Heart of England NHS
NHS Foundation Trust

Building healthier lives

Risk Management Strategy and Policy v6.0

Document reference:	POL 038
Document Type:	Policy
Version:	6.0
Purpose:	• Provides detail regarding the Risk Management Strategy within the Trust • Outlines the risk management cycle to be used for the management of Trust risks • Defines risk types and escalation processes • Defines roles and responsibilities of all staff in relation to risk identification, management and review
Responsible Directorate:	Safety and Governance
Executive Sponsor:	David Burbridge, Director of Corporate Affairs
Document Author:	Head of Risk and Compliance
Approved by:	Chief Executive or Board of Directors
Date Ratified:	24/07/2017
Review Date:	24/07/2020
Related Controlled documents	Incident Reporting and Management Policy & Procedure Clinical Audit Policy Patient Complaints Policy & Procedure Claims Management Policy Health and Safety Policy Being Open Policy Datix risk module user guide Privacy Impact Assessments
Relevant External Standards/ Legislation	• Care Quality Commission • NHS Improvement • Health & Safety at Work Acts
Target Audience:	All staff involved in Risk management
Further information:	Head of Risk and Compliance

Paper Copies of this Document

If you are reading a printed copy of this document you should check the Trust's Policy website (http://sharepoint/policies) to ensure that you are using the most current version.

Version History:

Version	Status	Date	Consultee	Comments
5.0	Approved	July 2015	Quality Committee	No comments received from committee
6.0	Draft	May 2017	General consultation	

Summary of changes from last version:

- Includes strategic risk
- Provides updated listing of definitions including Trust risk register
- Includes details of Assurance route
- Clarifies approval and escalation of risk
- Clarifies new roles and responsibilities

Table of Contents

1 Strategy Statement

In pursuit of its strategic objectives the Trust is committed to:

- Adopting best practice in the identification, evaluation and cost effective control of risk to ensure that they are reduced to an acceptable level or eliminated as far as is reasonably practicable;
- Maximising opportunities to achieve the Trust's objectives and deliver a cost effective, high quality health service.

The Trust's strategic aim is to make the effective management of risk an integral part of everyday management practice. This is achieved by having a comprehensive and cohesive risk management system in place which is underpinned by clear responsibility and accountability arrangements throughout the organisational structure of the Trust. These arrangements are set out in more detail in the Trust's Financial Instructions, Standing Orders and Chief Executive's Scheme of Delegation and Accountability.

The Trust takes a holistic approach to risk management incorporating both clinical and non-clinical risks. The risk management strategy is integrated into the achievement of the Trust's business objectives and will in turn support the Trust's strategic plan. The aims and objectives are developed with consideration of the assurance framework and risk register which reflect internal and external threats that may impact on finance, strategy, operations, compliance, environment and reputation.

The Trust has the following key risk management objectives:

- To minimise the potential for harm to patients, staff and visitors to a level as low as is reasonably practicable.
- To protect everything of value.
- To anticipate and respond to changing circumstances and events.
- To maximise opportunity by adapting and remaining resilient to changing risk factors.
- To ensure that risk management is clearly and consistently integrated into the Trust as a whole.
- To consider compliance with health and safety, insurance and legal and other statutory requirements as a minimum standard.
- To inform policy and operational decisions by identifying risks and their likely impact.
- To continually raise awareness of the need for risk management by all those connected with the Trust's delivery of service.

These objectives will be achieved by:

- Clearly defining roles, responsibilities and reporting lines within the Trust for risk management.
- Including potential risk discussion when writing reports and considering decisions.
- Continuing to demonstrate the application of risk management principles in all activities of the Trust.
- Reinforcing the importance of effective risk management as part of the everyday work of all staff employed or engaged by the Trust.
- Maintaining a comprehensive register of risks (clinical and non-clinical) and reviewing this on a regular basis.
- Ensuring effective controls are in place to mitigate risk and they are understood by those expected to apply them.
- Ensuring gaps in control are rectified and assurances are reviewed and acted upon in a timely manner.
- Maintaining documented procedures of the control of risk and provision of suitable information, training and supervision.
- Maintaining an appropriate system for recording health and safety incidents and identifying preventative measures against recurrence.
- Preparing contingency plans to secure business continuity where there is potential for an event to have a major impact upon the Trust's ability to function.
- Monitoring risk management arrangements and seeking continuous improvement.

2 Policy Statement

This policy is applicable to all staff employed by The Trust. It is essential reading for all directors, senior managers and department heads.

This policy aims to:

- Enable the Trust to take all reasonable and appropriate steps in the management of risk in order to protect patients, staff, the public, its assets and reputation.
- Enable the Trust to meet its statutory, regulatory and legal obligations.
- Deliver the highest quality of care within the available resources.
- Provide a standardised, systematic mechanism to identify, assess, manage and review risks across the organisation, principally through the development and maintenance of risk registers.
- Offer staff appropriate training and support in the principles and practice of risk assessment and management.
- Provide assurance to the Board of Directors regarding the robust implementation of the Risk Management Policy.

3 Scope

Includes:

This policy applies to the management of clinical, non-clinical and strategic risks within the Trust. It also applies to all individuals employed by the Trust including contractors, volunteers, students, locums and agency staff and staff employed on honorary contracts.

