NHS
Mid Essex Hospital Services
NHS Trust

<table>
<tr><td>Document Title:</td><td colspan="3">Risk Management Policy and Procedures</td></tr>
<tr><td>Document Reference/Register no:</td><td>04061</td><td>Version Number:</td><td>11.1</td></tr>
<tr><td>Document type:
(Policy/ Guideline/ SOP)</td><td>Policy</td><td>To be followed by:
(Target Staff)</td><td>All staff</td></tr>
<tr><td>Ratification Issue Date:
(Date document is uploaded onto the intranet)</td><td>19th June 2018</td><td>Review Date:</td><td>May 2021</td></tr>
<tr><td>Developed in response to:</td><td colspan="3">National Guidance/Recommendations
(i.e. NICE; RCOG) Best Practice</td></tr>
<tr><td colspan="3">Contributes to HSC Act 2008 (Regulated Activities) Regulations 2014(Part 3); and CQC Regulations 2009 (Part 4)
CQC Fundamental Standards of Quality and Safety:</td><td>17

(Insert no. of Standard)</td></tr>
<tr><td>Issuing Division/Directorate:</td><td colspan="3">Corporate Nursing</td></tr>
<tr><td>Author/Contact:
(Asset Administrator)</td><td colspan="3">Helen Clarke, Head of Governance</td></tr>
<tr><td>Hospital Sites:
(tick appropriate box/es to indicate status of policy review i.e. joint/ independent)</td><td colspan="3">x MEHT
□ BTUH
□ SUH</td></tr>
<tr><td>Consultation:</td><td colspan="3">(Refer to page 2)</td></tr>
<tr><td>Approval Group / Committee(s):</td><td>Site Directors

PS&Q</td><td>Date:</td><td>31/05/18

07/06/18</td></tr>
<tr><td>Professionally Approved by:
(Asset Owner)</td><td>Claire Panniker, Chief Executive Officer</td><td>Date:</td><td>18th June 2018</td></tr>
<tr><td>Ratification Group(s):</td><td>Document Ratification Group</td><td>Date:</td><td>19th June 2018</td></tr>
<tr><td>Executive and Clinical Directors
(Communication of minutes from Document Ratification Group</td><td>Date:

June 2018</td><td>Distribution Method:</td><td>Trust Intranet/ Internet</td></tr>
</table>

Consulted With:	**Post/ Approval Committee/ Group:**	**Date:**
	Site Directors	21/05/18
	Divisional Directors	21/05/18
	Associate Directors of Operations	21/05/18
	Associate Directors of Nursing	21/05/18
	Health & Safety Group	21/05/18
Alison Felton	Head of Pharmacy	21/05/18
Louise Teare	DIPC	21/05/18
Kate Stevens	Risk & Safety Manager	21/05/18
Goolam Ramjane	Information Governance Manager	21/05/18

Consulted With:	Post/ Approval Committee/ Group:	Date:
Alison Felton	Head of Pharmacy	21/05/18
Louise Teare	DIPC	21/05/18
	Associate Directors of Operations	21/05/18
	Health & Safety Chair	21/05/18
	Divisional Directors	21/05/18
	Associate Directors of Nursing/ Head of Midwifery	21/05/18
	Heads of Department	21/05/18
Goolam Ramjane	Information Governance Manager	21/05/18
Kate Stevens	Risk & Safety Manager	21/05/18

Related Trust Policies (to be read in conjunction with)	(Refer to the main body of the text) 1. Risk Management Strategy 2. Incident Policy 3. Serious Incidents Policy 4. Health and Safety Policy and Procedures 5. The Complaints Policy and Procedure 6. Information Governance Policy 7. Business Continuity Policy and Plan 8. Policy for the Management of Conduct and Capability 9. All policies and procedures associated with Healthcare Acquired Infections 10. Violence and Antisocial Behaviour Policy 11. Safeguarding policies and procedures (Adult and Child)

Document Review History:

Version No:	Authored/Reviewer:	Summary of amendments:	Issue Date:
2.1	N Paull		July 2005
3.1	N Paull		April 2007
3.2 / 3.3	N Paull / T Lafferty		July 2008
4.0	T Lafferty		Sept 2009
5.0	T Lafferty	Amendment to 7.6	13 Jan 2010
5.1	S Barnes	Amendment to section 7	15 Jan 2010
5.2	H Clarke	to include monitoring processes and extend review date	25 Feb 2011
5.3	J Day / L Wilson/H Clarke	Full review	29 July 2011
6.0	H Clarke	Updated PS&QC reporting structure and ToR	11 Nov 2011
6.1	J Day	Amended to reflect amendments to RAF process and templates, attached terms of reference and to reflect requirements identified at NHSLA assessment	23rd May 2012
6.2	J Day, D Miller, H Clarke	Full review	16 Aug 2012
7.0	J Day, A O'Connor, H Clarke	Full review	16 Jan 2014
8.0	J Day	Full review	23 Sep 2014
8.1	J Day	Update PS&Q Terms of Reference	18 Nov 2014
8.2	J Day	Update risk assessment templates	27 Mar 2015
9.0	H Clarke	Full review	27 May 2016
10.0	H Clarke	Full review	15th May 2017
11.0	H Clarke	Full review	June 2018
11.1	H Clarke	Addition of risk escalation framework as appendix 7 and point 4.6.3	30th January 2019

RISK MANAGEMENT POLICY AND PROCEDURES

CONTENTS

Section	Section Title	Page
1	Introduction	4
2	Scope	4
3	Roles and Responsibilities	4
4	Process	12
5	Risk Management Tools	17
6	Implementation and Communication	18
7	Equality Impact Assessment	18
8	Review	18
Appendices:		
Appendix 1	Risk Management Process	20
Appendix 2	Sources of Risk Identification	21
Appendix 3	Risk Assessment Guidelines	22
Appendix 4	Corporate Risk Assurance Framework	25
Appendix 5	Definitions	27
Appendix 6	Training Needs Analysis	30
Appendix 7	Risk escalation and de-escalation framework	31

1.0 Introduction

1.1 Mid Essex Hospitals Services Trust (the Trust) recognises that the activities associated with caring for patients, employing staff, providing facilities and services and managing finances are all, by their nature, activities that involve risk. These risks are present on a day-to-day basis throughout the organisation and whilst it may not always be possible to eliminate these risks, they can be managed to an acceptable level.

1.2 Risk management is both a statutory requirement and an indispensable element of good management at the Trust. It is a fundamental part of the total approach to quality, corporate and clinical governance and is essential to the Trust's ability to discharge its functions as a partner in the local health and social care community, as a provider of health services to the public and an employer of significant numbers of staff.

1.3 It is expected that all risk management activities in the Trust will follow the process described within this document to ensure a common and robust approach is adopted to risk management.

2.0 Scope

2.1 This Policy and Procedures document applies equally to all members of staff either permanent or temporary, and to those working within, or for, the Trust under a contract for services.

2.2 It is the responsibility of staff within wards, departments, Directorates and Divisions to identify, assess, control and document their own risks and to record these on the Trust risk management system.

2.3 The risk management process applies to all categories of risk.

2.4 This Policy and Procedures document should be read in conjunction with the Trust's Risk Management Strategy.

3.0 Roles and Responsibilities

3.1 Chief Executive

3.1.1 The Chief Executive, as the Accountable Officer, has overall responsibility for ensuring that the Trust operates effective risk management and health and safety systems, meeting all statutory requirements and adhering to risk guidance issued by the Department of Health.

3.1.2 The Chief Executive provides leadership and strategic direction to risk management processes. This responsibility includes consideration of the Trust's Corporate Risk Assurance Framework and resource allocation relating to the significant risks of the Trust.

3.1.3 As Accountable Officer, the Chief Executive will ensure:

- The Trust's Principal Objectives are agreed.
- Sound systems of internal control based on an ongoing management process designed to identify the principal risks to the achievement of the Trust's objectives; to evaluate the nature and extent of those risks; and to manage them efficiently, effectively and economically.
- Internal Audit Plans review the effectiveness of the system of internal control.
- Systems of internal control are underpinned by compliance with the core controls assurance standards of Governance, Financial Management and Risk Management.

3.1.4 The Chief Executive will use the Trust Board Sub Committees and groups as the principal means by which these responsibilities are made operational and effectiveness monitored.

3.1.5 The Chief Executive will prepare and sign an annual Governance Statement for inclusion in the Trust Annual Report. He/she will ensure an Annual Quality Account is prepared.

3.1.6 The Chief Executive has delegated lead responsibility for risk management to Executive Directors and the Trust's Managing Director who are accountable to the Board for the management of a specified group of risks.

3.2 Chief Finance Officer

3.2.1 The Chief Finance Officer is accountable to the Trust Board and Chief Executive for the Trust's financial risk management and control activities. The Chief Finance Officer is responsible for ensuring that the Trust carries out its business of providing healthcare within sound Financial Governance arrangements that are controlled and monitored through robust audit and accounting mechanisms that are open to public scrutiny on an annual basis.

3.2.2 The Chief Finance Officer will have an infrastructure in place across the organisation to fulfil these requirements.

