Risk Management Policy and Procedure v5.0

Key Points

- 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

Key changes:

- Review of committee and individual responsibilities in line with the new Trust structure.
- Clarification of Directorate, Divisional and Corporate risks
- Clarification of risk proximity and risk appetite

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.

Ratified Date: 31/07/15
Ratified By: Quality Committee
Review Date: 31/07/18
Accountable Directorate: Corporate Nursing
Corresponding Author: Deputy Director of Governance

Meta Data

Document Title:	Risk Management Policy and Procedure v5.0
Status	Approved
Document Author:	Deputy Director of Governance
Source Directorate:	Corporate Nursing
Date Of Release:	31/07/15
Ratification Date:	31/07/15
Ratified by:	Quality Committee
Review Date:	31/07/18
Related documents	Risk Management Strategy Incident Reporting and Management Policy & Procedure Clinical Audit Policy Customer Relations and Complaints Policy & Procedure Claims Management Policy Health and Safety Policy Being Open Policy Datix risk module user guide
Superseded documents	Risk Management Policy and Procedures v4.0
Relevant External Standards/ Legislation	• Care Quality Commission • Monitor, Compliance Framework • Health & Safety at Work Acts
Stored Centrally:	Trust Intranet
Key Words	Risk; Register; Mitigation

Revision History

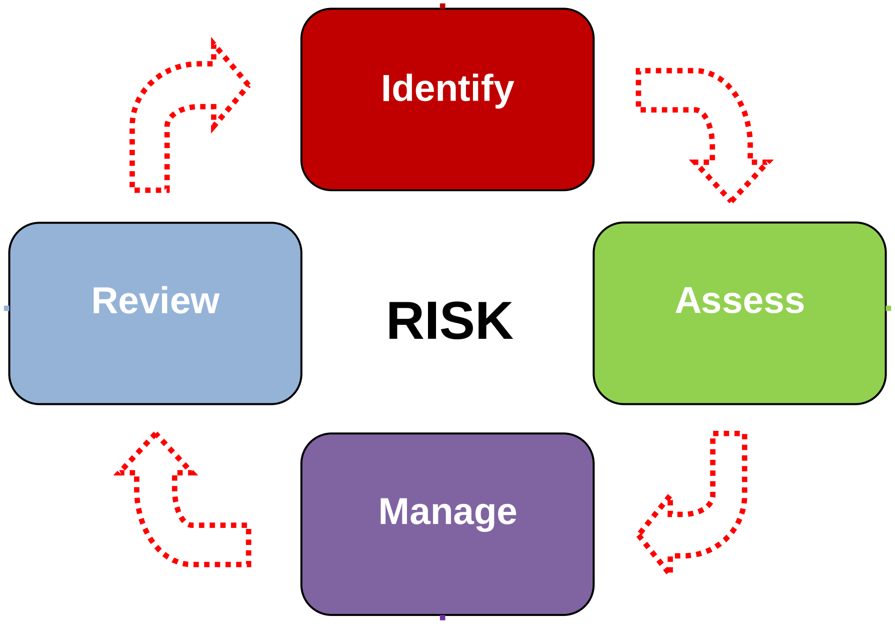
Version	Status	Date	Consultee	Comments	Action from Comment
4.1	Draft	May 2015	Governance and compliance teams	Amendments following meeting to review 6th May 2015	Update draft
4.2	Draft	June 2015	Governance and compliance teams	Revise procedure and definitions	Update draft
4.3	Draft	June 2015	Governance and compliance teams	Role of Divisional Managemnet Team. Incorporate final comments	Update draft
4.4	Draft	July 2015	Deloittes	Quality assurance Clarify divisional responsibilities Update monitoring section	Update draft
5.0	Approved	July 2015	Quality Committee	No comments received from committee	Publish revised policy

