### Risk Management Policy

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Version</th>
<th>Status</th>
<th>Executive Lead(s) Name and Job Title</th>
<th>Author(s) Name and Job Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>52</td>
<td>6</td>
<td>Current</td>
<td>Neil Riley Trust Secretary</td>
<td>Andy Challands Assurance Manager</td>
</tr>
</tbody>
</table>

**Approval Body**: TEG  
**Date Approved**: 11/01/2012  
**Ratified by**: Board of Directors  
**Date Ratified**: TBC  
**Date Issued**: TBC  
**Review Date**: 01/01/2013

**Contact for Review Name and Job Title**: Andy Challands, Assurance Manager
Associated Documentation:

Trust Controlled Documents
Maternity Risk Management Strategy
Incident Management Policy
Health and Safety at Work Policy Statement
Management of Health and Safety at Work Policy
Mandatory Training Strategy
Mandatory Training Policy
Induction Policy
Whistleblowing Policy

External Documentation
Risk Management Standards NHSLA (2011)
Code of Governance Monitor (2011)

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:-
Andy Challands
Assurance Manager
Chief Executive’s Office
0114 27 11708
andrew.challands@sth.nhs.uk

Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date Issued</th>
<th>Brief Summary of amendments</th>
<th>Owner's Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>December 2009</td>
<td>Major re-write</td>
<td>Andy Challands</td>
</tr>
<tr>
<td>4.1</td>
<td>Amended September 2010</td>
<td>Minor updates to fit with changes to website, committee name, function of group and new Mandatory &amp; Job Specific Training Policy</td>
<td>Andy Challands</td>
</tr>
<tr>
<td>5</td>
<td>14/02/2011</td>
<td>Minor word changes. Clarification of Board of Director responsibilities. Change in monitoring reports to Audit Committee rather than Healthcare Governance Committee. Separate development of annual Risk Management objectives.</td>
<td>Andy Challands</td>
</tr>
<tr>
<td>6</td>
<td>TBC</td>
<td>Minor word changes. 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.</td>
<td>Andy Challands</td>
</tr>
</tbody>
</table>

(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
Copyright ©Sheffield Teaching Hospitals NHS Foundation Trust 2012: All Rights Reserved
Re-use of all or any part of this document is governed by copyright and the
Information on re-use can be obtained from:
The Department for Information Governance & Caldicott Support, Sheffield Teaching Hospitals.
Tel: 0114 226 5151. E-mail: infogov@sth.nhs.uk
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, Trust Secretary; Information Governance, Information Governance Caldicott and SIRO Support, Audit Committee.

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) and the Healthcare Governance Risk Management Audit Programme (reported to Healthcare Governance Committee).


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, (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, General Managers

- have a good working knowledge of the document
  - Governance and Risk Management Leads
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>5</td>
</tr>
<tr>
<td>2 Scope</td>
<td>5</td>
</tr>
<tr>
<td>3 Purpose</td>
<td>5</td>
</tr>
<tr>
<td>4 Definitions</td>
<td>5</td>
</tr>
<tr>
<td>5 Strategic Aims and Objectives</td>
<td>6</td>
</tr>
<tr>
<td>6 Roles and Responsibilities</td>
<td>7</td>
</tr>
<tr>
<td>7 Organisational arrangements</td>
<td>8</td>
</tr>
<tr>
<td>8 Risk Management process</td>
<td>9</td>
</tr>
<tr>
<td>9 Training</td>
<td>9</td>
</tr>
<tr>
<td>10 Implementation</td>
<td>10</td>
</tr>
<tr>
<td>11 Monitoring compliance and effectiveness</td>
<td>10</td>
</tr>
<tr>
<td>12 References</td>
<td>11</td>
</tr>
<tr>
<td>Appendix A: Guidelines to Identify, Assess, Action and Monitor Risks</td>
<td>12</td>
</tr>
<tr>
<td>Appendix B: Guidelines for completing a Risk Assessment Form</td>
<td>18</td>
</tr>
<tr>
<td>Appendix C: Guidelines for the Use of the Risk Register</td>
<td>20</td>
</tr>
<tr>
<td>Appendix D: Identifying, Assessing and Reviewing Risks Flowchart</td>
<td>25</td>
</tr>
</tbody>
</table>
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 Excellence as Standard (1) Sheffield Teaching Hospitals NHS Foundation Trust (STH) set out a 3-year strategy to realise its vision to become a provider of world class services and top quality teaching and research.