3.2.3 The Chief Finance Officer seeks the Internal Auditor's Opinion on the effectiveness of Internal Control and Internal Financial Control on behalf of the Chief Executive.

3.3 Chief Medical Officer and Chief Nurse

3.3.1 The post holders are accountable to the Chief Executive and to the Board for the delivery of the Trust's patient safety strategy. A key element of this relates to the management of an efficient and effective clinical governance system.

3.3.2 The post holders are responsible for ensuring that the Trust has systems to learn from experience and that lessons learned are systematically shared across the organisation.

3.3.3 The post holders are responsible for identifying the principal risks to the Clinical Governance arrangements and through working with the appropriate Executive Directors, Site Directors, Divisional Directors, Associate Directors of Operations, Associate Chief Nurses, Senior Managers or clinicians to ensure risks identified through risk profiling/ assessment are eliminated or reduced.

3.4 Site Medical Officer

3.4.1 The Site Medical Director is responsible for the management of risks within their areas of operational responsibility.

3.4.2 The Site Medical Director has lead responsibility for Clinical Audit, National Clinical guidance/NICE guidance and Medical Staff education

3.4.3 The Site Medical Director acts as the lead for Research and Development.

3.4.4 The Site Medical Director will have specific roles as defined in specific Trust Policies and procedures and will fulfil these roles as required.

3.5 Chief Nurse and Site Director of Nursing

3.5.1 The Chief Nurse is accountable to the Trust Board and Chief Executive for the Trust's Governance and Risk Management activities. With Executive responsibility for governance, quality, complaints, safeguarding and patient experience advocacy for the Trust, the Chief Nurse provides a clear focus for the management of organisational risks and for coordinating and integrating all of the Trust's risk management arrangements on behalf of the Trust Board.

3.5.2 Aspects of these responsibilities will be delegated to the Site Director of Nursing and Head of Governance.

3.5.3 The Site Director of Nursing is the site lead for risk and is responsible for ensuring that mechanisms are robust so as to assure the Trust Board that standards of responsible risk management are applied at all levels within the Trust and enabling corporate compliance with the national requirements and standards set by the Care Quality Commission and Regulatory Bodies

3.5.4 The Site Director of Nursing is responsible for the management of risks within their areas of operational responsibility and will be accountable for the professional management of the nursing teams and the development of clinical nursing practice to achieve excellence in all aspects of nursing. The Site Director of Nursing will ensure the highest standards of care at ward level and lead on the improvements to the patient's experience.

3.5.5 The Site Director of Nursing ensures all identified serious incidents are managed appropriately and has responsibility for the development and implementation of the Trust incident reporting systems and processes. The Site Director of Nursing, or in their absence, an appointed deputy will jointly chair the Executive Review Group (ERG) with the Medical Directors meeting in accordance with the Serious Incident Policy. The attendees including the Associate Directors of Nursing and Head of Midwifery should raise any significant risks arising and the Site Director of Nursing will ensure appropriate action is taken and followed up. This will include escalating immediate risks to other members of the Executive Team and Site Directors where indicated.

3.5.6 The Site Director of Nursing will have specific roles as defined in specific Trust policies and procedures and will fulfil these roles as required ensuring appropriate and proportionate delegation to designated officers as identified.

3.6 Site Director of HR and Site Chief Operating Officer

3.6.1 The post holders will be accountable for the operational management of their respective patient service delivery teams, (Appendix 2) supporting the Trust's risk management systems and processes.

3.6.2 They have statutory obligations for the management of risk within the workplace, conduct assessments for all work-based activity and foster a culture of risk awareness throughout the Directorates. Risk assessment should cover all areas of activity – operational, financial, clinical, fire and health and safety. They are expected to set a high standard of pro-active risk management and to be seen as exemplar role models.

3.7 Director of Infection Prevention & Control (DIPC)

3.7.1 Reporting to the Chief Executive, the DIPC is responsible for the management of infection risk within the Trust. The DIPC will ensure that systems are in place to promptly identify and mitigate infection risks to patients, staff and visitors.

3.7.2 The DIPC will maintain the Infection Prevention & Control Risk Assurance Framework ensuring compliance with statutory requirements; produce an Annual Report, plan the Infection Protection work programme and action plan for approval by the Patient Safety and Quality Committee.

3.8 Trust Secretary

3.8.1 The Trust Secretary is responsible for ensuring that the Trust operates in accordance with statutory regulations and that there is appropriate stewardship and corporate governance of the business of the Trust. The Trust Secretary is responsible for informing the Board through the Chair of the Trust's governance matters including processes and systems.

3.8.2 The Trust Secretary is responsible for ensuring the Trust complies with relevant legislation and regulation.

3.8.3 Ensures that the Board is adequately informed as to the significant risks facing the organisation through the management and presentation of the Board Assurance Framework and Corporate Risk Assurance Framework.

3.8.4 The Trust Secretary is responsible for facilitating the smooth operation of the Trust's formal decision and reporting processes maintaining the registers of interests of members of the Board, hospitality and tenders and coordinating and monitoring audit findings on behalf of the Trust Board in order to ensure that actions required by the Board are implemented according to agreed timetables set.

3.8.5 The Trust Secretary ensures that Committees of the Board are properly constituted with clear terms of reference and is responsible for ensuring they are observed and reviewed as required and on at least an annual basis. They will ensure effective and well managed meetings and effective management of the Board and Sub Committee business programme, in accordance with the governance agenda and Trust Standing Orders and Standing Financial Instructions ensuring actions required in relation to risk management and corporate governance are completed.

3.8.6 The Trust Secretary acts independently of the Board to provide advice on corporate governance issues to the Board and the Chairman and ensures that Directors meet the requirements of the Fit and Proper Person Test, that effective arrangements for the proper induction of Directors are in place and provides advice and support regarding the discharge of their duties.

3.8.7 The Trust Secretary has responsibility for overseeing the Claims and Coronial requests processes and management of any issues arising within Preventing Further Deaths communications.

3.9 Head of Governance

3.9.1 The Head of Governance supports the Director of Nursing and Chief Nurse who is the Executive Lead for risk management across the Trust. The Head of Governance will provide specialist advice on all Governance issues and will:

- Monitor and report on the risk profile of the Trust creating the Trust-wide RAF from those of the contributing Directorates and Departments.
- Ensure that the Board, managers and clinicians have the information they need to manage their identified risks. This includes supporting Directorate Managers in maintaining and developing the Trust's 'local' Risk Assurance Frameworks.
- Ensure an effective incident reporting process is in place with an emphasis on developing learning outcomes from investigations.
- Analysing any correlation between the various clinical governance work streams.

3.9.2 Have defined responsibilities as a lead manager for ensuring that systems are in place to monitor progress against the Care Quality Commission's fundamental standards and regulatory requirements

3.10 Chief Human Resources Director / Site Head of Human Resources

3.10.1 The Chief Human Resources Director is accountable for Human Resource issues across the Trust. They are responsible for workforce and organisational development activities.

3.10.2 The Chief Human Resources Director is responsible for the learning and development agenda of the Trust, including the Mandatory training programme. There are close working arrangements with the Executive Team and Site Directors with regard to ensuring that workforce planning and risk management integrates with the Trust's clinical and organisational risk management activities and is closely involved in consideration of the recommendations of the Board sub-Committees.

3.10.3 The Site Head of HR is responsible for the management of risks within their own areas of operational responsibility.

3.10.4 The Site Head of HR is responsible for ensuring provision of employment services across the Trust and ensuring that there is a systematic approach to managing the risks of employment checks and professional clinical registration.

3.10.5 The Site Director of HR will have specific roles as defined in specific Trust policies and procedures and will fulfil these roles as required.

3.11 **Chief Estates & Facilities Officer**

3.11.1 The Chief Estates & Facilities Director is the executive lead responsible for Health and Safety, Fire Safety, Security, Waste Management, and the Trust Estate.

3.12 Directors of Estates & Facilities Services

3.12.1 The Estates & Facilities Director of Operations and the Estates & Facilities Specialist Services Director is responsible for the operational management of risks within their own areas of operational responsibility all services managed by the Estates and Facilities directorate

3.12.2 The Estates & Facilities Director of Operations and the Estates & Facilities Specialist Services Director will have specific roles as defined in specific Trust policies and

3.13 **Site Chief Operating Officer**

3.13.1 The Chief Operating Officer is responsible for the overall management of all patient services, ensuring that all key access targets are met together with finance, waiting lists, human resources management.

3.13.2 The Chief Operating Officer is responsible for the management of risks within their own areas of operational responsibility including Bed and Flow Management and Discharge.

3.13.3 The Chief Operating Officer will have specific roles as defined in specific Trust policies and procedures and will fulfil these roles as required;

3.14 **Chief Information Officer / Senior Information Risk Owner (SIRO)**

3.14.1 The Chief Information Officer is responsible for the effective management of risks within their areas of operational responsibility including Information Technology and Security, Data Quality and Information Governance. The Chief Information Officer will ensure Privacy Impact Assessments are carried out prior to the installation of any networked IT system in relation to the management of person identifiable information.

3.14.2 The Chief Information Officer will act as the Senior Information Risk Officer and takes ownership of the Trust's information risk policy, acts as advocate for information risk on the board and provides written advice to the Accountable Officer on the content of their Statement of Internal Control in regard to information risk.