Table of Contents

1 Circulation 5
2 Scope 5
3 Definitions 5
4 Reason for Development 6
5 Aims and Objectives 7
6 Standards 7
7 Responsibilities 8
7.1 Individual responsibilities 8
7.2 Board and Committee Responsibilities 10
8 Training Requirements 11
9 Monitoring and Compliance 12
Attachment 1: Risk Management Procedure 13
Attachment 2: Common sources of information for Risk Identification. 19
Attachment 3: Risk Assessment Matrix 20
Attachment 4: Ratification Checklist 21
Attachment 5: Equality and Diversity - Policy Screening Checklist 23
Attachment 6: Launch and Implementation Plan 25

HEFT Risk Assessment and Escalation Process

Risks may be identified from a number of clinical and non clinical sources (att 2 provides further detail). Risks are also identified in terms of the threat that they present to DIRECTORATE, DIVISIONAL or CORPORATE objectives.



Assessment of risk is undertaken in terms of likelihood and consequence. This gives the risk an initial 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 new risk assessed as RED must be presented to the Executive Risk Group for final approval.

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

A target score should also be recorded at this time.

Risks may be aggregated to inform an overarching risk assessment that subsequently has a DIVISIONAL or CORPORATE owner.

Risks may be managed by a DIRECTORATE, DIVISION or CORPORATE owner. Level and proximity of the risk should be considered in the development of a SMART action plan and to inform the prioritisation of actions.

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

RED DIRECTORATE risks will be escalated to the DIVISIONAL management team for review.

RED DIRECTORATE and DIVISIONAL risks will be escalated to the Executive Risk Group.

RED CORPORATE risks wil be escalated to the Executive Risk Group.

GREEN, YELLOW and AMBER risks will be reviewed on a quarterly basis by the owner and any updates in relation to current level and progress of actions recorded on the risk record.

1 Circulation

This policy is applicable to all staff employed by Heart of England NHS Foundation Trust (HEFT). It is essential reading for all directors, senior managers and department heads.

2 Scope

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

Excludes:

- This policy excludes the management of individual patient specific risk assessments (for example falls risk and Waterlow score).
- Strategic risks.
- 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.

3 Definitions

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

Control
The mitigating action intended to reduce the potential of likelihood or impact of the risk occurring.

Corporate Risk
A risk that may threaten the objectives of the Trust. This type of risk should be owned by a member of the executive team.

Directorate Risk
A risk that may threaten the objectives of a Directorate . This type of risk should be owned by a member of the directorate management team

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.

Issue
An issue can be defined as 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.

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.

Risk assessment:
Risk assessment is the process, by which an individual or an organisation identifies, assesses and prioritises risks and, where appropriate, identifies additional controls and actions that will reduce the risk to a level which can be accepted.

Risk lead
The member of staff responsible within each directorate for the day to day administration of risk management procedures.

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 grading of 15, 16, 20 or 25
- Amber risk – a moderate level risk with a grading of 9, 10 or 12
- Yellow risk – a low level risk with a grading of 4, 5, 6 or 8
- Green risk – a very low level risk with a grading 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.

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.

4 Reason for Development

This policy has been developed to:

- Provide a framework to ensure the provision of safe, quality care, for patients, staff, and the public through the effective assessment and management of risks.

- Support the delivery of the Trust's risk management strategy and defines how the Trust will achieve this through a structured approach to risk assessment and management.
- Provide assurance to the Board regarding the effectiveness of the Risk Management process in order to enable it to make effective strategic and operational decisions.

5 Aims and Objectives

The aims and objectives of this policy are to:

5.1 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.

5.2 Enable the Trust to meet its statutory, regulatory and legal obligations.

5.3 Deliver the highest quality of care within the available resources.

5.4 Provide a standardised, systematic mechanism to identify, assess, manage and review risks across the organisation, principally through the development and maintenance of risk registers.

5.5 Offer staff appropriate training and support in the principles and practice of risk assessment and management.

5.6 Provide assurance to the Board (via the Quality Committee) regarding the robust implementation of the Risk Management Policy.

6 Standards

6.1 All staff should follow the standardised approach to risk assessment and risk management as outlined within the procedure attached to this policy (**Attachment 1**).

6.2 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.

