The Shrewsbury and Telford Hospital NHS Trust

Board of Directors' Meeting
10 March 2022

Agenda item	037/22			
Report	Policy Approval – Risk Management			
Executive Lead	Director of Governance and Communications			
	Link to strategic pillar:		**Link to CQC domain:**	
	Our patients and community		Safe	
	Our people		Effective	
	Our service delivery		Caring	
	Our partners		Responsive	
	Our governance	√	Well Led	√
	Report recommendations:		**Link to BAF / risk:**	
	For assurance			
	For decision / approval	√	**Link to risk register:**	
	For review / discussion			
	For noting			
	For information			
	For consent			
Presented to:	Audit & Risk Assurance Committee, 16 February 2022 SaTH Leadership Committee – Operational, 24 February 2022			
Dependent upon (if applicable)**:**				
Executive summary:	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. This report focuses on the new risk management processes that are currently being put in place. The Board of Directors is asked to: • **Review** the refreshed Risk Management Policy, and associated Risk Management Process Guide; and • **Approve** the refreshed Risk Management Policy.			
Appendices:	Appendix 1: Risk Management Policy Appendix 2: Risk Management Process Guide			
Lead Executive:				

The Shrewsbury and Telford Hospital NHS Trust

Risk Management Policy RM02

Additionally, refer to:

- Clinical Incident Reporting Policy (CG04)
- Trust Fire Safety Policy (FS00)
- Health and Safety Policy (HS01)
- Incident reporting and investigation Policy (staff, contractors, and members of the public)including RIDDOR (HS02)
- Control of Hazardous Substances (COSHH) Policy (HS06)
- Safe Moving and Handling policy (HS08)
- Risk Management Strategy (RM01)
- Violence and Aggression Policy (SY02)
- Risk Management Process Guide (RM03)
- Risk Management Information System Toolkit (RM04)
- Major Incident Policy

Version:	V1.6
V1 issued	Jan 2022
V1 approved by	Trust Board of Directors
V1 date approved	
V1 Ratified by:	-
V1 Date ratified:	-
Document Lead	Director of Governance (was Chief Risk Officer)
Lead Director	Director of Governance & Comms
Date issued:	January 2022
Review date:	January 2027
Target audience:	All Trust staff

Document Control Sheet

Document Lead/Contact:	Anna Milanec, Director of Governance &Communications
Version	V1.6
Status	Draft
Date Equality Impact Assessment completed	tbc
Issue Date	January 2022
Review Date	January 2027
Distribution	Please refer to the intranet version for the latest versionof this policy. **Any printed copies may not necessarily be the mostup to date**
Key Words – including abbreviations if these would bereasonably expected to be used as search terms	Risk management, risk assessment, risk appetite, risk scoring, risk escalation
Dissemination plan	Trust intranet

Version history

Version	Date	Author	Status	Comment – include reference to Committee presentations and dates
1	October 2020	Chief Risk Officer	Draft	New document – aligned to ISO31000
1.1	October 2020	Chief Risk Officer	Draft	Minor amend to guidelines to identify, assess, action andmonitor risks. Document reference number added.
1.2	October 2020	Chief Risk Officer	Draft	Formatting and other minor administrative amendments
1.3	Novembe r2020	Chief Risk Officer	Draft	Further development of guidelines to identify, assess,action and monitor risks
1.4	May 2021	Director of Governance	Draft	Amendment to some sections following feedback fromExecutive Risk Management Committee
1.5	June 2021	Director of Governance	Draft	Amendment to some sections following feedback fromARAC and Board
1.6	January 2022	Head of Risk (LB)	Draft	Addition to roles and responsibilities. Brief definitions included within the body of the policy. Appendix A addition- further definitions. Accepted/closed risks. Risk reporting structure Risk Tolerance Levels – aligned to Risk Appetite Appendix c – Risk Event Assessment Tool Risk Matrix – Consequence domains added

Contents

1. Policy Statement:

The provision of healthcare and the activities associated with the treatment and care of patients, employment of staff, maintenance of premises and managing finances, by their nature, incur risks.

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 strategic objectives.

This document should be read in conjunction with the Trust Risk Management Strategy, Risk Management Process Guide and DATIX Risk Management Toolkit.

2. Overview:

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.

The Risk Management Policy is regularly reviewed and updated to ensure it continues to be consistent with the Trust Risk Strategy and reflects national guidance and relevant legislation.

3. Aims and objectives:

3.1. **The overarching aim of the Policy** is to provide assurance that the Trust is providing high qualitycare in a safe environment, that it is complying with legal and regulatory requirements, and that it is achieving its strategic objectives and promoting its values

3.2 Policy objectives are:

a) To clearly define roles and responsibilities for risk management.
b) To embed risk management systems and processes into the day-to-day management and delivery of healthcare, and to promote the ethos that 'risk management is everyone's business'.
b) To communicate the internal risk reporting structure, enabling a comprehensive understanding of risks, and the risk process at all levels of the Organisation.
d) To establish and review on an annual basis, the Trusts risk appetite statement, aligned to the strategic objectives
e) To establish and review on an annual basis, the Trusts agreed levels to tolerate/accept risks.
f) To ensure that appropriate risk-based information is available to support decision making.
g) To ensure conformity with applicable rules, regulations, and mandatory obligations.
h) To provide required levels of assurance that risk management and internal control activities are in place and understood by all levels of the Organisation
I) To create an environment which is safe as is reasonably practicable by ensuring thatrisks are continuously identified, assessed, and appropriately managed i.e., wherepossible eliminate, transfer, or reduce risks to an acceptable level.
j) To establish an integrated approach to risk management.
k) To ensure effective implementation of this policy and associated documents, by providing regular training to all identified within the results of the annual training needs analysis.
l) To adopt an organisational culture of openness and willingness to report risks, incidents and near misses that is used for organisation-wide learning.

4. Scope:

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

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

5. Definitions:

Below is a brief list of common words and their definitions that are referred to within this document. Please refer to ***Appendix A***, for a more comprehensive list that is commonly used within the 'risk management' world.

Risk:
International Organisation for Standardisation (ISO) defines risk as an **'Effect of uncertainty on objectives'**. Note that an effect may be positive (bring about opportunities), negative (pose a threat), or a deviation from the expected.

Risks are things that **might happen** and stop us achieving objectives, or otherwise impact on the success of the Trust.

Issues:
Issues are things that have happened, which were not planned and require management action. Issues are similar to the types of incidents that the Trust will report and investigate. The aim is to detect the root cause that led to the issue, and to put controls in place in order to prevent the issue recurring.

Risk Management:
International Organisation for Standardisation (ISO) defines risk management as **'Coordinated activities to direct and control and Organisation with regard to risk'.**
This is the recognition and effective management of all threats and opportunities that may have an impact on the Trust's reputation, its ability to deliver its statutory responsibilities and the achievement of its objectives and values.

Organisational perspective:
It is important to recognise that there are four main organisational perspectives to consider when performing risk management:

1. **Strategic:** Relate to overall success, vitality, and viability of the Trust. Enabling the Trust to make better strategic decisions

2. **Operational:** relate to delivering the existing day to day healthcare services. Events causing disruption identified in advance and allow for immediate action to be taken

3. **Programme/Project:** relate to transformational activities into new ways of working that deliver measurable benefits to the Trust Enabling the Trust to deliver projects on time and within a set budget

4. **Compliance:** Enabling the Trust to identify risks associated with failure to achieve compliance with regulatory or statutory requirements

Risk Management Information System (RMIS):
Computer software system or part of the intranet of the Organisation that records and communicated risk information. Currently the Trust uses the 4Risk platform.

Risk Register:
This is the standard listing report which can be generated from 4Risk, showing all or a subset of Trust risks. These can be readily generated in Excel format.

Risk Appetite:
Amount and type of risk that an organisation is willing to pursue or retain in the short term, to achieve its objectives

Risk Tolerance:
An organisation's or stakeholder's readiness to bear the risk after risk treatment, in order to achieve its objectives.

Summary Risk Report (SRR):
This is the monthly Risk Report, which identifies the key strategic, programme/project and operational risks and their current status. These are usually (although not exclusively) to risks with ratings of 15 and above.

Board Assurance Framework:
Risk management by the Board is underpinned by a number of interlocking systems of control, which demonstrates that an effective risk management approach is in operation within the Trust. The Board Assurance Framework (BAF) report sets out the strategic objectives, identifies risks in relation to each strategic objective along with the controls in place and assurances available on their operation. The Summary Risk Report (SRR) and the BAF report are interlocked given their nature and as such should have a clear relationship between them. If a report is received which has the potential to impact upon the strategic objectives of the Trust; then this needs to be reflected in the BAF and appear on the SRR. Likewise, should a risk be present on the SRR which has the potential to impact upon the strategic objectives of the Trust, this should be present within the BAF.

Business Continuity Planning (BCP):
Plan to ensure continuity of business operations in the event of a serious incident that impacts on the Organisation. It is expected for the risk owner and team to consider whether they need to seek advice from the Emergency Planning Manager to introduce a BCP in response to the risk event. BCP introduce can support the prevention of this risk event from occurring/recurring and is an effective risk control.

Annual Governance Statement:
The Annual Governance Statement is signed by the Chief Executive as the Accountable Officer and sets out the organisational approach to internal control. This is produced at the year-end (following regular reviews of the internal control environment during the year) and scrutinised as part of the Annual Accounts process and brought to the Board with the Accounts.

6. Roles and Responsibilities:

All Staff are expected to:

- Be aware of the principles for the management of risk.
- Follow the risk management systems and processes.
- Adopt the appropriate practices to reduce risk.
- Follow the risk and incident reporting procedures; and
- Provide safe and high-quality patient care.

All staff are encouraged to use risk management processes as a mechanism to highlight areas they believe need to be improved. Where staff feel that raising issues may compromise them or may not be effective, they will be aware and encouraged to follow the 'Freedom to Speak Up' Policy incorporating guidance on raising concerns.

Non-Executive Directors	The role of the non-executive director has the following specific key elements: • **Strategy:** constructively challenge and help develop proposals on strategy • **Performance:** scrutinise the performance of management • **Risk:** challenge the integrity of the information • **Controls:** seek assurance that controls and systems of risk management are robust and defensible • **Confidence:** seek to establish and maintain confidence in the conduct of the Organisation • **Independence:** be independent in judgement and promote openness and trust
Chief Executive	• Responsible officer for Shrewsbury and Telford NHS Trust

	• Accountable for ensuring that the Trust can discharge its legal duty for all aspects of risk. • As Accountable Officer, the Chief Executive has overall responsibility for maintaining a sound system of internal control, as described in the Annual Governance Statement. • Operationally, the Chief Executive has delegated responsibility for implementation of risk management as outlined below
Trust Secretary	• The Director of Governance is the Trust Secretary. • Responsible for corporate assurance including legal risk • Executive lead for maintaining the Board Assurance Framework and its supporting processes.
Executive Directors and Deputy Directors	• Managing risks in accordance with their portfolios. • for risk management policy development, developing and communicating the Board's appetite for taking risk, establishing mechanisms for scanning the horizon for emergent threats and keeping the Board sighted on these, and monitoring the management of risk across the Trust. • ensuring effective systems for risk management, compatible with this Policy, are in place within their Divisions and Departments, specifically, they must ensure that: a) staff are familiar with this Policy and aware of their responsibility for risk. b) staff attend appropriate risk training (including induction and mandatory training). c) risks (strategic and operational) are effectively managed i.e., identified, assessed and that action plans to mitigate risks are developed, documented, and regularly reviewed.
Director of Governance and Communications	• Works closely with the Chair, Chief Executive, Executive Directors, Divisional Directors and Deputy Directors to implement and maintain appropriate risk management strategies and processes, ensuring that effective governance systems clinical and non-clinical risk processes are in place to assure the delivery of Trust objectives. • On behalf of the Chief Executive, is the Board lead for risk management processes across the Trust. They shall, on behalf of the Board, implement and maintain an effectivesystem of risk management. • Lead and participate in risk management oversight at the highest level, covering all risksacross the organisation, on a Trust-wide basis. • Work closely with the Chief Executive and Directors to support the provision of strategic, corporate, and operational, level risk registers. • Develop and oversee the effective execution of the Board Assurance Framework and ensure effective processes are embedded to rigorously manage the risks therein, monitoring the action plans and reporting to the Board and relevant Committee.
Senior Information Risk Owner (SIRO)	• The Director of Governance is the SIRO and is the nominated executive lead to ensure theTrust's information risk is properly identified and managed and that appropriate assurancemechanisms exist.
Medical Director	• Responsible for the professional leadership of doctors and associated clinical risk.
Divisional Directors	• Are accountable for ensuring that appropriate and effective risk management processes are in place within the Divisions, and that all staff are aware of their responsibilities. • They must ensure that risks are identified, assessed, recorded, and acted upon. • They must ensure that risks are reviewed by an appropriate divisional group and that appropriate arrangements are in place to escalate risks from care unit to divisional level.

	• All risks recorded within their allocated Divisions, that are escalated to a 'current risk rating' of 15 and/or above, must be agreed by the DD prior to the rating being changed on the risk management information system.
Head of Risk	• Accountable to the Director of Governance and Communications • Develop the risk management policy and keep it up to date • Facilitate a risk aware culture within the Trust • Establish internal risk policies and risk reporting structures • Compile risk information and prepare reports for Board. • Responsible for overseeing the effective operation of risk management systems, • Ensuring compliance with risk management standards and that staff receive the relevant elements of risk management training. • It will be the responsibility of the **Head of Risk** to ensure that there are effective systems in place, to identify, report, and act upon themes and trends and accumulated risk across the Trust.
Emergency Planning Manager	• Responsible for providing specialist advice to the Organisation, both in planning and response to a major incident. It is expected that Divisions/Directorates will approach the ERM and seek advice as to whether the introduction of a Business Continuity Plan (BCP) is required as a response control to a specific risk event. BCP will then be aligned to the specific risk event.
Senior staff (Clinical Directors, of Operations/ General Managers/Lead Nurses/Ward Sisters/Charge Nurses/Senior Managers)	Senior staff with management responsibility will take the lead on risk management within their areas of operation, and set the example through visible leadership of their staff by: • Taking personal responsibility for managing risk; • Sending a message to staff that they can be confident that escalated risks will be acted upon; • Ensuring risks are updated regularly and acted upon; • Identifying and managing risks that cut across delivery areas; • Discussing risks on a regular basis with staff and up the line to help improve knowledge about the risks faced; increasing the visibility of risk management and moving towards an action focussed approach; • Communicating downwards what the top risks are, and doing so in plain English; • Escalating risks from the front line; • Linking risk to discussions on finance, and stopping or slowing down non-priority areas or projects to reduce risk as well as stay within budget, demonstrating a real appetite for setting priorities; • Ensuring staff are suitably trained in risk management; • Monitoring mitigating actions and ensuring risk and action owners are clear about their roles and what they need to achieve; • Ensuring that people are not blamed for identifying and escalating risks, and fostering a culture which encourages them to take responsibility in helping to manage them; • Ensuring that risk management is included in appraisals and development plans where appropriate. • Staff with responsibility for maintaining risk registers are expected to be aware of and adhere to the risk management best practice and will: • Identify risks to the safety, effectiveness and quality of services, finance, delivery of objectives and reputation – drawing on the knowledge of front line colleagues; • Identify risk owners with the seniority to influence and be accountable should the risk materialise; • Assess the rating of individual risks looking at the likelihood that they will happen, and the consequence if they do; • Identify the actions needed to reduce the risk and assign action owners;

	• Consider whether there is an opportunity to benefit from the risk or the work done to mitigate against the risk materialising; • Record risks on a risk register; • Check frequently on action progress, especially for high severity risks; • Apply healthy critical challenge, without blaming others for identifying and highlighting risks, or consider that they are being unduly negative in doing so; and • Implement a process to escalate the most severe risks, and use it.
Clinical Governance Leads	Clinical Governance Leads, will ensure that there are effective systems in place within their areas of operation, to effectively manage risk across the Trust: • ensure the Trust has a comprehensive and dynamic Risk Register and working with teams to ensure that they understand their accountability and responsibilities for managing risks in their areas; and • ensure all risks are up to date, and not overdue. • ensure risks management reports, including monthly and annual governance and risk reports are available.
Risk Owners	• Responsible for the day-to-day management of the risk(s) assigned to them on the risk register. • It is the responsibility of the risk owner to keep all aspects of the risk record updated including details of risk reviews, dates of upcoming reviews, re-evaluation of the current risk rating and associated actions. • Risk Owners should be familiar with the risks on their workload and their associated actions and should they face any difficulties with managing the risk, be familiar with the routes of escalation and how to seek assistance. If the 'current level' of risk increases to a level of 15 and/or above, authority needs to be gained from a member of the Leadership Team, prior to the risk 'going live' on the risk management information system.
Action Owners	• Responsible for the management of action(s) that have been assigned to them, to assist with mitigating a particular risk. • It is the responsibility of the action owner, to ensure that the action record linked to the risk is up to date, and progress is being made to close this action down. • Action owners should maintain regular contact with the risk owners, to provide a progress update, and assurance that the action is being managed.