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 its objectives and 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 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 can 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, operating effectively and its objectives are being achieved.

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 objectives and promoting its values.

5.2 Key strategic objectives are:

5.2.1 To support the achievement of the Trust’s 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 maintain continued compliance with national standards, regulatory requirements and legislation.
6 ROLES AND RESPONSIBILITIES

6.1 In line with the Trust’s Management Arrangements (2), 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.

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 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 Director of Service Development is the SIRO and is the nominated executive lead to ensure the Trust’s information risk is properly identified and managed and that appropriate assurance mechanisms exist.

6.6 Executive Directors and Associate Directors

6.6.1 Executive Directors and Associate Directors have delegated responsibility for managing risks in accordance with their portfolios and as reflected in their job descriptions. For example, the Director of Finance has executive responsibility for financial governance and associated financial risks.

6.6.2 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 the Policy and aware of their responsibility for risk

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

   (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

6.7 Clinical Directors, General Managers and Nurse Directors 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.

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

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

6.10 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.
6.11 **Risk Management Specialist Officers** (see the Patient and Healthcare Governance website <<add hyperlink>>for a comprehensive list) 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. It receives and reviews high-level and strategic risks via the Top Risk Report (reported quarterly) and the Assurance Framework (reported six-monthly). In addition, it receives relevant risk reports from its committees.

7.1.2 **Audit Committee**  
A non-executive committee established by and accountable to the Board of Directors, the committee has overall responsibility for integrated governance, risk management and internal control. It receives and reviews external and internal audit reports, the Assurance Framework and the Annual Governance Statement.

7.1.3 **Healthcare Governance Committee**  
A committee established by and accountable to the Board of Directors, it is responsible for healthcare related governance (including risk management) and receives and reviews reports from the Trust’s key healthcare governance groups and committees according to an annual workplan.

7.1.4 **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 Top Risk Report (reported quarterly) and the Assurance Framework (reported six-monthly) and reviews the Annual Governance Statement. 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 reviewed by directorate local governance group (or equivalent); and, risks that have been closed.
7.1.5 **Safety and Risk Management Board**
Accountable to the Healthcare Governance Committee, the board 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 TEG and the Healthcare Governance Committee.

7.1.6 **Risk Validation Group**
Accountable to the Safety and Risk Management Board, the group is responsible for reviewing 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.

7.1.7 **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. The governance groups report to Safety and Risk Management Board.

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

7.1.8 **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.

7.1.9 **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 etc) that have specific risk management responsibilities. A list of specialist risk groups is available on the Patient and Healthcare Governance website <<add hyperlink>>.

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 training which means that it is mandatory for some staff employed by the Trust, depending on their job role. There is more than one training option available for Risk Management and staff should complete the most relevant option to suit the responsibilities and risks associated with their role.
9.2 The Line Manager or Designated Supervisor should inform their staff about their personal Mandatory and Job Specific Training requirements during induction or when there is a significant change in role. The Line Manager/Designated Supervisor should consult the Training Needs Analysis for Risk Management/Health and Safety on the Mandatory Training Intranet Site to find out if training is mandatory for the post, and if so which training option is appropriate.

9.3 The 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 Training Courses**
The Line Manager/Designated Supervisor should book the employee onto any relevant training courses and confirm these arrangements with the employee. This process should be completed as part of induction and repeated when updates are due. Instructions on how to book training places is included in the Mandatory and Job Specific Training Policy together with a full explanation of the mandatory training system. E-learning can be accessed on the Learning and Development Intranet Site. Any member of staff can access the Mandatory Training Intranet Site to view the Training Needs Analysis and Prospectus.

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 Mandatory and Job Specific Training Policy for recording attendance using signing-in sheets. Trust e-learning packages include automatic recording of compliance. The Administrative staff who enter attendance records into OLM 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 Mandatory and Job Specific Training Policy for checking compliance and following-up non-compliance. This includes using reports generated from OLM records 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 Compliance with this policy is monitored through the Healthcare Governance Risk Management Audit Programme which will be launched and co-ordinated by the Patient and Healthcare Governance Department each year. The audit schedule, guidance and documentation are posted on the Patient and Healthcare Governance intranet site. The Healthcare Governance Committee will review the audit results.
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 Assurance Framework 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, 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 (2009) *Excellence as Standard: Corporate Strategy 2009 -12*
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.

