Sheffield Teaching Hospitals NHS
NHS Foundation Trust

D

Risk Management Policy

Reference Number	Version	Status	Executive Lead(s) Name and Job Title	Author(s) Name and Job Title	
52	7	Current	Neil Riley Assistant Chief Executive	Pete Tanker Risk & Assurance Manager	
Approval Body		TEG		**Date Approved**	27/07/2016
Ratified by		Board of Directors		**Date Ratified**	tbc
Date Issued		tbc		**Review Date**	01/07/2019
Contact for Review Name and Job Title: Pete Tanker, Risk & Assurance Manager					

Associated Documentation:

Trust Controlled Documents

Incident Management Policy
Induction and Mandatory Training Policy
Information Risk Management Policy
Internal Incident Policy
Health and Safety at Work Policy Statement
Management of Health and Safety at Work Policy
Maternity Risk Management Strategy (Jessop Wing)
Raising Concerns at Work Policy and Procedure ("whistleblowing")

External Documentation

Code of Conduct for NHS Managers Department of Health. (2002)
Code of Governance for Foundation Trusts - Monitor (2014)
Risk Assessment Framework – Monitor (2015)

Legal Framework

Health and Safety at Work Act 1974
Management of Health and Safety at Work Regulations 1999

For more information on this document please contact:-

Pete Tanker
Risk & Assurance Manager
Chief Executive's Office
0114 27 11652
peter.tanker@sth.nhs.uk

Version History

Version	Date Issued	Brief Summary of amendments	Owner's Name:
6	20/01/2012	Separation of the Risk Management Strategy - to be developed from Trust's new Quality Strategy. Re-write of the *Monitoring Compliance and Effectiveness* section to ensure NHSLA Level 1 compliance. Further clarification of Risk Validation Group role and reporting arrangements with TEG.	Andy Challands
7	2016	Link to Information Risk Management Policy and Business Continuity- Internal Incident Policy Changes to Appendix C to reflect the introduction of the Integrated Risk & Assurance Report and change from Datix Rich Client to Datix Web Minor Change to Risk Assessment Form	Pete Tanker

(Please note that if there is insufficient space on this page to show all versions, it is only necessary to show the previous 2 versions)

Document Imprint

Executive Summary

Risk Management Policy

Document Objectives:	To ensure a structured and systematic approach to risk management to support delivery of the Trust's strategic objectives.
Group/Persons Consulted:	Safety and Risk Management Board, Head of Patient and Healthcare Governance; Patient Safety Manager, Assistant Chief Executive; Information Governance, Information Governance Caldicott and SIRO Support.
Monitoring Arrangements and Indicators:	The policy will be monitored for compliance via an annual Risk Management audit undertaken by Internal Audit reported to Audit Committee.
Training Implications:	See Section 9 and the Health, Safety, Welfare & Risk Training Needs Analysis available on the Trust's Mandatory Training intranet site.
Equality Impact Assessment:	An Equality Impact Assessment has been undertaken. A copy is published on the Trust's external website.
Resource implications:	Cost of Risk Management training as outlined in the Training Needs Analysis, the training is funded as part of the Mandatory & Job Specific Training (see above).

Intended Recipients:

Who should:-

• be **aware** of the document and where to access it	Staff, including contractors and agency staff
• **understand** the document	Executive Directors, Clinical Directors, Nurse Directors, Operations Directors, Service Managers, Head of Departments
• have a **good working knowledge** of the document	Governance and Risk Management Leads

CONTENTS

1 INTRODUCTION

1.1 The Trust is committed to the principles of good governance and recognises the importance of effective risk management as a fundamental element of the Trust's governance framework and system of internal controls.

1.2 In *Making a Difference* (1) Sheffield Teaching Hospitals NHS Foundation Trust (STH) set out a 5-year strategy, to be recognised as the best provider of health care, clinical research and education in the UK and a strong contributor to the aspiration of Sheffield to be a vibrant and healthy city region.

1.3 The Risk Management Policy is regularly reviewed and updated to ensure it continues to be consistent with the corporate strategy and reflects national guidance and legislation. It is approved by the Board of Directors.

2 SCOPE

The Policy applies to all staff including contractors and agency staff.

3 PURPOSE

3.1 The purpose of the Policy is to define the framework and systems the Trust will use to identify, manage and eliminate or reduce to a reasonable level risks that threaten the Trust's ability to meet it's aims and objectives, and the achievement of its values.

3.2 The Policy applies equally to all areas of the Trust with regard to all types of risk, both clinical and non-clinical.

4 DEFINITIONS

4.1 **Risk** is the threat or possibility that an action or event will adversely or beneficially affect the Trust's ability to achieve its aims and objectives. It is measured in terms of likelihood and consequence.

4.2 **Risk management** is about the Trust's culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse events. The risk management process covers all processes involved in identifying, assessing and judging risks, assigning ownership, taking action to mitigate or anticipate them, and monitoring and reviewing progress.

4.3 **Risk Assessment** is a systematic process of assessing the likelihood of something happening (frequency or probability) and the consequence if the risk actually happens (impact or magnitude).

4.4 **Strategic risks** are those that represent a threat to achieving the Trust's strategic objectives or to its continued existence. They also include risks that are widespread beyond the local area and risks for which the cost of control is significantly beyond the scope of the local budget holder. Strategic risks must be reported to the Board of the Directors and should be managed at executive level, directly or by close supervision.

4.5 **Operational risks** are by-products of the day-to-day running of the Trust and include a broad spectrum of risks including clinical risk, financial risk (including fraud), legal risks (arising from employment law or health and safety regulation), regulatory risk, risk of loss or damage to assets or system failures etc. Operational risks should be managed by the department or directorate which is responsible for delivering services.

4.6 **Risk Registers** are repositories for electronically recording and dynamically managing risks that have been appropriately assessed. Risk Registers are available at different organisational levels across the Trust.

4.7 **Risk appetite** is the type and amount of risk that the Trust is prepared to tolerate and explain in the context of its strategy.

4.8 **Governance** is the systems and processes by which the Trust leads, directs and controls its functions in order to achieve its organisational objectives, safety, and quality of services, and in which it relates to the wider community and partner organisations.