Organisational Arrangements:

The Organisational management of risk forms part of the Trusts overall approach to governance. The key forums for the management of risk in the Trust are outlined within the below table:

Board of Directors	The Trust Board of Directors has overall responsibility for ensuring the Trust has effective systems for managing risk to enable the organisation to deliver its objectives.
Audit & Risk Committee	Receives the Trust Risk Report to seek assurance that the structures and procedures in place regarding operational risk management within the Trust are robust. The Audit and Risk Committee will liaise with other board assurance subcommittees and internal and external audit to support this role and will report to the Board with a level of assurance gained from the information presented to them.

Risk Management Committee	The purpose of the risk committee is to support the Risk and Audit Committee, by obtaining objective assurance that the framework and systems for risk management are robust and effective. The risk Committee has overall responsibility for establishing a pro-active approach to risk management across the various divisions and directorates across the Trust. Divisions/Directorates will be expected to present new risks/provide updates on all risks with a current (residual) rating of 15 and above, to allow for constructive challenge, and provide assurances that effective controls to mitigate the risk are in place.
Divisions	The Divisions are responsible for reviewing and controlling the risks within their areas
Specialities	Speciality Governance Teams are responsible for reviewing and controlling the risks within their areas.

7. The Management of Risk Process

The Trust follows a process that is presented as a set of iterative steps that are undertaken in a coordinated manner, but not necessarily in a strict sequence.

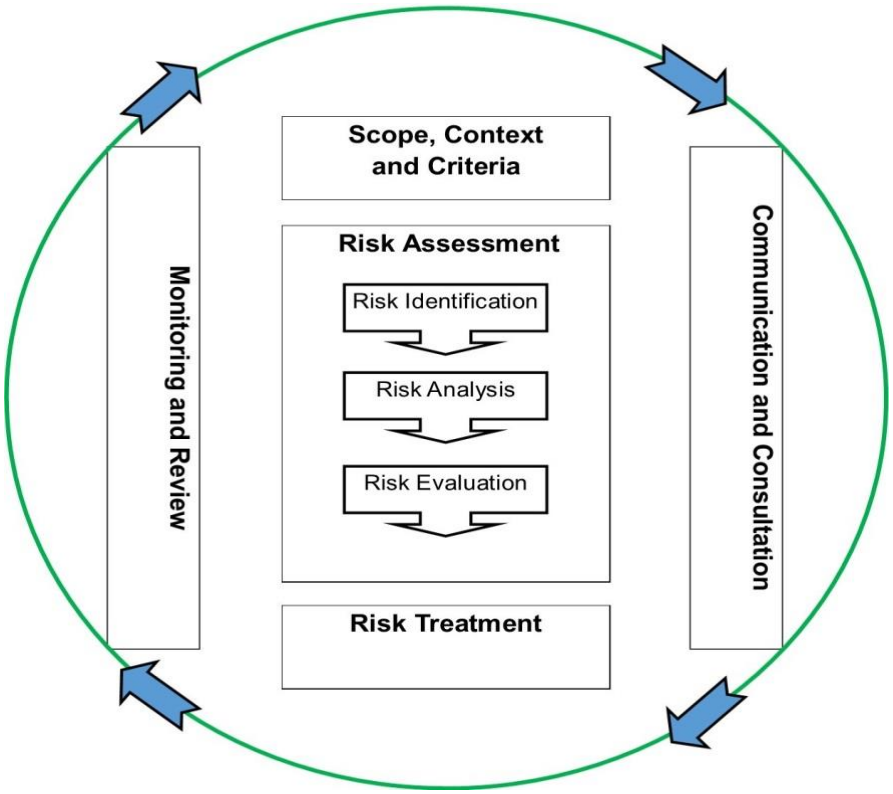


Figure 1 – ISO 31000 Risk Management Process

Please ***refer to the Management of Risk Process Guide*** for further information and guidance. The Management of Risk Process Guide explains each step recorded within the above image in a bit more detail and will introduce you to some tools and techniques to support you and your teams undertaking this process.

8. Reporting and Approval of Risks:

Risks **MUST** be approved, reported, and managed in line with the management responsibility table below:

Risk Score	Risk Level	Management Level
1-3	**Low Risk**	These **must be** reported and approved at the speciality governance meeting, prior to the risk being entered onto the risk management information system. To be managed at local ward/team level.
4-6	**Moderate Risk**	These **must be** reported and approved at the speciality governance meeting, prior to the risk being entered onto the risk management information system. There should be oversight by the Divisional Leadership Team (via Divisional Governance reporting mechanisms).
8-12	**High Risk**	Approval to be sought prior to the risk being entered onto the risk management information system. These **must be** reported and approved by the General Managers, Deputy Divisional Directors, Divisional Directors to the monthly Senior Management Meetings led by the Executives, along with to the Divisional Governance Meeting. Executive Directors will manage risks at this level within their own portfolio.
15-25	**Extreme Risk**	Approval to be sought prior to the risk being entered onto the risk management information system. These **must be** reviewed at both the Specialty Governance and Divisional Governance Meetings and approved by the Risk Management Committee and the Executive Team at each meeting. Extreme risks to be managed by the most appropriate Divisional Director. In extraordinary circumstances the approval of the extreme risk may bypass the Risk Management Committee, but the risk must be reported to and approved by the Divisional Director, prior to the risk being entered onto the risk management information system.

**** All risks to be approved, prior to being inputted onto the Risk Management Information System****

9. Risk Escalation Structure:

Risk Reporting, Escalation and Assurance arrangements can be represented in flowchart form, as depicted in **Appendix B (page 20)**

Report	Forum	For	Schedule	Content
NEW RISKS	1.Speciality Governance Meeting (Low risks) 2.Divisional Governance Team Meeting (Moderate/High/Extreme) 3. Risk Management Committee (Extreme)	Approval	Monthly. New risks should be approved prior to being entered onto the risk management information system.	
RISKS TO BE CLOSED/TOLERATED	1.Divisional Governance Team Meeting 2. Risk Management Committee (Extreme)	Approval	Monthly	

Report	Forum	For	Schedule	Content
NEW APPROVED RISKS (SCORING 15 AND ABOVE)	1.Divisional Governance Team (DGT) Meeting	Approval and recommendation to Risk Management Committee	Monthly	All risks with a current risk score of 15 or above will be reported to DGT in line with its meeting schedule
NEW APPROVED RISKS (SCORING 15 OR ABOVE)	Risk Management Committee (RMC)	Approval	Monthly	All risks approved by DGT with a current score of 15 or above will be reported to RMC in line with its meeting schedule
RISK PROFILE (AGE/SCORE/TYPE)	Divisional Governance Team Meeting Risk Management Committee	Review for action Debate	Monthly Bi- Monthly	Risk profiles detailing all recorded risks within each Division/Dept will be published on the first working day of the month
OVERDUE RISKS (PAST REVIEW DATE)	Divisional Governance Team Meeting Risk Management Committee	Review for action Information	Monthly Bi- Monthly	Risks past review date per Division/Dept will be published on the first working day of the month
NEW APPROVED RISKS MORE THEN 15	Executive Leadership Meeting	Debate	Monthly	All newly approved risks with a score of 15 or more following approval at RMC
RISKS BEING TREATED	Divisional Governance Team Meeting	Review for action	Monthly	All risks not yet at target score
RISKS MORE THEN 15	Board of Directors Assurance and Risk Committee	Review for action/assurance Challenge description/ rating/obtain assurance that risk is being managed	Quarterly Quarterly	Risks reporting 15 of above following approval at RMC

The escalation (and de-escalation) of risks is an important facet of risk management and there are mechanisms in place within the Trust for this to happen. Risks are **monitored** at Speciality Governance and Divisional Governance Meetings and at committee, subject specific group, and senior management team levels. Within these meetings, **confirm and challenge** is applied to the risks:

- **Confirm –** That the risk is scored appropriately, the correct risk owner is identified, and that identification of controls, gaps and actions are in place.
- **Challenge –** What actions are currently being undertaken – are these sufficient? What are the timescales – have they been met? Has the risk been reviewed in a timely manner by the risk owner and any other questions people may have about the risk.

10. Risk Review

The frequency of review for a risk should be based upon the profile and seriousness of that risk. The below table provides guidance on normally appropriate review frequencies based upon the 'current' risk rating of the risk:

Risk Level	Risk Review Frequency
Low (1-3)	Quarterly
Moderate (4-6)	Quarterly
High (8-12)	Bi – Monthly
Extreme (15-25)	Monthly

To ensure that all our risks are rated accurately and consistently, please refer to the Risk Matrix measurement tool **(Appendix C)** to assist with identifying the most appropriate Initial (inherent), Current (residual) and Target Risk rating

To ensure that all our risks are described accurately, and the risk owner and teams have completed a thorough assessment of the specific risk event, please refer to **Appendix D** the Risk Event Assessment Tool. This is to act as an 'aide memoire' and **does not replace** the function of the risk management information system (RMIS). All risks are to be inputted onto the RMIS.

11. Accepted and closed risks

When all mitigating action has been completed for the gaps identified in the control measures, consideration needs to be made as to whether the risk becomes an **accepted risk (also known as a tolerated risk)**. This is a decision, which is made at the relevant monitoring committee / subject specific group, to accept the risk at its current risk rating (as long as it is within the risk appetite/tolerance levels for that type of risk). Accepted risks are subject to longer time period between reviews as the Trust has accepted that all mitigations have been implemented. However, as the risk still remains present, it is important that periodic reviews continue to be undertaken. This is different to a **closed risk** which is where the risk has been removed completely and is no longer a risk.

12. Risk appetite statement

The Board of Directors is responsible for determining the extent of risk it is willing to take in achieving its strategic objectives and has agreed the following risk appetite statement to support strategic decision making. The Trust recognises that its long-term sustainability depends upon the delivery of its strategic objectives and its relationships with its patients, staff, the public and strategic partners. Please see **Appendix E** for further information.

13. Risk Tolerance

The Board of Directors is responsible for determining the Organisations readiness to bear the risk after risk treatment to achieve its objectives. Agreed risk tolerance levels will be aligned to a specific strategic objective,

providing risk owners and their teams with required guidance to 'accept a risk' recorded on the risk management information system. Please refer to **point 11, accepted and closed risks** for further guidance.

14. Training Requirements

Knowledge on how to manage risk is essential to the successful embedding and maintaining a successful and open 'risk aware' culture. The Trust is committed to the provision of training and education to ensure that the workforce is informed, competent and prepared, possessing the necessary skills and knowledge to identify, assess and manage risk.

Specific training will be provided in respect of high-level awareness of risk management for the Board. Risk awareness sessions will be included as part of the Board's development programme.

Training available	Achievable outcomes
The Risk Management Process Guide	Aligned to ISO31000 – A Nationally recognised process.
The Risk Management Information System Toolkits	Provides practical guidance regarding recording risks within the risk management information system.
E-Learning package	Risk Management methodology aligned to ISO31000
Risk workshops	Annual schedule of risk workshops will be in place for staff to access, for them to meet their specific training needs with respect to risk management.
Bite size 'How To' recorded videos	Several sessions will be recorded and made available to staff. Will cover a series of topics from 'How to input a risk onto the risk management information system' to 'How to use the Bow Tie risk management tool'.

Finally, it is recognised that the 70-20-10 rule applies to risk management training, i.e.

- 70% of learning is by 'on the job' doing
- 20% by 'on the job' coaching and mentoring
- 10% by learning/training

15. Review process

This document will be appraised annually to ensure it remains fit-for-purpose, and formally reviewed every 5 years unless there are significant changes at either at national policy level, or locally In order that this document remains current, any of the appendices to the policy can be amended and approved during the lifetime of the document without the document strategy having to return to the ratifying committee.

16.Standards of Business Conduct

The Trust follows good NHS Business practice as outlined in the Code of Conduct and Managing Conflicts of Interest in the NHS and has robust controls in place to prevent bribery. Due consideration has been given to the Bribery Act 2010 in the review of this policy document and no specific risks were identified.

17.Process for monitoring compliance

Describe how this will be done including which elements will be monitored; by whom, frequency of monitoring; mechanism for reporting; and how action plans will be developed and monitored. It is recommended that the monitoring template (below) is used and advice on completion is sought from Head of Assurance

Minimum requirement to be monitored	Process for monitoring e.g., audit/ review of incidents/ performance management	Job title of individual(s) responsible for monitoring and developing action plan	Minimum frequency of monitoring	Name of committee responsible for review of results and action plan	Job title of individual/ committee responsible for monitoring implementation of action plan
Risks entered onto the risk register are completed according to Trust methodology	Audit	Line managers	Dependant on current (residual) risk rating level – see table below	Divisions	Divisional/ Service Area Governance Lead
All risks are graded accordingly	Audit	As above	Dependant on current (residual) risk rating level – see table below	As above	As above
All risks have action plans	Audit	As above	Dependant on current (residual) risk rating level – see table below	As above	As above
Risks are entered onto 4Risk/DATIX risk register.	Audit	As above	Monthly	As above	As above
Risk registers and associated action plans are monitored at the Divisions/ServiceAreas	Audit	Relevant chair of Division/Service Area Governance & Risk Group	Monthly	As above	Relevant Division Director/ Headof Service

18. Keywords:

Risk, Risk Management, Management of Risk, Risk Identification, Risk Process, Risk Analysis, Risk Evaluation, Risk Committee, Risk Register, Board Assurance Framework, Confirm and Challenge, Risk Management Information System, Risk Matrix, Risk tool and techniques, Risk Response, Risk Appetite, Risk Tolerance

19. References:

1. A Risk Matrix for Risk Managers, National Patient Safety Agency (2008)
2. NHS Audit Committee Handbook, Department of Health (2011)
3. UK Corporate Governance Code, Financial Reporting Council (2010)
4. Taking it on Trust: A Review of How Boards of NHS Trusts and Foundation Trusts Get Their Assurance, Audit Commission (2009)

5. The Orange Book (Management of Risk – Principles and Concepts), HM Treasury (2004)
6. Risk Management Assessment Framework, HM Treasury (2009)
7. Defining Risk Appetite and Managing Risk by Clinical Commissioning Groups and NHS Trusts, Good Governance Institute (2012)
8. Care Quality Commission Essential Standards of Quality and Safety (March 2010)
9. NHSLA Risk Management Standards (January 2012)