3.15 **Associate Directors of Operations, Associate Directors of Nursing and Head of Midwifery, Divisional Directors and Heads of Department**

3.15.1 Divisional Directors, Associate Directors of Operations, Associate Directors of Nursing, Head of Midwifery and Heads of Department have a key role for governance within Directorates / Departments including risk management. The main duties include:

- Monitoring compliance with the Directorate / Department risk management procedures in line with this policy
- Maintaining and reviewing the Directorate / Department RAF
- Ensuring the progressive reduction of risk to the lowest reasonable level
- Ensuring action plans are completed on time
- Escalating risk to the appropriate Trust committee as required by this policy

- Ensuring learning takes place from incidents, claims and complaints and that over time there is a tangible reduction in severity and frequency of adverse events

3.16 **Head of Midwifery (HoM)**

3.161 The HoM is the most senior midwife in the Trust and as such is professionally accountable for the Governance and Risk arrangements within the Directorate. For maternity this includes ensuring risks are identified, reported, managed and that lessons are learned through formalised risk management processes. The following structures are in place within Maternity Services to support this process:

- Labour Ward Forum
- Multidisciplinary Risk Management Meeting

3.16.2 These report into the Clinical Audit: Paediatric and Obstetric and Perinatal Mortality Meetings which subsequently report into the Directorate Clinical Governance Meetings.

3.16.3 The Head of Midwifery is responsible for overseeing clinical and non-clinical risks including clinical outcomes, health and safety, patient experience and complaints. All incidents are reported via the DATIX system and mitigation managed locally by the risk management midwife and Head of Midwifery, monitoring of recommendations, action plans and formal feedback to staff is the responsibility of the risk management midwife

3.16.4 The Head of Midwifery has direct access to the Executive Team and Board via the Site Director of Nursing and the Executive Lead for the Directorate for the instant escalation of concerns about governance and risk.

3.17 **Lead Nurses, Lead Midwives and Heads of Department**

3.17.1 The Lead Nurses, Midwives and Heads of Department are responsible for:

- The active implementation of risk assessment and risk management in their work areas, supporting the maintenance of the directorate RAF
- Ensuring appropriate risk assessments are reviewed for each of their departments on a minimum of an annual basis to comply with Health and Safety legislative.
- Ensuring action plans are completed on time
- Ensuring learning takes place from incidents, claims and complaints such that over time there is a reduction in severity and frequency of adverse incidents.

3.18 **Lead Midwife for Clinical Governance**

- Supports the HoM in the management and mitigation of risk within maternity
- Chairs the risk management meeting and sits on the Labour Ward Forum
- All Datix incidents are reviewed daily and responded to
- The management of incidents and Serious Incidents is centralised through the Lead Midwife for Clinical Governance
- There is a specific remit for ensuring lessons are learned from clinical and non-clinical incidents by embedding through clinical visible leadership
- The monitoring of actions and recommendations is shared between this role and the HoM
- The Lead Midwife for Clinical Governance meets daily with the HoM to review all incidents and potential risks on the unit
- The Lead Midwife for Clinical Governance deputises at the SIMG for the HoM.

3.19 **Ward sisters / Charge Nurses / Departmental Managers**

3.19.1 Ward sisters, Charge Nurses and Department Managers are responsible for:

- The active implementation of risk assessment and risk management in their work areas, supporting the maintenance of the directorate RAF.
- Ensuring that all permanent staff within their areas attend appropriate training including mandatory training in accordance with the Mandatory Training Policy.
- Ensuring that all staff, including agency, bank and locum staff, receive a local induction documented using the appropriate checklist from that policy.
- Ensuring learning takes place from incidents, claims and complaints such that over time there is a reduction in severity and frequency of adverse incidents.

3.20 **Caldicott Guardian**

3.20.1 The Chief Medical Officer holds this responsibility and advises and leads on issues relating to patient information which includes investigation and reporting of information related incidents and ensuring that information risks are logged and notified to the relevant divisions.

3.20.2 Ensuring that all Information risks are reported to Patient Safety and Quality Committee, Mid Essex CCG, the Information Commissioner and are detailed in the Trust's annual report.

3.20.3 Ensuring that all information governance serious incidents are investigated and reported appropriately as required and that these are recorded on the Information Governance Toolkit Reporting Tool so that incidents that are rated at Level 2 are automatically reported to the Information Commissioner.

3.21 **Line managers**

Those with line management responsibilities will be accountable for the day-to-day aspects of risk management, including the management of incident reporting, investigation and that risk assessment processes are undertaken. They will:

- Identify the significant risks within the day to day practice of the Directorate or Department, with authority to take remedial action;
- Review hazards within their area and monitor the controls in place;
- Undertake identified specific risk assessments;
- Advise their line Manager and the Governance Team of any risks which cannot be adequately controlled; and work with directorate representatives to ensure compliance with current legislation and best practice;
- Include the identified risk in the relevant local Directorate or Department Risk Assurance Framework.

3.22.1 **Directorate Governance Facilitators / nominated risk leads**

Governance Facilitators / local risk leads will ensure that:

- Risks within their areas are recorded and reviewed appropriately;
- New risks are escalated for approval by the Divisional triumvirate.

3.23 **Employee responsibilities**

3.23.1 All staff are encouraged to use risk management as a mechanism to highlight areas for improvement.

3.23.2 All staff should:

- Comply with the risk management/health and safety arrangements appropriate to the work task being undertaken.

- Report to their line manager any deficiencies that could impact upon the health, safety and welfare of individuals (patients, staff, contractors, etc.).
- Complete and submit an incident report form in the event of a reportable incident (refer to the Trust's Incident Policy).
- Escalate by the quickest means possible incidents where serious harm has occurred or the potential for serious harm exists/existed (refer to the Trust's Incident Policy).
- Follow the Speak Up policy if they feel unable to raised issues via alternative routes
- Participate as directed by line management in any training deemed necessary to effectively manage risk.
- Comply with the Trust's key policies for risk management and any professional guidelines and standards set by the relevant professional bodies and associations.
- Use protective equipment as provided for the task to be undertaken if risk assessment determines its necessity.
- Not intentionally or recklessly interfere with or prejudice equipment that has been provided for the safety of them or others.

3.24 **Senior and Corporate Management**

A number of corporate post holders have specific responsibilities in the implementation of this policy including Workforce Delivery, Commercial, HR, Finance and Governance Leads. All senior managers have responsibility to support directorates by providing specific expertise on their specialist subjects, (e.g. risk management, radiation safety, pharmacy, Internal Audit, Waste management etc.).

3.25 **Trade Union and Staff Association Responsibilities**

3.25.1 All recognised Trade Union and Staff Associations may nominate Safety Representatives in accordance with national policy.

3.25.2 Registered Safety Representatives must provide notification of their appointment to the Director of HR and are entitled to such time off and facilities as necessary for the effective performance of their duties. These arrangements are negotiated through the JCNC through partnership agreements.

3.25.3 Health and Safety representatives should attend the Health and Safety Group.

3.26 **Contractors, Agency Staff and Volunteers**

3.26.1 Bank, Agency, Locum staff and Volunteers must acknowledge that management of risk is an individual as well as collective responsibility. They must expect to receive a local induction so they can work safely and if this does not happen they should report this to the employing agency

3.26.2 Contractors are required to comply with the contractual arrangements that specify the health, safety and risk management activities that must be observed while working in the Trust. This includes maintaining appropriate communication with the Trust Contract Administrator who is responsible for each Contract in accordance with the Trust's Control of Contractor Policy.

3.27 **Patients and visitors**

Have a role in identifying and reducing risk. They are expected to co-operate with Trust staff on request. They also have a responsibility to identify any issues or information that may place them at risk whilst receiving care within the Trust. Patients and visitors are encouraged to report incidents, to follow infection prevention and control procedures and share knowledge in relation to their care or condition which may minimise the likelihood of an adverse event.

4.0 Process

There are five steps to the risk management process which form a continuous cycle (refer to appendix 1):

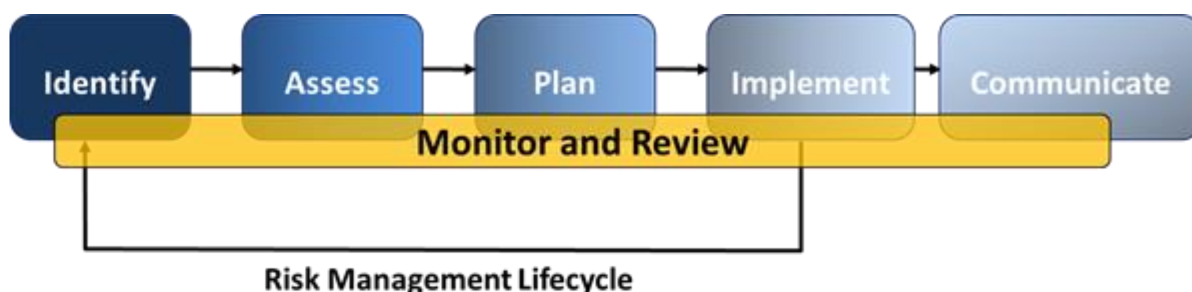
I. Identify the hazard and its risk – this information may be gathered from a number of different sources – refer to Appendix 2;

II. Risk assess;

III. Develop plan to manage / control the risk - identify controls and their effectiveness;

IV. Implement the plan - risk management

V. Communicate, monitor, and review the risk – share the risk and management plan with relevant staff. If unable to manage the risk locally, escalate to the Directorate / Divisional lead.