4.9 **Internal controls** are Trust policies, procedures, practices, behaviours or organisational structures to manage risks and achieve objectives.

4.10 **Assurance** is the confidence the Trust has; based on sufficient evidence that controls are in place and are operating effectively and its objectives are being achieved. Assurance has two dimensions Type and Strength.

Type:

- positive
- neutral
- negative

Strength (related to independence)

- Level 1- Directorate or equivalent
- Level 2- Trust Wide
- Level 3- External

5 STRATEGIC AIMS AND OBJECTIVES

5.1 The overarching aim of the Policy is to provide assurance that the Trust is providing high quality care in a safe environment, that it is complying with legal and regulatory requirements and that it is meeting its strategic aims and objectives, and promoting its values.

5.2 Key strategic objectives are:

5.2.1 To support the achievement of the Trusts corporate objectives and directorate objectives by developing a more dynamic approach to strategic risk management.

5.2.2 In line with the Trust's commitment to integrated governance, to adopt an integrated approach to risk management which includes risks related to clinical care, health and safety, financial and business planning, workforce planning, corporate and information governance, performance management, project/programme management, education and research.

5.2.3 To embed risk management systems and processes within the organisation and to promote the ethos that risk management is everyone's business.

5.2.4 To clearly define roles and responsibilities for risk management.

5.2.5 Create an environment which is safe as is reasonably practicable by ensuring that risks are continuously identified, assessed and appropriately managed i.e. where possible eliminate, transfer or reduce risks to an acceptable level.

5.2.6 To foster an organisational culture of openness and willingness to report risks, incidents and near misses that is used for organisation-wide learning.

5.2.7 To establish clear and effective communication that enables a comprehensive understanding of risks at all levels of the organisation by developing the use of directorate, specialist and trust-wide risk registers.

5.2.8 To provide appropriate training to staff to ensure effective implementation of this Policy as set out in the Training Needs Analysis.

5.2.9 To set out a process for the validation and appropriate escalation of risks

5.2.10 To maintain continued compliance with national standards, regulatory requirements and legislation.

6 ROLES AND RESPONSIBILITIES

6.1 In line with the Trust's management arrangements , responsibilities for key staff are outlined below:

6.2 The Board of Directors is responsible for ensuring the Trust has effective systems for managing risk. Board committees provide additional oversight to high level risk within their remit.

6.3 The Chief Executive, as the Trust's Accounting Officer, is personally responsible for maintaining a sound system of internal control including risk management.

6.4 The Assistant Chief Executive in the Role of Trust Secretary has delegated responsibility for ensuring effective systems for risk management are in place across the Trust.

6.5 Senior Information Risk Owner (SIRO). The Informatics Director is the SIRO and is the nominated lead to ensure the Trust's information risk is properly identified and managed and that appropriate assurance mechanisms exist.

6.5.1 Executive Directors and Senior Managers who attend the Board have delegated responsibility for managing risks in accordance with their portfolios as reflected in their job descriptions. For example, the Director of Finance has executive responsibility for financial governance and associated financial risks.

6.5.2 Executive Directors are responsible for ensuring effective systems for risk management, compatible with this Policy, are in place within their directorate. Specifically, they must ensure:

(i) suitably competent staff are identified to lead on risk management in the directorate and that their role and responsibilities are clearly understood

(ii) staff are familiar with this Policy and aware of their responsibility for risk

(iii) staff attend appropriate risk training (including induction and mandatory training) as necessary

(iv) risks (strategic and operational) are effectively managed i.e. identified, assessed and that action plans to mitigate risks are developed, documented and regularly reviewed.

(v) service developments, business cases and capital plans are formally risk assessed

6.6 Clinical Directors, Operations Directors and Nurse Directors or equivalent are responsible for ensuring effective systems for risk management are in place within their directorates, as described in 7.1.7, and ensuring their staff are aware of the Risk Management Policy.

6.7 Ward Sisters/Charge Nurses, Service Managers and Departmental Managers or equivalent are responsible for ensuring effective systems for risk management are in place at ward or departmental level.

6.8 Directorate Risk/Governance Leads or equivalents are responsible for coordinating risk management processes in their directorate and for maintaining the directorate Risk Register.

6.9 Staff (including contractors and agency staff) must ensure they are familiar and comply with the Trust's risk-related policies and relevant professional guidelines and standards.

6.10 Risk Management Specialist Officers (have Trust-wide risk related roles and responsibilities to:

(i) support and contribute to the development of Trust-wide and directorate risk management and governance arrangements

(ii) provide specialist advice to ensure compliance with statutory requirements and best practice

(iii) be involved in development of relevant policies and procedures

(iv) identify and disseminate relevant new legislation and guidance

(v) share information and good practice

(vi) support relevant investigations and reviews as required

(vii) provide education and training

(viii) participate in specialist risk related groups as required

7 ORGANISATIONAL ARRANGEMENTS

7.1 The organisational management of risk forms part of the Trust's overall approach to governance. The key forums for the management of risk in the Trust are outlined below:

7.1.1 Board of Directors
The Board of Directors is responsible and accountable for ensuring the Trust has effective systems and processes for managing risk. It approves the Risk Management Policy and the Annual Governance Statement.

7.1.2 Audit Committee
A non-executive committee established by and accountable to the Board of Directors, the committee has delegated authority from the Board overall responsibility for integrated governance, risk management and internal control. It receives and reviews external and internal audit reports, the Integrated Risk and Assurance Report (IRAR) and the Annual Governance Statement. The IRAR is structured by the Principal Risks to the achievement of the Trust's strategic aims. It records the Trust's high level risks, controls in place, mitigating actions and the assurance available. It is the responsibility of the Chair to identify any further risk assessments required and to instruct the relevant executive.

7.1.3 Healthcare Governance Committee
A committee established by and accountable to the Board of Directors, it is responsible for healthcare related governance and receives and reviews reports from the Trust's key healthcare governance groups and committees according to an annual work plan. The relevant sections of the IRAR are provided to this committee for assurance to be scrutinised. It is the responsibility of the Chair to identify any further risk assessments required and to instruct the relevant Executive.