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
- Risk assessment as part of Trust business – at all levels of the organisation
- 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) 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
- 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:

<table>
<thead>
<tr>
<th>Objective: To travel from the Northern General (NGH) to Weston Park Hospital (WPH) for a meeting at a certain time</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk description</strong></td>
</tr>
<tr>
<td>Failure to get from the NGH to WPH for a meeting at a certain time</td>
</tr>
<tr>
<td>Being late and missing the meeting</td>
</tr>
<tr>
<td>Eating on the shuttle bus is not allowed so I was hungry</td>
</tr>
<tr>
<td>Missing the shuttle bus causes me to be late and miss the meeting</td>
</tr>
<tr>
<td>Severe weather prevents the shuttle bus from running and me getting to the meeting</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Domain</th>
<th>Consequence Score and Descriptor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Insignificant</td>
<td>Minor</td>
</tr>
<tr>
<td>Injury or Harm Physical or Psychological</td>
<td>No / minimal injury requiring no / minimal intervention or treatment</td>
</tr>
<tr>
<td>No time off work required</td>
<td>Requiring time off work for &lt; 4 days</td>
</tr>
<tr>
<td>Quality of the Patient Experience / Outcome</td>
<td>Unsatisfactory patient experience not directly related to the delivery of clinical care</td>
</tr>
<tr>
<td>Statutory</td>
<td>Coroner’s verdict of natural causes, accidental death, open</td>
</tr>
<tr>
<td>No or minimal impact of statutory guidance</td>
<td>Breach of statutory legislation</td>
</tr>
<tr>
<td>Business/Finance &amp; Service Continuity</td>
<td>Minor loss of non-critical service</td>
</tr>
<tr>
<td>Financial loss &lt;£10K</td>
<td>Financial loss £10 - 50k</td>
</tr>
<tr>
<td>Potential for Complaint or Litigation / Claims</td>
<td>Complaint possible</td>
</tr>
<tr>
<td>Unlikely to cause complaint or litigation</td>
<td>Claim(s) &lt; £10k</td>
</tr>
<tr>
<td>Short-term low staffing level that temporarily reduces patient care / service quality (&lt;1 day)</td>
<td>Ongoing low staffing level that reduces patient care / service quality</td>
</tr>
<tr>
<td>Concerns about competency / skill mix</td>
<td>Minor error(s) due to levels of competency (individual / team)</td>
</tr>
<tr>
<td>Staffing and Competence</td>
<td></td>
</tr>
<tr>
<td>Reputation or Adverse Publicity ¹</td>
<td>Within the Trust Local media 1 day e.g. inside pages, limited report</td>
</tr>
</tbody>
</table>

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

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

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.

Table 3: Risk Score

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Consequence</th>
<th>Insignificant (1)</th>
<th>Minor (2)</th>
<th>Moderate (3)</th>
<th>Major (4)</th>
<th>Catastrophic (5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rare (1)</td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Unlikely (2)</td>
<td></td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>Possible (3)</td>
<td></td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>15</td>
</tr>
<tr>
<td>Likely (4)</td>
<td></td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>20</td>
</tr>
<tr>
<td>Almost certain (5)</td>
<td></td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>20</td>
<td>25</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Scores</th>
<th>Risk grade</th>
<th>Responsibilities and Accountability</th>
</tr>
</thead>
</table>
| 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 Top Risk 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.

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.

   Further guidance and support is available from directorate Risk/Governance Leads or Patient and Healthcare Governance.
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 (see over) 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(s) must be notified of all risks scored at 4 or above.

3) COMPLETING THE FORM
i) Department / Directorate - Specify the department(s) / directorate(s) responsible for managing the risk.

ii) 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.

iii) 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.

iv) 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.

v) 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).

vi) 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.

vii) Assessor(s) - If the assessment involved more than one person, list the key persons and identify the Lead Assessor.

viii) Date of assessment - The date the assessment was undertaken.

ix) 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.

4) WHAT TO DO WITH A COMPLETED FORM
Please ensure all completed Risk Assessment Forms are filed safely.