Excludes:

- This policy excludes the management of individual patient specific risk assessments (for example Falls and Waterlow score).
- Project risks.
- Quality Impact risk Assessments in relation to Cost Improvement Programmes.

There are separate policies that detail the management of risks excluded from the scope of this policy.

4 Definitions

For the purpose of this policy, the following definitions apply:

Clinical risk A risk to patients/patient care

Control The mitigating action that is implemented to reduce the likelihood or consequence of a risk occurring. Controls should be monitored to provide assurance that they continue to mitigate risk to an acceptable level.

Corporate risk register A register of risks from clinical and non-clinical directorates where the current score is 15, 16, 20 or 25 (Red). Together with the strategic risk register this constitutes the trust risk register

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 should 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. Issues should be captured on an issue log and managed in a timely manner.

Non-clinical Risk A risk other than a clinical risk.

Risk A risk is a future uncertain event or set of events that, should it 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 The amount of risk the organistion, division or directorate 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 lead The member of staff responsible within each directorate for the day to day administration of risk management procedures. See also risk owner.

Risk level After a risk has been assessed it may be categorised under one of four levels, they are:

Red risk – the highest level of risk within the Trust with a current score of 15, 16, 20 or 25
Amber risk – a moderate level risk with a current score of 9, 10 or 12
Yellow risk – a low level risk with a current score of 4, 5, 6 or 8
Green risk – a very low level risk with a current score of 1, 2 or 3.

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 assessment and management are ongoing dynamic processes that should form part of everyday management activity. Risk should be managed so far as is reasonably practical.

Risk owner The member of staff responsible for the management of individual risks. See also risk lead

Risk proximity The estimate of the timescale as to when the risk is likely to occur. It 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 should 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 development and maintenance of a 'live' risk register is an integral element of good risk management practice. The Trust uses the Datix Risk Management System to support this.

Strategic risk A risk that may threaten the strategic objectives of the Trust. This type of risk should 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.

Trust risk register The risk register that includes risks on both the Corporate and Strategic risk registers

5 Policy Framework

5.1 Risk Assessments and Management

All staff should follow the standardised approach to risk assessment and risk management as outlined within the procedure attached to this policy at Appendix B.

All directorates and departments will maintain a register of the risks in Datix which may impact on their objectives and the quality of the services that they provide.

5.2 Risk Identification

Risks will be identified from a wide range of internal and external sources as outlined in Appendix C.

5.3 Risk Scoring and Grading

All risks will be scored and graded according to likelihood and consequence using the Trust's risk assessment matrix at Appendix D.

5.4 Risk review and escalation

All risks will be reviewed and updated, as a minimum, on a quarterly basis.

Risks scoring 15 and above will be reviewed on a monthly basis by the risk owner and progress in the mitigation of the risk will be recorded.

New risks with a current score of 15 and above will be presented to the appropriate Executive or Divisional Management Team for approval.

Where a risk is approved as red (15 or above) it will be reported on the Corporate Risk Register which is presented to the Executive Team and Board of Directors.

When a risk reaches its target score it will be reviewed with a view to closing the risk.

Risks will be escalated from ward to Board according to the level of risk identified, to ensure effective and timely management of risks to the organisation. This process is outlined in the procedure attached to this policy at Appendix B.

Any risk recorded on a register for a period (lifespan) of more than 24 months will be escalated to the Divisional/Executive lead to confirm whether the assessment is still valid and the management is active.

5.5 Risk Action Plans

All risks should have a robust (SMART) action plan outlining the actions appropriate for the management and mitigation of the risk. This process is outlined in procedure attached to this policy at Appendix B.

6 Assurance

The Board needs to be aware of the current state of progress with regard to its strategic objectives (as detailed on page 4 of this document) including threats to achievement (risk), controls that have been put in place and actions that are planned.

The resource of the Board 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 requires regular assurance that the Trust is working to achieve strategic objectives in the expected way with the expected outcomes. This arrangement is formalised in the signing of the Annual Governance Statement which, as the Good Governance Institute (2014) explains, will allow the Board:

"to state that they are properly informed about the controls in place to support achievement of strategic objectives; the actual performance against strategic objectives; and the totality of their risks, as well as how they impact on the achievement of strategic objectives."

Assurance can come from many sources within the Trust. A framework for helping to identify and understand the different contributions the various sources can provide is described in the Three Lines of Assurance Model as follows:

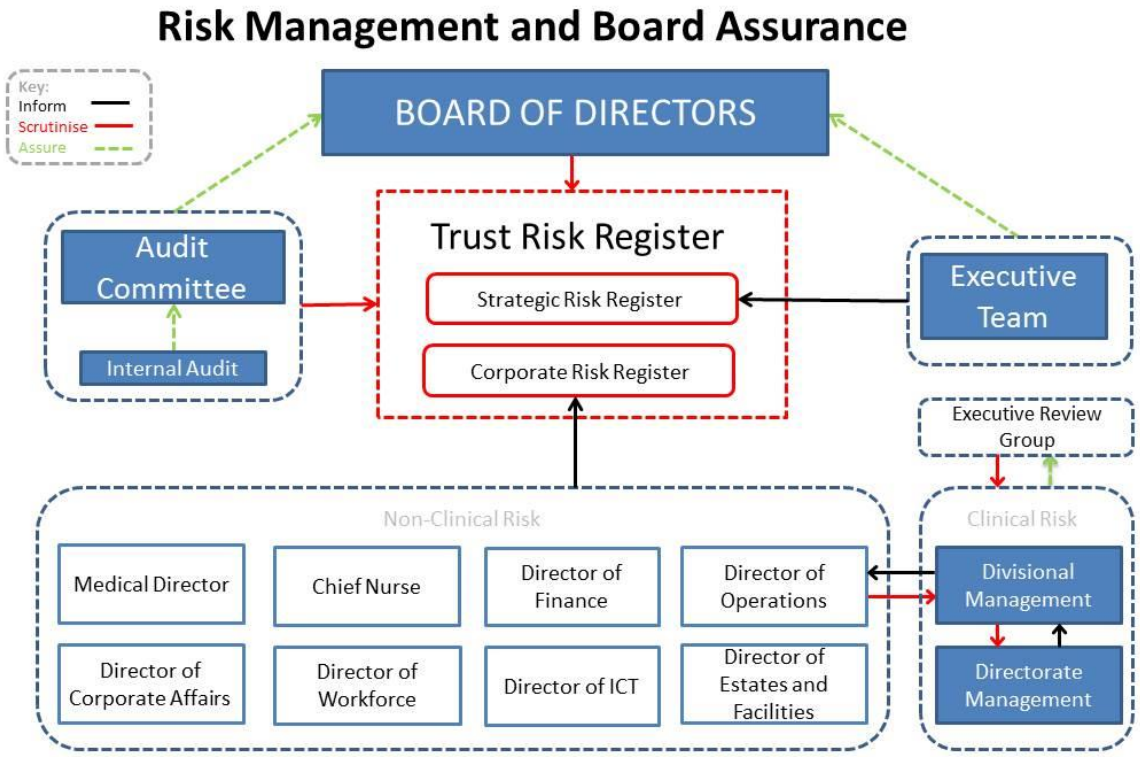
Assurance level	Assurance source
Level 1 – Functions that own and manage risk. Generally the operational areas who identify, assesses, control, and mitigate risks.	This comes direct from those responsible for delivering specific objectives or operations; it provides assurance that performance is monitored, risks identified and addressed and objectives are being achieved. By its nature this type of assurance may be subjective, but its value is that it comes from those who know the business, culture and day-to-day challenges.
Level 2 – Functions that oversee risk. Associated with oversight of management activity but separate from those responsible for delivery, but not independent of the Trust's management.	The assurance provides valuable management insight into how well work is being carried out in line with set expectations and policy or regulatory considerations. It will be distinct from and more objective than first level assurance.
Level 3 – Functions that provide independent assurance. Generally the role of internal audit, but may be provided by regulators or other external bodies.	Independent of the first and second levels of assurance providing a more objective opinion.

The Board should 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. Knowing that assurance has been subject to different levels of scrutiny should 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.

The sum of assurances received by the Board constitutes the Board Assurance Framework. The Audit Committee Handbook (2005) identified this as:

"the key source of evidence that links strategic objectives to risks and assurances, and the main tool that the Board should use in discharging its overall responsibility for internal control".

The following diagram (Risk Management and Board Assurance) shows how this process is enacted within the Trust.



7 Training Requirements

Training and support on principles and practices of risk management will be available to staff as required. Further detail can be found in the risk management training needs analysis.

It is the responsibility of risk leads to identify and support the training needs of all staff involved in the risk management process.

The Governance teams will advise and support individuals, where required, in relation to risk management. Further information on the training that is available is in the Trust's risk management training needs analysis.

8 Individual Responsibilities

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. Some staff have specific responsibilities, they are:

8.1 Chief Executive

The Chief Executive (CEO), as accountable officer, has overall accountability for the Trust's risk management framework and ensuring that this operates effectively. The CEO must take 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.

8.2 Director of Corporate Affairs

The Director of Corporate Affairs (DoCA) is responsible to the Trust Board and Chief Executive in relation to risk management and will provide regular reports to the Trust Board in this regard. The DoCA is also responsible for providing expert advice to the Trust Board in relation to risk management and ensuring the Trust Board has access to regular and appropriate risk management information, advice, support and training where required. The DoCA will be assisted in their role by Executive colleagues and the Head of Risk and Compliance.

The DoCA is designated as the Trust's Senior Information Risk Officer (SIRO), providing assurance to the Trust Board in an annual report on the management of information risk.

8.3 Director of Operations

The Director of Operations (DOP) is responsible for providing assurance to the Executive Team and Board of Directors on the management of clinical risk on the Corporate Risk register. In doing this the DOP will review the current score, controls and actions to mitigate red risks escalated by Divisional management Teams.

8.4 Executive Directors

All Executive Directors (ED) are responsible for overseeing a programme of risk management activities for their directorates and areas of responsibility, in accordance with this policy. This will include the consideration of risk for inclusion on the Trust's Strategic Risk Register and approval of red risks as appropriate.