6.3 Risks will be identified from a wide range of internal and external sources as outlined in the risk management procedure (**Attachment 2**).

6.4 All risks will be scored and graded according to likelihood and consequence using the Trust's risk assessment matrix (**Attachment 3**).

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

6.6 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 more detail in **Attachment 1**.

6.7 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.

6.8 New risks scoring 15 and above will be presented to the Executive Risk Group (ERG) for approval. Where the risk is not approved as red then the ERG will decide the current score of the risk.

6.9 Where a risk is approved as red (15 or above) it will be reported on the Safety SITREP[1], which is presented to Quality Committee and Trust Board.

[1] Safety SITREP is a management report that includes a summary of red and amber risks.

6.10 All risks should have a robust (SMART) action plan outlining the actions appropriate for the management and mitigation of the risk. **Attachment 1** provides further detail.

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

6.12 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.

7 Responsibilities

7.1 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:

Chief Executive

The Chief Executive (CEO), as accountable officer, has overall accountability for the Trust's risk management programme 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 Chief Nurse.

Chief Nurse

The Chief Nurse (CN) 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 CN 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 CN will be assisted in their role by Executive colleagues and the Deputy Director of Governance.

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.

Divisional Management Teams

The Trust's 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.

- The review of all new red risks proposed by directorates under their management before they are presented to ERG.

- Authorising the current score of any risk owned by directorates under their management through scheduled review.

Directorate Management Teams

Directorate management teams have day to day accountability for the identification, management, review and escalation of all risks that fall within their areas of responsibility. They have responsibility for establishing local arrangements which enable the appropriate communication, monitoring and learning from risks. They are responsible for ensuring that risks are escalated, where appropriate through divisional governance structures via the appropriate divisional quality group.

Deputy Director of Governance
The Deputy Director of Governance is responsible to the Chief Nurse for the implementation of the Trust's Risk Management Policy and Procedure. This inlcudes:

- 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

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

- Providing advice on risk assessment, scoring, mitigation, and risk escalation.
- Monitoring progress of actions to mitigate all risks.
- Development and maintenance of reporting processes to divisional quality groups.
- Provision of training or individual support as required or requested by directorates.
- Implementation and monitoring of this policy.
- Undertaking periodic risk assessment audits and quality improvement programmes.

Health and Safety Team
The H&S team are responsible for the development and implementation of an annual work plan which provides a framework to enable:

- Environmental safety inspections
- 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

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).

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

7.2 Board and Committee Responsibilities

Trust Board
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.

Quality Committee
The Quality Committee is responsible for overseeing the implementation of the risk management strategy and policy as part of the Trust's assurance framework. It is responsible for advising and providing assurance to the Trust Board on all aspects of risk and ensuring effective mechanisms are in place to manage these risks.

Executive Risk Group (ERG)
The purpose of the Executive Risk Group is to have overall responsibility for establishing a strategic approach to risk management across the organisation, ensuring that the approach is pro-active.

The role of the ERG is to provide the Board, via appropriate assurance committees, with assurance regarding the implementation of the Trust's risk management processes and highlighting to them any areas where this is not happening. The group will maintain oversight of risk in the Trust, reviewing the effectiveness of the risk management policy, ensuring that staff are aware of their risk identification and management responsibilities, escalating key risks to the appropriate assurance committee and reviewing the integrity of the risk management arrangements within the Trust.

ERG is responsible for approving all red risks.The group is also responsible for the overall co-ordination of risk management activity. It is also a forum for discussing emerging issues and risks to assess any early mitigation opportunities and identify any Trust-wide themes.

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.

Safety Committee
The Safety Committee has particular responsibility for:

- Continued, implementation and monitoring of the Health and Safety programmes;
- Receiving reports from Trust assurance groups with a specific responsibility for particular risks as detailed in the committee terms of reference.

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.

Corporate Directorates
Corporate (non clinical) directorates have delegated responsibility for the quality of the services that they provide. These directorates are responsible for:

- Ensuring appropriate governance and risk management arrangements are in place within their directorates
- 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.