If the Initial Risk Score is more that 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 D of the Risk Management Policy). An electronic copy of the Risk Assessment Form must be attached as a document in the DATIX risk record.
To be completed for newly identified risks and on each occasion the risk is formally reviewed. For further guidance on completing this form please refer to Guidelines for Completing a Risk Assessment Form (available on STH intranet) or contact your directorate Risk/Governance Lead.

<table>
<thead>
<tr>
<th>Department / Directorate</th>
<th>Description of risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Existing controls in place</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

Risk Score i.e. with existing controls in place

<table>
<thead>
<tr>
<th>Consequence (1-5)</th>
<th>Likelihood (1–5)</th>
<th>Risk Score (1 – 25)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Action Plan to reduce the risk to an acceptable level

<table>
<thead>
<tr>
<th>Description of actions</th>
<th>Cost</th>
<th>Responsibility (Job title)</th>
<th>Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Register risk on DATIX (for all risks &gt; 3)</td>
<td>nil</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Target Risk Score i.e. after full implementation of action plan

<table>
<thead>
<tr>
<th>Consequence (1-5)</th>
<th>Likelihood (1–5)</th>
<th>Risk Score (1 – 25)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Assessment undertaken by:

<table>
<thead>
<tr>
<th>Name</th>
<th>Job title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Lead:

<table>
<thead>
<tr>
<th>Date of assessment</th>
<th>Date of next review</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 by Patient and Healthcare Governance.

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. Top Risk Report, Assurance Framework

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 expected risk score
- action plan
- review date (up to a maximum of 1 year)

A summary of risk registers shall be maintained by the Patient and Healthcare Governance department.

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. 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 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 (ensuring that all the subordinate risks are fully described) and 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 aggregated risk will supersede the subordinate risks, which should be removed from DATIX. 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.

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. All risks must be reviewed at least once a year.

A new Risk Assessment Form shall be completed for all subsequent reviews and must be uploaded on to DATIX.

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 Top Risk Report and the Assurance Framework, although this has been delegated to the Trust Secretary and Assurance Manager. The Top Risk Report which includes high-level and strategic risks, is reviewed at least four times a year by TEG and the Board of Directors. The Assurance Framework which identifies risks to the achievement of the Trust’s strategic objectives is reviewed twice a year by TEG, the Audit Committee and the Board of Directors.
d) 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 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Further guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Mandatory field. Please ensure the title gives a brief and unique description.</td>
</tr>
<tr>
<td>Trust</td>
<td>This field is automatically populated.</td>
</tr>
<tr>
<td>Reference</td>
<td>Optional field. May be used for local purposes or left blank.</td>
</tr>
<tr>
<td>ID</td>
<td>This field is automatically populated.</td>
</tr>
<tr>
<td>Site</td>
<td>Mandatory field. Choose from the options list.</td>
</tr>
<tr>
<td>Group</td>
<td>Mandatory field. Choose from the options list.</td>
</tr>
<tr>
<td>Directorate</td>
<td>Mandatory field. Choose from the options list.</td>
</tr>
<tr>
<td>Specialty</td>
<td>Mandatory field. Choose from the options list.</td>
</tr>
<tr>
<td>Location - type</td>
<td>Mandatory field. Choose type of location of risk(s) from the options list.</td>
</tr>
<tr>
<td>Location - specific</td>
<td>Mandatory field. Choose precise location from the options list e.g. R Ward</td>
</tr>
<tr>
<td>Risk Type</td>
<td>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)</td>
</tr>
<tr>
<td>Sub-type</td>
<td>Mandatory field. Choose from the options list.</td>
</tr>
<tr>
<td>Objectives</td>
<td>Mandatory field. Assess whether the risk threatens achievement of any of the corporate objective(s) and select as appropriate from the options list.</td>
</tr>
<tr>
<td>Assurance sources</td>
<td>Mandatory field. As appropriate, select positive assurance source(s) from the options list.</td>
</tr>
<tr>
<td>Field</td>
<td>Further guidance</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Handler</td>
<td>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.</td>
</tr>
<tr>
<td>Manager</td>
<td>Mandatory field. Select the person from the options list with overall responsibility for managing the risk to an acceptable level.</td>
</tr>
<tr>
<td>Description</td>
<td>Mandatory field. Please ensure the risk is fully described as reflected on the Risk Assessment Form.</td>
</tr>
<tr>
<td>Controls in place</td>
<td>Mandatory field. Please list in full the current controls in place as recorded on the Risk Assessment Form.</td>
</tr>
<tr>
<td>Consequence</td>
<td>Mandatory fields. Choose appropriate descriptor from the options list to score Initial, Current and Target risk.</td>
</tr>
<tr>
<td>Likelihood</td>
<td>Mandatory field. Choose appropriate descriptor from the options list to score Initial, Current and Target risk.</td>
</tr>
<tr>
<td>Score</td>
<td>The final risk score is automatically calculated.</td>
</tr>
<tr>
<td>Rating</td>
<td>The final risk rating is automatically calculated.</td>
</tr>
<tr>
<td>Cost of risk</td>
<td>Please leave blank.</td>
</tr>
<tr>
<td>Type</td>
<td>Please leave blank.</td>
</tr>
<tr>
<td>Approx. investment</td>
<td>Please leave blank.</td>
</tr>
<tr>
<td>Adequacy of controls</td>
<td>Mandatory field. Select from the options list, on the basis of controls in place at the time the risk was initially assessed.</td>
</tr>
<tr>
<td>Cost/Benefit</td>
<td>Please ignore. (This field should default to £0.00)</td>
</tr>
<tr>
<td>Opened</td>
<td>Mandatory field. Enter the date the risk was registered on the system. This field should not be amended.</td>
</tr>
<tr>
<td>Review date</td>
<td>Mandatory field. Enter the date when the risk is scheduled to be reviewed. This field must be updated after each review.</td>
</tr>
<tr>
<td>Closed date</td>
<td>Optional field. Only enter this date when the risk has been reduced to an acceptable level (i.e. the target risk score).</td>
</tr>
<tr>
<td>Number of actions</td>
<td>Optional field. Enter the total number of discrete mitigating actions as identified in the Action Plan (see below).</td>
</tr>
<tr>
<td>Open actions</td>
<td>Optional field. Enter the total number of outstanding actions as identified in the Action Plan (see below). This field should be updated at every review.</td>
</tr>
</tbody>
</table>