8.5 Divisional Management Teams

The Divisional management teams have day to day accountability for the identification, management and review of all risks relating to their division. They are responsible for:

- Ensuring that risk management processes are in place and functioning properly within the Directorates under their management.
- Validate risks owned by directorates under their management that have a current score of less than 15.
- Authorise risks owned by directorates under their management that have a current score of more than or equal to 15.
- Review of risks that are more than 2 years old to confirm their validity.
- Communicate with other divisional teams where risks may impact or require action across these boundaries.

8.6 Directorate Management Teams

All Directorate management teams (clinical and non-clinical) have day to day responsibility for the identification, management, review and escalation of all risks that fall within their areas of responsibility. They have responsibility for:

- Ensuring appropriate governance and risk management arrangements are in place within their directorates which enables communication, monitoring and learning from risks.
- 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.
- Ensuring appropriate prioritisation and allocation of resources to most effectively mitigate these risks.

8.7 Head of Risk and Compliance

The Head of Risk and Compliance is responsible to the Director of Corporate Affairs for the implementation of the Trust's Risk Management Policy and Procedure. This includes:

- Ensuring that the Trust's risk management framework takes account of the requirements of external regulators.
- Providing assurance to the Board with regards to the implementation of this policy.

The Head of Risk and Compliance is designated as the Trust's Deputy Senior Information Risk Officer (SIRO), supporting the DoCA and deputising as necessary.

8.8 Governance Team

The governance team will support the implementation of this policy through:

- Ensuring that clinical risks are actively managed, meeting with Directorate teams to review and administer risk registers.
- Producing a monthly risk profile for each clinical division.
- Providing risk management training to an agreed training needs analysis.
- Developing reports on the risk management system and the risks managed within it to an agreed schedule.

8.9 Health and Safety Team

The Health and Safety team are responsible for the development and implementation of an annual work plan which provides a framework to provide assurance against statutory and regulatory legislation. To enable compliance the following is in place:

- Environmental safety inspections.
- Quarterly health and safety self assessments undertaken by wards/departments throughout the Trust.

- The implementation of NHS Protect initiatives.
- Risk assessment to address the requirements of COSHH and other more specific risk assessment (see the Health and Safety Policy for further details).
- A programme of education, guidance and advice.

8.10 Corporate Risk Advisor

The Corporate Risk Advisor is responsible to The Head of Risk and Compliance for leading a programme of work to systematically identify, analyse, manage and report risk throughout the Trust. This will include:

- Working collaboratively with colleagues to develop and implement local risk management practices compliant with the requirements of the Risk Management Policy.
- Actively engaging with those who are managing risk and co-ordinating risk management activities to ensure sufficient rigour and compliance with the Trusts risk management system and the appropriate escalation of risks.
- Devising and providing risk management training to an agreed training needs analysis to ensure that the risk management system is understood and implemented effectively.
- Ensuring that non-clinical risks are actively managed, meeting with Directorate teams to review and administer risk registers.
- Developing reports on the risk management system and the risks managed within it to an agreed schedule, including an Annual Risk Management Report, the Board Assurance Framework and the Corporate Risk Register.
- Maintaining the Trust risk register.
- Monitoring compliance with the standards in the Risk Management Policy, providing assurance and escalating concerns as appropriate.

8.11 Risk Lead

Each directorate should have an identified risk lead that is responsible for:

- Ensuring that directorate staff receive information, instruction and support in their duties relating to risk management. (Risk Identification)
- Ensuring that staff within the Directorate are able to identify risks and know how to report them to the risk lead. (Risk Identification)
- Ensuring risk assessments are completed for risks identified within the directorate and documented on Datix according to the Trust's Risk Management Policy. (Risk assessment and recording)
- Ensuring that directorate staff implement their risk assessment action plans to reduce risk, according to the Trust's Risk Management Policy. (Risk management and mitigation)

- Ensuring that risks are monitored and reviewed appropriately and that the risk record is updated to reflect progress and is closed when action plans are complete. (Risk management and mitigation)
- Through scheduled Directorate meetings to report information relating to risk to the directorate management team including whether or not risks have been escalated and managed appropriately, agreed actions are taking place, and the level of risk is reducing. This information will form a part of reports that are presented at Directorate and Divisional Quality Groups. (Risk monitoring and reporting).

8.12 Risk Owner

All risks will have an identified risk owner who is responsible for ensuring that risk is managed appropriately. This includes the ongoing monitoring and scheduled review with appropriate update on Datix of the risk, ensuring controls and further actions are in place to mitigate the risk and reporting on the overall status of the risk.

9 Board, Committee and Group Responsibilities

9.1 Board of Directors

The Board is accountable for ensuring that appropriate risk management systems are in place to enable the organisation to deliver its objectives. It delegates overall responsibility for risk management to its assurance committees.

9.2 Audit Committee

The Audit Committee is responsible for monitoring and reviewing the adequacy of the Trust's internal control systems for risk management and, ensuring that these are effective and comply with national standards.

9.3 Other Groups

There are a range of other committees that play a role in the monitoring and scrutiny of risks, they include:

- Clinical Quality Monitoring Group
- Executive RCA Group
- Clinical and Professional Review Group
- Executive Review Group

9.4 Divisional Quality Groups

Divisional Quality Groups have delegated responsibility for the quality of the services that they provide. These groups are responsible for:

- Ensuring appropriate governance and risk management arrangements are in place for all directorates under their management.
- Overseeing and monitoring the management of all risks which fall within their responsibility, escalating risks where appropriate.
- Ensuring appropriate prioritisation and allocation of resources to most effectively mitigate these risks.