7.1.4 Finance Performance & Workforce Committee

A committee established by and accountable to the Board of Directors, to give detailed consideration to the Trust's financial, performance and workforce issues in order to provide the Board with reassurance, information on key issues and clear decision points. The relevant sections of the IRAR are provided to this committee for assurance to be scrutinised. It is the responsibility of the Chair to identify any further risk assessments required and to instruct the relevant Executive.

7.1.5 Trust Executive Group (TEG)

As the executive group of the Board of Directors, it has overall responsibility for the operational management of risk. It receives and reviews high level and strategic risks reported in the IRAR (reported quarterly). In addition it receives a monthly report from the Risk Validation Group. The report provides details of changes to the Trust's Risk Register over the previous month i.e. newly registered risks; existing risks on the register that have been formally approved by directorate local governance group (or equivalent); and, risks that have been closed. Risk Assessments generated with the Trust Executive Team will be validated through the Trust Executive Group (TEG) and not the Risk Validation Group.

7.1.6 Safety and Risk Management Board (SRMB)

Accountable to the Healthcare Governance Committee, SRMB is responsible for the Trust-wide operational management of risk ensuring local systems and processes are in place and are operating effectively to ensure appropriate reporting and escalation. It reports to the Healthcare Governance Committee.

7.1.7 Risk Validation Group (RVG)

The group is responsible for reviewing locally approved new and existing risks scored as 4 and above, to validate the risk score and grade; to scrutinise and challenge the adequacy of the risk description, the controls and the mitigating action plan; and to consider any cross-cutting issues and the implications for risk aggregation. Findings are discussed with the Risk Owner and appropriate changes agreed. The group also reviews closed risks and considers the appropriateness of the decision to close. The group reports to the Safety and Risk Management Board and TEG on a monthly basis.

7.1.8 Directorate Governance Groups

Directorates have local governance groups (or equivalent) which are accountable to their directorate management team. The governance groups are responsible for ensuring effective directorate risk management systems and processes (including the maintenance of a directorate Risk Register) are in place and for reviewing risks within the directorate. All Risk Assessments should be approved either by these groups or a local equivalent meeting before going to RVG for validation. The governance groups report issues for escalation to Safety and Risk Management Board.

Once a risk is identified follow the process identified in Appendix D.

7.1.9 Business Planning Team (BPT) and Capital Investment Team (CIT)

Both BPT and CIT are accountable to the Trust Executive Group. BPT is responsible for business planning processes in the Trust and CIT is responsible for the Trust's 5-year capital programme. Both groups use a risk based approach.

7.1.10 Specialist risk groups

In addition to the above, there are a number of specialist Trust-wide groups (e.g. Infection Prevention and Control Committee, Radiation Safety Steering Group, Information Governance etc.) that have specific risk management responsibilities. A list of specialist risk groups is part of the Trust Meetings Map available on the Patient and Healthcare Governance intranet site.

8 RISK MANAGEMENT PROCESS

The Trust's process for risk management is detailed in:

(i) Appendix A: Guidelines to Identify, Assess, Action and Monitor Risks

(ii) Appendix B: Guidelines for completing a Risk Assessment Form

(iii) Appendix C: Guidelines for the Use of the Risk Register.

(iv) Appendix D: Identifying, Assessing and Reviewing Risks Flowchart

9 TRAINING

9.1 Risk Management has been classed as Mandatory and Job Specific Essential training. There is more than one training option available for Risk Management training and staff should complete the mandatory training requirement and the most relevant job specific essential training option to suit the responsibilities and risks associated with their role.

9.2 The Line Manager or Designated Supervisor should inform staff about their personal Mandatory and Job Specific Essential Training requirements during induction, at appraisal or when there is a significant change in role. The Line Manager/Designated Supervisor should consult the Training Needs Analyses for Health, Safety, Welfare & Risk on the Mandatory Training SharePoint site to find out if job specific training is essential for the post, and if so which training option is appropriate.

9.3 The Assistant Chief Executive in the role of Trust Secretary will ensure systems are in place for meeting Risk Management Training requirements for Corporate/Clinical Directors and Senior Managers (i.e. members of the Board of Directors, Operational Board and Clinical Management Board).

9.4 Accessing Mandatory and Job Specific Essential Training Courses
The Line Manager/Designated Supervisor should arrange for the employee to attend any relevant training courses, confirm these arrangements with the employee and book places on PALMS or with the course provider if the course is external to the Trust. This process should be completed as part of induction, appraisal and repeated when updates are due. Instructions on how to book training places on PALMS is included in the Induction and Mandatory Training Policy together with a full explanation of the mandatory training system. E-learning can be accessed via PALMS. Any member of staff can access PALMS to view their required learning, record of learning and access prospectus information.

9.5 Staff should complete the specified training or notify their Line Manager or Designated Supervisor if they are unable to comply so that alternative training can be arranged.

9.6 Recording Completion
Training Providers should follow the processes described in the Induction and Mandatory Training Policy for recording attendance using signing-in sheets. Trust e-learning packages include automatic recording of compliance. The Administrative staff that enter attendance records into PALMS check the signing-in sheets and report any non-attendance to the relevant manager.

9.7 Checking Compliance and Following up Non-compliance
Line Managers/Designated Supervisors should follow the processes described in the Induction and Mandatory Training Policy for checking compliance and following-up non-compliance. This includes using reports generated from PALMS and re-booking employees onto training courses or facilitating e-learning until compliance is achieved.

9.8 Specialised training in specific aspects of risk management such as risk assessment or use of DATIX Risk Module is available via Patient and Healthcare Governance and / or directorate Risk/Governance Leads.

10 IMPLEMENTATION

10.1 The Risk Management Policy is available on the Trust Corporate Policies intranet site.

10.2 Directors and senior managers are responsible for ensuring that their staff are aware of the Policy.

11 MONITORING COMPLIANCE AND EFFECTIVENESS

11.1 The Assistant Chief Executive in the Role of Trust Secretary has delegated responsibility for ensuring effective systems for risk management are in place across the Trust. Compliance with this policy is monitored by the Chief Executive's Office working with the Patient and Healthcare Governance Department.

11.2 Internal Audit undertakes a risk-based programme of audits agreed with the Trust which provides independent assurance. The programme includes an annual audit of Risk Management and annual reviews of the Integrated Risk & Assurance Report and the Statement on Internal Control. The Audit Committee receives and monitors implementation of recommendations.

