that staff within the Specialty/Department/Division are able to identify Risks and know how to report them to the Risk Lead;

6.12.2. Ensuring Risk Assessments are completed for Risks identified within the Specialty/Department/Division and documented on Datix® according to this Policy;

6.12.3. Ensuring that Specialty/Department/Divisional staff implement action plans to reduce Risk, according to this Policy;

6.12.4. Ensuring that Risks are monitored and reviewed appropriately and that

the Risk Assessment is updated to reflect progress and is accepted when the Target Score is met; and

6.12.5. Attending Specialty/Department/Division meetings to report information relating to Risk to the relevant management team including whether or not Risks have been escalated and managed appropriately, agreed actions are taking place, and the Risk Level reducing. This information will form a part of reports produced by the Clinical and Corporate Governance Teams to be presented at Specialty/Department and Divisional Quality meetings.

6.13. Risk Owner

All Risks will have an identified Risk Owner who is responsible for ensuring that relevant Risks are managed appropriately, this includes:

6.13.1. The ongoing actions, monitoring of Controls and scheduled review with appropriate update on Datix® of the Risk;

6.13.2. Deciding when and if Accepted Risks are subject to further review; and

6.13.3. Reporting on the overall status of the Risk including the need for escalation.

Wherever possible the role of Risk Lead and Risk Owner should be separate to avoid any potential conflict of interest.

6.14. All Staff

All staff have a responsibility for the identification, reporting, assessment and management of Risks and to ensure they make themselves aware of and comply with Trust Policies and procedures.

7. Implementation and Monitoring

7.1. Implementation

7.1.1. This Policy will be available on the Trust's intranet site. The Policy will also be disseminated through the management structure within the Trust.

7.1.2. A training needs analysis will be developed that will determine the level of training required for specific staff groups.

7.1.3. Members of the Clinical and Corporate Governance Teams in the Corporate Affairs Directorate will support the implementation of this Policy through:

a. Supporting nominated Risk Leads to ensure that Risks are actively managed and Risk Registers are administered and reviewed;

b. Ensuring that Specialty/Department/Division staff receive information, instruction and support in their duties relating to Risk Management;

c. Producing and publishing a monthly Risk Profile that is shared with their respective Divisions and Specialties;

d. Providing Risk Management training to an agreed training needs analysis;

e. Developing reports on the Risk Management system, and the Risks managed within it, to an agreed schedule

f. Monitoring and reporting the escalation of Risk; and

g. Reviewing risks that are awaiting final approval, taking action to either return them to the Risk Lead/Owner or approving onto the risk register.

7.2. Monitoring

Appendix A provides full details on how the Policy will be monitored by the Trust.

8. References

8.1. A Risk Management Standard, Institute of Risk Management (2002)

8.2. A Risk Matrix for Risk Managers, National Patient Safety Agency (2008)

8.3. ISO 31000 – Risk Management, International Standards Organisation (2009) updated 2018

8.4. COBIT5 for Risk, ISACA (2013)

8.5. Home Office Risk Management Policy and Guidance, Home Office (2017)

8.6. NHS Audit Committee Handbook, Department of Health (2014)

8.7. Risk Management Assessment Framework, HM Treasury (2009)

8.8. Taking it on Trust: A Review of How Boards of NHS Trusts and Foundation Trusts Get Their Assurance, Audit Commission (2009)