10 Monitoring and Compliance

See Appendix A

Appendix A: Monitoring Matrix

Standards 6.1, 6.3 and 6.4 will not be monitored as they are compulsory through the Datix risk assessment proforma.

MONITORING OF IMPLEMENTATION	MONITORING LEAD	MONITORING PROCESS	REPORTED TO PERSON/GROUP	MONITORING FREQUENCY
All directorates and departments will maintain a register of the risks in Datix which may impact on their objectives and the quality of the services that they provide.		Risk profile	-Divisional Quality Groups and Non-clinical management teams -DOps risk review	Monthly Quarterly
All risks will be reviewed and updated, as a minimum, on a quarterly basis.		Risk profile	-Divisional Quality Groups and Non-clinical management teams -DOps risk review	Monthly Quarterly
Risks will be escalated from ward to Board according to the level of risk identified, to ensure effective and timely management of risks to the organisation		Risk profile Trust risk register	- Divisional Quality Groups - Trust Board	Monthly Quarterly
Risks scoring 15 and above will be reviewed on a monthly basis by the risk owner and progress in the mitigation of the risk will be recorded		Risk profile	- Divisional Quality Groups and Non-clinical management teams -Executive Review Group	Monthly Quarterly
New risks scoring 15 and above will be presented to the appropriate Divisional Management Team or Executive Director for approval.		Risk profile	Divisional Quality Groups and Non-clinical management teams	Monthly

Where a risk is approved as red (15 or above) it will be reported on the Trust Risk Register, which is presented to Trust Board		Trust risk register	- Trust Board - Executive Review Group - CQMG	Quarterly
All risks should have a robust (SMART) action plan outlining the actions appropriate for the management and mitigation of the risk		Annual Audit	Internal audit	Annual
When a risk reaches its target score it will be reviewed with a view to closing the risk		Annual Audit	Internal audit	Annual
Any risk recorded on a register for a period (lifespan) of more than 24 months will be reviewed to confirm whether the assessment is still valid and the management is active.		Risk profile	-Divisional Quality Groups and Non-clinical management teams -DOps risk review	Monthly Quarterly

Appendix B: Risk Management Procedure

All RED risks will be reviewed each month by the risk owner and any updates in relation to current level and progress of actions will be recorded.

RED Clinical risks will be escalated to the Divisional management team for approval and then to the Director of Operations for information.

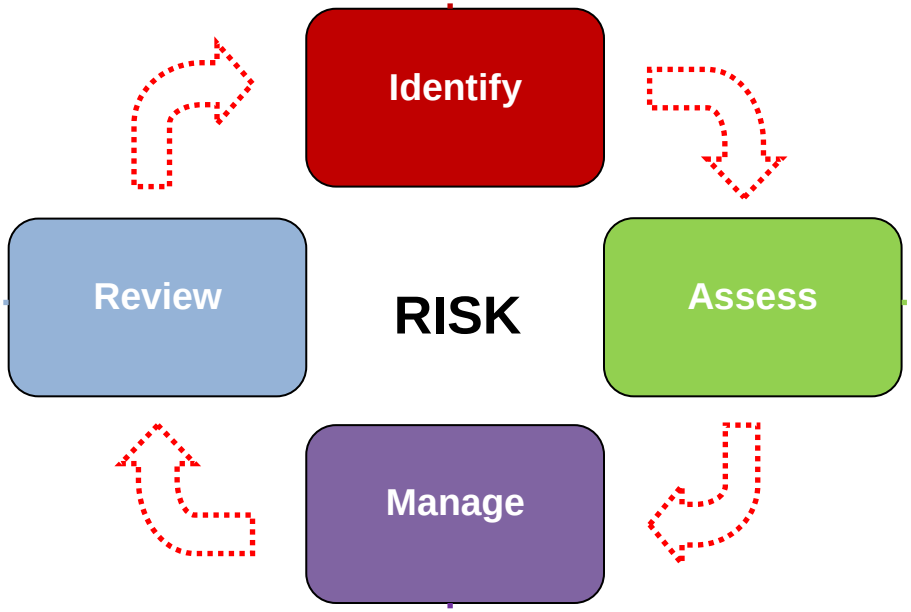
RED Non-clinical risk will be escalated to the appropriate Executive for approval.

RED clinical and non-clinical risks will form the Corporate risk register.

GREEN, YELLOW and AMBER risks will be reviewed on a quarterly basis by the owner and any updates will be recorded.

Strategic risk will be reviewed on a quarterly basis.

Risks may be identified from various sources (Appendix C provides further detail) by clinical and non-clinical Directorates. Strategic risks will be identified and managed by Executive Directors.



Risks may be managed by a Directorate (clinical or non-clinical), Division or Executive owner. Level and proximity of the risk should be considered in the monitoring of controls and development of a SMART action plan.

Assessment of risk is undertaken in terms of likelihood and consequence. This gives the risk a score and a level as follows:

GREEN: 1, 2, or 3

YELLOW 4, 5, 6, or 8

AMBER: 9, 10 or 12

RED: 15, 16, 20 or 25

A risk with a current score that is RED must be presented to the appropriate Executive for final approval.