11.3 High level *ad hoc* risk-related investigations and reviews (such as Root Cause Analyses, Assurance Reviews etc) which address specific concerns and are intended to provide assurance or identify areas for improvement or development. Responsibility for undertaking the investigations and reviews, methodology, timescales and reporting arrangements are individually decided by the project commissioners which include the Chief Executive, the Board of Directors, and the Healthcare Governance Committee etc.

11.4 Patient Incidents, Concerns, Claims, and Inquests Report compiled by Patient and Healthcare Governance and reported to and reviewed four times a year to the Healthcare Governance Committee. The report includes statistics and trend analysis and provides assurance to the Committee and/or identifies areas of concern requiring remedial action plans.

12 REFERENCES

1 STH (2012) Making a Difference: Corporate Strategy 2012 -17

Sheffield Teaching Hospitals NHS
NHS Foundation Trust

GUIDELINES TO IDENTIFY, ASSESS, ACTION AND MONITOR RISKS

1) INTRODUCTION

Risk Management covers all the processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them and monitoring and reviewing progress. As outlined in the Risk Management Policy, the Trust has a single process for risk management, (with specific information risk guidance in the Information Risk Management Policy). In order for the Trust to manage and control the risks it faces, it needs to identify and assess them. This document provides a step-by-step guide to help staff undertake risk management systematically and will ensure consistency of approach across the organisation.

2) IDENTIFYING A RISK

There is no unique method for identifying risks. Risks may be identified in a number of ways and from a variety of sources, for example:

- Risk assessment of everyday operational activities, especially when there is a change in working practice or environment
- Clinical risk assessments
- Environmental / workplace risk assessments
- Any risk identified through Directorate Business Continuity planning process/ single point of failure
- Risk assessment as part of Trust business – at all levels of the organisation
- Information Governance Risks are assessed using ISO 27001
- Annual planning cycle
- Performance management of key performance indicators
- Internal risk assessment processes e.g. requirements to assess risks as part of development and approval of policies, procedures, strategies and plans
- Claims, incidents (including Serious Untoward Incidents and Serious Incidents Requiring Investigation) complaints and Patient Services Team enquiries
- Organisational learning e.g. assurance reviews
- External reviews, visits, inspections and accreditation e.g. Health and Safety Inspections, Fire Inspections, external consultant reports
- Information Governance Toolkit using ISO 27001
- Staff and patient surveys
- National recommendations including Confidential Inquiries, safety alerts, NICE guidance etc.
- Internal and External Audit
- Clinical audits
- Information from partner organisations
- Environment scanning of future risks (both opportunities and threats)

This list is not exhaustive. In general, the more methods that are used the more likely that all relevant risks will be identified.

There are two distinct phases to risk identification:

a) Initial Risk identification - relevant to new services, new techniques, projects

b) Continuous Risk Identification – relevant to existing services and should include new risks or changes in existing risks e.g. external changes such as new guidance, legislation etc.

3) DESCRIBING THE RISK

Failure to properly describe risk is a recognised problem in risk management. Common pitfalls include describing the *impact* of the risk and not the risk itself, defining the risk as a statement which is simply the converse of the objective, defining the risk as an absence of controls etc. A simple tip is to consider describing the risk in terms of cause and effect.

The example below provides a useful guide to help staff define the risk accurately and precisely:

Objective: To travel from the Northern General (NGH) to Weston Park Hospital (WPH) for a meeting at a certain time		
Risk description		Comment
Failure to get from the NGH to WPH for a meeting at a certain time	✗	This is simply the converse of the objective
Being late and missing the meeting	✗	This is a statement of the **impact** of the risk and not the risk itself
Eating on the shuttle bus is not allowed so I was hungry	✗	This does not impact on the achievement of the objective
Missing the shuttle bus causes me to be late and miss the meeting	√	This is a risk that can be controlled by ensuring I allow enough time to get to the shuttle bus stop
Severe weather prevents the shuttle bus from running and me getting to the meeting	√	This is a risk that I cannot control but against which I can make a contingency plan

4) ASSESSING THE RISK

Having identified and described the risk, the next step is to assess the risk. This allows for the risk to be assigned a standard rating which determines what actions (if any) need to be taken.

Ideally, risk assessment is an objective process and wherever possible should draw on independent evidence and valid quantitative data. However such evidence and data may not be available and assessor(s) will be required to make a subjective judgement. When facing uncertainty, the assessor(s) should take a precautionary approach.

The risk assessment should be undertaken by someone competent in the risk assessment process and should involve staff familiar with the activity being assessed. Depending on the severity of the risk, the directorate Risk/Governance lead should be notified. Trade union representatives, external assessors or experts should be involved or consulted, as appropriate.

Risks are assigned a score based on a combination of the **likelihood** of a risk being realised and the **consequences** if the risk is realised.

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 risks 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 expected after the action plan has been fully implemented.

a) Scoring the consequences

Use *Table 1 Measures of Consequence*, to score the consequence, with existing controls in place:

Choose the most appropriate domain(s) from the left hand column of the table. Then work along the columns in the same row and, using the descriptors as a guide, assess the severity of the consequence on the scale 1 = Insignificant, 2 = Minor, 3 = Moderate, 4 = Major and 5 = Catastrophic.

Table 1: Measures of Consequence

See Information Risk Management Policy for the scoring of information risks.