**Additional Functionality** (see buttons on right-hand side of Risk Module screen)

<table>
<thead>
<tr>
<th>Field</th>
<th>Further guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contacts</td>
<td>Not applicable for Risk Module. Please leave blank.</td>
</tr>
<tr>
<td>Documents</td>
<td>Optional field. This should be used to attach relevant documents such as Risk Assessment Form and any associated documentary evidence.</td>
</tr>
<tr>
<td>Field</td>
<td>Further guidance</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Extra Fields</td>
<td>Not applicable for Risk Module. Please leave blank.</td>
</tr>
<tr>
<td>Notepad</td>
<td>Optional field. This may be used as an aide memoir etc.</td>
</tr>
<tr>
<td>Events</td>
<td>Not applicable for Risk Module. Please leave blank.</td>
</tr>
<tr>
<td>Actions</td>
<td>Mandatory field. This must be completed for each discrete mitigating action. This field must be updated at every review.</td>
</tr>
<tr>
<td>Links</td>
<td>Not applicable for Risk Module. Please leave blank.</td>
</tr>
<tr>
<td>Assurance</td>
<td>Optional field. Handlers are encouraged to use this to record relevant local objectives that are threatened by the risk; principal controls and identify any gaps in controls; and assurances and identify any gaps in assurance.</td>
</tr>
<tr>
<td>Ratings Audit</td>
<td>This is automatically populated and provides an audit trail of changes to the risk ratings fields.</td>
</tr>
</tbody>
</table>
FLOWCHART OF THE PROCESS FOR IDENTIFYING, ASSESSING, ACTIONING AND REVIEWING DIRECTORATE RISKS

Risk identified

Low risks (i.e. 3 and below) managed locally and risk assessments stored in local workplace for review once per year

Risk assessed and scored

Risks of 4 and above notified to Risk/Governance Lead

Scheduled Review

Risk discussed and minuted at directorate risk group (or equivalent). Action plan and review date(s) agreed

Risk & Actions entered/amended on risk register (Datix) with review date

No action i.e. risk ‘tolerated’ at current level. Risk entered/amended on risk register (Datix)

RVG review
Risk Validated? Y/N

Risk closed
Risk register (Datix) updated

No
Feedback to Risk/Governance Lead

Yes

TEG/Safety & Risk Management Board

Yes