Proximity of risk, i.e. when the risk is likely to occur, should be considered.

A target score that reflects risk appetite should also be recorded at this time.

Risks may be aggregated to inform an overarching risk assessment that is subsequently owned at a higher level.

1. Introduction

To ensure a systematic and consistent approach to risk management, the Trust uses the online Datix® Risk management system to ensure that risks are recorded, managed, escalated and reported at the appropriate organisational level consistently. A guide on how to use this system is available on the Intranet.

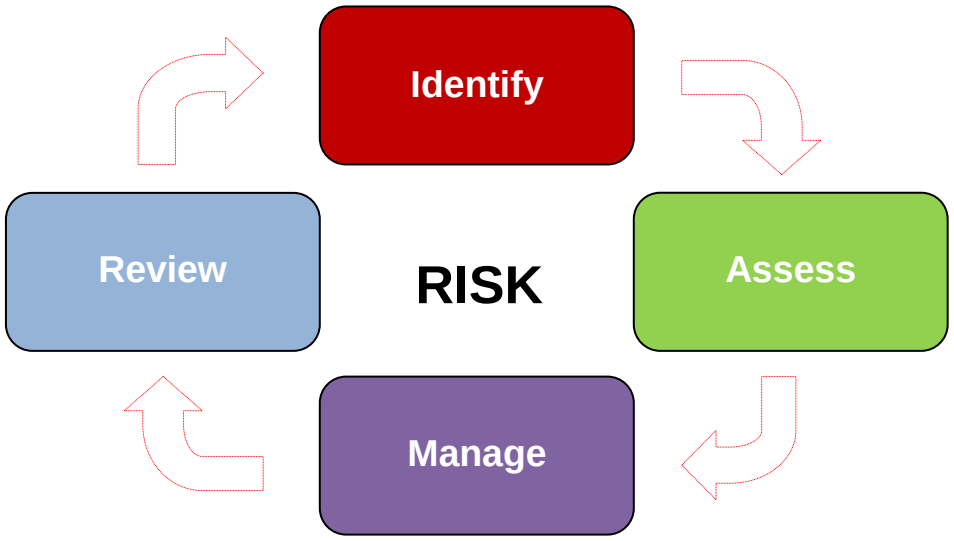
Once a risk is identified it must be documented on the Datix® risk assessment form, assessed and an action plan developed and implemented to reduce the risk to an appropriate level.

This procedure does not replace specific policies which describe the method and documentation of risk assessments for specific issues e.g. Health & Safety policy / risk of falls / waterlow etc.

2. Risk Management Cycle:

Risk assessment is the responsibility of all members of staff. Risk assessments are best undertaken as a multidisciplinary team approach and should involve staff familiar with the activity being assessed.

There are four steps to risk management:



2.1. IDENTIFY the Risk:

It is essential that the risk identification process is both wide-ranging and comprehensive. Undertaking a risk assessment can be subjective and will involve using professional judgment about what constitutes a risk.

Identifying risk involves thinking about the objectives of the service you provide and considering the following questions:

- What service do we provide?

- Who do we deliver it to?
- Who undertakes the activity?
- When do we provide the service?
- Where do we deliver the service?
- Is there any information that we have available that could threaten our ability to deliver the service?

The following are examples of the types of risk that may be considered:

Safety:
- Risks that could result in accidental death, disability or severe distress to patients and/or staff;
- Risks that could result in unintentional harm;
- Risks that may be less serious but are more frequent or could affect a large number of patients/staff.

Reputational:
- Risks that could lead to adverse publicity or affect the reputation of the Trust;
- Risks that could lead to litigation or may be the cause of a formal complaint;
- Risks that could affect the Directorate / Department or Trust in meeting corporate objectives (e.g. failure to meet service delivery targets / operational loss or delay / national requirements).

Resource:
- Risks that could result in financial loss to the Trust;
- Risks to service provision;
- Risks to equipment / buildings

Appendix C identifies common sources of internal and external information that may help to identify risks.

2.2. ASSESS the Risk:

Having identified and described the risk, the next step is to assess this risk. This allows for the risk to be assigned a rating which determines at which level the risk will be managed. Assessing risks will involve looking at:

- What is the likelihood of a risk being realised?
- What is the consequence if the risk is realised?
- What controls do we have in place to prevent a risk occurring?
- What actions have been or will be implemented to reduce the risk?
- What is the current level of risk in light of these considerations?
- What is the level of risk that we would accept once further controls have been implemented?

The Trust uses three risk scores:

- **Initial Risk Score:** This is the score when the risk is first identified and is assessed **without** existing controls in place. This score will not change for the lifetime of the risk and is used as a benchmark against which the effect of risk management will be measured.

- **Current Risk Score:** This is the score **with** existing controls in place. It is expected that the current risk score will reduce and move toward the Target Risk Score as controls are considered and action plans to mitigate the risks are developed and implemented.

- **Target Risk Score:** This is the score that is intended after the action plan has been fully implemented and should reflect the appetite of the risk owner.

Risks are assigned a score based on a combination of likelihood and consequence using the Risk Assessment Matrix at Appendix D.