Domain	Consequence Score and Descriptor				
	1	2	3	4	5
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Injury or Harm Physical or Psychological	No / minimal injury requiring no / minimal intervention or treatment No time off work required	Minor injury or illness, requiring intervention Requiring time off work for < 4 days Increase in length of hospital stay by 1-3 days	Moderate injury requiring intervention Requiring time off work for 4 -14 days Increase in length of hospital stay by 4 -14 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 >14 days	Incident leading to death Multiple permanent injuries or irreversible health effects
Quality of the Patient Experience / Outcome	Unsatisfactory patient experience not directly related to the delivery of clinical care	Unsatisfactory patient experience directly related to clinical care – readily resolvable	Mismanagement of patient care, short term effects < 7 days	Mismanagement of patient care, long term effects >7 days	Totally unsatisfactory patient outcome or experience
Statutory	Coroners verdict of natural causes, accidental death, open No or minimal impact of statutory guidance	Coroners verdict of misadventure Breech of statutory legislation	Police investigation. Prosecution resulting in fine >£50k Issue of a statutory notice	Coroners verdict of neglect/system neglect Prosecution resulting in fine >£500k	Coroners verdict of unlawful killing Criminal prosecution (incl Corporate manslaughter) > imprisonment of Director/ Executive
Business/ Finance & Service Continuity	Minor loss of non-critical service Financial loss <£10K	Service loss in a number of non-critical areas <2 hours or 1 area or <6 hours Financial loss £10 - 50k	Loss of services in any critical area Financial loss £50 - 500k	Extended loss of essential service in more than one critical area Financial loss £500k to £1m	Loss of multiple essential services in critical areas Financial loss > £1 m
Potential for Complaint or Litigation / Claims	Unlikely to cause complaint or litigation	Complaint possible Litigation unlikely Claim(s) < £10k	Complaint expected Litigation possible but not certain Claim(s) £10-100k	Multiple complaints / Ombudsmen inquiry Litigation expected Claim(s) £100k - £1m	High profile complaint(s) with national interest Multiple claims or high value single claim >£1m
Staffing and Competence	Short-term low staffing level that temporarily reduces patient care / service quality (<1 day) Concerns about competency / skill mix	Ongoing low staffing level that reduces patient care / service quality Minor error(s) due to levels of competency (individual / team)	Ongoing problems with levels of staffing that results in late delivery of key objective/service Moderate error(s) due to levels of competency (individual / team)	Uncertain delivery of key objective/service due to lack of staff. Major error(s) due to levels of competency (individual / team)	Non-delivery of key objective/service due to lack of staff / lloss of key staff. Critical error(s) due to levels of competency (individual / team)
Reputation or Adverse Publicity[1]	Within the Trust Local media 1 day e.g. inside pages, limited report	Local media <7 day coverage e.g. front page, headline Regulator concern	National media <3 day coverage Regulator action	National media >3 day coverage. Local MP concern. Questions in the House	Full public enquiry Public investigation by regulator
Compliance Inspection / Audit	Non-significant / temporary lapses in compliance / targets.	Minor non-compliance with standards / targets. Minor recommendations from report	Significant non-compliance with standards / targets. Challenging report	Low rating. Enforcement action. Critical report	Loss of accreditation / registration. Prosecution. Severely critical report

[1] Organisational reputation risks can relate to impact on how the organisation is viewed by staff within the organisation, by other organisations in the health and social care economy, by elected representatives and by patients and the general public.

Scoring the likelihood

Use *Table 2 Likelihood*, to score the likelihood of the consequence(s) occurring with existing controls in place , using the frequency scale of Rare = 1, Unlikely = 2, Possible = 3, Likely = 4 and Certain = 5.

Likelihood can be scored by considering

- Frequency i.e. how many times the consequence(s) being assessed will actually be realised

or

- Probability i.e. what is the chance the consequence(s) being assessed will occur in a given period

Table 2: Likelihood

Descriptor	Score	Frequency	Probability
Rare	1	This will probably never happen / recur	> 1 in 100 000
Unlikely	2	Do not expect it to happen / recur but it is possible	> 1 in 10 000
Possible	3	Might happen / recur occasionally	> 1 in 1 000
Likely	4	Will probably happen / recur but it is not a persistent issue	> 1 in 100
Almost Certain	5	Will undoubtedly happen / recur, possibly frequently	> 1 in 10

b) Scoring the risk

Calculate the risk score by multiplying the consequence score by the likelihood score. See *Table 3 Risk Score*

IMPORTANT: It may be appropriate to assess more than one domain of consequence. This may result in generating different scores. Use your judgement to decide on the **overall** score, however as a rule-of-thumb take the highest domain score. For the Scoring of Information Risks see: Information Risk Management Policy.

Table 3: Risk Score

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

Directorate Risk/Governance Lead(s) must be notified of all risks scored at 4 or above.

5) RATING THE RISK

Risk rating 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 overseen in the organisation; prioritise remedial action and availability of resources to address risks; and, direct which risks should be included on the Trust's risk register.

Having assessed and scored the risk, use *Table 4 Risk Rating* to rate the risk. The table provides guidance on the documentation/registration of the risk, the urgency of actions to mitigate the risk and clarifies reporting and oversight arrangements.

Table 4: Risk Rating

Scores	Risk grade	Responsibilities and Accountability
1 – 3	Low	▪ Risk Assessment Form completed. Registering on to DATIX at the discretion of the directorate(s) ▪ Directorate Governance groups (or equivalent) to monitor action plan and review.
4 – 6	Moderate	▪ Risk Assessment Form completed and risk registered on DATIX ▪ New Moderate Risks reported to Safety and Risk Management Board. ▪ Directorate Governance groups (or equivalent) to monitor action plan and review.
8 – 12	High	▪ Risk Assessment Form completed and risk registered on DATIX ▪ New High Risks reported to Safety and Risk Management Board. ▪ Wherever possible, the action plan should include urgent action to reduce risk ▪ Directorate Governance groups (or equivalent) to monitor action plan and review ▪ Patient and Healthcare Governance to review progress on High Risks.
15 - 25	Extreme	▪ Risk Assessment Form completed and risk registered on DATIX. ▪ New Extreme Risks to be reported to Safety and Risk Management Board and to Trust Executive Group and Board of Directors via the Integrated Risk & Assurance Report. ▪ Wherever possible, the action plan should include immediate action to reduce risk. ▪ Directorate Governance groups (or equivalent) to monitor action plan and review. ▪ Trust Executive Group and Board of Directors to review progress on Extreme Risks.

6) DOCUMENTING THE RISK

It is important that identified risks are appropriately documented in a standardised format using the Risk Assessment Form set out at Appendix B or alternative risk forms if specified.

7) ADDRESSING RISKS

Having identified, assessed, scored and rated the risk, the next stage is to decide and document an appropriate response to the risk. The response should describe how the Target Risk Score will be achieved. Information Risks are addressed by the controls described in ISO 27001 & ISO 27002.