8.9. The Orange Book (Management of Risk Principles and Concepts), HM Treasury (2020)

8.10. UK Corporate Governance Code, Financial Reporting Council (2018)

8.11. Understanding and Articulating Risk Appetite, KPMG, (2009)

9. Associated Policy and Procedural Documentation

9.1. Board of Directors Risk Appetite Statement

9.2. Health and Safety Policy

9.3. Risk Management Procedure

Appendix A - Monitoring Matrix

MONITORING OF IMPLEMENTATION	MONITORING LEAD	REPORTED TO PERSON/GROUP	MONITORING PROCESS	MONITORING FREQUENCY
1. Identifying Risk - All specialties, departments, divisions and directors will have a nominated Risk Lead and this is published on the trust intranet.	Corporate Risk Lead	- Director of Corporate Affairs - Clinical Risk Lead	Review of Risks on Datix®	6 Monthly
2. Managing Risk - Operational Risks reported on the Corporate Risk Register (current score 15 or above) have been approved within 1 month (maximum of 30 days) of being reported on Datix®.	Corporate Risk Lead	- Chief Legal Officer - Director of Corporate Affairs - Head of CG and Patient Safety - Clinical Risk Lead	Review of Risks on Datix®	Monthly
3. Managing Risk - Operational Risks (current score 12 or below) have been approved onto the risk register within 3 months (maximum of 90 days) of being reported on Datix®.	Corporate Risk Lead	- Director of Corporate Affairs - Head of CG and Patient Safety - Clinical Risk Lead	Review of Risks on Datix®	Monthly
4. Reviewing Risk - All Risks with a Current Score of 15 (Red) or above must be reviewed each month. (a minimum of once every 30 days)	Corporate Risk Lead	- Director of Corporate Affairs - Head of CG and Patient Safety - Clinical Risk Lead	Review of Risks on Datix®	Monthly
5. Reviewing Risk - All Risks with a Current Score of 12 or below (Amber and Green) will be reviewed each quarter (a minimum of once every 90 days)	Corporate Risk Lead	- Director of Corporate Affairs - Head of CG and Patient Safety - Clinical Risk Lead	Review of Risks on Datix®	Monthly

6. Reviewing Risk - When the Current Score of a Risk reaches the Target Score it will be reviewed by the Risk Owner with a view to accepting the Risk.	Corporate Risk Lead	- Director of Corporate Affairs - Head of CG and Patient Safety - Clinical Risk Lead	Review of Risks on Datix®	Quarterly
7. Reviewing Risk – Any risk that is accepted is reviewed according to a timescale determined by the Risk Owner.	Corporate Risk Lead	- Director of Corporate Affairs - Head of CG and Patient Safety - Clinical Risk Lead	Review of Risks on Datix®	6 Monthly
8. **Reviewing Risk** - Strategic Risk will be reviewed each quarter with the appropriate Executive Director or Director and recorded on the BAF which will be reported to the Board.	Corporate Risk Lead	- Board of Directors	Board Assurance Framework	6 Monthly
9. Risk Escalation - Where a Risk cannot be managed to an acceptable Risk Level within the available resource or in an agreed timescale then the Risk must be escalated to a Divisional or Executive owner for consideration.	Corporate Risk Lead	- Director of Corporate Affairs - Head of CG and Patient Safety - Clinical Risk Lead	Review of Risks on Datix®	6 Monthly

Appendix B – Risk Assessment Matrix

Risk scores are a combination of the likelihood of the Risk occurring multiplied by the consequence as follows:

	Consequence				
Likelihood	**(1) Insignificant**	**(2) Minor**	**(3) Moderate**	**(4) Severe**	**(5) Catastrophic**
(5) Highly Likely	**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 likelihood will be assessed according to the following criteria:

Descriptor	**Rare 1**	**Unlikely 2**	**Possible 3**	**Likely 4**	**Highly Likely 5**
Frequency	May not occur for several years (i.e. more than 5)	Could occur at least once in a 5 year period	Could occur at least once a year	Could occur at least once in 6 months	Could occur at least once per month
Probability	<1%	1% - 24%	25% - 50%	51% - 85%	> 85%

Risk Consequence will be assessed according to the following criteria:

Risk Category	Insignificant 1	Minor 2	Moderate 3	Severe 4	Catastrophic 5
Quality	- Potential for minimal injury requiring no/ minimal intervention or treatment. - Peripheral element of treatment or service may suboptimal.	- Potential for minor injury or illness that requires extra observations or minor treatment and caused minimal harm to one or more patients. - Overall treatment or service may suboptimal.	- Potential for moderate injury which resulted in additional treatment and that caused significant but not permanent harm. - Treatment or service may significantly reduce effectiveness.	- Potential for major injuries, or long term incapacity or disability. Permanent harm to one or more patients. - Potential failure to meet internal standards. - Potential noncompliance with national standards.	- Event may lead directly to death, multiple permanent injuries or irreversible health effects. - Potential totally unacceptable level of service or quality. - Potential repeated failure to meet internal standards. - Potential gross failure to meet national standards.
Compliance & Regulatory	- No or minimal impact or breach of guidance/ statutory duty/ national standards.	- Single failure to meet guidance/ national standards.	- Repeated failure to meet guidance or national standards. - Single breach of statutory duty. - Challenging external recommendations/Improvement notices.	- Non-compliance with national standards with significant Risk to patients if unresolved. - Multiple breaches in statutory duty - Enforcement action.	- Totally unacceptable level of quality of treatment/ service. - Multiple breaches in statutory duty. - Prosecution.
Financial	- Loss or Overspend of £100,000 or less. - Risk of claims remote.	- Loss or Overspend > £100,000 but no more than £500,000. - Claim < £100,000.	- Loss or Overspend > £500,000 but no more than £1,000,000. - Claim(s) between £100,000 and £1million.	- Loss or Overspend > £1million but no more than £5million. - Claims between £1million and £5 million.	- Overspend or Loss of >£5m - Claim(s) >£5 million. - Loss of contract /payment by results.