8 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 which is available on the Trust’s intranet.

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.

9 Monitoring and Compliance

Standard	Monitoring Method	Frequency	Monitoring Committee
1 All staff should follow the standardised approach to risk assessment and risk management as outlined within the procedure attached to this policy	Compulsory through electronic risk assessment proforma		
2 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	Quarterly	ERG Divisional Quality Groups
3 Risks will be identified from a wide range of internal and external sources as outlined in the risk management procedure	Compulsory through electronic risk assessment proforma		
4 All risks will be scored and graded according to likelihood and consequence using the Trust's risk assessment matrix	Compulsory through electronic risk assessment proforma		
5 All risks will be reviewed and updated, as a minimum, on a quarterly basis.	Quality Governance Report	Quarterly	Safety and Governance
6 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	Safety SITREP	Monthly	Quality Committee Trust Board
7 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	Safety SITREP	Monthly	Quality Committee Trust Board
8 New risks scoring 15 and above will be presented to the Executive Risk Group (ERG) for approval. Where the risk is not approved as red then the ERG will decide the current score of the risk	Minutes of ERG Risk Profile	Monthly	Safety and Governance
9 Where a risk is approved as red (15 or above) it will be reported on the Safety SITREP, which is presented to Quality Committee and Trust Board	Safety SITREP	Monthly	Quality Committee Trust Board

10 All risks should have a robust (SMART) action plan outlining the actions appropriate for the management and mitigation of the risk	Annual Audit	Annual	Safety and Governance
11 When a risk reaches its target score it will be reviewed with a view to closing the risk	Annual Audit	Annual	Safety and Governance
12 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	Quarterly	ERG Divisional Quality Groups
Health and Safety risk assessment audit	Health and Safety team audit	Annual	Safety Committee

Attachment 1: Risk Management Procedure

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.

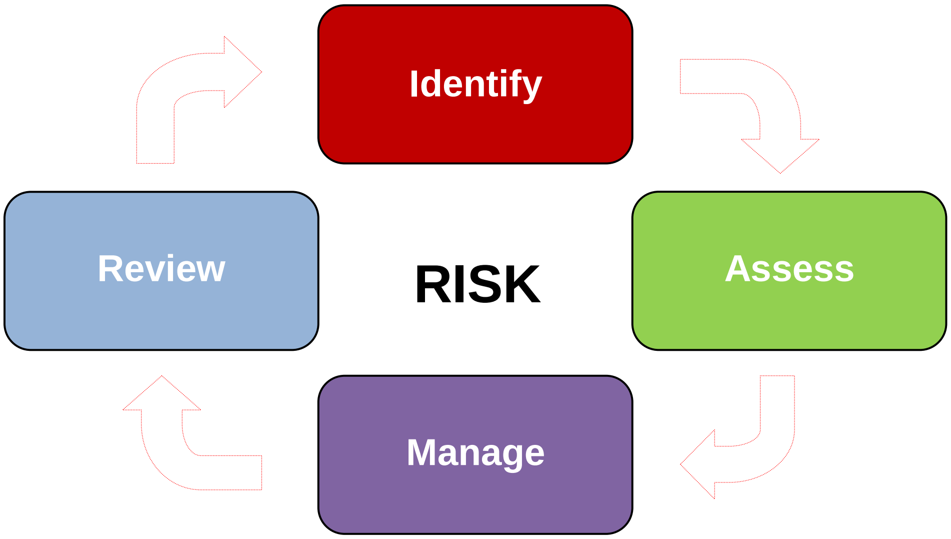
Once a risk is identified it must be documented on the Datix® risk assessment form, assessed and an action plan developed and implemented to reduce the risk to an appropriate level.

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 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?
- How 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 you need to consider:

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

Attachment 2 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 with 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 at the time the risk was last reviewed in line with review dates. It is expected that the current risk score will reduce and move toward the Target Risk Score as 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.

Risks are assigned a score based on a combination of likelihood and consequence using the Risk Assessment Matrix (**Attachment 3**).