In general, there are four potential responses to address a risk once it has been identified and assessed – commonly known as the 4 T's:

- Tolerate
- Treat
- Transfer
- Terminate

a) Tolerate the risk

The risk may be considered tolerable without the need for further mitigating action, for example if the risk is rated LOW or if the Trust's ability to mitigate the risk is constrained or if taking action is disproportionately costly.

If the decision is to tolerate the risk, consideration should be given to develop and agree contingency arrangements for managing the consequences if the risk is realised.

b) Treating the Risk

This is the most common response to managing a risk. It allows the organisation to continue with the activity giving rise to the risk while taking mitigating action to reduce the risk to an acceptable level i.e. as low as reasonably practicable. In general, action plans will reduce the risk over time but not eliminate it.

It is important to ensure that mitigating actions are proportionate to the identified risk and give reasonable assurance to the Trust that the risk will be reduced to an acceptable level.

Action plans must be documented on the risk assessment form, have a nominated owner and progress monitored by the appropriate risk forum.

c) Transfer the risk

Risks may be transferred for example by conventional insurance or by sub-contracting a third party to take the risk. This option is particularly suited to mitigating financial risks or risks to assets.

It is important to note that reputational risk cannot be fully transferred.

d) Terminate the risk

The only response to some risks is to terminate the activity giving rise to the risk or by doing things differently.

However, this option is limited in the NHS (compared to the private sector) where many activities with significant associated risks are deemed necessary for the public benefit.

8) APPROVAL AND VALIDATION

Once documented all risks should be ***approved*** via a Directorate Governance Meeting, Management Team meeting or similar group prior to ***validation*** at Risk Validation Group. The exact route for approval will depend on the type and score of the risk. Further guidance and support is available from directorate Risk/Governance Leads, Risk & Assurance Manager or Patient and Healthcare Governance. If a review or update means a significant change in a risk assessment particularly an increase in the risk it should returned to the Approving body for further consideration.

GUIDELINES FOR COMPLETING A RISK ASSESSMENT FORM

1) INTRODUCTION

As set out in the Trust's Risk Management Policy, it is important that identified risks are appropriately documented in a standardised format using the Risk Assessment Form, or alternative risk form if specified.

2) WHO SHOULD COMPLETE THE FORM?

Ideally, the assessment process should involve the person familiar with the activity being risk assessed and a person competent in the risk assessment process. Sometimes this might be the same person.

Depending on an initial impression of the risk it may be appropriate to involve other people e.g. relevant managers, union or professional representatives, external experts etc, as appropriate.

Directorate Risk/Governance Lead/ Business Continuity lead(s) must be notified of all risks scored at 4 or above.

3) COMPLETING THE FORM

i) ID – insert the Datix ID number for all risks added to the system
ii) Title- Please ensure the title gives a brief and unique description, use the same wording on the form and in Datix.
iii) Department / Directorate - Specify the department(s) / directorate(s) responsible for managing the risk.
iv) Description of risk - Please include as much detail of the risk as possible i.e. the cause, the consequence, the location, who may be affected by the risk (e.g. staff, patients, public etc). For further guidance refer to Section 3 of the Guidelines to identify, assess, action and monitor risks.
v) Existing controls - List the existing controls in place at the time the risk is first identified. Controls include relevant policies, procedures, practices, training, organisational structures etc that are used to manage risk. Assess whether controls are strong (i.e. operate effectively and provide reasonable assurance that the risk is adequately controlled) or weak.
vi) Calculating the Initial Risk Score – i.e. the score when the risk is first identified with existing controls in place. For further guidance on risk scoring refer to Section 4 of the Guidelines to identify, assess, action and monitor risks.
vii) Action Plan - Please list the main actions planned to reduce the risk to an acceptable level i.e. the Target Risk Score. When estimating the projected cost of action, please ensure consideration is given to both capital and revenue costs. Please note, the person responsible for an identified action may be different from the assessor(s).
viii) Calculating the Target Risk Score – i.e. the score that is expected after the action plan has been fully implemented. For further guidance on risk scoring refer to Section 4 of the Guidelines to identify, assess, action and monitor risks.
ix) Assessor(s) - If the assessment involved more than one person, list the key persons and identify the Lead Assessor.
x) Date of assessment -The date the assessment was undertaken.
xi) Date of next review - This is dependent upon the severity of the risk but as a minimum it should be undertaken at least once a year.
xii) Date of Approval: the date the risk was locally approved
xiii) Approval Body: the group that approved the risk

4) WHAT TO DO WITH A COMPLETED FORM

Please ensure all completed Risk Assessment Forms are filed safely and copies are available to staff who need access to them.

If the Initial Risk Score is more than 3 you must contact your directorate Risk/Governance Lead to ensure it is registered on DATIX, (see *Guidelines for the use of the Risk Register* - Appendix C of the Risk Management Policy). An electronic copy of the Risk Assessment Form must be attached as a document in the DATIX risk record.

APPENDIX C

Sheffield Teaching Hospitals NHS
NHS Foundation Trust

GUIDELINES FOR THE USE OF THE RISK REGISTER

1) INTRODUCTION

A Risk Register is a management tool that provides a comprehensive and dynamic understanding of an organisation's risk profile. Effectively used, a Risk Register will not only drive risk management but should be used to inform decision-making processes.

2) OVERVIEW

Using the DATIX Risk Management system, the Trust uses tiered risk registers to ensure risks are managed, escalated and reported at the appropriate organisational level. Risk registers will be managed and monitored by relevant local risk forums (see hierarchy of risk registers below) and will be supported through the Chief Executive's Office by the Risk & Assurance Manager and or the Patient and Healthcare Governance Team.

The current hierarchy of risk registers is:

- Clinical and corporate directorate registers e.g. Acute Medicine
- Thematic registers e.g. Infection Control, Information Governance, Radiation Safety, Business Continuity and Emergency Planning
- Executive registers e.g. Integrated Risk & Assurance Risk Report

As a minimum these risk registers will include details of:

- a description of the risk and existing controls
- the source of the risk
- risk ownership
- initial, current and target risk score
- rationale for the target score
- action plan
- review date (up to a maximum of 1 year)

3) REGISTERING A RISK ON DATIX

As outlined in *Guidelines to Identify, Assess, Action and Monitor Risks* (see Appendix A of the Risk Management Policy), risks can be identified in a number of ways and from a range of sources. Once a risk is identified it must be documented using a Risk Assessment Form, assessed and an action plan developed to reduce the risk to an acceptable level.