Risk Management Lifecycle

4.1 Risk Identification

4.1.1 Staff should initially consider what their main areas of work are and how these relate to their local objectives, and the objectives of the Trust. Every work activity that has a significant hazard should be assessed for risk. Identification using a systematic approach is critical, because a potential risk not identified at this stage will be excluded from further analysis.

4.1.2 All risks, whether under the control of the Trust or not, should be included at this stage. The aim is to generate an informed list of events that might occur. Key sources that will inform this exercise include:

- Compliance requirements with regulators and stakeholders such as the CQC, NHSI, the Clinical Commissioning Groups (CCGs) and NHS England;
- Recommendations from recent internal / external audit reports
- Root cause analysis of incidents, inquiries, complaints or claims
- Care pathway analysis
- Performance data
- Evaluation reports
- Trend and forecasting analysis
- Risks associated with the achievement of corporate objectives
- Other methods of horizon scanning.

4.1.3 Key questions staff should always address are:

- What could possibly go wrong; and at what point during the activity?
- How could it happen and why?
- What could be the effect?
- Who could be affected?

4.1.4 An overview of sources of risk identification is given in Appendix 2.

4.2 **Risk Assessment**

4.2.1 The risk assessment stage involves the analysis of individual risks to identify the consequences and likelihood of the risk being realised. A single method of assessment adopted from the National Patient Safety Agency is used for all risks and is detailed at Appendix 3.

4.2.2 The risk assessment guidance in Appendix 3 incorporates the following key features:

- Impact descriptors that cover different areas of risk – **table A**
- Likelihood descriptors for frequency and probability - **table B**
- A matrix to identify the risk evaluation score that uses impact and likelihood scales – **table C.**

4.2.3 The Trust risk assurance framework details three ratings to manage the risk:

1. **Inherent (initial) risk rating** – the (impact x likelihood) without any controls in place. The inherent risk is sometimes referred to as the *initial* or *gross* risk;
2. **Residual (current) risk rating** – the (impact x likelihood) with controls in place at the time of assessment or review. The residual risk is sometimes referred to as the *net* risk;
3. **Mitigated (target) risk rating** – the (impact x likelihood) with all controls in place and all controls being fully implemented and working effectively. The mitigated risk sometimes referred to as the *target* risk.

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

- Zero to three months
- Three to six months
- Six to nine months
- Nine to twelve months and
- Twelve months plus

4.2.5 All wards, departments, Corporate Directorates and Divisions are responsible for identifying all risks associated with the service provided (clinical and non-clinical), assessment and entry onto the risk assurance framework.

4.2.3 The initial risk assessment can be documented by direct entry onto the Datix System for those with access or by using the Trust Risk Assessment Template included as Appendix 4 or available on the Intranet.

4.2.4 Each risk assessor, upon identification of a risk, will complete all electronic fields (or the entire hard copy template) to ensure every aspect of the risk and its control is addressed. This shall include **what** the risk is, **where** it is, **who** may be harmed, how it is **controlled,** what further **action** is required and **how assurance** will be provided that the risk is being managed.

4.2.5 The key to understanding the true meaning of a risk is ensuring that the risk has a clear description. As a rule, always ensure the risk is fully visible by stating the risk failure followed by the cause of the risk, and impact of the risk

For example:

A failure to…..

Caused by…

May result in…

4.2.6 If a paper version of the Risk Assessment has been used, the assessment must be sent to the appropriate Governance Facilitator for entry onto the electronic system.

4.2.7 Upon receipt of a risk assessment, the Governance Facilitator will discuss the risk with the relevant manager to ensure the risk is appropriately described, the assessment is accurate and all required information as part of the assessment is completed. Once satisfied the risk is accurate and all the required information is recorded, they will ensure the risk is recorded on the Trust risk register reporting system.

4.2.6 If, during the completion of the risk assessment form, it becomes apparent that one or more of the hazards identified is a significantly higher risk than others, the risk should be entered onto the risk register separately, so as not to dilute high impact risks. Where a pattern or theme is apparent, then an overarching risk will be developed to take into account the wider context.

4.2.7 Each new risk added to the Datix system must be reviewed and approved by a member of the divisional triumvirate or Site Director.

4.2.7 The Trust has identified key risk issues which require regular review to ensure a consistent approach to risk assessment. There are templates available for each specialty to adapt for their own areas. These risk assessments should be reviewed regularly and following any relevant incidents. The frequency of review will be determined by the severity of the risk involved however annual review will be required as a minimum. The key specific risk assessments relate to:

- Environment incorporating Slips, Trips and Falls for staff and others
- Security including physical security of premises and violence and aggression and lone working
- Fire
- Moving and Handling
- Stress

Refer to specific related policies for further information.

The specific risk assessment templates are accessible via the Trust's Health and Safety Intranet page.

4.3 Control Identification

4.3.1 Controls are identified measures that are intended to minimise the likelihood or severity of a risk. An effective control will always reduce the probability of a risk occurring. If this is not the case, then the control is ineffective and needs to be reconsidered. Controls are intended to improve resilience.

4.3.2 Improvement of control effectiveness is a never ending quest. Controls can represent any of the following examples, but must exist and be fully developed or realised at the time of identification:

- Policy or procedure;

- Process;
- Approved action plan;
- Committee or working group in a monitoring capacity;
- Training;
- Performance monitoring.

4.3.3 It is important to note the following points when considering controls:

- **Resources** including structured training, processes, procedures supervision or quality assurance can dramatically reduce the likelihood of a risk occurring;
- **Processes** including press/communications management and contingency planning are effective at minimising the impact of most adverse events.

4.3.4 Where there are gaps in current controls or controls that are in development prior to maturity, then risk owners need to establish the most appropriate way forward and develop a risk action plan for implementation.

4.3.5 Controls may also be actions that are repeated, either regularly or in response to events, or they may be one-off actions or decisions. A control may be implemented to:

- **Avoid** risk;
- Take **opportunity** in a safe manner;
- **Modify** the risk;
- **Transfer** risk; or
- **Retain and reduce risk**.

4.3.6 Trust controls fall into three main categories:

- **Prevention** – these controls prevent a hazard or problem from occurring for example Policies, Procedures, Guidelines, Techniques, Processes, Training, Use of Equipment, Checklists, Computer Systems, Protective Clothing etc.
- **Detection** – these controls provide an early warning of control failure; (for example Audit, Inspection, Monitoring, Incident Reporting, Smoke detectors, Complaints, Surveys, Tests etc): and
- **Contingency** – these controls provide effective reaction in response to a significant control failure or overwhelming event and are designed to mitigate harm and improve resilience; (for example Evacuation Plan, Escalation Procedure, Continuity Plan, Backup Generator, Locum/Agency cover, Insurance etc).

4.3.7 Ward, departmental, corporate and divisional managers must ensure specific, measurable, appropriate, realistic and timely (SMART) actions are taken to address identified gaps in control. There is an expectation that managers will ensure that action plans are delivered by the required date

4.4 Assurance of Control Effectiveness

It is the policy within the Trust for assessors to consider the effectiveness of each control through the process of obtaining assurances that the control is in place and is operating effectively. These assurances are obtained from a variety of sources, such as:

- Management reports,
- Internal and external audit
- Other external assessors such as the Care Quality Commission and the NHSLA

Both positive and negative assurances must be explained, which means that a clear description of what would be seen, known, understood if the controls were effective or not effective in mitigating the risk.

Ward, departmental, corporate and divisional managers must ensure that any gaps in the assurances are clearly identified, and that appropriate actions are taken to identify any gaps in the assurance processes. There is an expectation that managers will ensure that actions to control assurance gaps are delivered within the same timescale as closing gaps in controls.

4.5 **Management of Risks**

4.5.1 The options for managing identified risks need to be assessed on the basis of cost and benefits derived. Options can be taken in combination or separately. In general the cost of managing risks needs to be commensurate with the benefits obtained. However, decisions should take account of the need to carefully consider rare but severe risks, which may warrant risk reduction measures that are not justifiable on strictly economic grounds.

4.5.2 There are three options for treating identified risks.

- **Avoid** the risk by deciding not to proceed with the activity likely to generate risk. Often this is not an option in the provision of health care. Risk aversion can lead to missed opportunities and increase in other risk areas by failure to engage with appropriate decision making around risk management.
- **Transfer** the risk to another party in its entirety or partially. For example, service level agreements or jointly managed services. Where risks are transferred in whole, or in part, the organisation acquires a new risk in that the organisation to which the risk has been transferred may not managed the risk or their share in it appropriately.
- **Accept** the risk and manage the risk.