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 three months;
- three to six months;
- six to nine months;
- nine to twelve months; and
- 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:

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 have 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:

- List 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 to the level of the current risk.

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.

2.5 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.

3. 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 (which is the initial score for new risks). 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 and accountable lead (where appropriate). • 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 and accountable lead (where appropriate). • The progress with managing these risks should be reviewed **quarterly** (at a minimum) by the directorate
Amber	9, 10 or12	Moderate	• Amber risks should be reviewed **quarterly** by the directorate management team. • In addition amber risks will be reviewed by the ERG and recorded on the Trust Safety SITREP. • They will therefore be reported to the ERG and Trust Board as considered appropriate. • Amber risks should be reported to the division who will consider whether they should be escalated • Non clinical risks should be discussed by the corporate management teams.
Red	15, 16, 20 or 25	High	• New Red risks should be reported immediately to the governance (clinical) and compliance (non clinical) teams. • They will be reviewed by the relevant Divisional Management Team before being presented to ERG. • They will be considered for final approval at the ERG. • Where red risks are approved at ERG they will be included on the Trust Safety SITREP. • Where red risks are presented to ERG but not approved then ERG will decide the current score. • Red risks should be reviewed **monthly** by the directorate or department management team. • These risks should be reported to the division team who will consider whether they should be recorded as a divisional risk.

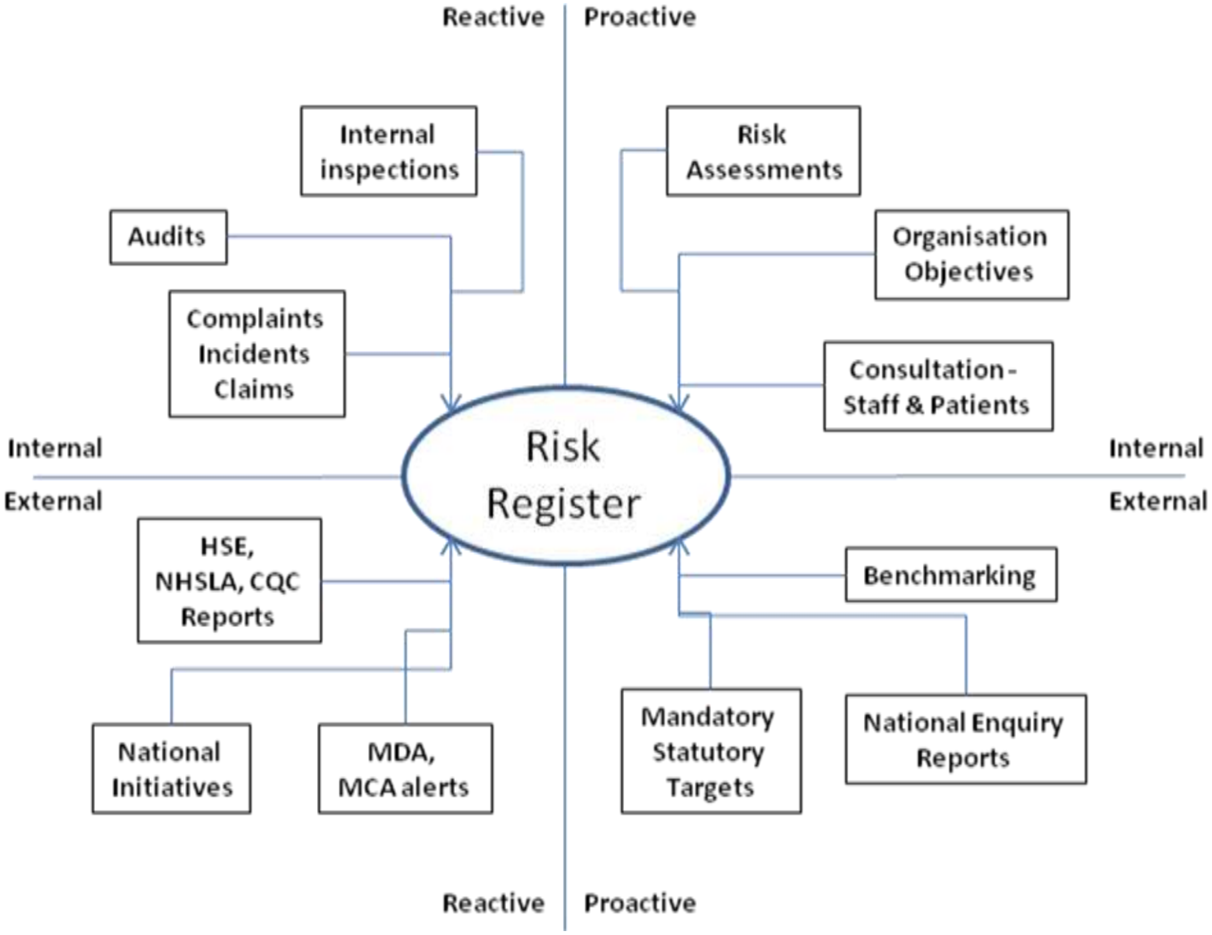
Red risks and all amber risks will be included in the Trust Safety SITREP which is presented to Quality Committee and Trust Board.