Risk assessments can and should be made at any level in the organisation. However, before a risk can be formally recorded on DATIX it must be reviewed and approved by the relevant risk forum to ensure that the minimum level of information required is captured and facilitate appropriate challenge. Draft risk assessments should be added to Datix and given the status 'awaiting review' or 'being review' prior to Approval at the appropriate forum.
Specifically, the risk forum is required to assess and approve:

- The initial / current risk score with existing controls but prior the treatment plan.
- The achievability of the treatment plan, considering such aspects as affordability, timescales, service delivery etc.
- The rationale and scoring of the target risk score.
- The frequency of review.

Guidance and support is available from the Patient and Healthcare Governance department.

4) ESCALATING A RISK

Risks must be escalated within the Trust in accordance with *Guidelines to Identify, Assess, Action and Monitor Risks*. Risks rated as Moderate or above (i.e. risk score 4 or more) shall be reported to the Risk Validation Group (RVG) who will validate the score and risk grade and provide a monthly report to Safety and Risk Management Board and TEG.

This provides further opportunity to scrutinise and challenge the risk assessment and action plan. It also allows for consideration of where the management of the risk best lies.

5) RISK AGGREGATION

Ensuring appropriate aggregation of common risks is a key challenge of any risk management process especially in a large, complex and highly devolved organisation such as STH. Many departments and directorates face similar risks e.g. in-year cost pressures, recruitment problems etc which may be assessed as low rating and locally managed. Taken individually these risks will not significantly impact on the organisation but collectively have the potential to threaten achievement of Trust's strategic objectives.

On an ongoing basis, relevant risk forums must consider the potential for risk aggregation when reviewing new risks. The potential may result from several common risks being identified across a number of areas or as a result of a risk having been identified in one area that has implications across a wide number of services.

In such circumstances, a new risk assessment of the aggregated risk should be undertaken and documented on the Risk Assessment Form as a 'Parent Risk' with links to the subordinate risks registered on DATIX. It is possible that the aggregated impact score will be different from the individual risks and also that the action plan will require revision. The Risk Validation Group will consider the implications for risk aggregation and will report these issues as they arise to Safety and Risk Management Board and TEG. There may be circumstances when the aggregated risk will supersede the subordinate risks rather than become Parent & Child Risks, RVG will consider if this is the case, and if the subordinate risks should be closed on DATIX.

6) REVIEWING A RISK REGISTERED ON DATIX

Risks registered on DATIX must specify when the current risk score, action plan 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. Risks must be reviewed at least once a year.

A new Risk Assessment Form shall be completed for subsequent reviews and each review must be uploaded onto DATIX providing a history of risk reviews.

7) RESPONSIBILITIES

a) Directorate Risk Register

Responsibility for the management and maintenance of clinical and corporate directorate risk registers sits with Clinical Directors and Executive Directors respectively. This responsibility is normally delegated to directorate governance groups (or equivalent). These groups should review their Directorate risk registers at least four times a year.

b) Thematic Risk Registers

Responsibility for the review of themed risk registers will sit with the designated Trust Lead for the theme areas. This responsibility can be met through the actions of the appropriate risk forum e.g. Infection Prevention and Control Committee, Radiation Steering Group etc. The designated theme leads should review their themed risk registers at least once a year.

c) Executive Risk Registers

The Chief Executive is responsible for the management and maintenance of the Integrated Risk and Assurance Report although this has been delegated to the Trust Secretary and Risk & Assurance Manager. The Integrated Risk and Assurance Report includes high-level and strategic risks, is reviewed at least four times a year by TEG and the Audit Committee on behalf of the Board of Directors.

Trust-wide Risk Register

The Chief Executive is responsible for the management and maintenance of the Trust-wide Risk Register although this has been delegated to the Risk and Assurance Manager who works closely with key staff from Patient and Healthcare Governance. The Trust-wide risk register is reviewed in its entirety by the Risk Validation Group via an annual rolling programme and is reported to TEG and the Safety and Risk Management Board following each meeting.

8) QUALITY ASSURANCE

Quality Assurance of the Risk Registers will be secured via a number of mechanisms:

- designated risk forums have primary responsibility for their risk registers
- Patient and Healthcare Governance through the Risk Validation Group provides ongoing oversight of all risk registers, supplemented by random detailed reviews to assess risk scoring and treatment plans, appropriate escalation and aggregation and that all risks remain in date
- Internal Audit will review risk registers as part of their annual review of Risk Management.

Further guidance and support is available from Patient and Healthcare Governance.