4.6 **Reporting / Communication, monitoring and review**

4.6.1 Accountability through monitoring, reporting and communication are key considerations throughout the risk management process for both internal and external stakeholders. This ensures those who are responsible for implementing risk management and those with a vested interest, understand the decision making process and why particular actions are required.

4.6.2 **Review of Low Risks – the following is a guide only**

- Risks with a **residual** risk assessment of **5 or below** are reviewed, managed, monitored and owned within the wards or departments where they were initially identified. These risks are monitored locally by ward/ departmental managers. At any time that the ward or departmental manager feels that they are unable to manage the risk, they should seek advice with regards to escalation from their Divisional Lead or the Divisional Governance Facilitator.

4.6.3 **Medium to High Risks – the following is a guide only**

Divisional / Directorate Governance Meeting

- Risks with a **residual** risk assessment of **6 to 25** are owned by the host Division/ Directorate and monitored at the monthly Governance Meeting. Where a risk is no longer manageable within the division/ directorate; has a wider impact on other divisions or has a **residual risk rating of 12 or higher**, then the risk can be considered for escalation to the **Corporate Risk Register** via the **Senior Management Group / Site Directors.** (Refer to appendix 7)
- The Chair of the Governance Meeting (or designated person) will escalate the risk in one of two ways:

1. **If non-urgent** through the scheduled monthly Divisional Accountability meeting;
2. **If urgent (outside the schedule of meetings)** – report the risk to the Head of Governance who will escalate to the appropriate Site Director within one working day. The Site Director, with support from relevant members of the Site Team and advisors would determine the most appropriate course of action to manage the risk. During out of hours, the Director on call is responsible for taking immediate action and reporting the next working day.

In order to provide a robust audit trail the Risk and Safety Manager must be informed of risks that require escalation, or have been extraordinarily escalated, and ensure that a **Candidate Risk Form is** completed (Appendix 5).

4.6.4 **Senior Management Group**

The Senior Management Group convenes monthly and is chaired by the Managing Director. The Group may decide on escalation of individual risks to the Corporate Risk Assurance Framework or make recommendations to the Site Directors for a risk to be escalated to the Corporate Risk Assurance Framework.

4.6.5 **Site Directors**

- The Site Directors will review the Trust Corporate Risk Assurance Framework. The Corporate Risk Assurance Framework is owned by the Site Directors with each risk allocated to one of the corresponding Assurance Committees for monitoring/oversight.
- The Site Directors decide on the proposed escalation of divisional/ directorate risks to either the Corporate Risk Assurance Framework or the Board Assurance Framework (BAF). Unlike the Corporate Risk Assurance Framework, the BAF is owned and monitored by the Trust Board of Directors and hosts risks that directly impact on the strategic objectives of the organisation.
- Site Directors will also review the Board Assurance Framework.

5.0 Risk Management Tools

5.1 Risks may be identified proactively by managerial compliance self-assessments and review and analysis of incidents, complaints, claims or outcomes of safety inspection and/or audit. Root cause analysis may also be a source of risk identification. To ensure that all risks are identified, accurately described, appropriately controlled and consistently documented the following risk management tools are in place:-

5.2 **Risk Assessment Template**

A Risk Assessment Template has been developed for ward, department and Divisional and Corporate Directorate managers to assist them in documenting the risk, controls, assurances and action plan for each risk. This template may be used as an input document prior to recording on the Electronic Risk Register. Please refer to Appendix 4.

5.3 **Risk Assurance Framework**

5.3.1 The organisational Risk Assurance Framework (RAF) is a part of the Trust risk management system and provides a mechanism for recording details of each risk within a database so that risk records can be analysed and facilitate effective oversight of risk management at all levels.

5.3.2 The RAF is a register of risks which have been evaluated but not yet fully controlled or which the Trust accepts it must retain; these are therefore risks which may impact upon meeting Trust objectives. The RAF includes details of the nature of the risk, the severity, likelihood and overall rating, the service(s) which owns the risk, the controls currently in

place, assurances including the forum where progress in mitigating the risk is monitored, and progress achieved.

5.3.3 Each Clinical Directorate will review the relevant risks via their monthly governance meetings.

5.3.4 The Corporate RAF comprises those risks escalated to and agreed for inclusion by the Site Directors.

5.4 Board Assurance Framework

- The Board Assurance Framework reflects the principal strategic risks to delivering the Trust's objectives. It reflects an amalgam of the information from the risk assurance frameworks, organisational performance and the Board Committees and their direct reports.
- All risks are linked to the annually agreed Principal Risks and the Board Assurance Framework is considered at every in public Board meeting.

5.5 Risk Management Training

- In order to ensure that staff possess sufficient awareness of risk management and are competent to identify, assess and manage risk within their working environment, risk awareness/ assessment training will be made available to relevant staff as part of the Risk Management / Health and Safety Training Programme.
- In respect of new staff, information on risk management including information on incident reporting is included in the general induction arrangements for all staff.
- Please refer to Appendix 6 for further details within the Training Needs Analysis.

6.0 Implementation & Communication

The Trust's Risk Management Policy and Procedures will be disseminated and made available:

- Internally – Divisional Managers / Heads of Department are expected to communicate the Policy and Procedures as part of local induction procedures. All staff are introduced to the principles outlined in the strategy at corporate induction and through Junior Doctors' Handbooks. Risk Management Training will refer to the Strategy. The document is available on the Trust Intranet.
- Amendments will be communicated as and when they occur.
- Externally – The Policy and Procedure is freely available on request to Trust stakeholders.

7.0 Equality Impact Assessment

7.1 As part of its development, this policy and its impact on equality have been reviewed in line with the Trust's Equality Scheme.

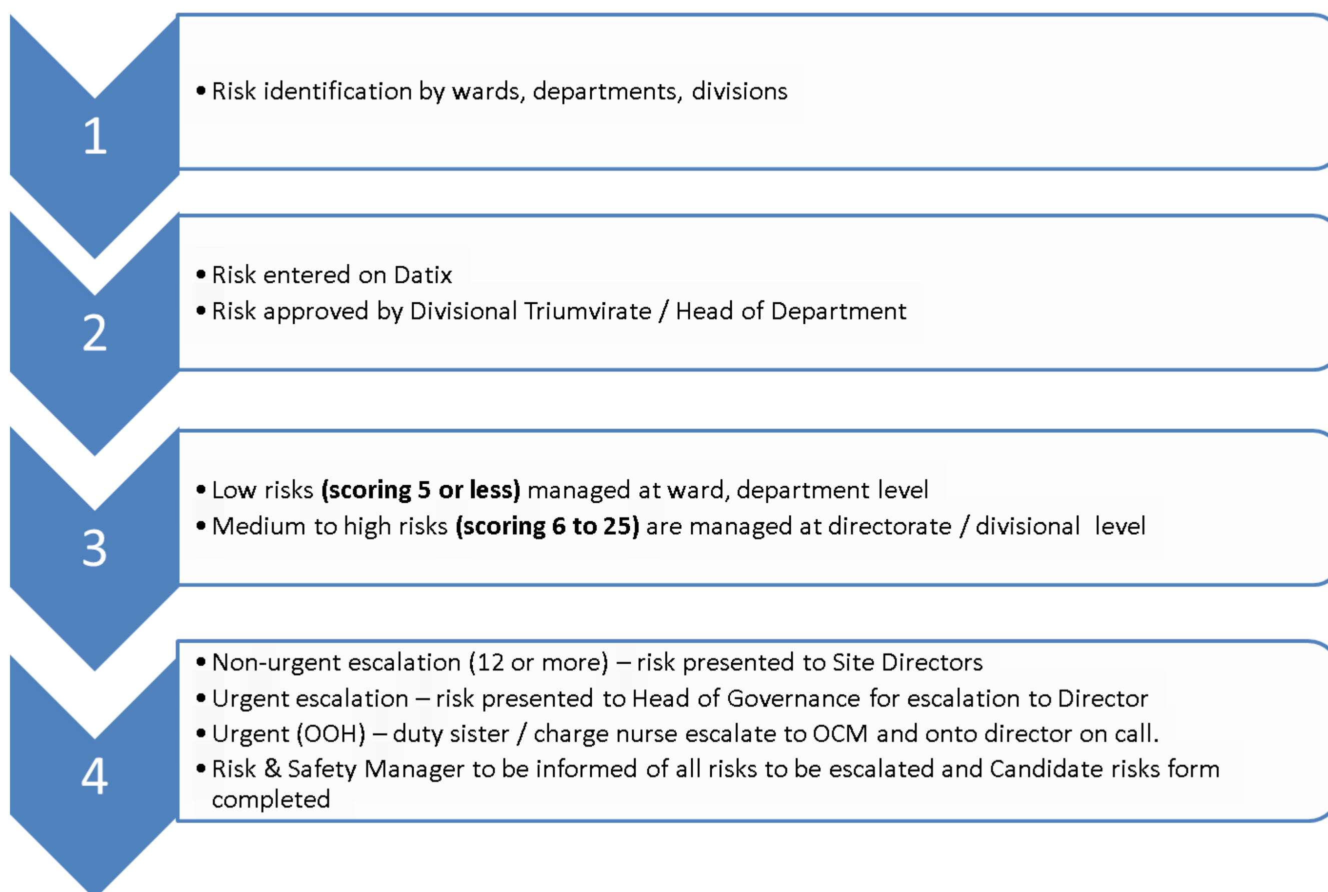
7.2 The purpose of the assessment is to minimise and, if possible, remove any disproportionate impact on employees on the grounds of race, sex, disability, age, sexual orientation or religious belief. No detriment was identified.