Appendix A

ISO31000 – Risk Definitions

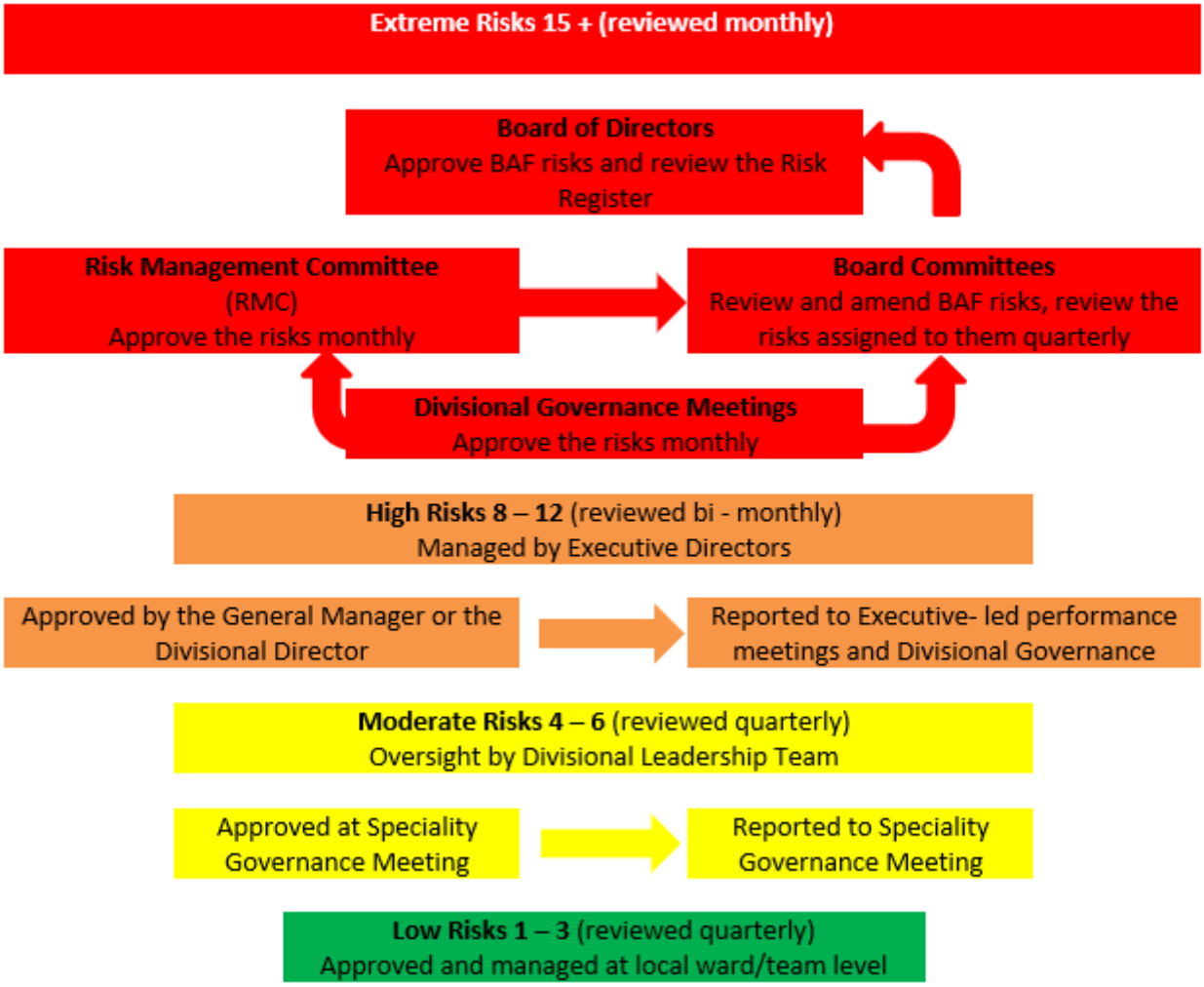
Word	Description
Risk	Effect of uncertainty on objectives
Effect	An effect is a deviation from the expected — positive and/or negative.
Objective	Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product and process).
Uncertainty	Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.
Risk management	coordinated activities to direct and control an organisation with regard to risk
Risk management framework	Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation
Risk management policy	Statement of the overall intentions and direction of an organisation related to risk management.
Risk management process	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk
Communication and consultation	Continual and iterative processes that an organisation conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk
Risk perception	Stakeholders view on a risk. Risk perception reflects the stakeholder's needs, issues, knowledge, belief and values.
External context	External environment in which the organisation seeks to achieve its objectives External context can include: • the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; • key drivers and trends having impact on the objectives of the organisation; and • relationships with, and perceptions and values of external stakeholders
Internal context	Internal environment in which the organisation seeks to achieve its objectives Internal context can include: • Governance, organisational structure, roles and accountabilities; • Policies, objectives, and the strategies that are in place to achieve them; • The capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies); • Information systems, information flows and decision-making processes (both formal and informal); • Relationships with, and perceptions and values of internal stakeholders; • The organisation's culture; • Standards, guidelines and models adopted by the organisation; and • Form and extent of contractual relationships.

Word	Description
Risk criteria	Terms of reference against which the significance of a risk is evaluated. Risk criteria are based on organisational objectives, and external and internal context Risk criteria can be derived from standards, laws, policies and other requirements.
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation
Risk identification	Process of finding, recognising and describing risks
Risk description	Structured statement of risk usually containing four elements: sources, events, causes and consequences
Risk source	Element which alone or in combination has the intrinsic potential to give rise to risk
Hazard	Source of potential harm
Risk owner	Person or entity with the accountability and authority to manage a risk
Action owner	Person or entity with the accountability and authority to manage an action in place to mitigate a potential risk.
Risk analysis	Process to comprehend the nature of risk and to determine the level of risk
Likelihood	Chance of something happening
Exposure	Extent to which an organisation and/or stakeholder is subject to an event
Consequence	Outcome of an event affecting objectives
Probability	Measure of the chance of occurrence expressed as a number between 1 and 5, where 1 is rare and 5 is almost certain
Frequency	Number of events or outcomes per defined unit of time
Risk matrix	Tool for ranking and displaying risks by defining ranges for consequence and likelihood
Level of risk	Magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood
Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable
Risk attitude	Organisation's approach to assess and eventually pursue, retain, take or turn away from risk
Risk appetite	Amount and type of risk that an organisation is willing to pursue or retain
Risk tolerance	Organisation's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives
Risk aversion	Attitude to turn away from risk
Risk aggregation	Combination of a number of risks into one risk to develop a more complete understanding of the overall risk
Risk acceptance	Informed decision to take and 'accept' a particular risk. Accepted risks are subject to monitoring and review
Risk treatment	Process to modify. Risk treatment can create new risks or modify existing risks.

Word	Description
Risk avoidance	Informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk.
Risk sharing	Form of risk treatment involving the agreed distribution of risk with other parties
Current/Residual risk	Risk remaining after risk treatment
Initial Risk	Risk level at the time of raising the risk without any new controls applied and actions put in place
Target Risk	Realistic expectation of what the risk level should be once the planned mitigation actions are taken.
Monitoring	Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives
Risk reporting	Form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management
Risk register	Record of information about identified . This is the standard listing report which can be generated from DATIX, showing all or a subset of Trust risks. These can be readily generated in Excel or PDF format from DATIX.
Risk profile	Description of any set of risks. The set of risks can contain those that relate to the whole organisation, part of the organisation, or as otherwise defined.
Risk management audit	Systematic, independent and documented process for obtaining evidence and evaluating it objectively in order to determine the extent to which the risk management framework, or any selected part of it, is adequate and effective
BAF (Board Assurance Framework)	Risk management by the Board is underpinned by a number of interlocking systems of control, which demonstrates that an effective risk management approach is in operation within the Trust. The Board Assurance Framework (BAF) report sets out the strategic objectives, identifies risks in relation to each strategic objective along with the controls in place and assurances available on their operation. The TRR and the BAF report are interlocked given their nature and as such should have a clear relationship between them. If a report is received which has the potential to impact upon the strategic objectives of the Trust; then this needs to be reflected in the BAF and appear on the TRR. Likewise, should a risk be present on the TRR which has the potential to impact upon the strategic objectives of the Trust, this should be present within the BAF.
Annual Governance Statement	The Annual Governance Statement is signed by the Chief Executive as the Accountable Officer and sets out the organisational approach to internal control. This is produced at the year-end (following regular reviews of the internal control environment during the year) and scrutinised as part of the Annual Accounts process and brought to the Board with the Accounts.
Risk Management Information System (RMIS)	Computer software system or part of the intranet of an Organisation that records and communicates risk information e.g., 4Risk/DATIX.

Appendix B

Risk Reporting, Escalation and Assurance arrangements:



Appendix C

Risk Matrix

How do I assess the likelihood?

Consider how likely it is that the risk will occur using the following descriptors:

Descriptor	Rare 1	Unlikely 2	Possible 3	Likely 4	Almost certain 5
Frequency (general) How often might it/does it happen?	This will probably never happen/recur	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it is not a persisting issue	Will undoubtedly happen/recur, possibly frequently
Frequency (timeframe)	Not expected to occur for years	Expected to occur at least annually	Expected to occur at least monthly	Expected to occur at least weekly	Expected to occur at least daily
Probability % Will it happen or not?	<5 per cent	6-25 per cent	26-50 per cent	51-75 per cent	76-100 per cent

How do I assess the consequence?

Consider how severe the impact, or consequence, of the risk would be if it did materialise.

Consequence is the term given to the resulting loss, injury, disadvantage, or gain if a risk materialises. Remember – there are likely to be a range of outcomes for this event.

Note - Evaluating risk is an iterative process. Once you calculate the risk rating, it could lead to the conclusion that, for example, a particular risk seems to have too high a risk rating. In such cases the rating may need to be reviewed, checking the likelihood and/or consequence ratings.

Domains	Negligible 1	Minor 2	Moderate 3	Major 4	Severe 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 Affects 1-2 people	Moderate injury or illness requiring professional intervention RIDDOR/Agency reportable incident (8-14 days lost) Adverse event which impacts on a small number of patients (3-15)	Major injury/long term incapacity/ disability (e.g. loss of limb) >14 days off work. Affects 16-50 people Increase in length of hospital stay by >15 days	Fatalities Multiple permanent injuries Irreversible health effects An event which impacts on >50 people

		>3 days off work	4-14 days off work		
Patient Experience	Reduced level of patient experience which is not due to delivery of clinical care	Unsatisfactory management of patient experience directly due to clinical care – readily resolvable Increase in length of hospital stay by 1-3 days	Unsatisfactory management of patient care – local resolution (with potential to go to independent review) Increase length of hospital stay by 4-15 days	Unsatisfactory management of patient care with long term effects Misdiagnosis Increased length of hospital stay by >15 days	Incident leading to death Totally unsatisfactory level of quality of treatment/ service
Environmental Impact	Onsite release of substance averted Minimal or no impact on the environment	Onsite release of substance contained Minor damage to Trust property <£10K Minor impact on the environment	On site release of substance, no detrimental effect Moderate damage to Trust property-remedied by staff/replacement of items required £10K-£50K Moderate impact on the environment	Offsite release of substance, no detrimental effect/on site release with potential detrimental effect Major damage to Trust property-external organisations required to remedy – associated costs >£50K Major impact on the environment	Offsite/on site release of substance, no detrimental/catastrophic effects Loss of building/ major piece of equipment vital to the Trusts business continuity Catastrophic impact on the environment
Staffing & Competence	Short term low staffing level (<1 day) – temporary disruption to patient care Minor competency related failure reduces services quality <1 day	On-going low staffing level - minor reduction in quality of patient care Unresolved trend relating to competency reducing service quality	Late delivery of key objective/ service due to lack of staff 50-75% attendance at mandatory/key training Unsafe staffing level	Uncertain delivery of key objective /service due to lack of staff 25-50% staff attendance at mandatory/ key training	Non delivery of key objective/ services due to lack of staff On-going unsafe staffing levels Loss of several key staff

	Low staff morale affecting 1 person	75-95% staff attendance at mandatory/key training Low staff morale (1-25% of staff)	<5 days Moderate error due to ineffective training and/or competency Low staff morale (25-50% of staff)	Unsafe staffing levels >5 days Serious error due to ineffective training and/or competency Very low staff morale (50-75% of staff)	Critical error due to lack of staff or insufficient training and/or competency Less than 25% attendance at mandatory/ key training on an on-going basis Very low staff morale (>75% of staff)
Complaints/ Claims	Informal/ locally resolved complaint Potential for settlement/ litigation <£500	Overall treatment/ service substandard Formal justified complaint (stage 1) Minor implications for patient safety if unresolved Claim <10K	Justified complaint (stage 2) involving lack of appropriate care Claim (s) between £10K - £100K Major implications for patient safety if left unresolved	Multiple justified complaints Independent review Claims between £100K -£1M Non-compliance with National Standards with significant risk to patients if unresolved	Multiple justified complaints Inquest/ Ombudsman Inquiry Claims >1M
Financial	Small loss Theft or damage of personal property <£50	Loss <100K <5% over budget/ schedule slippage Theft or loss of personal property £500	Loss of £100K-500K 5-10% over budget/ schedule slippage Theft or loss of personal property >£750	Loss of >500K-£1M 10-25% over budget/ schedule slippage Purchasers failing to pay on time	Loss >£1M >25% over budget/ schedule slippage Loss of contract/ payment by results
Business/ Service Interruption	Loss/ interruption of >1hr – no impact on delivery of patient care/ability to provide services	Short term disruption, of >8 hrs with minor impact	Loss/ interruption of >1 week Disruption causes unacceptable impact on patient care	Loss/ interruption of >1 week Sustained loss of service which has serious impact on delivery of	Permanent loss of core service/ facility Disruption to facility leading to significant 'knock-on' effect across

			Non-permanent loss of ability to provide service	patient care resulting in major contingency plans being invoked Temporary service closure	local health economy Extended service closure
Inspection/ Statutory Duty	Small number of recommendations which focus on minor quality improvement No or minimal impact or breach of guidance	Minor recommendations which can be implemented by low level of management Breach of statutory legislation No audit trail to demonstrate that objectives are being met (NICE/HSE, NSF etc)	Challenging recommendations which can be addressed Single breach of statutory duty Non-compliance with core standards <50% objectives within standards met	Enforcement action Multiple breaches of statutory duty Improvement notice Critical Report Low performance rating Major non-compliance with core standards	Multiple breaches of statutory duty Prosecution Complete systems change requires Severely critical report Zero performance rating No objectives/ standards being met.
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 and 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
Fire Safety/ General Security	Minor short term (<1 day) shortfall in fore safety system Security incident with no adverse outcome	Temporary (<1 mth) shortfall in fire safety system/ single detector etc (non-patient area)	Fire code non-compliance/ lack of single detector - patient area etc Security incident leading to compromised	Significant failure of critical component of fire safety system (patient area) Serious compromise of	Failure of multiple critical components of fire safety system (high risk patient area)

		Security incident managed locally Controlled drug discrepancy – accounted for	staff/ patient safety Controlled drug discrepancy – not accounted for.	staff/ patient safety	Infant/ young person abduction
Information Governance/IT	Breach of confidentiality - no adverse outcome Unplanned loss of IT facilities < ½ day	Minor breach of confidentiality – readily resolvable Unplanned loss of IT facilities <1 day Health records incident/ documentation incident - readily resolvable	Moderate breach of confidentiality – complaint initiated Health records/ documentation incident - patient care affected with short term consequence	Serious breach of confidentiality – > 1 person Unplanned loss of IT facilities >1 day but less than 1 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
Project Time Plan	Insignificant schedule from baseline plan Insignificant impact on value/time and resources to realise declared benefits against profile	<5% variance in schedule from baseline plan <5% variance on value/time and resources to realise declared benefits against profile	5-10% variance in schedule from baseline plan 5-10% variance on value/time and resources to realise declared benefits against profile	10-25% variance in schedule from baseline plan 10-25% variance on value/time and resources to realise declared benefits against profile	>25% variance in schedule from baseline plan >25% variance on value/time and resources to realise declared benefits against profile

L↓ C→	Negligible	Minor	Moderate	Major	Severe
Almost certain	**5**	**10**	**15**	**20**	**25**
Likely	**4**	**8**	**12**	**16**	**20**
Possible	**3**	**6**	**9**	**12**	**15**
Unlikely	**2**	**4**	**6**	**8**	**10**
Rare	**1**	**2**	**3**	**4**	**5**

Low (1 – 3)	Moderate (4 – 6)	High (8 – 12)	Extreme (15 – 25)

Appendix D

Risk Event Assessment Tool

The Shrewsbury and Telford Risk Event Assessment Tool			
Please ensure that all the information contained within this form is recorded onto 4Risk ***Please ensure this risk is approved prior to being inputted onto DATIX***			
Division		Site	
Care Unit		Ward/Department	
Risk Event Title			
Date Risk opened:			
Cause	As a result of….		
Risk	There is a risk that…		
Impact	Which might result in…		
Consequence Domains (circle as appropriate)			
Injury	Patient Experience	Environmental Impact	Staffing & Competence
Complaints/Claims	Financial	Business/Service Interruption	Inspection/ Statutory Duty
Publicity/ Reputation	Fire Safety/General Security	Information Governance/IT	Project Time Plan
Link to Strategic Priorities			
Summary of current control measures:			
Consider equipment, staffing, environment, policy/procedure, training, documentation, information….			
Adequacy of controls (please circle)	None	Adequate	Inadequate	Uncontrolled

NPSA Risk Matrix 5 X 5 *(please refer to risk matrix – further information section below)*							
			Consequence				
			1	2	3	4	5
Likelihood Score			Negligible	Minor	Moderate	Major	Severe
	5	Almost certain	5	10	15	20	25
	4	Likely	4	8	12	15	20
	3	Possible	3	6	9	12	15
	2	Unlikely	2	4	6	8	10
	1	Rare	1	2	3	4	5

What is the **current (residual)** level of risk?