4. **Aggregation of Risk:**

Ensuring appropriate aggregation of common risks is a key challenge of any risk management process. Many departments and directorates face similar risks which may be assessed as low rating and locally managed. Taken individually these risks will not significantly impact on the organisation but collectively they could have the potential to threaten achievement of the Trust's objectives.

ERG will consider the implications for risk aggregation and will report these risks, via the Deputy Director of Governance, as they arise to the Executive Management Board and where appropriate Trust Board.

Attachment 2: Common sources of information for Risk Identification.



Attachment 3: 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

Table Four: Risk Level

Score	Impact	Level	Management
1-3	Very Low	**Green**	Manage locally, routine procedures, action plan and quarterly review.
4 - 8	Low	**Yellow**	Manage locally, manager/lead clinician review/assess risk & agree action plan. Quarterly review.
9 – 12	Moderate	**Amber**	Reviewed immediately by Directorate / Departmental management team, review & action plan. Quarterly review.
15 - 25	High	**Red**	Reviewed by Directorate / Departmental management team, Notify Relevant Governance Manager, Detailed review involving key staff & action plan, included on Division Quality Group/ Corporate operational group and reported to Quality Committee. Final approval from ERG for inclusion on Trust risk register. Monthly review.

The following table should be used as guidance is assessing the potential consequence of risk.

	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. An event which impacts on a small number of patients	Major injury leading to long-term incapacity/ disability. Requiring time off work for >14 days. Increase in length of hospital stay by >15 days. Mismanagement of patient care with long-term effects	Incident leading to 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

Source: NPSA Guidance for Risk Managers

Attachment 4: Ratification Checklist

Title		Risk Management Policy and Procedure v5.0
	Ratification checklist	**Details**
1	Is this a: Combined Policy & Procedure Yes	
2	Is this: Revised Yes	
3*	Format matches Policies and Procedures Template (Organisation-wide)	Yes
4*	Consultation with range of internal /external groups/ individuals	Yes
5*	Equality Impact Assessment completed	Yes
6	Are there any governance or risk implications? (e.g. patient safety, clinical effectiveness, compliance with or deviation from National guidance or legislation etc)	Provides framework for identifying and managing risk
7	Are there any operational implications?	No
8	Are there any educational or training implications?	Yes, a TNA has been developed in line with this policy
9	Are there any clinical implications?	No
10	Are there any nursing implications?	No
11	Does the document have financial implications?	No
12	Does the document have HR implications?	No
13*	Is there a launch/communication/implementation plan within the document?	Yes
14*	Is there a monitoring plan within the document?	Yes
15*	Does the document have a review date in line with the Policies and Procedures Framework?	Yes.
16*	Is there a named Director responsible for review of the document?	Yes
17*	Is there a named committee with clearly stated responsibility for approval monitoring and review of the document?	Yes, Quality Committee

Document Author / Sponsor

Signed ………………………

Title………………………

Date…………………

Ratified by Executive Lead,

Signed ....