8.0 Review

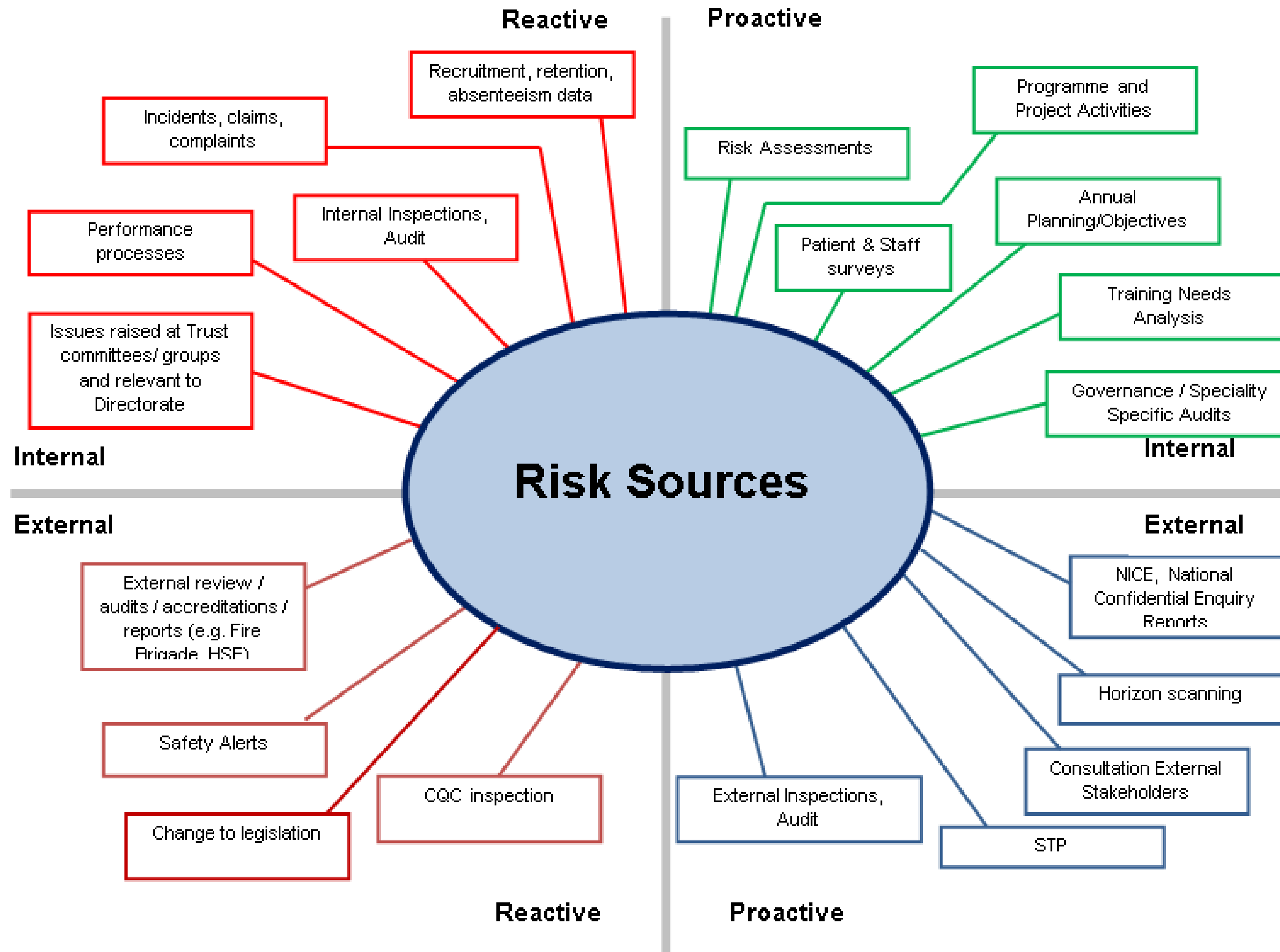
8.1 This Policy will be reviewed annually or sooner if circumstances dictate.

Appendix 1

Risk Management Process



Sources of Risk Identification **Appendix 2**



Appendix 3: Risk Assessment Guidelines

The following criteria has been developed to ensure consistency in measuring risk severity and risk likelihood on a 1 to 5 scale across different types of risk and also different parts of the business. For example, reputation risk or service delivery risk. Risk owners should select one [or if necessary, more] of the risk severity definitions on the left column to derive a measure of risk severity on a 1 to 5 scale. Where more than one definition has been selected, then risk owners need to ensure a consistent risk severity score is used.

Table A: RISK IMPACT

DESCRIPTOR	NEGLIGIBLE 1	MINOR 2	MODERATE 3	MAJOR 4	CATASTROPHIC 5
Injury (Physical/ Psychological)	►Adverse event requiring no/minimal intervention or treatment.	►Minor injury or illness – first aid treatment needed ►Health associated infection which may / did result in semi permanent harm ►Increase in length of hospital stay by 1-3 days ►Affects 1-2 people	►Moderate injury or illness requiring professional intervention to resolve the issue ►RIDDOR / Agency reportable incident (4-14 days lost) ►Adverse event which impacts on a small number of patients ►Increased length of hospital stay by 4 – 15 days ►Affects 3-15 people	►Major injury / long term incapacity / disability (e.g. loss of limb) ►>14 days off work ►increased length of hospital stay >15 days ►Affects 16 – 50 people	►Incident leading to death ►Multiple permanent injuries or irreversible health effects ►An event affecting >50 people
Environmental Impact	►Potential for onsite release of substance ►Minimal or no impact on the environment	►Onsite release of substance but contained ►Minor impact on the environment ►Minor damage to Trust property – easily remedied <£10K	►On site release of substance ►Moderate impact on the environment ►Moderate damage to Trust property – remedied by Trust staff / replacement of items required £10K - £50K	►Offsite release of substance ►Major impact on the environment ►Major damage to Trust property – external organisations required to remedy - associated costs >£50K	►Onsite /offsite release with catastrophic effects ►Catastrophic impact on the environment ►Loss of building / major piece of equipment vital to the Trusts business continuity
Staffing & Competence	►Short term low staffing level (<1 day) – temporary disruption to patient care ►Minor competency related failure reduces service quality <1 day	►On-going low staffing level - minor reduction in quality of patient care ►Unresolved trend relating to competency reducing service quality ► 75 % staff attendance at mandatory / key training	►Ongoing low staffing resulting in moderate reduction in the quality of patient care ►Late delivery of key objective / service due to lack of staff ►Error due to ineffective training / competency ►50% - 75% staff attendance at mandatory / key training	►Unsafe staffing level leading to a temporary service closure <5 days ►Uncertain delivery of key objective / service due to lack of staff ►Serious error due to ineffective training and / or competency ►25%-50% staff attendance at mandatory / key training	►Loss of several significant service critical staff leading to a service closure >5 days ►Non-delivery of key objective / service due to lack of staff ►Critical error leading to fatality due to lack of staff or insufficient training and / or competency ►Less than 25% attendance at mandatory / key training on an on-going basis
Complaints / Claims	►Informal / locally resolved complaint ►Potential for settlement / litigation <£500	►Overall treatment / service substandard ►Formal justified complaint ►Minor implications for patient safety ►Claim <£10K	►Justified complaint involving lack of appropriate care ►Moderate implications for patient safety ►Claim(s) between £10K - £100K	►Multiple justified complaints ►Findings of Inquest suggesting poor treatment or care ►Non-compliance with national standards implying significant risk to patient safety ►Claim(s) between £100K - £1M	►Multiple justified complaints ►Single major claim ►Ombudsman inquiry ►Totally unsatisfactory level or quality of treatment / service ►Claims >£1M

DESCRIPTOR	NEGLIGIBLE 1	MINOR 2	MODERATE 3	MAJOR 4	CATASTROPHIC 5
Business/ Service Interruption	►Loss/Interruption of >1 hour; no impact on delivery of patient care / ability to provide services	►Short term disruption, of >8 hours, with minor impact	►Loss / interruption of >1 day ►Disruption causing impact on patient care ►Non-permanent loss of ability to provide service	►Loss / interruption of > 1 week. ►Sustained loss of service which has serious impact on delivery of patient care resulting in major contingency plans being Invoked ►Temporary service closure	►Permanent loss of core service / facility ►Disruption to facility leading to significant 'knock-on' effect across local health economy ►Extended service closure
Inspection/ Regulatory Compliance/ Statutory Duty	►Small number of recommendations which focus on minor quality improvement issues ►Minimal breach of guidance / statutory duty ►Minor non-compliance with standards	►Single failure to meet standards ►No audit trail to demonstrate that objectives are being met (NICE; HSE; NSF etc.)	►Challenging recommendations which can be addressed with appropriate action plans ►Single breach of statutory duty ►Non-compliance with > one core standard	►Enforcement action ►Multiple breaches of statutory duty ►Improvement Notice ►Trust rating poor in National performance rating ►Major non compliance with core standards	►Multiple breaches of statutory duty ►Prosecution ►Severely critical report on compliance with national standards ►Zero performance rating ►Complete systems change required
Adverse Publicity / Reputation	►Rumours ►Potential for public concern	►Local Media – short term – minor effect on public attitudes / staff morale ►Elements of public expectation not being met	►Local media – long term – moderate effect – impact on public perception of Trust & staff morale	►National media <3 days – public confidence in organisation undermined ►Use of services affected	►National / International adverse publicity >3 days. ►MP concerned (questions in the House) ►Total loss of public confidence
Information Governance/ IT	► Minor breach of confidentiality – readily resolvable ►Unplanned loss of IT facilities < half a day ►Health records / documentation incident – no adverse outcome	►Minor Breach with potential for investigation ►Unplanned loss of IT facilities < 1 day ►Health records incident / documentation incident – readily resolvable	►Moderate breach of confidentiality – potential for complaint 1 – 5 persons affected ►Health records documentation incident – patient care affected with short term consequence	►Serious breach of confidentiality – more than 5 person or Very sensitive information ►Unplanned loss of IT facilities >1 day but less than one week ►Health records / documentation incident – patient care affected with major consequence	►Serious breach of confidentiality – large numbers ►Unplanned loss of IT facilities >1 week ►Health records / documentation incident – catastrophic consequence
Projects	►Insignificant cost increase ►Insignificant impact on value and/or time to realise declared benefits against profile	►<5% over project budget ►<5% variance on value and/or time to realise declared benefits against profile	►5 - 10% over project budget ►5 - 10% variance on value and/or time to realise declared benefits against profile	►10 - 25% over project budget ►10 - 25% variance on value and/or time to realise declared benefits against profile	►> 25% over budget ►> 25% variance on value and/or time to realise declared benefits against profile
Financial (Loss of contract / revenue / default payment)	►Small Financial loss < £1K ►Theft or damage of personal property <£50	►Loss <£1k - £50K ►Theft or loss of personal property <£750	►Loss of £50K - £500K ►Theft or loss of personal property >£750 - £10K	►Loss of £500K - £1M ►Theft or loss of personal property £10K - £50K	►Loss > £1M ► Theft or loss of personal property > £50K
Fire Safety / General Security	►Minor short term (<1day) shortfall in fire safety system. ►Security incident with no adverse outcome	►Temporary (<1 month) shortfall in fire safety system / single detector etc (non patient area) ►Security incident managed locally ►Controlled drug discrepancy – accounted for	►Fire code non-compliance / lack of single detector – patient area etc. ►Security incident leading to compromised staff / patient safety. ►Controlled drug discrepancy – not accounted for	►Significant failure of critical component of fire safety system (patient area) ►Serious compromise of staff / patient safety ►Loss of vulnerable adult resulting in major injury or harm ► Major controlled drug incident involving a member of staff	►Failure of multiple critical components of fire safety system (high risk patient area) ►Infant / young person abduction ►Loss of vulnerable adult resulting in death

Table B: RISK LIKELIHOOD

Description	1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
Frequency (How often might it / does it occur)	Highly unlikely but may occur in exceptional circumstances. It could happen but probably never will	Not expected but there is a slight possibility it may occur at some time	The event might occur at some time as there is a history of casual occurrence at the Trust or within the NHS	There is strong possibility the event will occur as there is a history of frequent occurrence at the Trust or within the NHS	Very likely. The event is expected to occur in most circumstances as there is a history of regular occurrence at the Trust or within the NHS
Probability	Less than 10%	11 – 30%	31 – 70 %	71 - 90%	> 90%

Table C: RISK SCORING MATRIX & GRADING

Likelihood

Impact	1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost certain
Catastrophic 5	5	10	15	20	25
Major 4	4	8	12	16	20
Moderate 3	3	6	9	12	15
Minor 2	2	4	6	8	10
Negligible 1	1	2	3	4	5

Risk Assessment	Grading
15 – 25	Extreme
8 – 12	High
4 – 6	Medium
1 – 3	Low

Appendix 4

Mid Essex Hospital Services NHS Trust

CORPORATE RISK ASSURANCE FRAMEWORK

CANDIDATE RISK (CR) FORM

RISK TITLE (to be completed by CR originator, for example: Infrastructure)

Principal Risk ID No:	Date Reviewed	Date Risk First Identified	Date Risk Referred to SMG
To be completed by Governance Department	To be completed by Governance Department		

Risk Category	Reported By	Risk Owner	Risk Manager

Risk Description
There is a risk that (TIART), X happens, which causes Y and results in Z *For Example: There is a risk that the inadequacy in current medical information management and systems will lead to an increased threat to patient safety, public health and the overall efficiency and effectiveness of the business, with subsequent damage to the reputation of the organisation.* Delete the detail above on completion of Risk Description.
Risk Detail
To be completed by the CR originator.

Pre Mitigation Risk *(Likelihood$^{(1-5)}$ / Impact $^{(1-5)}$/Score $^{(1-25)}$)*					
Likelihood		**Impact**		**Score**	
Impact if Risk Materialises					
To be completed by the CR originator.					

Description of Mitigation Actions / Control Measures Being Taken
To be completed by the CR originator and these should link back to the Risk Detail. Where new mitigation/measures are added they should show the date.

Post Mitigation Risk (*Likelihood*$^{(1-5)}$ */ Impact* $^{(1-5)}$*/Score* $^{(1-25)}$*)*					
Likelihood		**Impact**		Score	

Forecast to End of Year (31 Mar) *(Likelihood*$^{(1-5)}$*/Impact* $^{(1-5)}$*/Score* $^{(1-25)}$*)*					
Likelihood		**Impact**		Score	

Actions Recommended to Board
For Example: **09 April 2014** **R&CG to SMG** The Site Leadership group are invited to consider the risk for adoption to the Corporate Risk Register

PLEASE NOTE – if your risk has multiple risk descriptors, please pick the risk descriptor that holds the HIGHEST SCORE

If you require further assistance then please contact the Risk & Safety Manager via Switchboard

Appendix 5 DEFINITIONS

Acceptable/ tolerable Risk is 'the mitigated risk remaining after all reasonable controls have been applied to associated hazards that have been identified, quantified, analysed, communicated to the appropriate level of management and accepted after proper evaluation'. **Inherent** risks identified at operational level with an inherent risk rating below 5 will be the responsibility of the individual Division/ department to decide what level of risk is 'acceptable'. In respect of strategic and higher risks, it is the responsibility of the Chief Executive supported by the Executive Directors and other key individuals with delegated responsibility. Acceptability is defined in accordance with the Trust's defined risk appetite.

Adverse event is any event or harm or circumstance leading to unintentional harm or suffering.

Board Assurance Framework – the Board Assurance Framework provides the Trust with a simple but comprehensive method for the effective and focused management of the principal risks to meeting their objectives. It is reported regularly to the Trust Board and provides a structure for the evidence to support the Chief Executive's Annual Governance Statement.

Clinical Risk is the chance of something happening to a patient during NHS care that could have or did lead to unintended or unexpected harm, loss or damage. This is a broad definition that may range from dissatisfaction on the part of patients at having to wait so long for treatment or at lack of communication, to undergoing the wrong operation, or suffering permanent disability or death.

Consequence (Impact/ Severity) is the level of harm that has, or may be suffered and is measured at the Trust on a scale of 1 to 5. *(Please refer to appendix 2 for additional guidance.)*

Controls are arrangements and systems that are intended to minimise the likelihood or severity of a risk. An effective control will always reduce the probability of a risk occurring. If this is not the case, then the control is ineffective and needs to be reconsidered. Controls are intended to improve resilience.

Controls Assurance is a holistic concept based on best governance practice which conforms with the Combined Code of Practice on Corporate Governance and the Turnbull guidance on Internal Control. It is a process designed to provide evidence that NHS organisations are doing their 'reasonable best' to manage themselves to meet their objectives and protect patients, staff, the public and other stakeholders against risks of all kinds. Managers need to put in place control strategies which will offer the best chances of identifying and correcting errors at a reasonable cost

Essential Standards of Quality and Safety - the essential standards of quality and safety consist of 28 regulations (and associated outcomes) that are set out in two pieces of legislation: the Health and Social Care Act 2008 (Regulated Activities) Regulations 2010 and the Care Quality Commission (Registration) Regulations 2009. For each regulation, there is an associated outcome – the experiences the Care Quality Commission (the Regulator) expect people to have as a result of the care they receive. When the CQC check providers' compliance with the essential standards, it focuses on the 16 regulations (out of the 28) that come within Part 4 of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2010 – these are the ones that most directly relate to the quality and safety of care. Providers must have evidence that they meet the outcomes at every level in the organisation.

Gap in control is deemed to exist where adequate controls are not in place or where collectively they are not sufficiently effective. A negative assurance (a poor Internal Audit report for example) highlights gaps in control.

Gap in assurance is deemed to exist where there is a failure to gain evidence that the controls are effective.