(please place a **X** on the above table)

E (15-25)	**Extreme Risk.** • To be supported by Divisional Governance & approved by Risk Management Committee • Immediate action required. • Reviewed every month	H (8-12)	**High Risk.** • To be approved by General Managers/Divisional Directors • Oversight at Divisional Governance • Action planned immediately • Commence action within 1 month • Reviewed Bi-Monthly
M (4-6)	**Moderate Risk.** • To be approved/ oversight by Specialty Governance Meetings • Action planned within 1mth • Commence action within 3mths • Reviewed Quarterly	L (1-3)	**Low Risk** • To be approved/ oversight by Specialty Governance Meetings • Action planned within 3mths • Reviewed Quarterly

**** Please last sheet on form for risk reporting and escalation structure flowchart ****

Action Plan – Further control measures required				
Priority L/M/H	Action	Action Owner	Date started	Date completed

Target Risk Rating – Once all control	Level of consequence (1-5)	Level of Likelihood (1-5)	Category (Low/Moderate /High Extreme)	Predicted date to reach target rating

measures are implemented				

Date First review Due	

Risk Reporter Name	Designation	Date
Manager Name	Designation	Date
Risk Owner Name	Designation	Date risk owner was informed that risk had been assigned to them:
Risk Rating Approver Name:	Designation	Date

Review Date	**Risk Evaluation**			Print Name and Signature	Date of next review
	Level of consequence	Level of Likelihood	Low/Moderate/High/ Extreme Category		

Risk Matrix – Further information

How to rate a risk

For us to provide an accurate current (residual) risk rating, we need to ensure that this is **based on real time evidence** (complaints received/incidents reported/claims submitted etc) **and** is also taking into consideration all current controls that have been proven to be effective and efficient in our approach to mitigate the risk event.

Based on the **real time evidence**, I would ask myself the questions:

1. How often this risk event is happening, **and then based on that amount of time.**
2. What levels of consequence this risk event **has been evidentially proven to result in.**

How do I assess the likelihood?

Consider how likely it is that the risk will occur using the following descriptors:

Descriptor	Rare 1	Unlikely 2	Possible 3	Likely 4	Almost certain 5
Frequency (general) How often might it/does it happen?	This will probably never happen/recur	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it is not a persisting issue	Will undoubtedly happen/recur, possibly frequently
Frequency (timeframe)	Not expected to occur for years	Expected to occur at least annually	Expected to occur at least monthly	Expected to occur at least weekly	Expected to occur at least daily
Probability % Will it happen or not?	<5 per cent	6-25 per cent	26-50 per cent	51-75 per cent	76-100 per cent

How do I assess the consequence?

Consider how severe the impact, or consequence, of the risk would be if it did materialise.

Consequence is the term given to the resulting loss, injury, disadvantage, or gain if a risk materialises. Remember – there are likely to be a range of outcomes for this event.

Note - Evaluating risk is an iterative process. Once you calculate the risk rating, it could lead to the conclusion that, for example, a particular risk seems to have too high a risk rating. In such cases the rating may need to be reviewed, checking the likelihood and/or consequence ratings.

Domains	Negligible 1	Minor 2	Moderate 3	Major 4	Severe 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 Affects 1-2 people >3 days off work	Moderate injury or illness requiring professional intervention RIDDOR/Agency reportable incident (8-14 days lost) Adverse event which impacts on a small number of patients (3-15) 4-14 days off work	Major injury/long term incapacity/ disability (e.g. loss of limb) >14 days off work. Affects 16-50 people Increase in length of hospital stay by >15 days	Fatalities Multiple permanent injuries Irreversible health effects An event which impacts on >50 people
Patient Experience	Reduced level of patient experience which is not due	Unsatisfactory management of patient experience directly due to	Unsatisfactory management of patient care – local resolution (with potential	Unsatisfactory management of patient care with long term effects	Incident leading to death Totally unsatisfactory

	to delivery of clinical care	clinical care – readily resolvable Increase in length of hospital stay by 1-3 days	to go to independent review) Increase length of hospital stay by 4-15 days	Misdiagnosis Increased length of hospital stay by >15 days	level of quality of treatment/ service
Environmental Impact	Onsite release of substance averted Minimal or no impact on the environment	Onsite release of substance contained Minor damage to Trust property <£10K Minor impact on the environment	On site release of substance, no detrimental effect Moderate damage to Trust property- remedied by staff/replacement of items required £10K-£50K Moderate impact on the environment	Offsite release of substance, no detrimental effect/on site release with potential detrimental effect Major damage to Trust property- external organisations required to remedy – associated costs >£50K Major impact on the environment	Offsite/on site release of substance, no detrimental/catastrophic effects Loss of building/ major piece of equipment vital to the Trusts business continuity Catastrophic impact on the environment
Major Incident	??	Malicious food supply contamination Cyber Attack – telecommunications systems Accidental release of biological pathogen	Drought Major fire Widespread industrial action Major social care provider failure	Heatwave Low temperature and heavy snow Poor air quality High profile cyber crime Emerging infectious diseases	Marauding terrorist attack Radiological attack Failure of national electricity system
Staffing & Competence	Short term low staffing level (<1 day) – temporary disruption to patient care Minor competency	On-going low staffing level - minor reduction in quality of patient care Unresolved trend relating to competency	Late delivery of key objective/ service due to lack of staff 50-75% attendance at mandatory/key training	Uncertain delivery of key objective /service due to lack of staff 25-50% staff attendance at	Non delivery of key objective/ services due to lack of staff On-going unsafe staffing levels

	related failure reduces services quality <1 day Low staff morale affecting 1 person	reducing service quality 75-95% staff attendance at mandatory/key training Low staff morale (1-25% of staff)	Unsafe staffing level <5 days Moderate error due to ineffective training and/or competency Low staff morale (25-50% of staff)	mandatory/ key training Unsafe staffing levels >5 days Serious error due to ineffective training and/or competency Very low staff morale (50-75% of staff)	Loss of several key staff Critical error due to lack of staff or insufficient training and/or competency Less than 25% attendance at mandatory/ key training on an on-going basis Very low staff morale (>75% of staff)
Complaints/ Claims	Informal/ locally resolved complaint Potential for settlement/ litigation <£500	Overall treatment/ service substandard Formal justified complaint (stage 1) Minor implications for patient safety if unresolved Claim <10K	Justified complaint (stage 2) involving lack of appropriate care Claim (s) between £10K - £100K Major implications for patient safety if left unresolved	Multiple justified complaints Independent review Claims between £100K -£1M Noncompliance with National Standards with significant risk to patients if unresolved	Multiple justified complaints Inquest/ Ombudsman Inquiry Claims >1M
Financial	Small loss Theft or damage of personal property <£50	Loss <100K <5% over budget/ schedule slippage Theft or loss of personal property £500	Loss of £100K-500K 5-10% over budget/ schedule slippage Theft or loss of personal property >£750	Loss of >500K-£1M 10-25% over budget/ schedule slippage Purchasers failing to pay on time	Loss >£1M >25% over budget/ schedule slippage Loss of contract/ payment by results
Business/ Service Interruption	Loss/ interruption of >1hr – no impact on delivery of patient	Short term disruption, of >8 hrs with minor impact	Loss/ interruption of >1 week Disruption causes	Loss/ interruption of >1 week Sustained loss of service which	Permanent loss of core service/ facility Disruption to facility leading

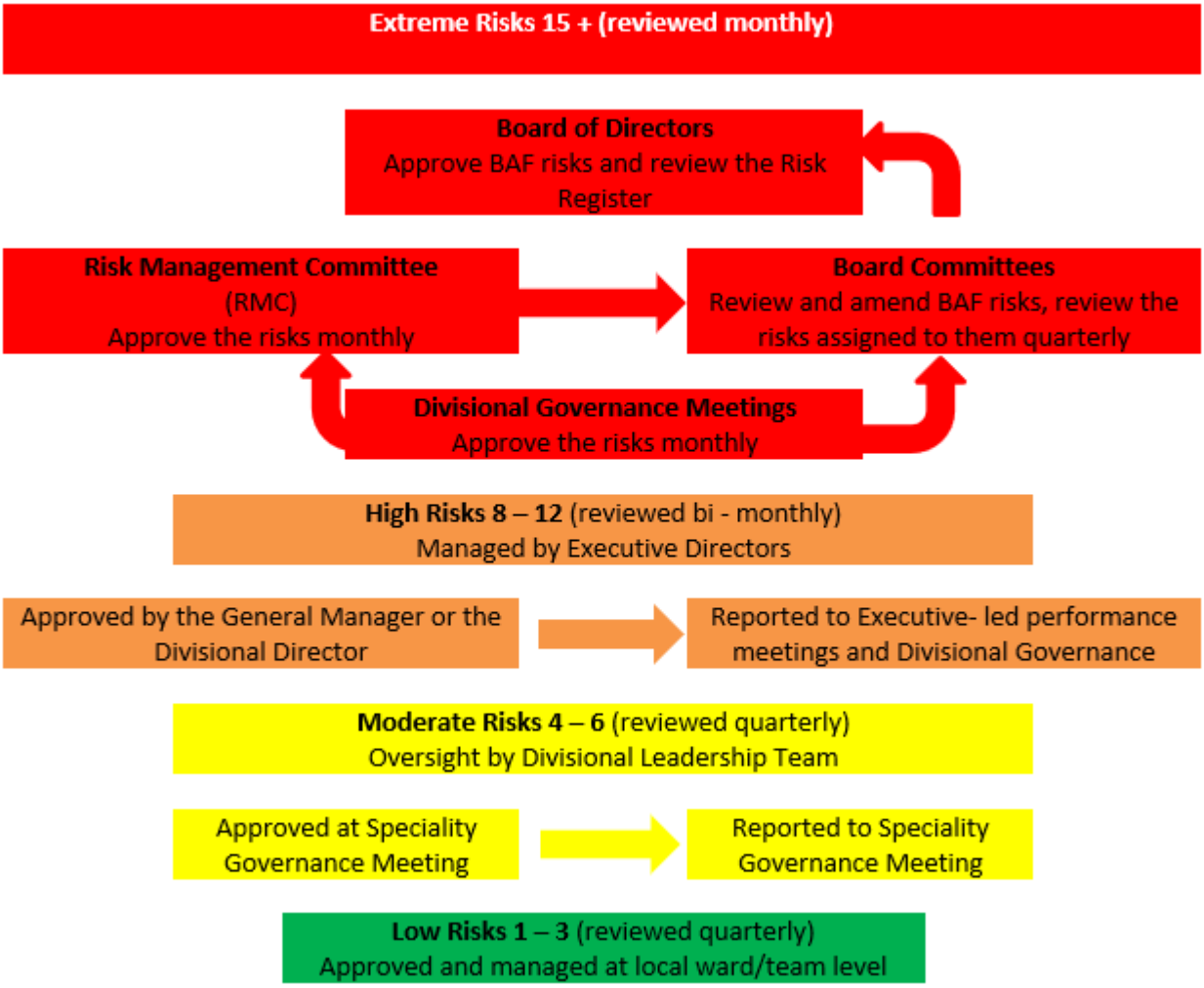
	care/ability to provide services		unacceptable impact on patient care Non-permanent loss of ability to provide service	has serious impact on delivery of patient care resulting in major contingency plans being invoked Temporary service closure	to significant 'knock-on' effect across local health economy Extended service closure
Inspection/ Statutory Duty	Small number of recommendations which focus on minor quality improvement No or minimal impact or breach of guidance	Minor recommendations which can be implemented by low level of management Breach of statutory legislation No audit trail to demonstrate that objectives are being met (NICE/HSE, NSF etc)	Challenging recommendations which can be addressed Single breach of statutory duty Non-compliance with core standards <50% objectives within standards met	Enforcement action Multiple breaches of statutory duty Improvement notice Critical Report Low performance rating Major non-compliance with core standards	Multiple breaches of statutory duty Prosecution Complete systems change requires Severely critical report Zero performance rating No objectives/ standards being met.
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 and 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
Fire Safety/ General Security	Minor short term (<1 day) shortfall in fore safety system Security incident with no	Temporary (<1 mth) shortfall in fire safety system/ single detector etc (non-patient area)	Fire code non compliance/ lack of single detector - patient area etc	Significant failure of critical component of fire safety system (patient area)	Failure of multiple critical components of fire safety system (high risk patient area)

	adverse outcome	Security incident managed locally Controlled drug discrepancy – accounted for	Security incident leading to compromised staff/ patient safety Controlled drug discrepancy – not accounted for.	Serious compromise of staff/ patient safety	Infant/ young person abduction
Information Governance/IT	Breach of confidentiality - no adverse outcome Unplanned loss of IT facilities < ½ day	Minor breach of confidentiality – readily resolvable Unplanned loss of IT facilities <1 day Health records incident/ documentation incident - readily resolvable	Moderate breach of confidentiality – complaint initiated Health records/ documentation incident - patient care affected with short term consequence	Serious breach of confidentiality – > 1 person Unplanned loss of IT facilities >1 day but less than 1 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
Project Time Plan	Insignificant schedule from baseline plan Insignificant impact on value/time and resources to realise declared benefits against profile	<5% variance in schedule from baseline plan <5% variance on value/time and resources to realise declared benefits against profile	5-10% variance in schedule from baseline plan 5-10% variance on value/time and resources to realise declared benefits against profile	10-25% variance in schedule from baseline plan 10-25% variance on value/time and resources to realise declared benefits against profile	>25% variance in schedule from baseline plan >25% variance on value/time and resources to realise declared benefits against profile

L↓ C→	Negligible	Minor	Moderate	Major	Severe
Almost certain	**5**	**10**	**15**	**20**	**25**
Likely	**4**	**8**	**12**	**16**	**20**
Possible	**3**	**6**	**9**	**12**	**15**
Unlikely	**2**	**4**	**6**	**8**	**10**
Rare	**1**	**2**	**3**	**4**	**5**

Low (1 – 3)	Moderate (4 – 6)	High (8 – 12)	Extreme (15 – 25)

Risk Reporting, Escalation and Assurance arrangements:



Risk Appetite

Organisational Goals	Risk Appetite	Risk appetite Statement
SG1: We deliver safe and excellent care, first time, everytime	**LOW**	SATH has a **LOW** risk appetite for risks thatmay compromise safety and the achievement of better outcomes for patients.
SG2: We work closely with our patients and communities to develop new models of care thatwill transform our services	**SIGNIFICANT**	SATH is eager to seek original/creative/pioneering delivery options and to accept the associated **SIGNIFICANT** risk levels in order to secure successful outcomes and transformation reward/return.
SG3: Our staff are highly skilled, motivated, engaged and live ourvalues. SATH is recognised as agreat place to work.	**MODERATE**	SATH has a **MODERATE** risk appetite toexplore innovative solutions to future staffing requirements, our ability to retainstaff and to ensure we are an employer of choice.
SG4: Our high performing and continuously improving teamswork together to support and enable the delivery of high-quality patient care.	**MODERATE**	SATH has a **MODERATE** risk appetite for Clinical Innovation and improvementthat does not compromise the quality ofcare
SG5: Our services are efficient, effective, sustainable and delivervalue for money.	**HIGH**	SATH has a **HIGH** risk appetite and is eager to pursue options which will benefitthe efficiency and effectiveness of services whilst ensuring we minimise the possibility of financial loss and comply with statutory requirements.
SG6: We deliver our services utilising safe, high quality estateand up to date digital systems and infrastructure.	**HIGH**	SATH is open to the **HIGH** risk appetite required to transform its digital systems and infrastructure to support better outcomes and experience for our patientsand public.
SG7: We have outstanding relationships with our partners and collectively strive to improvethe quality and integration of health and care services.	**SIGNIFICANT**	SATH has a **SIGNIFICANT** risk appetite for collaboration and partnerships which will ultimately provide a clear benefit andimproved outcomes for the people we serve.
SG8: We are a learning organisation that sets ambitiousgoals and targets, operates in an open and transparent way and delivers what is promised.	**HIGH**	SATH has a **HIGH** risk appetite for innovation and ideas which may affect the reputation of the organisation but aretaken in the interest of ensuring we deliver our goals and targets.