Scoring a risk makes it easier to understand the directorate and/or trust-wide risk profile. It provides a systematic framework to identify the level at which risks will be managed and monitored in the organisation (see section 4 - risk escalation) and prioritise remedial action and availability of resources to address risks.

Risks are also assessed in terms of proximity i.e. when the risk would occur. Estimating when a risk would occur helps prioritise the risk. The proximity scale used is as follows:

- zero to six months;
- six to twelve months;
- twelve months plus.

2.3. MANAGE the Risk:

Once the risk has been assessed and evaluated (scored), an action plan should be developed that details how to manage the risk. This could involve changing a treatment process or introducing a safer system that can control, limit, prevent or act as a barrier to the risk.

When managing identified risks consider:

- What are the existing controls?
- Are there any gaps?
- What further controls are practical and sustainable? (Check with staff who work in the area)
- Is the design of the control right? Is it helping you achieve your objectives?
- What further actions are needed to manage the risk?

All directorates and departments need to agree a programme of actions to manage all of their identified risks.

There are a number of ways to approach this which are outlined below:

Options for Managing Risk	
Prevent	By doing things differently, once the risk has been identified, this removes the risk immediately. By implementing counter measures, where it is feasible to do so, this could prevent the threat or problem from occurring or prevent it having any impact on the activity;
Reduce:	Treat the risk. Take action to control the risk by either reducing the likelihood of the risk happening or limiting the impact it will have on the activity;
Transfer	If you cannot manage the risk, it may be appropriate to transfer it to someone who can (with their knowledge and agreement) e.g. another Trust or Department.
Accept	If the risk is small, cannot be reduced, avoided or otherwise transferred, you may choose to accept the risk and prepare a contingency plan. Using the online Datix® risk management system, document an action plan for each risk you have identified. Actions will need to be monitored on a regular basis.

For each action plan ensure that you:

- Record any actions that are needed to manage the risk indicating the agreed time scale for each action;
- Ensure a designated person is chosen to take responsibility for managing the risk and signs up to the action plan.

Each action identified should be SMART:

- **S**pecific
- **M**easurable
- **A**chievable
- **R**ealistic
- **T**imely

Action plans must be appropriate and clearly show how they mitigate the level of the current risk to achieve the target.

2.4. REVIEW the Risk

It is the responsibility of the directorate / department to regularly review progress with risks to ensure:

- New risks are identified and controlled;
- Control measures are in place and effective;
- New systems, procedures and processes have not created new risks;
- Possible / actual weaknesses are highlighted and rectified.

Risks registered on Datix® must specify when the action plan, current risk score, and target risk score will be reviewed. It is expected that as action plans are progressed the current risk score will move towards the target risk score and may be closed (if the risk has been eliminated) or tolerated (if the risk remains but all planned mitigating action has been taken). This may be achieved within one review period but it may take longer, in which case a new review date must be set. **All green, yellow and amber risks must be reviewed at least once quarterly. All red risks must be reviewed on a monthly basis.**

3.5 CLOSE the Risk:

Risks that are reduced to the target level will only be closed on the risk register when the relevant management team is satisfied that the risk has been managed to an acceptable position. When closing a risk, the author will be required to state the rationale for closing the risk.

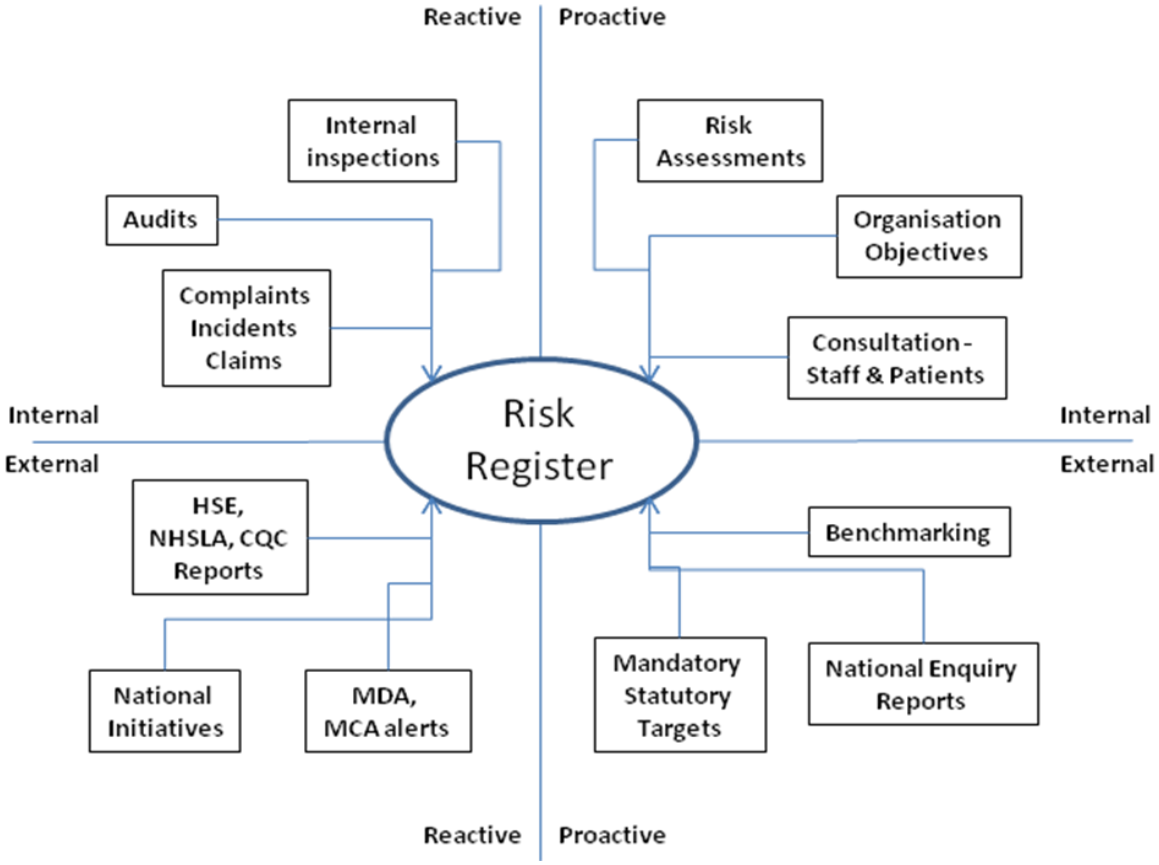
4. Escalation of Risk:

An integral part of effective risk management is ensuring that risks are escalated within the Trust in line with the relevant governance structure. This will ensure that appropriate action and prioritisation of resources can take place.

Risks are escalated according to their current risk score. This is summarised as follows:

Level	Score	Impact	Escalation
Green	1, 2 or 3	Very Low	• Green risks should be managed locally by the relevant risk owner. • The progress with managing these risks should be reviewed quarterly (at a minimum) by the directorate.
Yellow	4, 5, 6 or 8	Low	• Yellow risks should be managed locally by the relevant risk owner • The progress with managing these risks should be reviewed quarterly (at a minimum) by the directorate
Amber	9, 10 or 12	Moderate	• Amber risks should be reviewed **quarterly** by the directorate management team. • Amber risks should be reported to the division who will consider whether they should be escalated • Non clinical risks should be discussed by the non-clinical management teams.
Red	15, 16, 20 or 25	High	• New Red risks should be reported immediately to the appropriate member of the Governance team. • They will be approved by the relevant Divisional Management Team before being presented to the Director of Operations (DOP) for information. • Where red risks are approved by the Division they will be included on the Corporate risk register. • Red risks should be reviewed monthly by the directorate and Divisional management team.

Appendix C: Common sources of information for Risk Identification (including Privacy Impact Assessments)



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.

Details regarding the PIA process can be found on the Trust's Information Governance Sharepoint site via the following link

Appendix D: Risk Assessment Matrix

Table 1: Measurement of likelihood

Level	Descriptor	Probability	Description
1	Rare	<1%	The incident may occur only in exceptional circumstances
2	Unlikely	1-5%	The incident is not expected to happen but may occur in some circumstances
3	Possible	6-20%	The incident may happen occasionally
4	Likely	21-50%	The incident is likely to occur, but is not a persistent issue
5	Almost Certain	> 50%	The incident will probably occur on many occasions and is a persistent issue

Table 2: Measurement of consequence – Table on next page expands the risk descriptors

Level	Descriptor	Description
1	Insignificant	No injury or adverse outcome; First aid treatment; Low financial loss
2	Minor	Short term injury/damage (e.g. resolves in a month); a number of people are involved
3	Moderate	Semi-permanent injury (e.g. takes up to year to resolve)
4	Major	Permanent injury; major defects in plant, equipment, drugs or devises; the incident or individual involved may have a high media profile
5	Catastrophic	Death

Table 3 Assessment Matrix: The risk factor = likelihood x consequence

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

The table below should be used as guidance is assessing the potential consequence of risk.
Source: NPSA Guidance for Risk Managers

	1	2	3	4	5
Risk type	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Safety	Minimal injury requiring no/minimal intervention or treatment. No time off work required	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.	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 deaths. Multiple permanent injuries or irreversible health effects. An event which impacts on a large number of patients
Quality, Complaints or audit	Peripheral element of treatment or service sub-optimal Informal complaint/inquiry	Overall treatment or service sub-optimal. Formal complaint (stage 1) Local resolution Single failure to meet internal standards. Minor implications for patient safety or lower performance rating if unresolved	Significantly reduced effectiveness. Formal complaint (stage 2). 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	Incident leading to totally unacceptable level or quality of treatment/service. Gross failure of patient safety if findings not acted on. Inquest/ ombudsman inquiry Gross failure to meet national standards
Human resources/ organisational Development staffing competence	Short-term low staffing level that temporarily reduces service quality (<1 day)	Low staffing level that reduces service quality	Late delivery of key objective/ service due to lack of staff. Unsafe staffing level or competence (>1day). 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 attendance for mandatory 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 on an ongoing basis.
Statutory duty/ inspections	No or minimal impact or breech of guidance/ statutory duty	Breech of statutory legislation. 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. Total loss of public confidence
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 and £1 million. Purchasers failing to pay on time	Non-delivery of key objective/loss of >1 per cent of budget. Failure to meet specification/ slippage Loss of contract/ payment by results Claim(s) >£1 m
Service or 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