Risk Category	Insignificant 1	Minor 2	Moderate 3	Severe 4	Catastrophic 5
Reputation	- Rumours Potential for public concern.	- Local media coverage. - Elements of public expectation not being met.	- Local media coverage/short term reduction in public confidence.	- National media coverage/long term reduction in public confidence.	- Ongoing National media coverage/ total loss of public confidence.
Resource and People	- Minor schedule slippage – no effect on achievability of objectives. - Short term low staffing level temporarily reduces service quality (<1 day).	- Significant schedule slippage but no other effect on achievability of objectives. - Low staffing level that reduces service quality.	- Some non-key objectives not achievable. - Late delivery of key objective/ service due to lack of staff. - Unsafe staffing level or competence (>1 day).	- Uncertain delivery of key objectives or service due to lack of staff. Unsafe staffing level or competence (>5 days). - Loss of key staff.	- Non delivery of key objectives/ substantial failure to meet specification. - Non delivery of key objective/ service due to lack of staff. - Ongoing unsafe staffing levels or competence. - Loss of several key staff.
ICT	- Potential loss of non-critical ICT systems or services in a single specialty. - Potential degradation of non-critical ICT systems or services in multiple specialties. - There is absolute certainty that no adverse effect can arise even when a data or security breach may occur.	- Potential loss of a non-critical ICT systems or services in multiple specialties. - Potential for some minor adverse effect from a data or security breach or any event involving vulnerable groups even if no adverse effect is expected.	- Potential degradation of critical ICT systems or services in a single specialty. - Potential for some adverse effect from a data or security breach e.g. embarrassment from release of information into the public domain.	- Potential degradation of critical ICT systems or services in multiple specialties. - Potential loss of critical ICT systems or services in a single specialty. - Potential pain and suffering/ financial loss from a data or security breach.	- Potential loss of critical ICT systems or services in multiple specialties. - Potential for a catastrophic event or death as a result of a data or security breach.

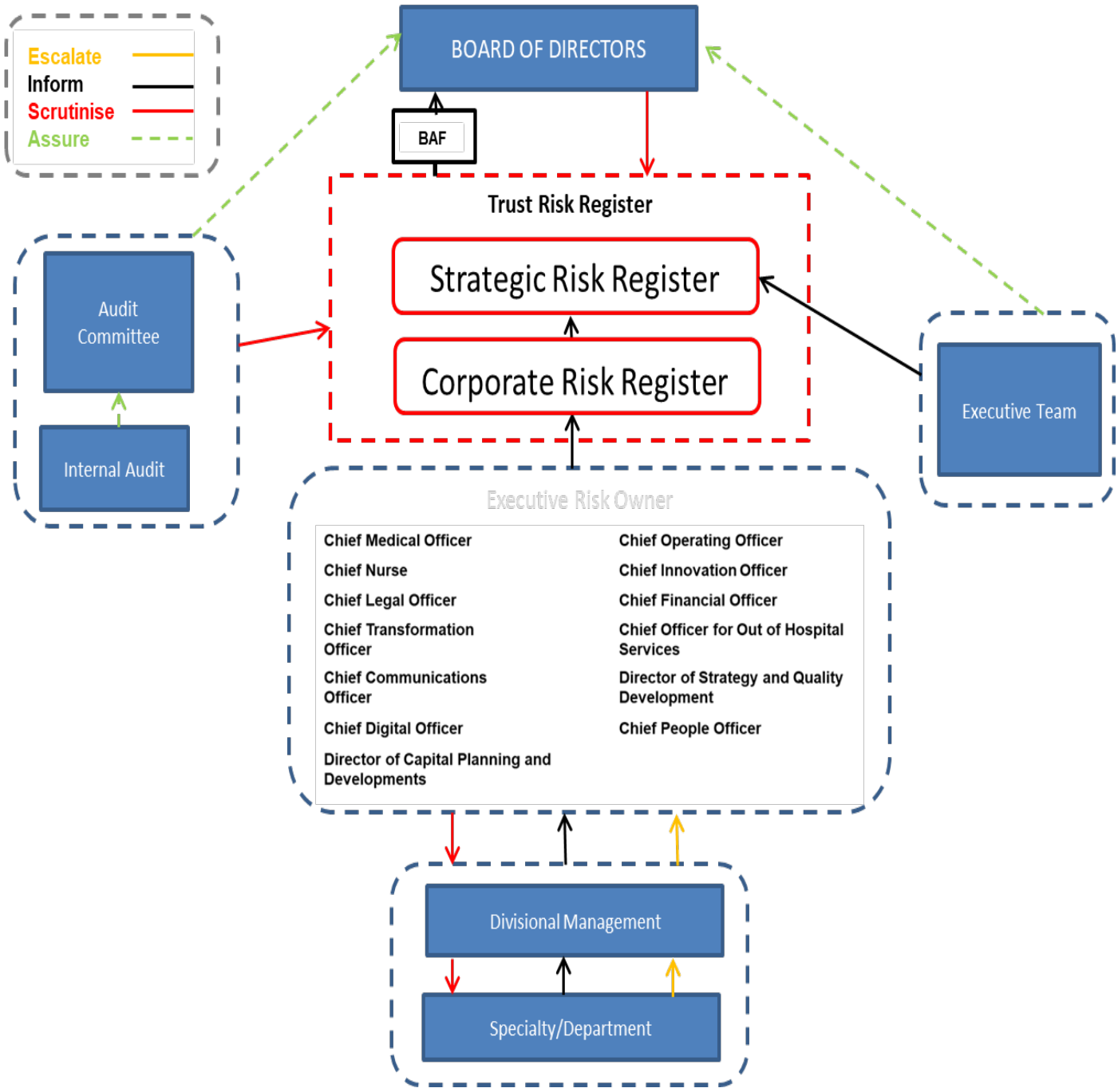
Risk Category	Insignificant 1	Minor 2	Moderate 3	Severe 4	Catastrophic 5
Health, Safety and Environment	- Minimal injury requiring no/ minimal intervention or treatment. - No time off work. - No or minimal impact or breach of guidance/ statutory duty. - Minimal or no impact on the environment.	- Minor injury or illness, first aid treatment needed. Requiring time off work <7 days. - Breach of statutory duty (no harm caused). - Minor impact on environment.	- Moderate injury requiring professional intervention RIDDOR reportable. Requiring time off work for 7-14 days. - Single breach in statutory duty (harm caused). - Moderate impact on environment.	- Major injuries, or long term incapacity/ disability. Requiring time off work for >14 days. - Multiple breaches in statutory duty (harm caused). - Major impact on environment.	- Event may lead directly to death. - Multiple permanent injuries or irreversible health effects. - Catastrophic impact on environment.

Appendix C – Sources of Risk

Privacy Impact Assessments

The purpose of the Privacy Impact Assessment (PIA) is to ensure that privacy Risks are minimised while allowing the aims of the project to be met whenever possible. Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice. This analysis can be tested by consulting with people who will be working on, or affected by, the project. These can be Risks to the individuals affected, in terms of the potential for damage or distress. There will also be corporate Risks to the organisation carrying out the project, such as the financial and reputational impact of a data breach. Projects with higher Risk Levels and which are more intrusive are likely to have a higher impact on privacy.

Appendix D - Risk Reporting, Escalation and Assurance



Appendix E - Glossary of Terms

Definitions provide an agreed vocabulary that supports consistent communication and quality of assessment. The following definitions will be applied to the management of Risk:

Board Assurance Framework (BAF): the key source of evidence that links strategic objectives to Risks and assurances, and the main tool that the Board will use in discharging its overall responsibility for internal Control. The BAF is approved by the Board of Directors.

Control: The mitigating action that is implemented to reduce the likelihood or consequence of a Risk occurring. Controls must be monitored to provide assurance that they continue to mitigate Risk to an acceptable Level.

Corporate Risk Register: A register of Operational Risks where the Current Score is 15, 16, 20 or 25 (Red). These Risks are agreed by Directors or Divisions with assurance being provided on their management to the Executive Team.

Current Score: The Level of Risk when the likelihood and consequence are assessed taking into consideration the effect of Controls.

Divisional Risk: A Risk that may threaten the objectives of a Division. This type of Risk will be owned by a member of the divisional management team.

Initial Score: The Level of Risk when the likelihood and consequence are assessed before any Control activities are applied, sometimes called the inherent Risk.

Issue: An event that has already happened was not planned and requires management action. Not to be confused with a Risk.

Operational Risk: an uncertain event or condition that may affect the achievement of operational objectives, often impacting the day to day activity of the Trust.

Project Risk: an uncertain event or condition that, if it occurs, has a positive or negative effect on a project's objectives related to cost, time or quality.

Risk: A Risk is a future uncertain event or set of events that, if it were to occur, will have an effect on the achievement of business, project or programme objectives. A Risk can be a threat or an opportunity to the objectives of the organisation.

Risk Appetite: A narrative statement that clarifies the amount of Risk the Board of Directors is willing to accept in pursuit of its objectives.

Risk Assessment: Risk Assessment is the process, by which the Trust identifies, describes, evaluates and estimates (quantitatively or qualitatively) a Risk.

Risk Escalation: Where a Risk cannot be managed to an acceptable Risk Level within the available resource or in an agreed timescale then the Risk must be escalated to a higher level for review. This may result in a change of Risk owner if the review shows that the Risk cannot be managed appropriately at the lower level.

Risk Lead: The member of staff responsible at Specialty/Divisional/Executive level for the day to day administration of Risk Management procedures. The Risk Lead supports the Risk Owner in the management and review of Risk. Wherever possible

the role of Risk Lead and Risk Owner should be separate to avoid any potential conflict of interest. See also Risk Owner.

Risk Level: After a Risk has been assessed the scores may be:

Red Risk – a high Risk with a Current Score of 15, 16, 20 or 25

Amber Risk – a significant Risk with a Current Score of 5 (L1xC5), 6, 8, 9, 10 or 12

Green Risk – a low Risk with a Current Score of 1, 2, 3, 4 or 5 (L5xC1)

Risk Management: Risk Management is the systematic application of processes and procedures that an organisation puts in place to ensure that it identifies, assesses, prioritises and takes action to manage Risks to ensure it continues to deliver its objectives. Risk Management is an ongoing process that must form part of everyday management activity. Risk must be managed so far as is reasonably practical.

Risk Owner: The member of staff responsible for the management of individual Risks who may be at Specialty, Division or Executive level. See also Risk Lead.

Risk Profile: An aggregated report of Risks at Divisional level produced on a monthly basis. This includes Risk in clinical and non-clinical areas

Risk Proximity: The estimate of when the Risk is likely to occur. Identifying Risk Proximity helps management to prioritise Risk and to identify the appropriate response.

Risk Register: A Risk Register is a log of all Risks that may threaten an organisation's success in achieving its declared aims and objectives. It provides a structure for collating information that enables Risks to be identified and quantified. It also helps to provide a Framework to make decisions about how each Risk must be managed; and it can be a useful prioritising tool to guide the allocation of resources and can be linked into the business planning process. The Trust uses the Datix® Risk Management System to support this.

Risk Status: this refers to the current management status of a Risk and is determined by the approach taken in terms of Terminate, Tolerate, Transfer or Treat.

Risk Tolerance: A translation of a Risk appetite statement into a range of Risk scores that the Board of Directors are willing to accept.

Strategic Risk: A Risk that may threaten the strategic objectives of the Trust. This type of Risk will be owned by an Executive Director.

Strategic Risk Register: A register of Strategic Risks owned by Executive Directors of the Trust. Together with the Corporate Risk Register this constitutes the Trust Risk Register.

Target Score: The Level of Risk when the likelihood and consequence are assessed taking into consideration the Appetite for Risk in pursuit of objectives.

Terminate Risk: an option for managing a Risk where the Risk owner decides that the current Level of Risk is too high and will not proceed with the activity that has led to the Risk e.g. closing a ward where there are insufficient staff to provide a safe level of care.

Tolerate Risk: an option for managing a Risk where the Risk Owner decides that the current Level of Risk is in line with the agreed Risk Appetite/tolerance and accepts that no further action is required other than monitoring Controls and quarterly review.

Transfer Risk: an option for managing a Risk where the Risk Owner decides that the current Level of Risk is too high and transfers the Risk to another owner e.g. purchase an insurance Policy so that if the Risk transpires then financial loss is covered or transfer the service to another accountable owner.

Treat Risk: an option for managing a Risk where the Risk Owner decides that the current Level of Risk is higher than the agreed Risk Appetite/tolerance and chooses to mitigate consequence or/and likelihood through further action.

Trust Risk Register: The Risk Register which includes Risks on both the Corporate and Strategic Risk Registers.