The Shrewsbury and Telford Hospital NHS Trust

Risk Management Process Guide

Additionally, refer to:

- Risk Management Policy
- Risk Management Information System (4Risk/DATIX) Toolkit
- Risk Management Strategy
- Clinical Incident Reporting Policy (CG04)
- Trust Fire Safety Policy (FS00)
- Health and Safety Policy (HS01)
- Incident reporting and investigation Policy (staff, contractors, and members of the public)including RIDDOR (HS02)
- Control of Hazardous Substances (COSHH) Policy (HS06)
- Safe Moving and Handling policy (HS08)
- Violence and Aggression Policy (SY02)
- Major Incident Policy

Version:	V1
V1 issued	Jan 2022
V1 approved by	
V1 date approved	
V1 Ratified by:	
V1 Date ratified:	
Document Lead	Head of Risk – Lisa Beresford
Lead Director	Director of Governance & Comms
Date issued:	January 2022
Review date:	January 2027
Target audience:	All staff.

Document Control Sheet:

Document Lead/Contact:	Head of Risk, Lisa Beresford
Version	V1
Status	Draft
Date Equality Impact Assessment completed	
Issue Date	January 2022
Review Date	January 2027
Distribution	Please refer to the intranet version for the latest versionof this policy. **Any printed copies may not necessarily be the mostup to date**
Key Words – including abbreviations if these would bereasonably expected to be used as search terms	Risk management, risk assessment, risk appetite, risk scoring, risk escalation
Dissemination plan	Trust intranet

Version history:

Version	Date	Author	Status	Comment – include reference to Committee presentations and dates
1.0	Jan 2022	Head of Risk, Lisa Beresford	Draft	To replace the out-of-date risk management handbook – aligned to ISO31000

Contents

1.Introduction:

The provision of healthcare and the activities associated with the treatment and care of patients, employment of staff, maintenance of premises and managing finances, by their nature, incur risks.

The purpose of the risk management process guide is to describe how the stages of the risk management process will be carried out within Shrewsbury and Telford NHS Trust

This document should be read alongside the guidance within the appendices, the **Risk Management Policy** and the **DATIX Risk Management toolkit**.

2. Definitions:

Below is a brief list of common words and their definitions that are referred to within this document. Please refer to ***Appendix 1***, for a more comprehensive list that is commonly used in the 'risk management' world.

Risk	International Organisation for Standardisation (ISO) defines risk as an **'Effect of uncertainty on objectives'.** Note that an effect may be positive (bring about opportunities), negative (pose a threat), or a deviation from the expected Risks are things that **might happen** and stop us achieving objectives, or otherwise impact on the success of the Trust.
Issues	Issues are things that **have happened (might still be happening)**, which were not planned and require management action. Issues are similar to the types of incidents that the Trust will report and investigate. Similar to a risk, the aim is to detect the root cause that led to the issue, and to put controls in place to prevent the issue recurring
Risk Management	International Organisation for Standardisation (ISO) defines risk management as **'Coordinated activities to direct and control and Organisation with regard to risk'.** This is the recognition and effective management of all threats and opportunities that may have an impact on the Trust's reputation, its ability to deliver its statutory responsibilities and the achievement of its objectives and values
Stakeholder	Any internal/external person or Organisation that can affect and/or be affected by a decision or activity. A stakeholder can include Trust staff, suppliers, agency supplied staff, volunteers, patients and/or their families

3. The Risk Management process

The risk management (RM) process may be applied at different levels. The below list, details the positive outcomes of a successful RM initiative when it's applied to those different levels:

- **Strategic:** Enabling the Trust to make better strategic decisions
- **Operational:** Events causing disruption identified in advance and allow for immediate action to be taken
- **Programme/Project:** Enabling the Trust to deliver projects on time and within a set budget
- **Compliance:** Enabling the Trust to identify risks associated with failure to achieve compliance with regulatory or statutory requirements

The Trust follows a process that is presented as a set of iterative steps that are undertaken in a coordinated manner, but not necessarily in a strict sequence.

The Risk Register module developed within DATIX is configured and deployed to support this risk management process and to generate automated reporting.

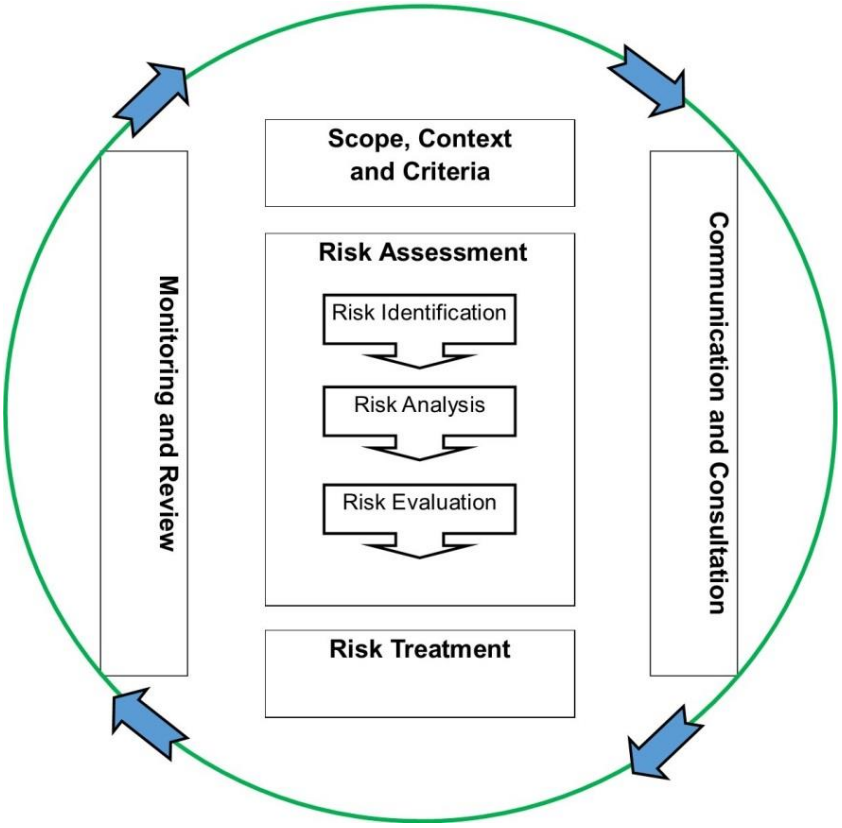


Figure 1 – ISO 31000 Risk Management Process

Figure 1, outlines the steps of the risk management process, built within the standards produced by the International Organisation for Standardisation (ISO). This document will now explain each step in a bit more detail and will introduce you to some tools and techniques to support you and your teams undertaking this process.

3.1 Scope, Context and Criteria

The purpose of establishing the scope, the context, and the criteria, is to customise the risk management process, enabling effective risk assessment and appropriate risk treatment relating to a specific area of risk.

Defining the Scope:

It is important to be clear about the scope under consideration. When planning the approach to a specific area of risk, we must consider:

1. Objectives and decisions that need to be made. ***What do we hope to achieve?***
2. Outcomes expected from the steps to be taken in the process. ***What do we think could happen?***
3. Time, location, and issues we wish to include as well as issues we wish to exclude. ***What else do we need to consider as part of this process to eliminate/mitigate this area of risk?***
4. Appropriate risk assessment tools and techniques
5. Resources required responsibilities and records to be kept. ***What do we need to effectively manage/monitor this risk?***
6. Relationships with other projects, processes and activities taking place around the Trust. ***Who else might be interested in this area of risk and its potential impact, and who could we work collaboratively with?***

Context:

The external and internal context is the environment in which the Trust seeks to define and achieve its end goal. The end goal is to eliminate this area of risk entirely, or to reduce it to a position that the Trust would be willing to accept. Either way, our ultimate mission is 'improvement'.

Understanding the context is important because:

1. Risk management takes place in the context of the priorities and activities of the Trust
2. Organisational factors can be a source of risk
3. The purpose and scope of the risk management process may be interrelated with the priorities of the Trust as a whole.

Defining Risk Criteria:

Risk criteria is also known as 'Risk Appetite'. The Trust should specify the amount and type of risk that it may or may not take connected to agreed priorities. Risk criteria should be aligned with the Risk Management Framework and reflect the Trusts values, priorities and resources and be consistent with policies and agreed risk appetite statement and tolerance levels. The risk criteria should be defined taking into consideration the Trusts obligations and the views of stakeholders.

To set risk criteria the following should be considered:

1. The nature and uncertainties that can impact on desired outcomes and priorities
2. How consequences and likelihood will be defined and measured
3. Time related factors
4. Consistent approaches to measuring the levels of risk
5. How the level of risk should be determined
6. How combinations and sequences of multiple risks will be considered
7. The Trusts capacity.

3.2 Risk Assessment

Step 1 - Risk Identification:

The purpose of risk identification (ID) is to find, recognise and describe risks that might help (opportunities) or prevent (threat) the Trust achieving its priorities. Relevant, appropriate, and up-to-date information is important in identifying risks.

The Trust can use a range of techniques for identifying uncertainties that may affect one of more objectives.

Techniques include:

- Checklists/questionnaires
- Workshops/brainstorming sessions
- Inspections/audits

- Flow charts/dependency analysis
- Bow Tie risk management tool *(see **Appendix 2** for template)*
- SWOT analysis (strengths, weaknesses, opportunities, and threats). See ***Appendix 3*** for template

Describing a risk:

The following best practice notation is used when describing the cause, risk event, and impact:

- **Cause – '*As a result of*….'** example, Increased requests from patients applying for copies of their healthcare records due to the fee being removed,

- **Risk Event – '*There is a risk that*….'** example, The Trust is unable to comply with General Data Protection Regulation time limits,

- **Impact- '*Which might result in*…..'**
  Example,
  1) Increased number of GDPR breaches
  2) The Information commissioning officer issuing an improvement notice to the Trust
  3) Financial penalties
  4) Increased number of complaints from applicant/patient

The DATIX risk management module is set up to allow those reporting risks to complete the description of the risk in the above notation.

The Bow Tie Risk Management Tool:

The Bow Tie was introduced in 1979, and was first used by the Chemical Industry. Utilising the bow tie template assists with being able to fully identify, understand, describe, manage and identify any gaps relating to a specific risk activity/event. This is a template that can be referred to and updated everytime a risk is reviewed. This will assist with deciding whether or not the current controls in place are effective or not.

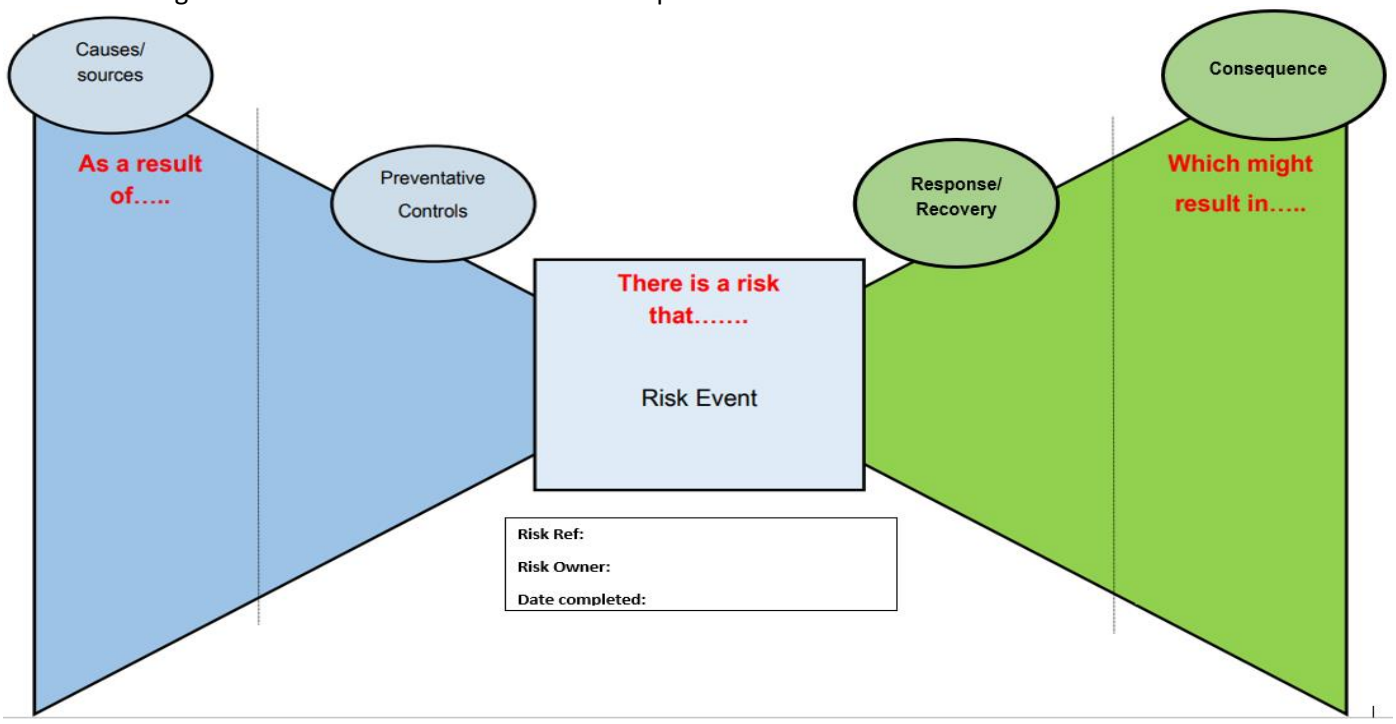


Figure 2 - The notation of risk embedded within the Bow Tie Template

This allows you to capture, and it is advised to complete this in the below order:

1. The Risk Event
2. Root Cause/Sources that have led to the risk event
3. Current controls we have in place now
4. Controls we need to put in place to mitigate risk/reduce impact/recover from the risk event
5. Consequences of this risk event

SWOT Analysis

The SWOT analysis is a simple but useful framework, for identifying your team's strengths, weaknesses, opportunities, and threats. Its helps both you and your teams to build on what you do well, to address what could be improved upon, to minimise risks, and to take the greatest possible advantage of chances for success.

The below framework can be utilised once your team has agreed upon the end goal. Following on from the example used within the 'describing a risk' section, the objective for this activity is to 'increase our levels of GDPR compliance'. Please see below table for a list of examples that were considered:

Strengths • 2 x WTE employed to support pro-cess • GDPR guidance available • All requests recorded on DATIX	**Weaknesses** • Ineffective redaction tools to redact • Scanners not fit for purpose
Opportunities • Submit a business case • Work in collaboration with other NHS to ensure a consistent process	**Threats** • Fines • Increase in complaints • Improvement notices

Step 2 - Risk Analysis:

The second step in the risk assessment is to analyse the risk.

The purpose of the risk analysis is to fully understand the nature of the risk and its characteristics including, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls, and their effectiveness.

Risk analysis techniques can be qualitative, quantitative or a combination of these depending on the circumstances and intended use.

Qualitative data: refers to non-numeric information such as healthcare records (paper based or held electronically), case studies, research outcomes, interview transcripts, type/handwritten notes, video and audio recordings, images and text documents.

Quantitative data: refers to Information that can be quantified. It can be counted or measured and given a numerical value—such as length in centimetres, revenue in pounds or staff/patient ratios.