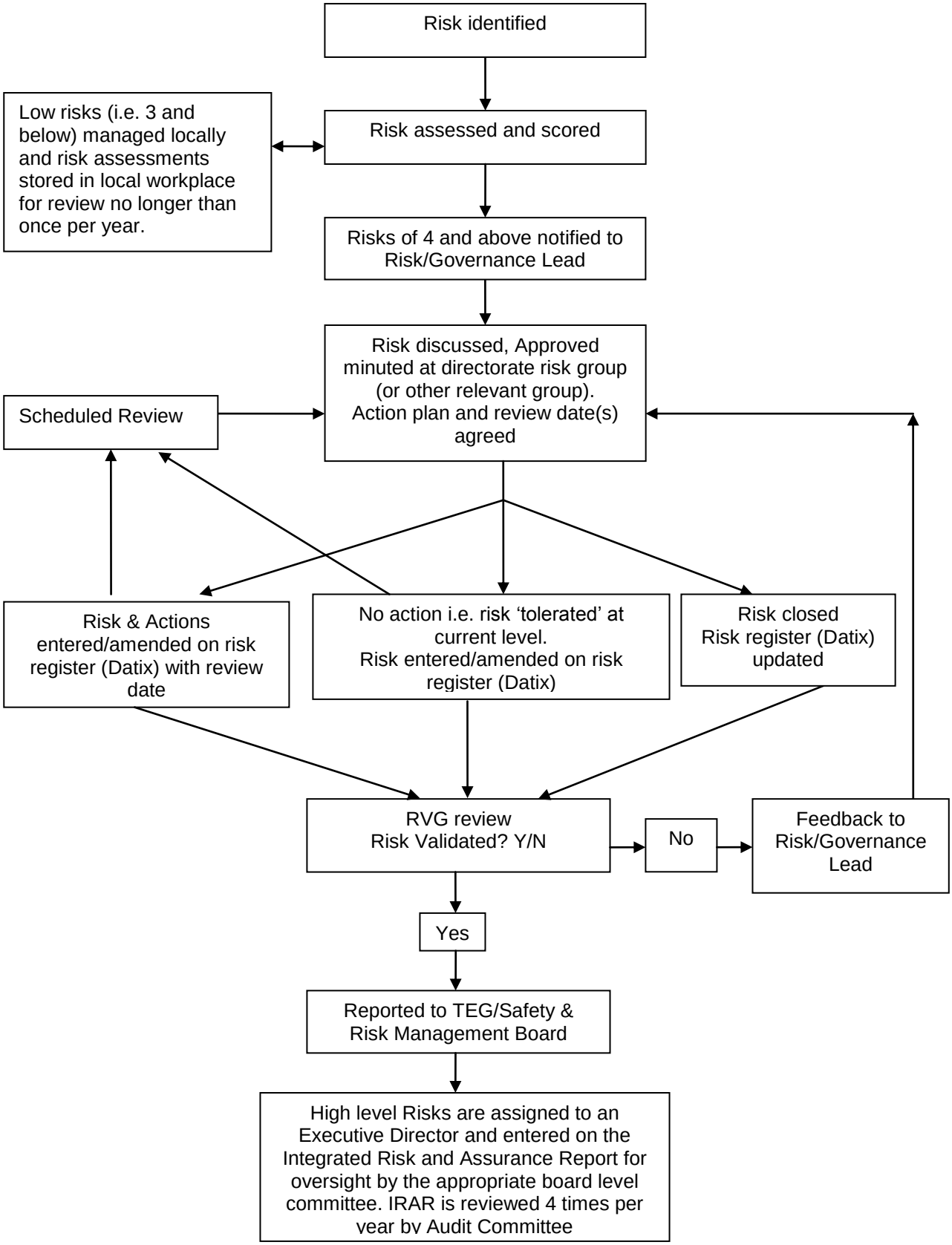
ADDITIONAL INFORMATION - DATIX RISK MODULE FIELDS

Field	Further guidance
Approval Status	Mandatory Field. Choose from the options list.
ID	This field is automatically populated.
Reference	Optional field. May be used for local purposes or left blank.
Title	Mandatory field. Please ensure the title gives a brief and unique description.
RVG Involvement	Mandatory Field. Choose from the options list- Local risk should only be chosen when Datix is being used to file low level local risks
Risk Type	Mandatory field. Choose whether the risk is operational (i.e. within the control of a directorate) or strategic (i.e. requires additional funding and/or coordinated cross-directorate, Group or Trust-wide action)
Sub-type	Mandatory field. Choose from the options list.
Handler	Mandatory field. This field will default to the person entering the risk on the system but should be changed to the directorate Risk/Governance Lead.
Manager	Mandatory field. Select the person from the options list with overall responsibility for managing the risk to an acceptable level.
Opened	Mandatory field. Enter the date the risk was registered on the system. This field should not be amended.
Review date	Mandatory field. Enter the date when the risk is scheduled to be reviewed. This field must be updated after each review. Maximum 12 months.
Closed date	Enter this date when the risk has been reduced to an acceptable level (i.e. the target risk score).
Site	Mandatory field. Choose from the options list.
Clinical Group	Mandatory field. Choose from the options list.
Directorate	Mandatory field. Choose from the options list.

Specialty	Mandatory field. Choose from the options list.
Description	Mandatory field. Please ensure the risk is fully described as reflected on the Risk Assessment Form.
Controls in place	Mandatory field. Please list in full the current controls in place as recorded on the Risk Assessment Form.
Are there any documents to be attached	**Yes.** This should be used to attach relevant documents such as Risk Assessment Form and any associated documentary evidence.
Consequence	Mandatory fields. Choose appropriate descriptor from the options list to score Initial, Current and Target risk.
Likelihood	Mandatory field. Choose appropriate descriptor from the options list to score Initial, Current and Target risk.
Score	The final risk score is automatically calculated.
Rating	The final risk rating is automatically calculated.
Extra Fields Top Left of the Screen on Datix	
Assurance	As appropriate, select the relevant Trust Objective that the risk relates to.
Actions	Use of this field continues is to be developed. Risk Leads and Governance Teams who are familiar with the system are encouraged to use it to record planned actions to reduce the risk
Contacts	Optional :Complete if relevant
Notepad	Optional field. This may be used as an aide memoir etc.
Linked records	Parent /Child Risks should be linked and risk relating to other Datix modules e.g.: Incidents or Safety Alerts the records should be linked.

Sheffield Teaching Hospitals NHS
NHS Foundation Trust

FLOWCHART OF THE PROCESS FOR IDENTIFYING, ASSESSING, ACTIONING AND REVIEWING DIRECTORATE RISKS



RISK ASSESSMENT FORM

Sheffield Teaching Hospitals NHS
NHS Foundation Trust

To be completed for all newly identified risks
For further guidance on completing this form please refer to Guidelines for Completing a Risk Assessment Form (available on the Trust's intranet) or contact your directorate Risk Lead

ID		Title	
Department / Directorate			
Description of risk			
Existing controls in place when risk was identified			

Initial Risk Score i.e. with existing controls in place	Consequence (1-5)	
	Likelihood (1–5)	
	Risk Score (1 – 25)	

Action Plan to reduce the risk to an acceptable level			
Description of actions	Cost	Responsibility (Job title)	Completion Date
Register risk on DATIX (for all risks > 3)	nil		

Target Risk Score i.e. after **full** implementation of action plan	Consequence (1-5)	
	Likelihood (1–5)	
	Risk Score (1 – 25)	
	Date for completion	

Rationale for Target score	

Assessment undertaken by: Name	Job title
Lead:	

Date of assessment		Date of next review	
Risk Approved by (Group):		Date	