Hazard is something which has the potential to cause harm, e.g substances, equipment, methods of work, and other aspects of work organisation.

Inherent risk is the risk linked to the activity itself without the application of controls.

Inherent Clinical Risk is the permanent or currently unavoidable clinical risk that is associated with a particular clinical investigation or treatment. It is the risk from undergoing a particular procedure in ideal conditions and performed by competent staff using the most up-to-date research, equipment and techniques. It can be considered permanent or currently unavoidable when used for the purpose of risk assessment. The risk that should be targeted by clinical risk assessment is the risk that is added to the inherent risk and results from, for example, a poor safety culture, poor communication and teamwork, inadequate supervision of inexperienced staff, unreliable equipment or an unsuitable environment.

Internal Control is the process effected by the Board of Directors designed to provide reasonable assurance that the Trust's objectives will be met with regards to: (1) Effectiveness and efficiency of operations; (2) Reliability of financial reporting and (3) Compliance with applicable laws and regulations.

Likelihood is measured by the frequency of exposure to the hazard or the probability of an event occurring on a scale of 1 to 5. *(Please refer to appendix 2 for additional guidance.)*

Mitigated Risk (Target Risk) is the remaining risk when **all** reasonable controls have been applied – when the additional controls to mitigate the Residual Risk have been applied and are effective. This equates to the **Tolerable Risk.** The additional benefit of additional controls must be weighed against the cost.

Patient Safety Incident is any unintended or unexpected incident which could have or did lead to harm for one or more patients receiving healthcare. It is a specific type of adverse event.

Principal Risks are those risks that can adversely affect the achievement of the Trust's corporate objectives and are identified, assessed and monitored by the Board Assurance Framework.

Probability is the chance that something will happen, calculated statistically.

Residual Risk which in this Trust refers to the **Current Risk** is the risk remaining with the current controls in place i.e. The risk remaining after the controls put in place to mitigate the inherent risk are fully effective.

Risk is the likelihood (probability) that an event with adverse consequences or impact (hazards) will occur in a specific time period, or as a result of a specific situation. This event may cause harm to patients, visitors, staff, property, or have an impact on the Trust reputation, corporate objectives, stakeholders or assets.

Risks differ from their hazard in that the former is the calculated probability of the event occurring whilst the consequences or impact measure the effect of the risk being realised as a hazard. Put simply, hazards represent risks that have been realised.

Risk Appetite - at the organisational level, is the amount of risk exposure, or potential adverse impact from an event, that the organisation is willing to accept/retain. Once the risk appetite threshold has been breached, risk management treatments and business controls are implemented to bring the exposure level back within the accepted range. The risk appetite may vary according to risk type.

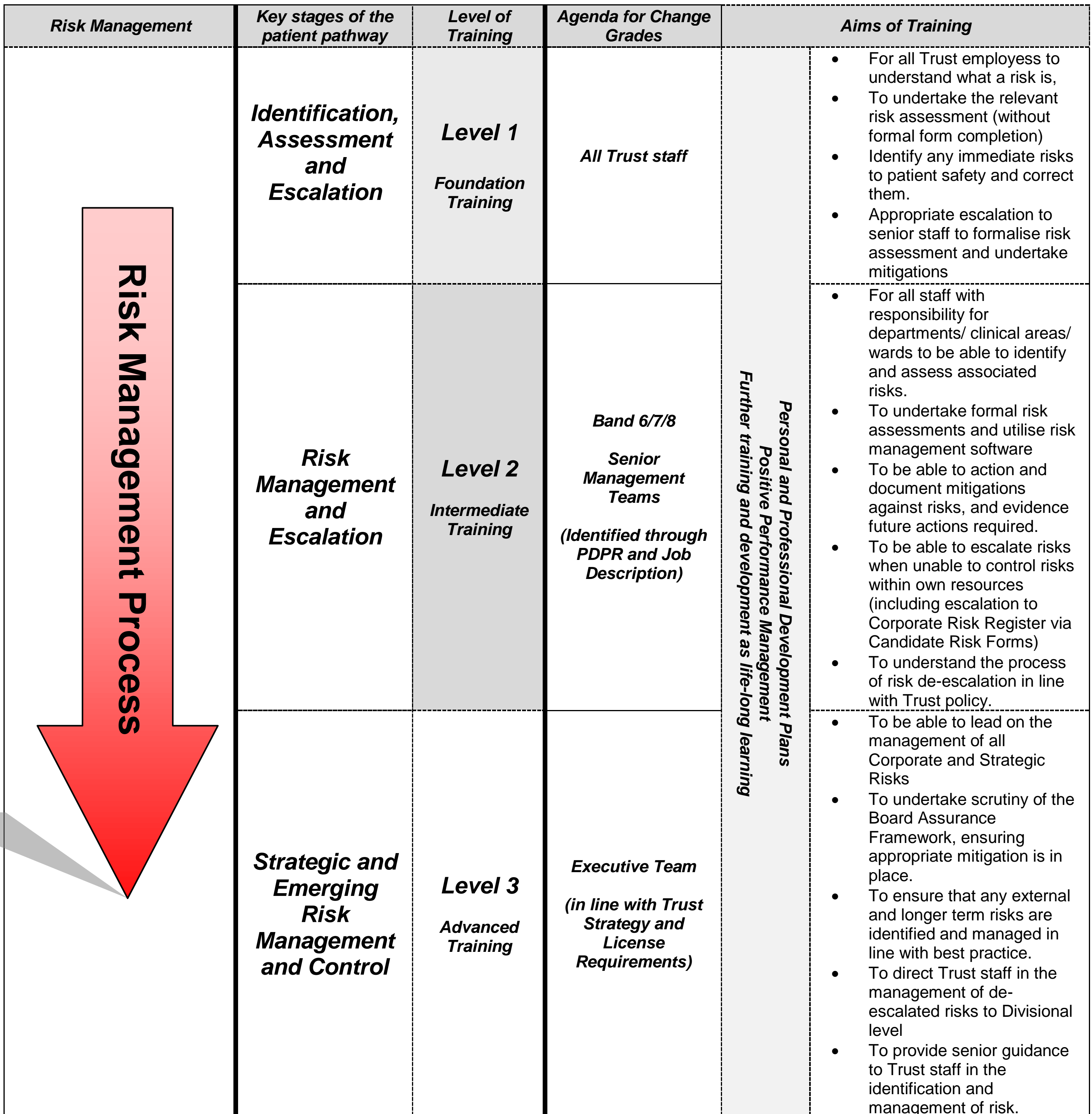
Risk Assessment is the process by which risks are prioritised and then categorised through the application of a 5 by 5 calculation to produce a composite score out of a maximum of 25 (25 being the most severe.) The risk assessment is based on the probability (likelihood) of a hazard occurring on a 1 to 5 scale, multiplied by its likely consequence or impact (severity) which is measured on a similar 1 to 5 scale. An account of the criteria for obtaining accurate measures of risk and severity of consequence or impact can be found in Appendix 3.

Risk Management is the systematic identification, assessment, treatment, monitoring and communication of risks. This process is followed by the application of current or planned resources to effectively control, monitor and minimise the overall likelihood (and in some instances, impact) of the identified risk.

Risk Owners – are throughout the organisation in accordance to the accountabilities and responsibilities outlined in section 7. The corporate risk register is owned by the Executive Directors of the Senior Management Group and the Board Assurance Framework is owned by the Trust Board of Directors.

Risk Register – is a management tool that allows the Trust to understand its comprehensive risk profile. It is simply a repository of risk information linking risks and controls for the whole organisation.

Appendix 6 TRAINING NEEDS ANALYSIS



Risk Management	Key stages of the patient pathway	Level of Training	Agenda for Change Grades	Aims of Training	
Risk Management Process	Identification, Assessment and Escalation	Level 1 Foundation Training	All Trust staff	Personal and Professional Development Plans Positive Performance Management Further training and development as life-long learning	• For all Trust employess to understand what a risk is, • To undertake the relevant risk assessment (without formal form completion) • Identify any immediate risks to patient safety and correct them. • Appropriate escalation to senior staff to formalise risk assessment and undertake mitigations
	Risk Management and Escalation	Level 2 Intermediate Training	Band 6/7/8 Senior Management Teams (Identified through PDPR and Job Description)		• For all staff with responsibility for departments/ clinical areas/ wards to be able to identify and assess associated risks. • To undertake formal risk assessments and utilise risk management software • To be able to action and document mitigations against risks, and evidence future actions required. • To be able to escalate risks when unable to control risks within own resources (including escalation to Corporate Risk Register via Candidate Risk Forms) • To understand the process of risk de-escalation in line with Trust policy.
	Strategic and Emerging Risk Management and Control	Level 3 Advanced Training	Executive Team (in line with Trust Strategy and License Requirements)		• To be able to lead on the management of all Corporate and Strategic Risks • To undertake scrutiny of the Board Assurance Framework, ensuring appropriate mitigation is in place. • To ensure that any external and longer term risks are identified and managed in line with best practice. • To direct Trust staff in the management of de-escalated risks to Divisional level • To provide senior guidance to Trust staff in the identification and management of risk.

Appendix 7 Risk escalation and de-escalation framework