Risk analysis should consider factors such as:

1. The likelihood of events and circumstances ***(refer to Appendix 4 - Risk Matrix)***
2. The nature and magnitude of the consequences. Magnitude refers to the size of the event that has occurred or might occur.
3. Complexity and connectivity with other similar Trust activities
4. Time related factors and possibility of the risk event rapidly changing.
5. The effectiveness of existing controls. Comparing the initial rating with the current rating is a way of establishing how effective current controls are.

Techniques used to support the analysis of risk include:

- Risk Matrix

Risk Matrix:

The tool that should be referred to, to effectively complete this stage is the **5 x 5 Risk Matrix.**

You can also access the risk matrix directly from the DATIX Web, embedded within the 'Risk Register' module.

The two elements to determine when assessing the risk are:

1. **Likelihood**: How often this risk event is happening?

and then based on that amount of time/probability

2. **Consequence:** What levels of consequence this risk event is resulting in?

To assist with this stage of the process, please refer to ***Appendix 4, Risk Matrix***. The risk matrix lists all possible consequence domains that could be impacted on if a risk event was to occur and provides a measurement in which to determine both the consequence and likelihood scores. Referring to the risk matrix also ensures that we are all consistently assessing our risks Trust wide.

Each of the consequences (C) and likelihood (L) has a range of between 1 and 5. To establish the most appropriate risk rating and level, both scores are multiplied together (**consequence x likelihood**)

L↓ C→	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
Almost certain (5)	5	10	15	20	25
Likely (4)	4	8	12	16	20
Possible (3)	3	6	9	12	15
Unlikely (2)	2	4	6	8	10
Rare (1)	1	2	3	4	5

Low (1 – 3)	Moderate (4 – 6)	High (8 – 12)	Extreme (15 – 25)

For example, if you had data to suggest that the likelihood of this risk occurring was **'likely' (4),** and if this risk was to occur would result in **'major' (4)** level of consequence, then the scores would be **C4XL4 = 16.**

The total score of **'16'** would consider to be 'an extreme risk', and prior to this being placed into the 'being reviewed' status within DATIX, would need to be agreed by a member of the Divisions/Directorates Leadership Team. Please ensure that the staff member agreeing to this current risk rating is recorded within the risk record.

When considering this stage of the process, you are required to complete the below fields:

Initial

- The risk assessment at the time of raising the risk **without** any new controls applied and actions put in place.
- This only needs to be considered and recorded within DATIX once when raising the risk.

Current

- This is the risk assessment which is recorded periodcally over time and shows where the risk is decreasing, remaining constant or increasing.
- This rating takes into consideration the effectiveness of **current controls**.
- This needs to be considered everytime a risk is reviewed on DATIX

Target

- This is the realistic expectation of what the risk assessment should be once the planned mitigation actions are taken.
- Once the risk has reached its target rating, consideration needs to be taken to look to 'accept' this risk, if we're unable to eliminate this area of risk completely.
- If we look to accept this risk, then we need to ensure thats is within the Trusts risk appetite levels

Controls:

There are 4 types of control to consider when managing a risk:

1) Preventive Control
2) Corrective Control
3) Directive Control
4) Detective Control

Preventive Control: These are the most important type of risk control, and all Organisations will use preventive controls to treat certain types of risk. Examples of preventative controls, include:

- Pre employment screening
- Maintenance of equipment
- Correct storage of hazardous chemicals/medication/healthcare records
- Limits of authorisation (financial)

Corrective Controls: These are in place when preventative controls are not workable. These types of controls assist with limiting the scope for loss and can reduce the possibility of a risk event occurring. Examples of corrective controls, include:

- Installation of a sprinkler system
- Passwords installed on devices
- Staff rotation/changes of supervisor

Directive Controls: This is the most common type of control used. This controls is based on giving directions to people and advising how to behave in certain circumstances. This type of control is the least reliable, as this is mainly based on behavioural responses. Examples of directive controls, include:

- Directions to staff in the event of a fire
- Training
- Contracts
- Standard operating procedures
- Business Continuity Plans

Detective Controls: These types of controls are designed to identify when the hazard (risk event) has materialised. Examples of detective controls include:

- Audit
- Freedom to speak up policy
- Fire detector
- Patrol of Trust estate.

Step 3 - Risk Evaluation:

The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine whether additional action is required. This can lead to a decision to:

1) Do nothing further
2) Consider risk treatment options (4 T's)
3) Undertake further analysis to better understand the risk
4) Maintain existing controls
5) Reconsider objectives.

Decisions should take account of the wider context and the actual and perceived consequences to external and internal stakeholders

The outcome of risk evaluation should be fully recorded, communicated, and then agreed at appropriate levels of the organisation.

Techniques used to support the evaluation of risks include:

- PESTLE Analysis

PESTLE Analysis:

Conducting a PESTLE analysis at this stage, would enable the team to identify key factors influencing an Organisation from **the outside**. These could be both positive and negative influences.

- **P – Political** (Employment laws, environmental regulations, trade restrictions and reform, tariffs, and political stability)
- **E – Economic** (Economic growth/decline, interest rates, wage rates, minimum wage, working hours, cost of living)
- **S – Social Factors** (Cultural norms and expectations, population growth rate, age distribution, emphasis on safety, global warming)
- **T- Technological** (Technology changes that impact your products, services, new technologies, financial decisions like outsourcing and supply chain)
- **L- Legal** (changes to legislation impacting on employment/imports & exports)
- **E- Environmental** (Disposal laws, environmental protection laws & energy consumption regulations)

Please refer to **Appendix 5** PESTLE analysis template

For the risk to remain accurately informed and rated, there needs to be an awareness of the external factors (drivers, trends, risks, stakeholder expectations) that can affect the success of the Organisation and its ability to achieve objectives.

External risk events, that if they were to occur could potentially impact on business activities within the Trust include:

1. Terrorist attacks
2. Flooding
3. Cybersecurity failure
4. Extreme Weather
5. Infectious diseases

3.3 Risk Treatment

The purpose of risk treatment (setting actions) is to select and implement options for addressing risk.

Risk treatment involves a repetitive process of:

1) Formulating and selecting risk treatment options
2) Planning and implementing risk treatment
3) Assessing the effectiveness of that risk treatment
4) Deciding whether the remaining risk is acceptable
5) In not acceptable, taking further treatment.

4T's – Treat/Tolerate/Transfer/Terminate:

Once we have completed the evaluation stage, a final decision needs to be made as to how we treat this risk. The following risk treatment options are available, and these are commonly known as the **4T's**:

- **T – Treat** - This is the option chosen in most cases, but consideration is required to establish whether the costs (financial and non-financial) associated with optimising the risk is proportionate to the risk it is controlling

- **T – Tolerate** - This option is when the likelihood and consequence of the risk is accepted, and it matches the Trust's risk appetite for this type of risk

- **T – Transfer** - This option is when the responsibility or burden for loss is shifted to another party; examples of which would be an insurance policy in place or subcontracted to another party.

- **T- Terminate** - This option is where an informed decision is made to not become involved in the risk situation; for example, termination of the activity or not entering a partnership.

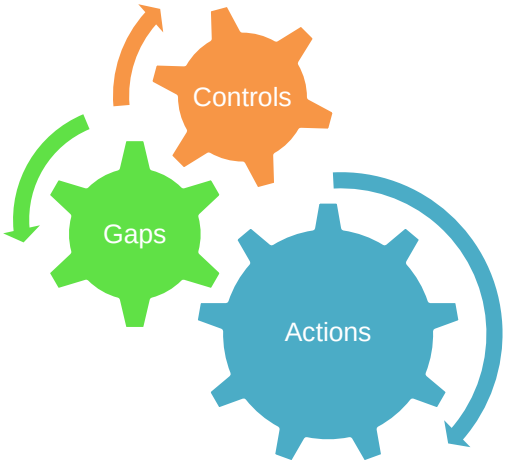
The most common of mitigation options is that of **Treat,** and this will be when gaps will have been identified and action taken to mitigate the risk. A risk should only be **Tolerated** once either all actions have been put into place and there has been a plateau in the risk scoring and if it is in accordance with the Trust's risk appetite for the risk. Please refer to ***Appendix 6*** for the Trusts agreed Risk Appetite Statement and associated tolerance levels

Risk treatments, even if carefully designed and implemented might not produce the expected outcomes and could produce unintended consequences. Monitoring and review need to be an integral part of the risk treatment implementation to give assurance that the different forms of treatment become and remain effective.

Risk treatment can also introduce new risks that need to be managed. These types of risks are commonly known as '**emerging risks'**. Emerging risks also require reporting, and actions putting in place to mitigate. Risk treatment can also enable us to identify any gaps that require immediate action to address them.

If there are no treatment options available or if treatment options do not sufficiently modify the risk, the risk should be recorded and kept under ongoing review.

Decision makers and other stakeholders should be aware of the nature and extent of the remaining risk after risk treatment. The remaining risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.



Gaps:

Despite having identified controls, it is the uncontrolled issues that are articulated as **'gaps'**. Gaps require clear and proportionate actions to address them

Actions:

For every gap identified there should be at least one action to address it. The action should specifically address the gap, should be SMART (**S**pecific, **M**easurable, **A**chievable, **R**ealistic and **T**ime bound) and have an owner responsible for completion.

The DATIX system has an Action sub-module which is integrated with the Risk Management module and due dates, action owners and progress within a specific action can be recorded. Please see the DATIX Risk Management Toolkit for more information about assigning actions.

3.4 Tolerated (accepted) and closed risks:

When all mitigating action has been completed for the gaps identified in the control measures, consideration needs to be made as to whether the risk becomes an **accepted risk (also known as a tolerated risk)**. This is a decision,

which is made at the relevant monitoring committee / subject specific group, to accept the risk at its current risk rating (as long as it is within the risk appetite/tolerance levels for that type of risk). Accepted risks are subject to longer time period between reviews as the Trust has accepted that all mitigations have been implemented. However, as the risk still remains present, it is important that periodic reviews continue to be undertaken. This is different to a **closed risk** which is where the risk has been removed completely and is no longer a risk.

3.5 Communication and Consultation

The purpose of the communication and consultation is to assist relevant stakeholders in understanding risk, the basis on which decisions are made and reasons why particular actions are required.
Communication seeks to promote awareness and understanding of risk

Consultation involves obtaining feedback and information to support decision making.

Communication and consultation with appropriate internal and external stakeholders should take place within and throughout all steps of the risk management process

Main aims:

- Bring different areas of expertise together for each step of the risk management process
- Ensure different views and appropriately considered when defining risk criteria and evaluating risks
- Provide sufficient information to facilitate risk oversight and decision –making
- Build a sense of inclusiveness and ownership among those affected by risk.

The risk management process and its outcomes should be documented and reported through appropriate mechanisms *(**see figure 2 below- risk escalation structure**).*

Risk Escalation Structure:

The escalation (and de-escalation) of risks is an important facet of risk management and there are mechanisms in place within the Trust for this to happen. Risks are **monitored** at Care Unit and Divisional Governance Meetings and at committee, subject specific group, and senior management team levels. Within these meetings, **confirm and challenge** is applied to the risks:

- **Confirm –** That the risk is scored appropriately, the correct risk owner is identified, and that identification of controls, gaps and actions are in place.
- **Challenge –** What actions are currently being undertaken – are these sufficient? What are the timescales – have they been met? Has the risk been reviewed in a timely manner by the risk owner and any other questions people may have about the risk.

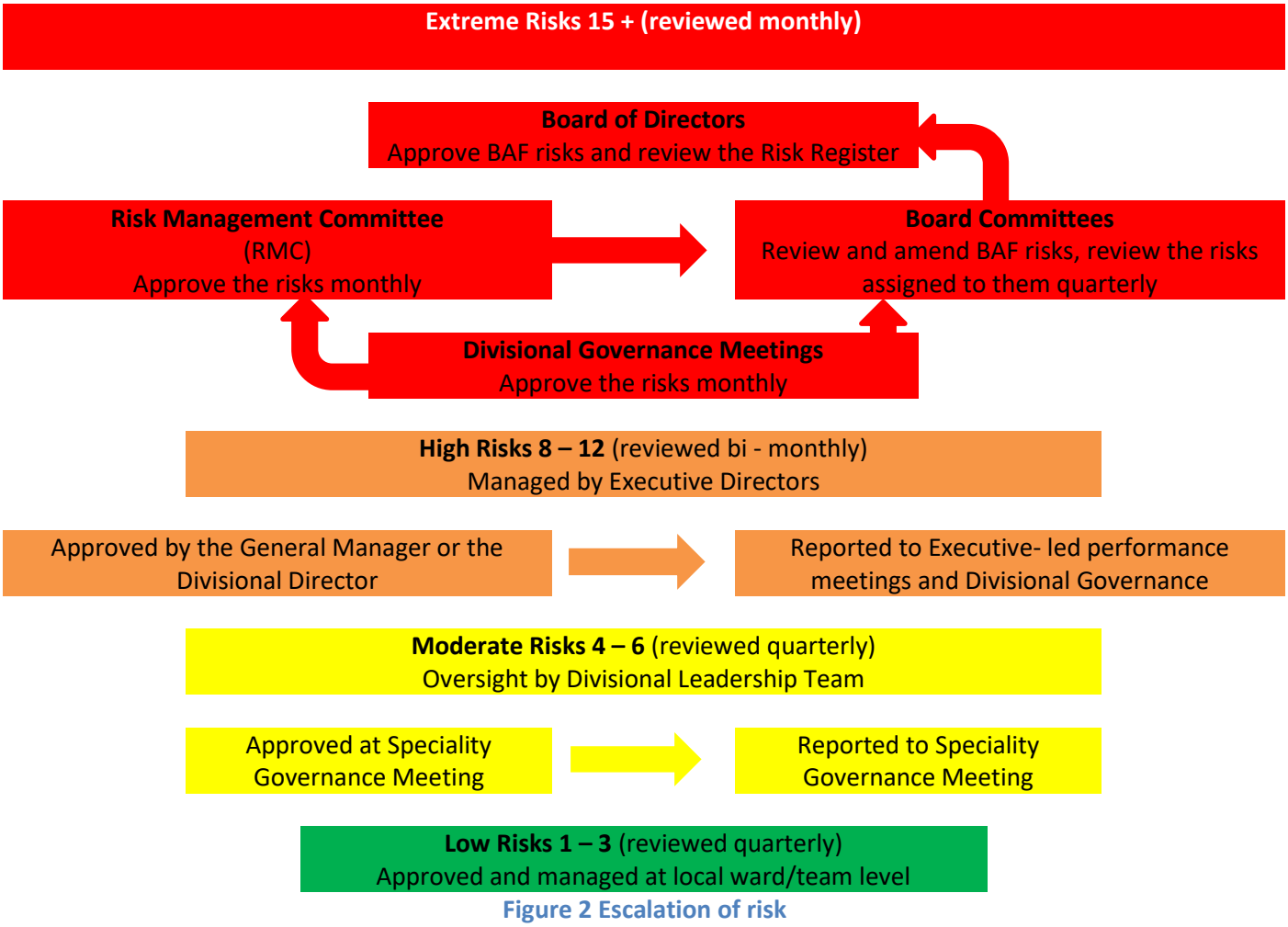


Figure 2 Escalation of risk

3.6 Monitoring and Review

The purpose of monitoring and review is to assure and improve the quality and effectiveness of the risk management process, its implementation, and outcomes. Ongoing monitoring and periodic review of the risk management process and its outcomes should be a planned part of the process, with responsibilities clearly defined.

Monitoring and review should take place in all stages of the process. Monitoring and review includes planning, gathering and analysing information, recording results within DATIX and providing feedback to all relevant stakeholders.

The frequency of review for a risk should be based upon the profile and seriousness of that risk. The below table provides guidance on normally appropriate review frequencies based upon the risk rating of the risk:

Risk Level	Risk Review Frequency
Low (1-3)	Quarterly
Moderate (4-6)	Quarterly
High (8-12)	Bi – Monthly
Extreme (15-25)	Monthly

As a risk owner, it is your responsibility to have oversight of the risk and all the associated actions. Some actions will be assigned to other people and it is the action owner's responsibility to keep their actions up to date with progress, updates, and completion dates. In some instances, the risk owner and the action owner may be the same person however action plans (even when assigned from and to by the same person) need to be evident within the risk record.