Title...

Date...

Attachment 5: Equality and Diversity - Policy Screening Checklist

Policy/Service Title: Risk Management Policy and Procedure v5.0	**Directorate: Nursing**
Name of person/s auditing/developing/authoring a policy/service: DD Safety & Governance	
Aims/Objectives of policy/service: Heart of England NHS Foundation Trust will use the risk management cycle and risk register processes as outlined in this Policy to identify and manage the wide variety of Strategic, Operational and Financial risks which it faces.	

Policy Content:

- For each of the following check the policy/service is sensitive to people of different age, ethnicity, gender, disability, religion or belief, and sexual orientation?
- The checklists below will help you to see any strengths and/or highlight improvements required to ensure that the policy/service is compliant with equality legislation.

1. Check for DIRECT discrimination against any group of SERVICE USERS:							
Question: Does your policy/service contain any statements/functions which may exclude people from using the services who otherwise meet the criteria under the grounds of:		**Response**		**Action required**		**Resource implication**	
		Yes	**No**	**Yes**	**No**	**Yes**	**No**
1.1	Age?		x				
1.2	Gender (Male, Female and Transsexual)?		x				
1.3	Disability?		x				
1.4	Race or Ethnicity?		x				
1.5	Religious, Spiritual belief (including other belief)?		x				
1.6	Sexual Orientation?		x				
1.7	Human Rights: Freedom of Information/Data Protection		x				
If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.							

2. Check for INDIRECT discrimination against any group of SERVICE USERS:							
Question: Does your policy/service contain any statements/functions which may exclude employees from operating the under the grounds of:		**Response**		**Action required**		**Resource implication**	
		Yes	**No**	**Yes**	**No**	**Yes**	**No**
2.1	Age?						
2.2	Gender (Male, Female and Transsexual)?		X				
2.3	Disability?		X				
2.4	Race or Ethnicity?		X				
2.5	Religious, Spiritual belief (including other belief)?		X				
2.6	Sexual Orientation?		X				

2.7	Human Rights: Freedom of Information/Data Protection		x				
If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.							
TOTAL NUMBER OF ITEMS ANSWERED 'YES' INDICATING DIRECT DISCRIMINATION =							
3. Check for DIRECT discrimination against any group relating to EMPLOYEES:							
Question: Does your policy/service contain any conditions or requirements which are applied equally to everyone, but disadvantage particular persons' because they cannot comply due to:		**Response**		**Action required**		**Resource implication**	
		Yes	No	**Yes**	**No**	**Yes**	**No**
3.1	Age?		x				
3.2	Gender (Male, Female and Transsexual)?		x				
3.3	Disability?		x				
3.4	Race or Ethnicity?		x				
3.5	Religious, Spiritual belief (including other belief)?		x				
3.6	Sexual Orientation?		x				
3.7	Human Rights: Freedom of Information/Data Protection		x				
If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.							
4. Check for INDIRECT discrimination against any group relating to EMPLOYEES:							
Question: Does your policy/service contain any statements which may exclude employees from operating the under the grounds of:		**Response**		**Action required**		**Resource implication**	
		Yes	No	**Yes**	**No**	**Yes**	**No**
4.1	Age?		x				
4.2	Gender (Male, Female and Transsexual)?		x				
4.3	Disability?		x				
4.4	Race or Ethnicity?		x				
4.5	Religious, Spiritual belief (including other belief)?		x				
4.6	Sexual Orientation?		x				
4.7	Human Rights: Freedom of Information/Data Protection		x				
If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.							
TOTAL NUMBER OF ITEMS ANSWERED 'YES' INDICATING INDIRECT DISCRIMINATION =							

When completed please return this action plan to the Trust Equality and Diversity Lead; Pamela Chandler or Jane Turvey. The plan will form part of the quarterly Governance Performance Reviews.

Signed by Responsible Manager: ______ Date: ______

Attachment 6: Launch and Implementation Plan

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

Action	***Who***	***When***	***How***