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:	005
Controlled Document Sponsor:	Director of Corporate Affairs
Controlled Document Lead:	Corporate Risk Lead
Will this Controlled Document impact upon any contracts held by the Trust?	☐ **Yes**[1] ☒ **No**
Approved By:	Board of Directors
On:	TBC
Review Date:	TBC
Distribution: • **Essential Reading for:** • **Information for:**	Executive Directors, Divisional, Specialty and Department Managers, Risk Leads All staff

[1] If this Controlled Document will have an impact on any contracts held by the Trust, once approved, this will need to be sent to the Procurement Team requesting that it be added to the Procurement Policy Portal

Contents

Paragraph		Page
1	Policy Statement	3
2	Scope	3
3	Framework	3
4	Roles and Responsibilities	9
5	Implementation and Monitoring	13
6	References	14
7	Associated Policy and Procedural Documentation	14
Appendices		
Appendix A	Monitoring Matrix	15
Appendix B	Risk Assessment Matrix	17
Appendix C	Sources of Risk	20
Appendix D	Trust Board Risk Appetite Statement	21
Appendix E	Glossary	22
Tables		
Table 1	Scheduled Risk Reports	7
Figures		
Figure 1	Risk Reporting, Escalation and Assurance	8

1. Policy Statement

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

1.2 The purpose of this policy and its associated procedures is to make clear the standards and accountabilities for the management of Risk within the Trust to ensure that:

- The highest possible quality of care is delivered;
- Statutory, regulatory and legal obligations are met;
- Patients, staff, the public, assets and the reputation of the Trust are protected;
- Standardised tools for the management of risk are provided, this includes the use of Datix® as the Trusts Risk Management system;
- Training and support for staff in the management of Risk is available; and
- 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 procedural documents.

3.2 The Director of Corporate Affairs 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.

3.3 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.

Strategic Risks

3.3.1 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).

Project Risks

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

3.3.3 Project Risks are managed the same 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 to the Trust is made clear. These details will be included in a Project Initiation Document (PID). The associated Project Management Policy may be referred to for further guidance.

Operational Risks

3.3.4 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. The subject of Operational Risks (i.e. which objective(s) is likely to be affected if the Risk occurs) identified at Specialty, Department and Divisional level will be classified as:

- **Quality** – Risks that may impact on the safety of patients (clinical incidents infection control), effectiveness (clinical audit, outcomes, delays, cancellations, operational performance), experience for patients and the ability to manage quality (governance).

- **People and resources –** Risks that may impact on staffing, security and welfare of people.

- **Information and communication technology (ICT) –** Risks that may impact on IT infrastructure (maintenance and security), systems and resources and their ability to support the Trust in pursuit of its objectives.

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

- **Regulation and compliance** – Risks that may impact on legal/regulatory requirements including but not limited to Care Quality Commission (CQC), Standing Financial Instructions (SFIs), fraud, inquests, claims, Information Governance, Duty of Candour.

- **Reputation –** Risk that may impact on the reputation of the service or Trust derived from internal or external issues.

- **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.

3.4 Risk Management Process

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:

Identifying the Risk

3.4.1 All staff have a role to play in identifying Risk which may arise from a wide range of internal and external sources outlined at Appendix C.

3.4.2 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.

Assessing the Risk

3.4.3 All staff must follow the standardised approach to Risk Assessment outlines 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.

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

Managing the Risk

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

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

Reviewing the Risk

3.4.7 All Risks with a Current Score of 15 (Red) or above must be reviewed each month while those Risks with a Current Score of 12 or below (Amber and Green) will be reviewed each quarter. The review 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, deterioration of Controls, implementation of actions or change in Risk Appetite.

3.4.8 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. Any Risk that reaches a score where it has been accepted must be reviewed every six months to ensure that there has been no significant change to the context of the Risk or deterioration in the effectiveness or the efficiency of Controls.

3.4.9 Strategic Risks will be reviewed each quarter with the appropriate Executive Director or Director and recorded on the BAF.

3.5 <u>Risk Escalation</u>

3.5.1 An integral part of effective Risk Management is ensuring Risks are escalated within the Trust to ensure 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.

3.5.2 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 for consideration.

3.6 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
Risk Profile	Monthly	Risk profiles detailing all recorded Risks within each Specialty, Department or Division will be published on the first working day of each month.
Corporate Risk Register	Monthly	Approved Operational Risk with a Current Score of 15 or above (Red).
Strategic Risk Register	Quarterly	Strategic Risks reported to Board of Directors via the BAF.

3.7 Risk Assurance

3.7.1 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.

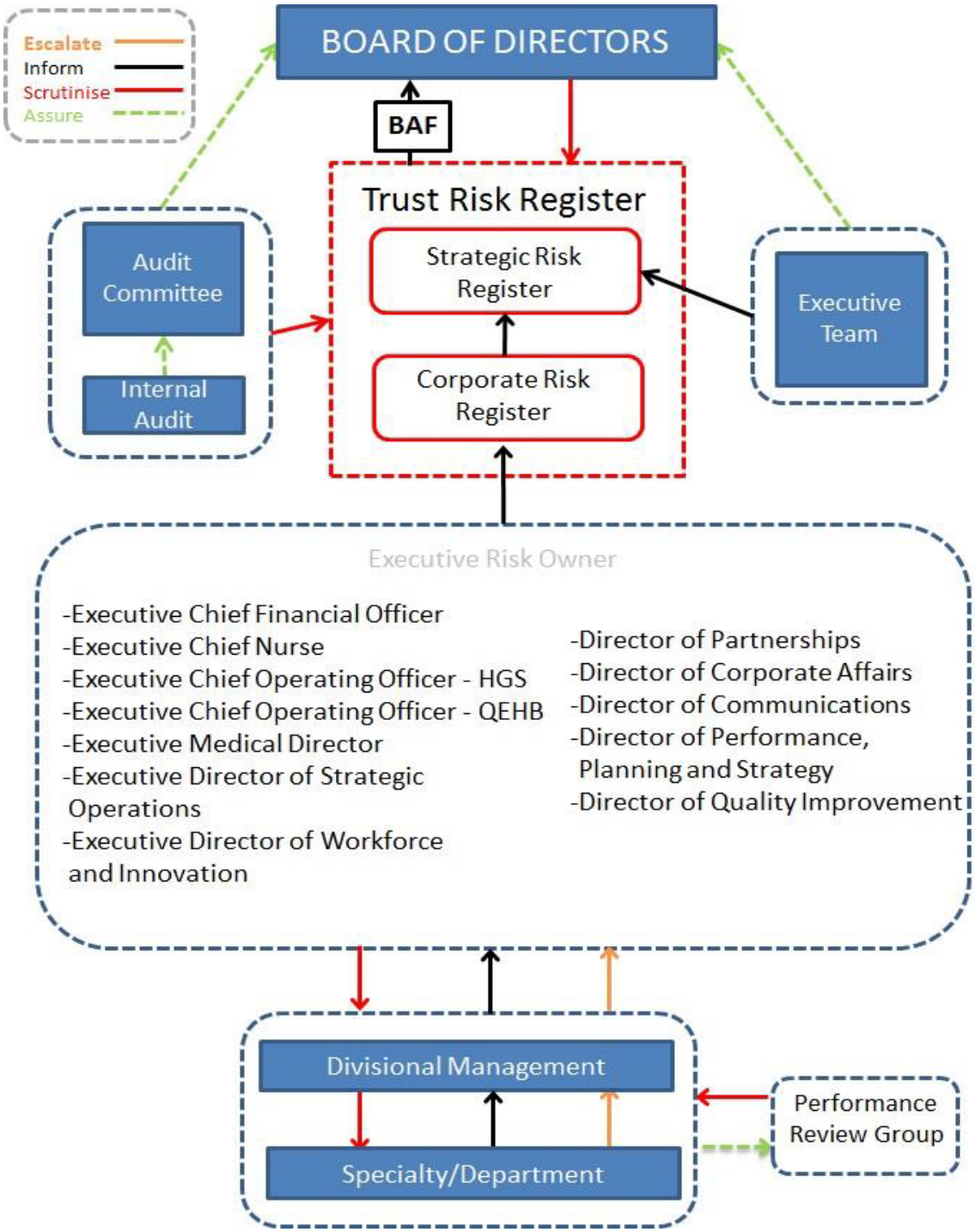
3.7.2 The resource of the Board of Directors is finite, members cannot be present at every meeting to oversee every transaction and therefore the responsibility for carrying out operational activity falls to the Trust's management. As a result, the Board of Directors requires regular assurance that the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

3.7.3 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.

Assurances will enable the Board to have a greater degree of trust in that assurance giving greater confidence about the likely achievement of strategic objectives and providing a sound basis for decision-making.

3.7.4 The sum of assurances received by the Board of Directors constitutes the BAF. The following diagram shows how this process is enacted within the Trust.

Figure 1. Risk Reporting, Escalation and Assurance



3.8 Risk Appetite

Risk Appetite identifies the amount of Risk the Board is willing to accept in pursuit of its objectives. The Board will agree a statement against each objective 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 Risk. The current Board Risk Appetite Statement is found at Appendix D.

4. 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 follows:

4.1 Audit Committee

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

4.1.1 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

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

4.2 Chief Executive

4.2.1 The Chief Executive (CEO), as the Accountable Officer, is accountable for the Trust's Risk Management Framework and ensuring that this operates effectively.

4.2.2 The CEO must seek assurance from the systems and processes for Risk Management and ensure these meet regulatory, statutory and legal requirements. The CEO delegates operational responsibility for Risk Management to the Director of Corporate Affairs.

4.3 Executive Directors and Directors

4.3.1 All Executive Directors and Directors are responsible for overseeing a programme of Risk Management activities for their Departments and areas of responsibility, in accordance with this policy.

4.3.2 This will include the provision of assurance to the Executive Team and 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.

4.4 Director of Corporate Affairs

4.4.1 The Director of Corporate Affairs (DCA) 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.

4.4.2 The DCA 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. The DCA will be assisted in their role by Executive colleagues and the Deputy Foundation Secretary.

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

4.5 Executive Chief Operating Officers

The Executive Chief Operating Officers (COO's) at QEHB and HGS are 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's will review the Current Score, Controls and actions to mitigate Red Risks approved by Divisional Management Teams.

4.6 Divisional Management Teams

Members of Divisional Management Teams will have day to day accountability for the management of all Risks relating to their Division. They are responsible for:

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

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

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

4.6.4 Reviewing Risks that are more than 2 years old to confirm their validity;

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

4.6.6 Taking ownership of Risks escalated from their Specialties; and

4.6.7 Escalating Risk to an Executive Director as appropriate.

4.7 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:

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

4.7.2 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; and

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

4.8 Deputy Foundation Secretary

The Deputy Foundation Secretary is responsible for providing oversight and assurance in relation to the Risk Management Framework in non-clinical areas and the timely submission of the Risk Report (BAF and Operational Risk) to the Board of Directors.

4.9 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.

4.10 Corporate Risk Lead

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

4.11 Clinical Risk Lead

The Clinical Risk Lead will be responsible for the implementation of the Risk Management Framework in clinical areas.

4.12 Clinical and Corporate Governance Teams

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

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

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

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

4.12.4 Providing Risk Management training to an agreed training needs analysis;

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

4.12.6 Monitoring and reporting the escalation of Risk.

4.13 Risk Lead

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

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

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

4.13.3 Ensuring that Specialty/Department/Divisional staff implement action plans to reduce Risk, according to this policy;

4.13.4 Ensuring that Risks are monitored and reviewed appropriately and that the Risk record is updated to reflect progress and is accepted when the Target Score is met; and

4.13.5 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.

4.14 **Risk Owner**

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

a) The ongoing action, monitoring of Controls and scheduled review with appropriate update on Datix® of the Risk; and

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

4.14.2 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.

4.15 **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.

5. Implementation and Monitoring

5.1 Implementation

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

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

5.2 Monitoring

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

6. References

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

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

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

COBIT5 for Risk, ISACA (2013)

Home Office Risk Management Policy and Guidance, Home Office (2011)

NHS Audit Committee Handbook, Department of Health (2011)

Risk Management Assessment Framework, HM Treasury (2009)

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

The Orange Book (Management of Risk Principles and Concepts), HM Treasury (2004)

UK Corporate Governance Code, Financial Reporting Council (2010)

Understanding and Articulating Risk Appetite, KPMG, (2008)

7. Associated Policy and Procedural Documentation

Health and Safety Policy

Project Management Policy

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.	Corporate Risk Lead	- DCA Governance Group	Monthly review of Risks on Datix®	6 months
2. Assessing Risk – All Risks will be scored and graded according to likelihood and consequence using the Trust's Risk Assessment Matrix.	Corporate Risk Lead	- Deputy Foundation Secretary	Monthly review of Risks on Datix®	Monthly
3. Managing Risk - New Operational Risks with a Current Score of 15 and above will be presented to the appropriate Executive or Divisional Management Team for approval within 1 month of being reported on Datix®.	Corporate Risk Lead	- Deputy Foundation Secretary - Risk Forum	Monthly review of Risks on Datix®	Monthly
4. Managing Risk - New Operational Risks with a Current Score of 12 and below will take a maximum of 3 months to proceed from the initial submission to approval onto the Risk Register.	Corporate Risk Lead	- Deputy Foundation Secretary - Risk Forum	Monthly review of Risks on Datix®	Monthly
5. Reviewing Risk - All Risks with a Current Score of 15 (Red) or above must be reviewed each month.	Corporate Risk Lead	- Deputy Foundation Secretary - Risk Forum	Monthly review of Risks on Datix®	Monthly

6. Reviewing Risk - All Risks with a Current Score of 12 or below (Amber and Green) will be reviewed each quarter.	Corporate Risk Lead	- Deputy Foundation Secretary - Risk Forum	Monthly review of Risks on Datix®	Monthly
7. 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	- Deputy Foundation Secretary - Risk Forum	Monthly review of Risks on Datix®	Monthly
8. Reviewing Risk - Any Risk that has been accepted is reviewed 6 monthly	Corporate Risk Lead	- Deputy Foundation Secretary - Risk Forum	Monthly review of Risks on Datix®	6 monthly
9. 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	Quarterly
10. 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 to a Divisional or Executive owner for consideration.	Corporate Risk Lead	- Deputy Foundation Secretary - DCA Governance Group	Monthly review of Risks on Datix®	Monthly
11. Risk Management Process – review of Trust's process undertaken by Internal Audit.	Deputy Foundation Secretary	- Audit Committee	Internal Audit review	Annual

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 be 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 be 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 for 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.
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.

Risk Category	Insignificant 1	Minor 2	Moderate 3	Severe 4	Catastrophic 5
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 service or interruption of 1-8 hours. - There is absolute certainty that no adverse effect can arise even when a data breach may occur.	- Potential loss of service or interruption of 8-12 hours. - Potentially some minor adverse effect even if no adverse effect may occur.	- Potential loss of service or interruption of 12-24 hours. - Potentially some adverse effect from a data breach e.g. embarrassment from release of information into the public domain.	- Potential loss of service or interruption of 1-7 days. - Potentially pain and suffering/ financial loss from a data breach	- Potential loss of service or interruption of >1 week - Potential for a catastrophic event or death as a result of a data breach.
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 - Board of Directors Risk Appetite Statement

The Board of Directors expects the Trust's management to identify risks that may impact on the achievement of objectives. The Risk Appetite Statement clarifies the level of such risk that is acceptable to the Board and translates this into an acceptable risk scores (their tolerance) that allow a freedom for managers to use their discretion when they implement controls to manage risk.

The acceptable levels of risk are explained as follows:

Risk Appetite	What this means
No Appetite	The Board is not prepared to accept uncertainty of outcomes at this level.
Low Appetite	The Board accepts that a low level of uncertainty exists but expects that risks are managed to a level that may not substantially impede the ability to achieve objectives.
Moderate Appetite	The Board accepts a moderate level of uncertainty but expects that risks are managed to a level that may only delay or disrupt achievement of objectives, but will not stop their progress.
High Appetite	The Board accepts a high level of uncertainty and expects that risks may only be managed to a level that may significantly impede the ability to achieve objectives.

Risks at an operational level will be considered under the following categories:

- Quality
- Regulation and Compliance
- Reputation
- People and Resource
- Information and Communication Technology
- Finance and Efficiency
- Health and Safety

Each category of risk may have various sub-categories, for instance Quality risks may be risks relating to safety, effectiveness or patient experience.

Acceptable risk scores are based on the Trust's Risk assessment matrix and the Board has specified the maximum acceptable target scores for each sub-category of risk.

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.

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. 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.