When reviewing the risk, it is important to view the actions and ascertain:

- Have the planned actions been progressed or completed by the target date? If not, is there a clear rationale for why this is?
- Are any additional actions required? Are the actions the correct ones?
- Are the assigned action owners the correct staff members?
- What is the trajectory of the actions and the risk overall – are the milestones being met?
- Do any actions require escalation to a more senior level?

The actions will form part of the risk owner's review of the overall risk which should also include the following aspects:

- Actions (see previous paragraph)
- Current risk rating
- Date of review, and date for the next review.
- Trajectory

3.7 Recording and Reporting

Recording and reporting aims to:

- Escalate and communicate risk management activities and outcomes across the Trust.
- Provide information for decision making.
- Improve risk management activities.

Risks **MUST** be approved, reported, and managed in line with the management responsibility table below:

Risk Score	Risk Level	Management Level
1-3	**Low Risk**	These **must be** reported and approved at the local care unit governance meeting, prior to the risk being entered onto the risk management information system. To be managed at local ward/team level.
4-6	**Moderate Risk**	These **must be** reported and approved at the local care unit governance meeting, prior to the risk being entered onto the risk management information system. There should be oversight by the Divisional Leadership Team (via Divisional reporting mechanisms).
8-12	**High Risk**	Approval to be sought prior to the risk being entered onto the risk management information system. These **must be** reported and approved by the General Managers, Deputy Divisional Directors, Divisional Directors to the monthly Senior Management Meetings led by the Executives, along with to the Divisional Governance Meeting. Executive Directors will manage risks at this level within their own portfolio.
15-25	**Extreme Risk**	Approval to be sought prior to the risk being entered onto the risk management information system. These **must be** reviewed at the Divisional Governance Meetings and approved by the Risk Management Committee and the Executive Team at each meeting. Extreme risks to be managed by the most appropriate Divisional Director. In extraordinary circumstances the approval of the extreme risk may bypass the Risk Management Committee, but the risk must be reported to and approved by the Divisional Director, prior to the risk being entered onto the risk management information system.

- **** All risks to be approved, prior to being inputted onto the Risk Management Information System****

4.0 References:

1. ISO31000 Management of Risk Guide (2018)
2. ISO31000 Management of Risk Vocabulary (2018)
3. A Risk Matrix for Risk Managers, National Patient Safety Agency (2008)
4. The Orange Book (Management of Risk – Principles and Concepts), HM Treasury (2020)
5. Risk Management Assessment Framework, HM Treasury (2009)
6. IRM – A Risk Practitioners Guide to ISO31000 (2018)
7. Management of Risk: Guidance for Practitioners (2010)

5.0 Related Policies and Documentation:

1. OP2.3 Incident Reporting Policy
2. OP1.16 Complaints, Concerns, Comments & Compliments Policy
3. Management of Risk Policy
4. DATIX Risk Management Toolkit
5. DATIX Toolkit
6. Clinical Incident Reporting Policy (CG04)
7. Trust Fire Safety Policy (FS00)
8. Health and Safety Policy (HS01)
9. Incident reporting and investigation Policy (staff, contractors, and members of the public) including RIDDOR (HS02)
10. Control of Hazardous Substances (COSHH) Policy (HS06)
11. Safe Moving and Handling policy (HS08)
12. Risk Management Strategy (RM01)
13. Violence and Aggression Policy (SY02)
14. Risk Management Process Guide (RM03)
15. Risk Management Information System Toolkit (RM04)
16. Major Incident Policy

ISO31000 – Risk Definitions

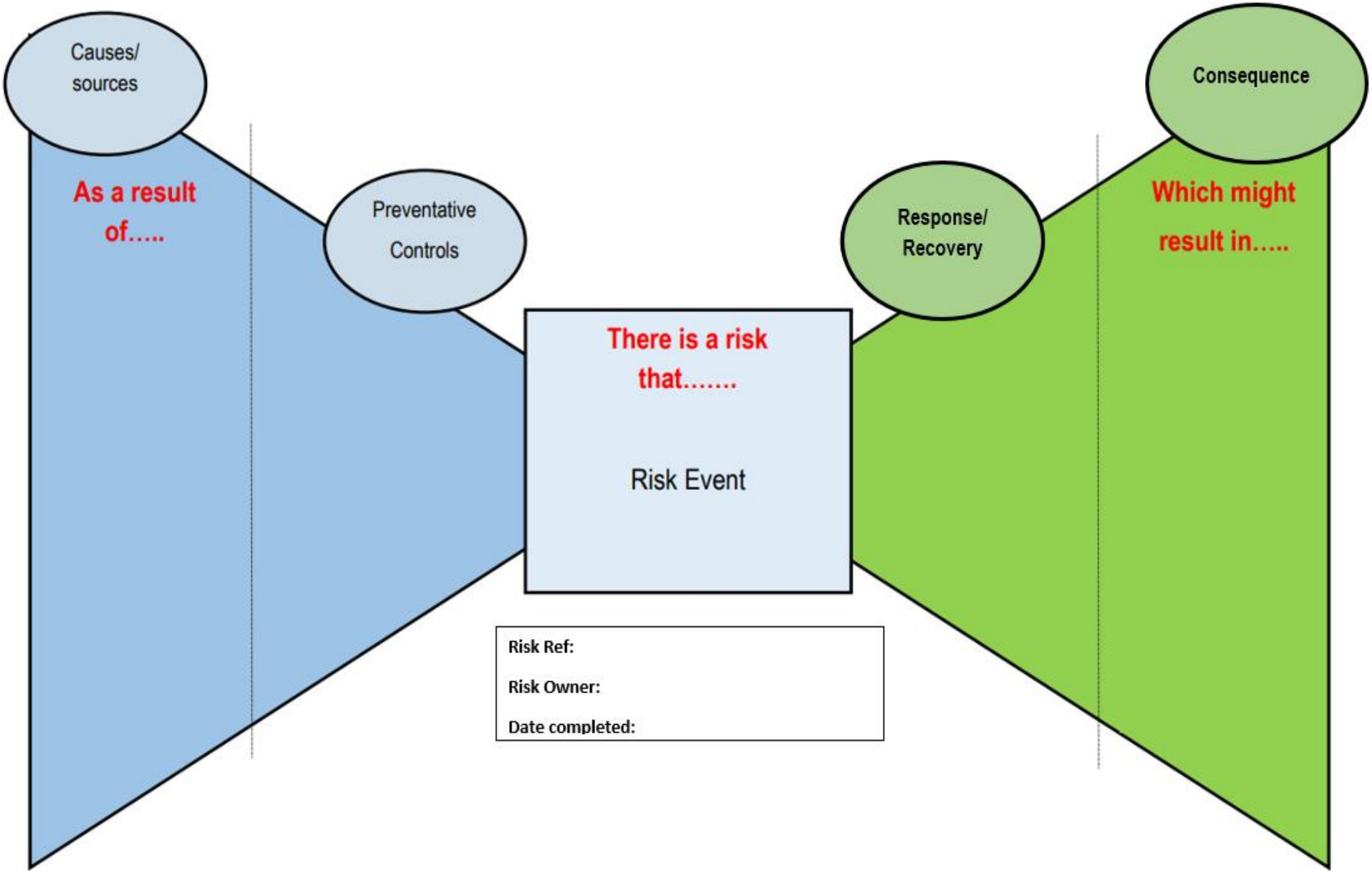
Word	Description
Risk	Effect of uncertainty on objectives
Effect	An effect is a deviation from the expected — positive and/or negative.
Objective	Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product and process).
Uncertainty	Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.
Risk management	coordinated activities to direct and control an organisation with regard to risk
Risk management framework	Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation
Risk management policy	Statement of the overall intentions and direction of an organisation related to risk management.
Risk management process	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk
Communication and consultation	Continual and iterative processes that an organisation conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk
Risk perception	Stakeholders view on a risk. Risk perception reflects the stakeholder's needs, issues, knowledge, belief and values.
External context	External environment in which the organisation seeks to achieve its objectives External context can include: • the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; • key drivers and trends having impact on the objectives of the organisation; and • relationships with, and perceptions and values of external stakeholders
Internal context	Internal environment in which the organisation seeks to achieve its objectives Internal context can include: • Governance, organisational structure, roles and accountabilities; • Policies, objectives, and the strategies that are in place to achieve them;

	• The capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies); • Information systems, information flows and decision-making processes (both formal and informal); • Relationships with, and perceptions and values of internal stakeholders; • The organisation's culture; • Standards, guidelines and models adopted by the organisation; and • Form and extent of contractual relationships.
Risk criteria	Terms of reference against which the significance of a risk is evaluated. Risk criteria are based on organisational objectives, and external and internal context Risk criteria can be derived from standards, laws, policies and other requirements.
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation
Risk identification	Process of finding, recognising and describing risks
Risk description	Structured statement of risk usually containing four elements: sources, events, causes and consequences
Risk source	Element which alone or in combination has the intrinsic potential to give rise to risk
Hazard	Source of potential harm
Risk owner	Person or entity with the accountability and authority to manage a risk
Action owner	Person or entity with the accountability and authority to manage an action in place to mitigate a potential risk.
Risk analysis	Process to comprehend the nature of risk and to determine the level of risk
Likelihood	Chance of something happening
Exposure	Extent to which an organisation and/or stakeholder is subject to an event
Consequence	Outcome of an event affecting objectives
Probability	Measure of the chance of occurrence expressed as a number between 1 and 5, where 1 is rare and 5 is almost certain
Frequency	Number of events or outcomes per defined unit of time
Risk matrix	Tool for ranking and displaying risks by defining ranges for consequence and likelihood
Level of risk	Magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood
Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable

Risk attitude	Organisation's approach to assess and eventually pursue, retain, take or turn away from risk
Risk appetite	Amount and type of risk that an organisation is willing to pursue or retain
Risk tolerance	Organisation's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives
Risk aversion	Attitude to turn away from risk
Risk aggregation	Combination of a number of risks into one risk to develop a more complete understanding of the overall risk
Risk acceptance	Informed decision to take and 'accept' a particular risk. Accepted risks are subject to monitoring and review
Risk treatment	Process to modify. Risk treatment can create new risks or modify existing risks.
Risk avoidance	Informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk.
Risk sharing	Form of risk treatment involving the agreed distribution of risk with other parties
Current/Residual risk	Risk remaining after risk treatment
Initial Risk	Risk level at the time of raising the risk without any new controls applied and actions put in place
Target Risk	Realistic expectation of what the risk level should be once the planned mitigation actions are taken.
Monitoring	Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives
Risk reporting	Form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management
Risk register	Record of information about identified risks
Risk profile	Description of any set of risks. The set of risks can contain those that relate to the whole organisation, part of the organisation, or as otherwise defined.
Risk management audit	Systematic, independent and documented process for obtaining evidence and evaluating it objectively in order to determine the extent to which the risk management framework, or any selected part of it, is adequate and effective

The Shrewsbury and Telford Hospital NHS Trust

The Risk Management Bow Tie



Risk Ref:	
Risk Owner:	
Date completed:	

Appendix 3

SWOT Analysis Template

STRENGTHS	WEAKNESSES
OPPORTUNITIES	**THREAT**

Risk Matrix

How do I assess the likelihood?
Consider how likely it is that the risk will occur using the following descriptors:

Descriptor	Rare 1	Unlikely 2	Possible 3	Likely 4	Almost certain 5
Frequency (general) How often might it/does it happen?	This will probably never happen/recur	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it is not a persisting issue	Will undoubtedly happen/recur, possibly frequently
Frequency (timeframe)	Not expected to occur for years	Expected to occur at least annually	Expected to occur at least monthly	Expected to occur at least weekly	Expected to occur at least daily
Probability % Will it happen or not?	<5 per cent	6-25 per cent	26-50 per cent	51-75 per cent	76-100 per cent

How do I assess the consequence?

Consider how severe the impact, or consequence, of the risk would be if it did materialise.

Consequence is the term given to the resulting loss, injury, disadvantage, or gain if a risk materialises. Remember – there are likely to be a range of outcomes for this event.

Note - Evaluating risk is an iterative process. Once you calculate the risk rating, it could lead to the conclusion that, for example, a particular risk seems to have too high a risk rating. In such cases the rating may need to be reviewed, checking the likelihood and/or consequence ratings.

Domains	Negligible 1	Minor 2	Moderate 3	Major 4	Severe 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 Affects 1-2 people >3 days off work	Moderate injury or illness requiring professional intervention RIDDOR/Agency reportable incident (8-14 days lost) Adverse event which impacts on a small number of patients (3-15)	Major injury/long term incapacity/ disability (e.g. loss of limb) >14 days off work. Affects 16-50 people Increase in length of hospital stay by >15 days	Fatalities Multiple permanent injuries Irreversible health effects An event which impacts on >50 people

			4-14 days off work		
Patient Experience	Reduced level of patient experience which is not due to delivery of clinical care	Unsatisfactory management of patient experience directly due to clinical care – readily resolvable Increase in length of hospital stay by 1-3 days	Unsatisfactory management of patient care – local resolution (with potential to go to independent review) Increase length of hospital stay by 4-15 days	Unsatisfactory management of patient care with long term effects Misdiagnosis Increased length of hospital stay by >15 days	Incident leading to death Totally unsatisfactory level of quality of treatment/ service
Environmental Impact	Onsite release of substance averted Minimal or no impact on the environment	Onsite release of substance contained Minor damage to Trust property <£10K Minor impact on the environment	On site release of substance, no detrimental effect Moderate damage to Trust property-remedied by staff/replacement of items required £10K-£50K Moderate impact on the environment	Offsite release of substance, no detrimental effect/on site release with potential detrimental effect Major damage to Trust property-external organisations required to remedy – associated costs >£50K Major impact on the environment	Offsite/on site release of substance, no detrimental/catastrophic effects Loss of building/ major piece of equipment vital to the Trusts business continuity Catastrophic impact on the environment
Staffing & Competence	Short term low staffing level (<1 day) – temporary disruption to patient care Minor competency related failure reduces services quality <1 day	On-going low staffing level - minor reduction in quality of patient care Unresolved trend relating to competency reducing service quality	Late delivery of key objective/ service due to lack of staff 50-75% attendance at mandatory/key training Unsafe staffing level	Uncertain delivery of key objective /service due to lack of staff 25-50% staff attendance at mandatory/ key training	Non delivery of key objective/ services due to lack of staff On-going unsafe staffing levels Loss of several key staff

	Low staff morale affecting 1 person	75-95% staff attendance at mandatory/key training Low staff morale (1-25% of staff)	<5 days Moderate error due to ineffective training and/or competency Low staff morale (25-50% of staff)	Unsafe staffing levels >5 days Serious error due to ineffective training and/or competency Very low staff morale (50-75% of staff)	Critical error due to lack of staff or insufficient training and/or competency Less than 25% attendance at mandatory/ key training on an on-going basis Very low staff morale (>75% of staff)
Complaints/ Claims	Informal/ locally resolved complaint Potential for settlement/ litigation <£500	Overall treatment/ service substandard Formal justified complaint (stage 1) Minor implications for patient safety if unresolved Claim <10K	Justified complaint (stage 2) involving lack of appropriate care Claim (s) between £10K - £100K Major implications for patient safety if left unresolved	Multiple justified complaints Independent review Claims between £100K -£1M Non-compliance with National Standards with significant risk to patients if unresolved	Multiple justified complaints Inquest/ Ombudsman Inquiry Claims >1M
Financial	Small loss Theft or damage of personal property <£50	Loss <100K <5% over budget/ schedule slippage Theft or loss of personal property £500	Loss of £100K-500K 5-10% over budget/ schedule slippage Theft or loss of personal property >£750	Loss of >500K-£1M 10-25% over budget/ schedule slippage Purchasers failing to pay on time	Loss >£1M >25% over budget/ schedule slippage Loss of contract/ payment by results
Business/ Service Interruption	Loss/ interruption of >1hr – no impact on delivery of patient care/ability to provide services	Short term disruption, of >8 hrs with minor impact	Loss/ interruption of >1 week Disruption causes unacceptable impact on patient care	Loss/ interruption of >1 week Sustained loss of service which has serious impact on delivery of	Permanent loss of core service/ facility Disruption to facility leading to significant 'knock-on' effect across

			Non-permanent loss of ability to provide service	patient care resulting in major contingency plans being invoked Temporary service closure	local health economy Extended service closure
Inspection/ Statutory Duty	Small number of recommendations which focus on minor quality improvement No or minimal impact or breach of guidance	Minor recommendations which can be implemented by low level of management Breach of statutory legislation No audit trail to demonstrate that objectives are being met (NICE/HSE, NSF etc)	Challenging recommendations which can be addressed Single breach of statutory duty Non-compliance with core standards <50% objectives within standards met	Enforcement action Multiple breaches of statutory duty Improvement notice Critical Report Low performance rating Major non-compliance with core standards	Multiple breaches of statutory duty Prosecution Complete systems change requires Severely critical report Zero performance rating No objectives/ standards being met.
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 and 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
Fire Safety/ General Security	Minor short term (<1 day) shortfall in fore safety system Security incident with no adverse outcome	Temporary (<1 mth) shortfall in fire safety system/ single detector etc (non-patient area)	Fire code non-compliance/ lack of single detector - patient area etc Security incident leading to compromised	Significant failure of critical component of fire safety system (patient area) Serious compromise of	Failure of multiple critical components of fire safety system (high risk patient area)

		Security incident managed locally Controlled drug discrepancy – accounted for	staff/ patient safety Controlled drug discrepancy – not accounted for.	staff/ patient safety	Infant/ young person abduction
Information Governance/IT	Breach of confidentiality - no adverse outcome Unplanned loss of IT facilities < ½ day	Minor breach of confidentiality – readily resolvable Unplanned loss of IT facilities <1 day Health records incident/ documentation incident - readily resolvable	Moderate breach of confidentiality – complaint initiated Health records/ documentation incident - patient care affected with short term consequence	Serious breach of confidentiality – > 1 person Unplanned loss of IT facilities >1 day but less than 1 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
Project Time Plan	Insignificant schedule from baseline plan Insignificant impact on value/time and resources to realise declared benefits against profile	<5% variance in schedule from baseline plan <5% variance on value/time and resources to realise declared benefits against profile	5-10% variance in schedule from baseline plan 5-10% variance on value/time and resources to realise declared benefits against profile	10-25% variance in schedule from baseline plan 10-25% variance on value/time and resources to realise declared benefits against profile	>25% variance in schedule from baseline plan >25% variance on value/time and resources to realise declared benefits against profile

L↓ C→	Negligible	Minor	Moderate	Major	Severe
Almost certain	**5**	**10**	**15**	**20**	**25**
Likely	**4**	**8**	**12**	**16**	**20**
Possible	**3**	**6**	**9**	**12**	**15**
Unlikely	**2**	**4**	**6**	**8**	**10**
Rare	**1**	**2**	**3**	**4**	**5**

Low (1 – 3)	Moderate (4 – 6)	High (8 – 12)	Extreme (15 – 25)

PESTLE Analysis Template

Political	Economic
Social	Technological
Legal	Environmental

Appendix 6

Risk appetite statement

Organisational Goals	Risk Appetite	Risk appetite Statement
SG1: We deliver safe and excellent care, first time, every time	**LOW**	SATH has a **LOW** risk appetite for risks that may compromise safety and the achievement of better outcomes for patients.
SG2: We work closely with our patients and communities to develop new models of care that will transform our services	**SIGNIFICANT**	SATH is eager to seek original/creative/pioneering delivery options and to accept the associated **SIGNIFICANT** risk levels in order to secure successful outcomes and transformation reward/return.
SG3: Our staff are highly skilled, motivated, engaged and live our values. SATH is recognised as a great place to work.	**MODERATE**	SATH has a **MODERATE** risk appetite to explore innovative solutions to future staffing requirements, our ability to retain staff and to ensure we are an employer of choice.
SG4: Our high performing and continuously improving teams work together to support and enable the delivery of high-quality patient care.	**MODERATE**	SATH has a **MODERATE** risk appetite for Clinical Innovation and improvement that does not compromise the quality of care
SG5: Our services are efficient, effective, sustainable and deliver value for money.	**HIGH**	SATH has a **HIGH** risk appetite and is eager to pursue options which will benefit the efficiency and effectiveness of services whilst ensuring we minimise the possibility of financial loss and comply with statutory requirements.
SG6: We deliver our services utilising safe, high quality estate and up to date digital systems and infrastructure.	**HIGH**	SATH is open to the **HIGH** risk appetite required to transform its digital systems and infrastructure to support better outcomes and experience for our patients and public.
SG7: We have outstanding relationships with our partners and collectively strive to improve the quality and integration of health and care services.	**SIGNIFICANT**	SATH has a **SIGNIFICANT** risk appetite for collaboration and partnerships which will ultimately provide a clear benefit and improved outcomes for the people we serve.
SG8: We are a learning organisation that sets ambitious goals and targets, operates in an open and transparent way and delivers what is promised.	**HIGH**	SATH has a **HIGH** risk appetite for innovation and ideas which may affect the reputation of the organisation but are taken in the interest of ensuring we deliver our goals and targets.

Risk Event Assessment Tool

The Shrewsbury and Telford Risk Event Assessment Tool				
Please ensure that all the information contained within this form is recorded onto 4Risk ***Please ensure this risk is approved prior to being inputted onto 4Risk***				
Division		Site		
Care Unit		Ward/Department		
Risk Event Title				
Date Risk opened:				
Cause	As a result of….			
Risk	There is a risk that…			
Impact	Which might result in…			
Consequence Domains (circle as appropriate)				
Injury	Patient Experience	Environmental Impact	Staffing & Competence	
Complaints/Claims	Financial	Business/Service Interruption	Inspection/ Statutory Duty	
Publicity/ Reputation	Fire Safety/General Security	Information Governance/IT	Project Time Plan	
Link to Strategic Priorities				
Summary of current control measures:				
Consider equipment, staffing, environment, policy/procedure, training, documentation, information….				
Adequacy of controls (please circle)	None	Adequate	Inadequate	Uncontrolled

NPSA Risk Matrix 5 X 5 *(please refer to risk matrix – further information section below)*							
			Consequence				
			1	2	3	4	5
Likelihood Score			Negligible	Minor	Moderate	Major	Severe
	5	Almost certain	5	10	15	20	25
	4	Likely	4	8	12	15	20
	3	Possible	3	6	9	12	15
	2	Unlikely	2	4	6	8	10
	1	Rare	1	2	3	4	5

What is the **current (residual)** level of risk?

(please place a **X** on the above table)

E (15-25)	**Extreme Risk.** • To be supported by Divisional Governance & approved by Risk Management Committee • Immediate action required. • Reviewed every month	H (8-12)	**High Risk.** • To be approved by General Managers/Divisional Directors • Oversight at Divisional Governance • Action planned immediately • Commence action within 1 month • Reviewed Bi-Monthly
M (4-6)	**Moderate Risk.** • To be approved/ oversight by Specialty Governance Meetings • Action planned within 1mth • Commence action within 3mths • Reviewed Quarterly	L (1-3)	**Low Risk** • To be approved/ oversight by Specialty Governance Meetings • Action planned within 3mths • Reviewed Quarterly

**** Please last sheet on form for risk reporting and escalation structure flowchart ****

Action Plan – Further control measures required				
Priority L/M/H	Action	Action Owner	Date started	Date completed

Target Risk Rating – Once all control measures are implemented	Level of consequence (1-5)	Level of Likelihood (1-5)	Category (Low/Moderate /High Extreme)	Predicted date to reach target rating

Date First review Due	

Risk Reporter Name	Designation	Date
Manager Name	Designation	Date
Risk Owner Name	Designation	Date risk owner was informed that risk had been assigned to them:
Risk Rating Approver Name:	Designation	Date

Review Date	**Risk Evaluation**			Print Name and Signature	Date of next review
	Level of consequence	Level of Likelihood	Low/Moderate/High/ Extreme Category		

Risk Matrix – Further information

How to rate a risk

For us to provide an accurate current (residual) risk rating, we need to ensure that this is **based on real time evidence** (complaints received/incidents reported/claims submitted etc) **and** is also taking into consideration all current controls that have been proven to be effective and efficient in our approach to mitigate the risk event.

Based on the **real time evidence**, I would ask myself the questions:

1. How often this risk event is happening, **and then based on that amount of time.**
2. What levels of consequence this risk event **has been evidentially proven to result in.**

How do I assess the likelihood?

Consider how likely it is that the risk will occur using the following descriptors:

Descriptor	Rare 1	Unlikely 2	Possible 3	Likely 4	Almost certain 5
Frequency (general) How often might it/does it happen?	This will probably never happen/recur	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it is not a persisting issue	Will undoubtedly happen/recur, possibly frequently
Frequency (timeframe)	Not expected to occur for years	Expected to occur at least annually	Expected to occur at least monthly	Expected to occur at least weekly	Expected to occur at least daily
Probability % Will it happen or not?	<5 per cent	6-25 per cent	26-50 per cent	51-75 per cent	76-100 per cent

How do I assess the consequence?

Consider how severe the impact, or consequence, of the risk would be if it did materialise.

Consequence is the term given to the resulting loss, injury, disadvantage, or gain if a risk materialises. Remember – there are likely to be a range of outcomes for this event.

Note - Evaluating risk is an iterative process. Once you calculate the risk rating, it could lead to the conclusion that, for example, a particular risk seems to have too high a risk rating. In such cases the rating may need to be reviewed, checking the likelihood and/or consequence ratings.

Domains	Negligible 1	Minor 2	Moderate 3	Major 4	Severe 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-	Moderate injury or illness requiring professional intervention RIDDOR/Agency reportable incident (8-14 days lost)	Major injury/long term incapacity/ disability (e.g. loss of limb) >14 days off work.	Fatalities Multiple permanent injuries Irreversible health effects

		permanent harm Affects 1-2 people >3 days off work	Adverse event which impacts on a small number of patients (3-15) 4-14 days off work	Affects 16-50 people Increase in length of hospital stay by >15 days	An event which impacts on >50 people
Patient Experience	Reduced level of patient experience which is not due to delivery of clinical care	Unsatisfactory management of patient experience directly due to clinical care – readily resolvable Increase in length of hospital stay by 1-3 days	Unsatisfactory management of patient care – local resolution (with potential to go to independent review) Increase length of hospital stay by 4-15 days	Unsatisfactory management of patient care with long term effects Misdiagnosis Increased length of hospital stay by >15 days	Incident leading to death Totally unsatisfactory level of quality of treatment/ service
Environmental Impact	Onsite release of substance averted Minimal or no impact on the environment	Onsite release of substance contained Minor damage to Trust property <£10K Minor impact on the environment	On site release of substance, no detrimental effect Moderate damage to Trust property-remedied by staff/replacement of items required £10K-£50K Moderate impact on the environment	Offsite release of substance, no detrimental effect/on site release with potential detrimental effect Major damage to Trust property-external organisations required to remedy – associated costs >£50K Major impact on the environment	Offsite/on site release of substance, no detrimental/catastrophic effects Loss of building/ major piece of equipment vital to the Trusts business continuity Catastrophic impact on the environment
Major Incident	??	Malicious food supply contamination Cyber Attack – telecommunications systems	Drought Major fire Widespread industrial action	Heatwave Low temperature and heavy snow Poor air quality	Marauding terrorist attack Radiological attack Failure of national

		Accidental release of biological pathogen	Major social care provider failure	High profile cyber crime Emerging infectious diseases	electricity system
Staffing & Competence	Short term low staffing level (<1 day) – temporary disruption to patient care Minor competency related failure reduces services quality <1 day Low staff morale affecting 1 person	On-going low staffing level - minor reduction in quality of patient care Unresolved trend relating to competency reducing service quality 75-95% staff attendance at mandatory/key training Low staff morale (1-25% of staff)	Late delivery of key objective/ service due to lack of staff 50-75% attendance at mandatory/key training Unsafe staffing level <5 days Moderate error due to ineffective training and/or competency Low staff morale (25-50% of staff)	Uncertain delivery of key objective /service due to lack of staff 25-50% staff attendance at mandatory/ key training Unsafe staffing levels >5 days Serious error due to ineffective training and/or competency Very low staff morale (50-75% of staff)	Non delivery of key objective/ services due to lack of staff On-going unsafe staffing levels Loss of several key staff Critical error due to lack of staff or insufficient training and/or competency Less than 25% attendance at mandatory/ key training on an on-going basis Very low staff morale (>75% of staff)
Complaints/ Claims	Informal/ locally resolved complaint Potential for settlement/ litigation <£500	Overall treatment/ service substandard Formal justified complaint (stage 1) Minor implications for patient safety if unresolved Claim <10K	Justified complaint (stage 2) involving lack of appropriate care Claim (s) between £10K - £100K Major implications for patient safety if left unresolved	Multiple justified complaints Independent review Claims between £100K -£1M Noncompliance with National Standards with significant risk to patients if unresolved	Multiple justified complaints Inquest/ Ombudsman Inquiry Claims >1M

Financial	Small loss Theft or damage of personal property <£50	Loss <100K <5% over budget/ schedule slippage Theft or loss of personal property £500	Loss of £100K-500K 5-10% over budget/ schedule slippage Theft or loss of personal property >£750	Loss of >500K-£1M 10-25% over budget/ schedule slippage Purchasers failing to pay on time	Loss >£1M >25% over budget/ schedule slippage Loss of contract/ payment by results
Business/ Service Interruption	Loss/ interruption of >1hr – no impact on delivery of patient care/ability to provide services	Short term disruption, of >8 hrs with minor impact	Loss/ interruption of >1 week Disruption causes unacceptable 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/ Statutory Duty	Small number of recommendations which focus on minor quality improvement No or minimal impact or breach of guidance	Minor recommendations which can be implemented by low level of management Breach of statutory legislation No audit trail to demonstrate that objectives are being met (NICE/HSE, NSF etc)	Challenging recommendations which can be addressed Single breach of statutory duty Non-compliance with core standards <50% objectives within standards met	Enforcement action Multiple breaches of statutory duty Improvement notice Critical Report Low performance rating Major non-compliance with core standards	Multiple breaches of statutory duty Prosecution Complete systems change requires Severely critical report Zero performance rating No objectives/ standards being met.

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 and 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
Fire Safety/ General Security	Minor short term (<1 day) shortfall in fore safety system Security incident with no adverse outcome	Temporary (<1 mth) 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	Failure of multiple critical components of fire safety system (high risk patient area) Infant/ young person abduction
Information Governance/IT	Breach of confidentiality - no adverse outcome Unplanned loss of IT facilities < ½ day	Minor breach of confidentiality – readily resolvable Unplanned loss of IT facilities <1 day Health records incident/ documentation incident - readily resolvable	Moderate breach of confidentiality – complaint initiated Health records/ documentation incident - patient care affected with short term consequence	Serious breach of confidentiality – > 1 person Unplanned loss of IT facilities >1 day but less than 1 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
Project Time Plan	Insignificant schedule from baseline plan Insignificant impact on value/time and	<5% variance in schedule from baseline plan <5% variance on value/time and resources to	5-10% variance in schedule from baseline plan 5-10% variance on value/time	10-25% variance in schedule from baseline plan 10-25% variance on value/time	>25% variance in schedule from baseline plan >25% variance on value/time

	resources to realise declared benefits against profile	realise declared benefits against profile	and resources to realise declared benefits against profile	and resources to realise declared benefits against profile	and resources to realise declared benefits against profile

L↓ C→	Negligible	Minor	Moderate	Major	Severe
Almost certain	**5**	**10**	**15**	**20**	**25**
Likely	**4**	**8**	**12**	**16**	**20**
Possible	**3**	**6**	**9**	**12**	**15**
Unlikely	**2**	**4**	**6**	**8**	**10**
Rare	**1**	**2**	**3**	**4**	**5**

Low (1 – 3)	Moderate (4 – 6)	High (8 – 12)	Extreme (15 – 25)

Risk Reporting, Escalation and Assurance arrangements: