Torbay and South Devon
NHS Foundation Trust

Risk Management Policy

Date: September 22

This is a controlled document. It should not be altered in any way without the express permission of the author or their representative.
On receipt of a new version, please destroy all previous versions.

Document Information

Date of Issue:	01/03/2016	Next Review Date:	September 2025
Version:	5.0	Last Review Date:	September 2022
Author:	Risk Officer		
Owner:	Director of Corporate Governance		
Directorate:	Corporate		
Approval Route			
Approved By:		Date Approved:	
Risk Group		06/09/22	
Audit Committee		08/09/22	
Trust Board		28/09/22	
Links or overlaps with other policies:			
Information Governance Policy			
Health and Safety Policy			
Incident Reporting and Management Policy			
We are committed to preventing discrimination, valuing diversity and achieving equality of opportunity. No person (staff, patient or public) will receive less favourable treatment on the grounds of the nine protected characteristics (as governed by the Equality Act 2010): Sexual Orientation; Gender; Age; Gender Reassignment; Pregnancy and Maternity; Disability; Religion or Belief; Race; Marriage and Civil Partnership. In addition to these nine, the Trust will not discriminate on the grounds of domestic circumstances, social-economic status, political affiliation or trade union membership. We are committed to ensuring all services, policies, projects and strategies undergo equality analysis. For more information about equality analysis and Equality Impact Assessments please refer to the Equality and Diversity Policy.			

Amendment History

Issue	Status	Date	Reason for Change	Authorised
V1	Active	01/03/2016	New Trust Policy	Trust Board
V1.1	Active	25/08/2016	Correction to Graphics and a Typo on page 12.	N/A
V1.2	Draft	04/05/2017	Annual Review & Update.	Risk Group & Exec Team
V2	Active	02/08/2017	Policy approved after first year.	Trust Board
V2.1	Active	19-01-2018	Appendix 9 updated	Co Sec
V3	Draft	18/06/2019	Annual Review & Update.	Risk Group Trust Board
V3.1	Active	27/11/2019	Appendix 3 & 4 Updated	Risk Group
V3.2	Active	21/07/2020 22/07/2020 29/07/2020	Annual Review & Update	Risk Group Audit Committee Trust Board
V3.3	Active	15/06/2021	Annual Review	Risk Group/Audit Cttee
V4.1	Active	08/09/2021	Internal Audit Review	Risk Group
V5.0	Active	24/05/2022	Review, minor updates and tone changes	Risk Group/Audit Cttee

Contents

1. Introduction

1.1. Torbay and South Devon NHS Foundation Trust (hereby referred to as the Trust) recognises that good risk management awareness, practice and recording at all levels ensures risks are managed systematically and consistently across all areas of the Organisation and where identified, risk factors can be reduced to a tolerable level. This will result in improved safety and quality of care for patients/clients and the minimisation of risks for staff and visitors.

1.2. We recognise that risk management is an essential component in fulfilling our responsibilities effectively and responsibly. The risk strategy specifies our philosophy, prime objectives and approach for the management of risk.

1.3. Good risk management is the responsibility of all staff and we recognise the importance of all staff ensuring risks are identified, recorded and managed.

1.4 A comprehensive risk management policy and procedure will not themselves ensure good risk management. Equally important is that risk management is seen as an important tool by managers and clinicians alike. Ensuring the existence of an effective risk management culture is therefore an important task for the Executive Team and the Board of Directors. An effective culture maximises the likelihood that risks and concerns are identified within the organisation. The policy and procedures ensure that risks are escalated to and managed at the right level, with the whole process underpinned by effective accountability and performance arrangements.

2. Statement/Objective

2.1. An effectively planned, organised and controlled approach to risk management is an essential component of successful corporate governance for any NHS organisation.

2.2. The intention of this policy is, therefore, to detail and support a risk based approach to decision making and to embed a culture of creativity and innovation that is founded on risk management as an integral part of our objectives, practices and management systems.

2.3. This document is intended to help and support staff, enabling and empowering them to confidently and competently make decisions on a risk-based approach.

3. Roles & Responsibilities

3.1. **All Staff**

All staff have a responsibility to familiarise themselves with the Risk Management Policy and Risk Management Strategy. Staff should report to their line manager/supervisor any risk they become aware of and take all necessary actions to reduce the risk.

All staff should be able to raise concerns about issues that may compromise any of our strategic objectives via their normal line management structure. Where it is felt that this could be difficult these concerns can be raised via the Risk Officer or through the Freedom to Speak Up: Raising Concerns (Whistleblowing) Policy (H30).

3.2 Responsibilities for the Chief Executive and other specific roles can be found in Appendix 1.

3.3 The risk management structure can be found in Appendix 2. The Chair of each Committee/Group will be responsible for ensuring the Terms of Reference (ToR) are kept up to date.

4. Risk Management

Risk management is the process by which risks are identified, assessed, recorded, mitigated and reviewed. A risk is the threat that an event or action will adversely affect the ability to achieve the organisations strategic objectives.

Each risk will be recorded by the Risk Owner with the support of their Risk Handler where applicable. Where appropriate, risks should be managed at a local level depending upon its current risk score as shown in Appendix 5.

The Risk Handler for the Area, Local Team, Department or Integrated Service Unit (ISU), will be responsible for adding and arranging the review of risks, ensuring they are assessed and managed in accordance with this policy. The risk owner will be responsible for the risk and for ensuring that the Risk Handler, if applicable, is carrying out their role effectively.

There will be some risks that cannot be dealt with at the local level; these risks should be escalated through the risk management system as soon as it is clear that the risk cannot be controlled locally.
These will include:

- Any risk that cannot be managed within the Area, Local Team, Department or ISU or Directorate,
- Any risk where the necessary adjustments cannot be funded from within the Area, Local Team, Division or ISU or Directorates budgets,
- Any risk that has a current risk score of 15 or more in accordance with the risk scoring matrix Appendix 5.

4.1. Identifying Risks

Risks can be identified through various means, including but not limited to:

- Audit recommendations.
- External recommendations.
- Fault reports.
- Incident reports.
- Process reviews.
- Risk assessments.

4.2. Assessing Risks

It is essential that all staff be alert to risks on an on-going basis to ensure that we respond to any emerging issues. Risk assessments can be done through a specific planned process at all levels. The type of assessment will vary dependant of the type of risk but all will follow the process as laid out in Appendix 8.

4.3. Risk Scoring

Risks are scored using a potential 'Consequence' score multiplied by a potential 'Likelihood' score.

- Consequence table (Appendix 3),
- Likelihood table (Appendix 4),
- Risks must be scored using the Risk Matrix (Appendix 5) for the following:
  - Initial Risk Score (when first identified).
  - Current Risk Score (once controls are put into place to reduce the Initial Risk Score).
  - Residual Risk Score (the level aimed for to either mitigate this risk or reduce it to a tolerable level) post completion of actions.
  - Tolerated Risk Score (used with all Board and corporate/high level risks where the tolerated risk score is set by the Executive Director for that risk).

4.4. Recording Risks

All risks that cannot be addressed immediately should be recorded on the risk management system. This process is explained in the how to guides on ICON and training on the HIVE.

4.5. Risk Tolerances, Accountability and Escalation

Risk tolerances and accountability are laid out in Appendix 5, the risk owner will ensure that reports are generated allowing information to be assimilated at the relevant levels.

Should the risk meet the criteria to be assessed for inclusion on the Corporate Risk Register, the Risk Officer will record this within the risks status and escalate it through the correct line of reporting as laid out in the Governance Organisational Structure.

It is important to note that the escalation of a risk will not negate the responsibilities of the risk owner or Area, Local Team, Department or ISU or Directorate.

4.6. Action Plan

An action plan is required to mitigate all risks that cannot be resolved immediately. These are to be recorded on the risk management system within the risk record for any risks with a current score of 12 or more. This is not limited to a single action plan/point as multiples may be required to reach the desired residual score.

4.7. Corporate Level Risk Register > Reviewing > Consultation and Approval

Any risk which has a current risk score of 15 or more in accordance with the Risk Scoring Matrix will be reported to the Risk Group via the correct line of reporting as laid out in Appendix 2.

Any strategic risk that may result in a failure to achieve one or more of our strategic objectives will be reported to the Risk Group via the correct lines of reporting as laid out in Appendix 2.

This full process is laid out in the Risk Management Standard Operating Procedure (SOP).

4.8. Board Assurance Framework > Reviewing > Consultation and Approval

The Board Assurance Framework (BAF) summarises our corporate objectives, the key risks in achieving these objectives and the controls and actions in place to prevent the occurrence of, or to mitigate the individual risks assurance(s) are recorded and linked to controls, as laid out in the process in Appendix 9

The Risk Group, Audit Committee and/or Board may ask for risk owners or action plan owners to provide reports on the progress and assurances that controls are sufficient. The framework is illustrated on the Risk Management pages on ICON.

The BAF will be reviewed by the Audit Committee at all of their meetings and then reported on to the Board.

4.9. Projects

It is understood that projects carried out by the organisation will be managed in accordance with standard protocols and a risk assessment will have been carried out and recorded as part of the project. It is not necessary for these to be recorded on the risk management system, unless the project has been delivered and a threat remains to one or more of our strategic objectives.

4.10. Risk Communication

All risks should be communicated locally with staff so that they can act accordingly in ensuring that all controls are carried out and any gaps in control are reported. Some risks will be reported on through the communications team to keep all staff informed.

4.11. Monitoring of the Risk Register on Datix

The risk register is monitored by the Risk Officer who in turn produces reports for the Risk Group, Audit Committee and Board of Directors.

The risk management system allows for risks to be updated and the current risk levels adjusted to show an up to date record of all risks and their associated action plans/points. Details on how to use the system are on the ICON Risk Management pages and in the Risk Management SOP and show how risks are to be reviewed, along with how reports can be generated from the system.(Template located on ICON)

4.12. Risk Reporting Structure

It is important that, depending on the level of risk, it is reported to the correct level within the organisation in a timely manner. The risk management accountability is laid out in Appendix 2.

5. Training

Risk management system training and guidance is available for all Risk Owners and Risk Handlers, this is available on the HIVE learning platform and must be completed before a login is provided.

6. Monitoring, Auditing, Reviewing & Evaluation

6.1 This policy and associated Risk Management Strategy and Risk Management SOP will be reviewed every 3 years (or sooner in the event of a major organisational or policy change) by the Director of Corporate Governance to ensure that it is relevant and effective.

6.2 Feedback from all staff regarding this policy is encouraged and should be sent to the Risk Officer.

6.3 Regular audits of the risk registers are carried out by the Risk Officer to ensure that each Area, Local Team, Department or ISU or Directorate is adhering to this policy and to identify any gaps, threats and opportunities presented in the current process.

6.4 An audit of risk system management and the BAF will be conducted by Internal Audit on an annual basis.

7. References

7.1. The key references for this policy can be found in Appendix 7.

8 Equality and Diversity Exceptions

8.1 None identified.

9 Distribution

9.1 This Policy is available to all staff and externally on the public website

10 Appendices

1. Roles and Responsibilities
2. Risk Management Structure & Accountability
3. Consequence Table
4. Likelihood Table
5. Risk Matrix
6. Summary of Risk Management Process
6a Risk Theme Identification Process
7. Key References
8. Risk Assessment Tools
9. Board Assurance Framework (BAF) Process
10. Equality Impact Assessment

Appendix 1 - Roles & Responsibilities

Title	Responsibilities
Chief Executive	Is ultimately accountable for ensuring that there is a comprehensive risk management system in place and is responsible for: • ensuring that management processes fulfil the responsibilities for risk management; • ensuring that full support and commitment is provided and maintained in every activity relating to risk management; • planning for adequate staffing, finances and other resources, to ensure the management of those risks which may have an adverse impact on the staff, finances or stakeholders of the Trust; • ensuring an appropriate corporate level risk register CLR Template is prepared and regularly updated and receives appropriate consideration; and, • ensuring that the governance statement, included in the annual reports and accounts, appropriately reflects the risk management processes in operation across the organisation..
Executive Directors	Have specific delegated responsibilities in relation to risk management, all directors must ensure that appropriate risk management processes are in place within their area of responsibility, and are responsible for: • ensuring the existence of an effective risk management culture is continually promoted; • ensuring that all relevant risks are identified and managed appropriately; • the maintenance of their area risk register, and to ensure that all relevant risks are added to the risk management system; • ensuring that the culture of their area of responsibility is such that staff are encouraged to participate in the risk management processes; • ensuring the performance management of risk management processes within their area of responsibility is linked to the performance and accountability framework for testing and assessing risk management priorities; • identifying relevant staff for risk management training; and • ensuring that they review and update the Board Assurance Framework (BAF) and the controls and assurances in place,

Systems Directors / Assistant Directors/ Senior Managers/ ISU Leads/ Department Heads/ Managers/ Matrons	Are responsible for the identification, recording, assessing and mitigating of risks within their areas of responsibility They are responsible for: • ensuring that the culture of their directorate is such that staff are encouraged to participate in the risk management processes; • ensuring their General Risk Assessment is reviewed and up to date; • escalating risks, onto the risk management system; • escalating, where appropriate to the relevant line manager; • the maintenance of a directorate risk register, and to ensure that all relevant risks are added to the risk management system; • ensuring, as a minimum, that on a quarterly basis the overall risk position for their area is considered. This must include a review of multiple low level risks that could contribute to a bigger issue / risk e.g. failed inspection; • monitoring corporate level risks to understand higher level risks with the organisation; and • identifying relevant staff for risk management training.
All Staff (Including Bank and Agency staff)	All staff have a personal responsibility to: • familiarise themselves with this policy; • report all unidentified or potential risks to their line manager/supervisor; and • record incidents and near misses on the incident reporting system.
The Senior Information Risk Owner (SIRO)	The SIRO for the organisation is responsible for: • ensuring our approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff; • providing a focal point for the resolution and/or discussion of information risk issues; and • ensuring the Board is adequately briefed on information risks.
Director of Corporate Governance	The Director of Corporate Governance is the lead for corporate governance, risk management and the Board Assurance Framework (BAF) and is responsible for: • ensuring that an effective risk management system is in place within the organisation which meets all statutory requirements and best practice guidance issued by the Department of Health and Social Care, as delegated by the Chief Executive; and • managing the strategic development and implementation of organisational risk management.

Risk Officer	The Risk Officer reports directly to the Corporate Governance Manager and in turn the Director of Corporate Governance. The Risk Officer will offer assistance, training and support to all involved in risk management and ensure the risk management system is kept up to date and is used in accordance with this policy and procedures across the organisation. The Risk Officer is responsible for: • the maintenance of a fully effective risk management system which supports the strategic direction of the Trust; • the day to day administration of the risk management system; • producing reports documenting progress of risks under various remits; • keeping an overview of all risks being entered on the system so as to report on any trends forming within the management of reported risks (Appendix 6A); • providing training and support to the Risk Handlers e.g. online training, drop in sessions and workshops on risk management and the risk management system; • providing training and support to all responsible for inputting on the risk management system; • attending key meetings to ensure the recording and actioning of risks discussed and reporting on these to the Risk Group; • ensuring maintenance and development of the Corporate/High Level Risk Register and the BAF; • providing input to the creation of and review of risk related documents; • receiving and collating information on risks within the organisation, monitoring new developments in risk management, developing knowledge and expertise and acting as a liaison point for risk management issues, both within the organisation and with external bodies; and • monitoring proposed developments and initiatives and checking they are compliant within good risk management practice.
Risk Handler	The Risk Handler will enter risks onto the risk management system and ensure these risks and their associated actions are reviewed by the Risk and Action Owners ensuring they remain current and up to date and is responsible for: • co-ordination and maintenance of their areas risk register entries, using the risk management system. • being the central contact point for the collation and escalation of key risks within their area; • being the distribution point within their area for the cascade of any information about risk management; • liaising throughout, and to lead within, their area on all aspects of risk management; and • receiving additional appropriate training on risk management and the risk management system via drop in sessions and workshops.
Chairs of meetings	Chairs of meetings should ensure that records of meetings are completed to include explicit identifiable detail of the risks discussed (Datix ID No.) and of the actions agreed to be taken. Chairs should regularly seek assurance that the corresponding entries on Datix are updated to reflect the discussion of individual risks at their meetings.

Appendix 2 - Risk Management Structure & Accountability

Title	Responsibilities
Board of Directors	Responsible for: • articulating the key risk management priorities for the organisation; • protecting the reputation of the organisation; • providing leadership in risk management; • determining our risk appetite; • ensuring our approach to risk management is consistently applied; • ensuring that assurances demonstrate that risk has been identified, assessed and all reasonable steps taken to manage it effectively and appropriately; and • endorsing risk related disclosure documents.
Audit Committee	On behalf of the Board, responsible for: • providing oversight of the establishment and maintenance of an effective system of assurance on risk management and internal control, across the whole of the organisation's activities that supports the achievement of our objectives; • ensuring the Board Assurance Framework (BAF) is received at each quarterly meeting, and appropriate consideration is taken during its review, • utilisation of Internal Audit, External Audit and other assurance functions as appropriate.
Quality Assurance Committee	Responsible for: • reviewing the establishment and maintenance of effective systems in relation to clinical and social care services to ensure the delivery of high quality, person-centred care against the Trust's quality strategy, local account of adult social care, carer's strategy and annual quality account; • receiving annual assurance reports in relation to clinical and social care services including infection control and safeguarding; • receiving and reviewing key person-centred submissions to national bodies and to make recommendations for sign-off by the Board of Directors; • receiving the annual clinical audit programme and assurance of the effectiveness of the organisation's clinical and social care audit function; • reviewing the quality related risks on the BAF and CRR.
Finance, Performance and Digital Committee	Responsible for: • scrutinising the development of our annual financial plan and long-term financial strategy and plan (both revenue and capital plans), including the underlying assumptions and methodology used, ahead of review and approval by the Board of Directors;

	• reviewing our monthly financial performance and identifying the key issues and risks requiring discussion or decision by the Board, recognising that the primary ownership and accountability for our financial performance rests with the Board of Directors; • conducting an annual review of service line reporting and discuss the implications for potential investment or disinvestment in services; • approving and keeping under review, on behalf of the Board of Directors, our investment and borrowing strategy and policies; • evaluating, scrutinising and approving the financial validity of individual investment decisions, including through the review of outline and final business cases; • reviewing post-implementation investment audits undertaken by or on behalf of the organisation. These should be carried out 12 months after business case approval; • receiving and reviewing our Financial, Performance and Digital risks scoring 15 and above; and • reviewing the financial, performance and digital related risks on the BAF.
People Committee	Responsible for: • reviewing national workforce guidance and strategies, for example the NHS People Plan, and their applicability to us. • considering and recommending to the Board of Directors, our overarching People Plan and associated activity/implementation plan(s) to support our forward strategy. • obtaining assurance and monitoring delivery of the People Plan through the associated activity/implementation plan. • considering and recommending to the Board of Directors the key people and workforce performance metrics and targets. • receiving regular reports to gain assurance that these targets are being achieved and to request and receive exception reports where this is not the case. • reviewing and providing assurance on those elements of the Board Assurance Framework identified as the responsibility of the Committee, seeking where necessary further action/assurance. • reviewing workforce related risks identified on the Corporate Risk Register and seeking assurance in relation to risk mitigation and future activity/plans. • reviewing workforce related elements of the Integrated Performance Report and seek assurance on the adequacy of our performance against operational workforce metrics. • conducting reviews and analysis of strategic people and workforce issues at national and local level and, if required, agree our response. • reviewing workforce performance and metrics at intervals to be decided by the Committee. • providing assurance to the Audit Committee that that arrangements are in place to allow staff to raise in confidence concerns about possible improprieties in financial, clinical or safety matters, and that those processes allow any such concerns to be investigated proportionately and independently.

	• seeking assurance on the adequacy and effectiveness of staff communication and levels of staff engagement
Building a Brighter Future Committee	Responsible for: • establishing a Programme of independent assurance to ensure the BBF Programme plan and its projects are managed and delivered in a controlled way. • receiving reports from the BBF Programme Group that address delivery progress, including, costs; key risks; outcome of assurance activities; and, actions to address recommendations including key decisions with reference to the capital development forward plan. • ensuring that prior to formal approval, confirmation of appropriate processes have been implemented and assurance activities completed on key BBF Programme documents, to include: o Programme and project delivery plans o Strategic Outline Case ('SOC') o Outline Business Case ('OBC') o Full Business Case ('FBC') o Contract and procurement strategies o Contract and works procurement documentation • ensuring that appropriate internal and external due diligence has been completed prior to appointment of any preferred bidders/contractors in connection with any contract. • ensuring that robust and effective governance arrangements are implemented to oversee the delivery of the BBF Programme and approved projects. • providing advice and support to the identification and effective control of the BBF Programme and any key project risks. • reviewing identified inter-dependencies across the Programme and its approved projects (and external to the BBF Programme) and ensure that controls are established to manage these effectively. • ensuring that effective control and risk management arrangements are implemented to manage the delivery of the BBF Programme and the approved projects within its control. • reviewing and providing assurance on those elements of the Board Assurance Framework identified as the responsibility of the Committee, seeking where necessary further action/assurance. • reviewing BBF Programme related risks identified on the Corporate Risk Register and seek assurance in relation to risk mitigation and future activity/plans. • reviewing and advising the Board on the risks associated with any material issues as required from time to time. In preparing such advice, the Committee shall satisfy itself that a due diligence appraisal of the proposition is undertaken and is within the risk appetite and tolerance of the organisation, drawing on independent external advice where appropriate and available, before the Board of Directors takes a decision whether to proceed.

	• considering within its agenda, material issues communicated to it by the Audit Committee, arising from the work of Internal Audit function relating to matters which fall within the scope of the Committee. The Committee shall provide feedback as to any shortcomings perceived in the scope or adequacy of the BBF Programme and shall respond to any other matters of an internal audit nature that are referred to it by the Audit Committee.
Executive Team	Responsible for: • collectively reviewing the BAF and updating so that it can be escalated through the Risk Group to the Audit Committee and on to the Board of Directors; • ensuring that strategic and operational risks are actively monitored and managed within their areas of the business; • being owner and action owner of individual Board level risks on the BAF (including those delegated by the CEO), and • devising short, medium and long-term strategies to tackle identified risk, including the production of any mitigating action plans.
Risk Group	Responsible for: • reviewing and approving validated potential Corporate/High Level Risks for addition to the Corporate Risk Register • reviewing and approving Corporate Level Risks that no longer meet the scoring requirements to remain at that status with the view to down grading them to Non-Corporate Level Risk status • reviewing the Corporate Level Risk Register and Board Assurance Framework (BAF); • creating a new theme or overarching risk identified through the 'risk theme identification process'; • ensuring the co-ordination of our BAF and supporting risks, acting as a forum for examining and rating Potential Corporate/High Level Risks and executing those recommendations; • implementing the Risk Management Strategy and providing an organisation-wide focus on the identification, control and management of risk in the development and delivery of the strategy in line with the International Standards Organisation (ISO) 31000 risk management standard; • ensuring that internal standards and procedures regarding strategic objectives / risks are developed, implemented and regularly reviewed by the relevant groups or managers; • ensuring the development and implementation of adequate, relevant and effective reporting, communication and information dissemination systems with managers and staff to comply with the ISO 31000 Risk Management Standard; • ensuring at each meeting that emerging risks are discussed; • ensuring any actions and/or action plans are being linked to risks and ensuring risks are being updated accordingly;

	• providing regular progress reports to the Audit Committee; and • responding to the recommendations of the Audit Committee, ensuring that, where appropriate they are acted upon.
Integrated Service Units (ISU)	Responsible for: • ensuring that strategic and operational risks are actively managed at the right level within their areas of the business; • ensuring risks and their associated actions within the ISU are reviewed in a timely manner, escalating any potential Corporate/High Level Risks to the Risk Group; • ensuring actions plans/points are in place, leads are identified and timescales for delivery are recorded and then monitored to completion; and • ensuring risks are discussed at ISU meetings and recorded within the minutes using the relevant risk number.
Executive Assurance Level Groups/Committees	Responsible for: • ensuring that strategic and operational risks are actively managed at the right level within their areas of the business; • ensuring risks and their associated actions within the Group/Committee are reviewed in a timely manner, escalating any potential Corporate/High Level Risks to the Risk Group • ensuring actions plans/points are in place, leads are identified and timescales for delivery are recorded and then monitored to completion; and • ensuring risks are discussed at meetings and recorded within the minutes using the relevant risk number.

Appendix 3- Potential Consequences

Choose the Risk Type from the rows below, then select the Consequence from the column.

Consequence (Impact) Score and Examples of Descriptor

Score >	1	2	3	4	5
Risk Type	**Minimal**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Clinical Safety Risk *(Physical/ Psychological)*	No physical harm or Injury. Adverse event requiring no/minimal intervention or treatment Impact prevented. Any adverse event that had the potential to cause harm but was prevented, resulting in no harm. Impact not prevented – any adverse event that ran to completion but no harm occurred.	Minor cuts or bruising, resulting in: - Any safety incident that required extra observation or minor treatment and caused minimal harm to one or more persons. Affects 1-2 people.	Moderate injury resulting in: - Professional intervention. - Increase in length of hospital stay by 4-15 days. - An event which impacts on a small number of patients. - A referral to A&E. Any patient safety incident that resulted in a moderate increase in treatment and which caused significant but not permanent harm to one or more persons. Moderate injury or illness requiring professional intervention. Affects 3-15 people**.**	Major injury resulting in: - Life changing injury/s. - Major injury/long term incapacity / disability (e.g. loss of limb). - Any incident /accident that could result in a RIDDOR reportable incident. Major untoward clinical / non-clinical issue leading to significant harm / death which requires investigation with executive director involvement. Increase in length of hospital stay by 15 days plus. Mismanagement of patient care with long-term effect. Affects 16 – 50 people.	Catastrophic injuries resulting in: - Multiple permanent injuries or irreversible health effects. - Any patient safety incident that directly resulted in the death of one or more persons. - Multiple Deaths / Fatalities. Major untoward clinical issue either in a single specialty which requires executive or an independent review. Or a single clinician referred to the GMC due to clinical management. An event effecting 50 people plus.
Performance Risk	Failure to meet departmental standards or KPIs.	Failure to meet Trust / local standards or KPIs.	Failure to meet National standards or KPIs.	Failure to meet professional standards or statutory requirements.	Sustained failure to meet professional standards or statutory requirements.

Consequence (Impact) Score and Examples of Descriptor *(continued)*					
Score >	**1**	**2**	**3**	**4**	**5**
Risk Type	**Minimal**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Environmental Impact Risk	Minimal or no impact on the environment. Minor onsite release of substance. Not directly coming into contact with patients, staff or members of the public.	Minor impact on environment. Onsite release of substance contained with potential contact with patients, staff or members of the public.	Moderate impact on environment. Onsite release of substance contained with potential contact with patients, staff or members of the public.	Major impact on environment. On-site release with potential for detrimental effect leading to off-site release with potential for detrimental effect. Involvement by the Environmental Agency	Catastrophic impact on environment. Onsite/Offsite release with realised detrimental/ catastrophic effects. Suspension of Activity by Environmental Agency.
Financial Risk	Small loss £0 – 49k	£50k – £99k	£100k – £249k	£250k – £499k	£500k +
Health & Safety Risk	No physical harm or Injury. Adverse event requiring no/minimal intervention or treatment Impact prevented. Any adverse event that had the potential to cause harm but was prevented, resulting in no harm. Impact not prevented – any adverse event that ran to completion but no harm occurred.	Minor cuts or bruising, resulting in: - No lost time or time off work. Affects 1-2 people.	Moderate injury resulting in: - Time off work for up to 7 days. - A referral to A&E. - Any patient safety incident that resulted in a moderate increase in treatment and which caused significant but not permanent harm to one or more persons. Affects 3-15 people.	Major injury resulting in: - Life changing injury/s. - Major injury/long term incapacity / disability (e.g. loss of limb). - More than14 days off work. - Any incident /accident that could result in a RIDDOR reportable incident. Affects 16 – 50 people.	Catastrophic injuries resulting in: - Multiple permanent injuries or irreversible health effects. - Any patient safety incident that directly resulted in the death of one or more persons. - Multiple Deaths / Fatalities. - Major untoward non-clinical issue either in a single specialty which requires executive or an independent review. An event effecting 50 people plus.

Consequence (Impact) Score and Examples of Descriptor *(continued)*					
Score >	**1**	**2**	**3**	**4**	**5**
Risk Type	**Minimal**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Infection Control & Prevention Risk	Business as usual	- Any Incident recorded for poor Infection control practices i.e cleanliness, hand hygiene practices, failure to perform HPV when requested by IP&C. - Failure to isolate a patient with an Alert organism (IP&CT will advise on level of risk) in a Moderate Risk area. - Sewage leaks. - Failure of Water supply. - Failure of Critical ventilation. - Failure of Decontamination. - Estates failure leading to closure of clinical areas. - HCAI e.g. Surgical Site Infections, CVC infections, Hospital acquired pneumonia, etc.	- Continued lack of compliance with infection control practices. - CDT infection TSDFT Hospital onset Healthcare associated. - MRSA infection (not colonisation) TSDFT Hospital onset Healthcare associated. - Failure to isolate a patient with an Alert organism in a High-Risk area.	- CDT infection >2 TSDFT Hospital onset Healthcare associated in 28 days in single clinical area. - MRSA infection (not colonisation) >2 TSDFT Hospital onset Healthcare associated in 28 days in single clinical area. - Seasonal flu cases leading to 2 ward closures in TSDFT. 4 or more cases of seasonal flu on ITU leading to cancellation of surgery and transfers out. - Norovirus cases leading to 2 ward closures in TSDFT. 4 or more cases of Norovirus on ITU leading to cancellation of surgery and transfers out. - Failure to isolate a patient with an Alert organism in a Very High Risk area.	- Pandemic, Swine Flu, Etc. CDT infection leading to death >2 TSDFT Hospital onset Healthcare associated in 28 days in single clinical area. - MRSA infection (not colonisation) leading to death >2 TSDFT Hospital onset Healthcare associated in 28 days in single clinical area. - Pandemic /seasonal Flu cases in hospital leading to cross infection and >2ward closure/and increased deaths. Staff sickness from pandemic/seasonal flu leading to low staffing levels. - Norovirus cases in hospital leading to cross infection and >2 ward closure/and increased deaths. Staff sickness from Norovirus leading to low staffing levels. - Failure to isolate >2 patient with an Alert organism in a Very High Risk area.

Consequence (Impact) Score and Examples of Descriptor *(continued)*					
Score >	**1**	**2**	**3**	**4**	**5**
Risk Type	**Minimal**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Information & Communications Technology Risk	Unplanned loss/interruption of service for up to 1 hour affecting one business critical system. Loss of data from a single business critical system that takes up to 1 hour to recover. Exposure of non-personal or confidential information to those not covered by a data sharing agreement or otherwise unintended.	Unplanned loss/interruption of service for up to 4 hours affecting one business critical system. Loss of data from a single business critical system that takes up to 8 hours to recover. Exposure of embarrassing information to unintended recipients.	Unplanned loss/interruption of service for up to 8 hours affecting one business critical system. Loss of data from a single business critical system that takes up to 24 hours to recover. Exposure of commercially confidential information to unintended recipients.	Unplanned loss/interruption affecting service of one business critical IT systems for up to 24 hours. Temporary loss of data from multiple business critical systems. Exposure of a single individuals' personal information to those not covered by a data sharing agreement or otherwise unintended.	Unplanned loss/interruption affecting service of many business critical IT systems for up to 1 hour. Permanent loss of data from a single business critical system. Exposure of multiple individuals' personal information to those not covered by a data sharing agreement or otherwise unintended.
Information Governance Risk	Failure to meet departmental standard.	Failure to meet Trust / local standard. - GDPR Incident raised on Datix.	Failure to meet national standards or KPI.	Failure to meet professional standards or statutory requirements.	Sustained failure to meet professional standards or statutory requirements.
Operational Risks	Loss/interruption of up to1 hour.	Loss/interruption of up to 8 hours.	Loss/interruption of up to 1 day.	Loss/interruption of up to 1 week.	Permanent loss of service or facility.
Patient Experience Risk	Reduced level of patient experience not directly related to delivery of care.	Unsatisfactory patient experience, readily resolvable.	Mismanagement of patient care. Unsatisfactory management of patient care – local resolution (with potential to go to independent review).	Serious concerns re patient experience for a particular patient or about a particular clinical service / clinician which required executive director involvement in investigation and onward action. Unsatisfactory management of patient care with long term effects. Significant result of misdiagnosis.	Totally unacceptable patient experience that would lead to an investigation by the CQC e.g. Mid Staffordshire. Totally unsatisfactory patient outcome or experience. Incident leading to death.

Consequence (Impact) Score and Examples of Descriptor*(continued)*					
Score >	**1**	**2**	**3**	**4**	**5**
Risk Type	**Minimal**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Reputation /Risk	Complaint / Rumours. Derogative posts on Social Media, (Facebook/Twitter/Instagram). Potential for public concern. Informal/locally resolved complaint. Potential for settlement/litigation up to £5K.	Local media coverage, short-term reduction in public confidence. Shared derogative posts on Social Media, (Facebook/Twitter/Instagram). Elements of public expectation not being met. Overall treatment/service substandard. Formal justified complaint Minor implication for patient safety if unresolved. Claim up to £10K.	Local media coverage. Long-term reduction in public confidence. Sustained postings of derogative posts on Social Media, (Facebook/Twitter/Instagram). Justified complaint involving lack of appropriate care. Major implications for patient safety if unresolved. Claim(s) between £10K-£100K.	National media coverage with <3 days service well below reasonable public expectation. Petition raised on Change.org or other social media platform. Multiple justified complaints leading to Independent review. Noncompliance with National standards with significant risk to patients if unresolved. Claim(s) between £100K-£1M.	National media coverage with >3 days service well below reasonable public expectation. MP concerned (questions in the House.) Total loss of public confidence. Multiple justified complaints - Single major claim - Inquest/ ombudsman inquiry -Claim >£1M

Appendix 4 - Assessment of Likelihood of a Risk

Qualitative and Quantitative Measures of Likelihood:

What is the likelihood of the consequence described in the Consequence Table, actually happening?

A frequency based score will be appropriate in most circumstances, except in the case of time-limited projects or objectives, where the probability or chance of reoccurrence based score could be used.

Level / Score	Matrix Description	Detailed Description	Frequency	Odds / Probability	% Chance of Occurrence / Reoccurrence
1	**Rare**	Highly unlikely, but it may occur in exceptional circumstance. It could happen but probably never will.	Not expected to occur for years	May occur = 1 in 1000 chance	1 - 5 %
2	**Unlikely**	Not expected but there is a slight possibility it may occur at some time.	Expected to occur at least annually	Could occur at some time = 1 in 100 to 1 in 1000	6 – 25%
3	**Possible**	The event might occur at some time if other factors precipitate or as there is a history of casual occurrence.	Expected to occur at least monthly	Might occur at some time = 1 in 10 to 1 in 100	26 – 50%
4	**Likely**	If the activity continues without controls in place, there is a strong possibility the event will occur as there is a history of frequent occurrences.	Expected to occur at least weekly	Will probably occur in most circumstances = 1 in 10 to evens odds	51 – 75%
5	**Almost Certain**	Very likely, The event is expected to occur in most circumstances if the activity continues without controls in place. Or may already be happening.	Expected to occur at least daily	Is expected to occur in most circumstances = evens to certain odds	76 – 100%

Appendix 5 – Risk Scoring Matrix

Consequence / Likelihood	1 - Minimal / Insignificant	2 - Minor	3 - Moderate	4 - Major	5 - Catastrophic
5 - Almost Certain	5	10	15	20	25
4 - Likely	4	8	12	16	20
3 - Possible	3	6	9	12	15
2 - Unlikely	2	4	6	8	10
1 - Rare	1	2	3	4	5

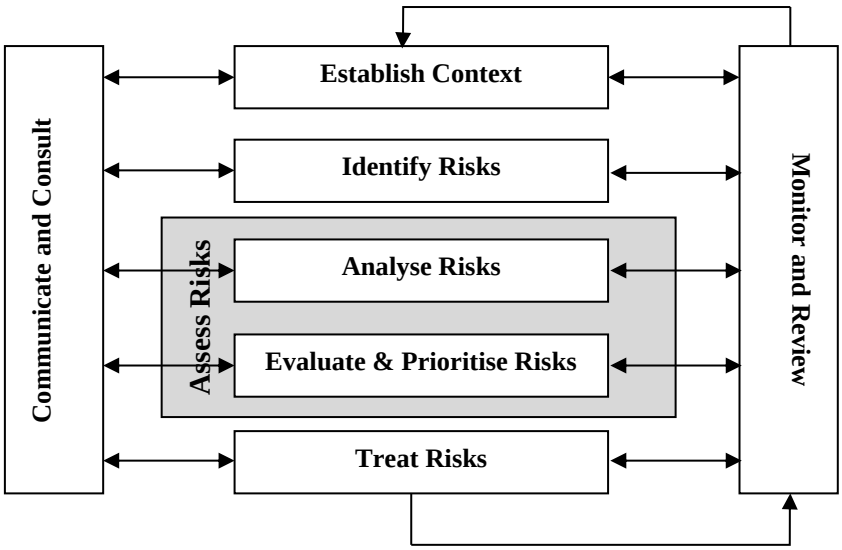
Risk scoring = consequence x likelihood (C x L)

KEY:

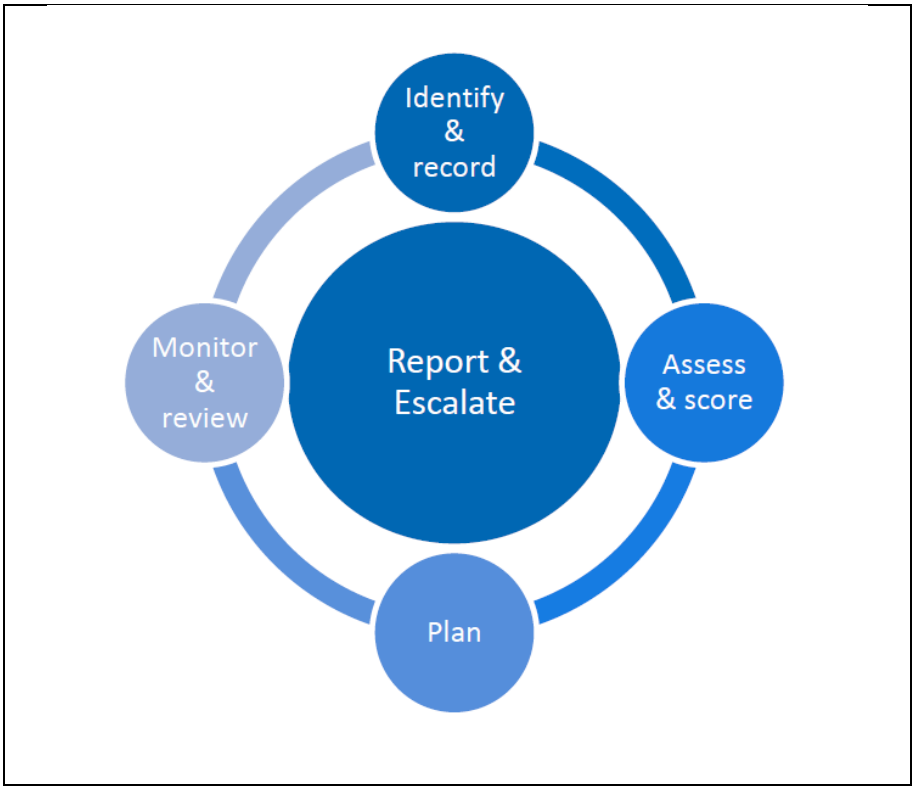
RAG Rating	Expected Level of Management
RED	Executive Team / Board
AMBER	Directorate / ISU
GREEN	General Manager

Appendix 6 - Summary of Risk Management Process

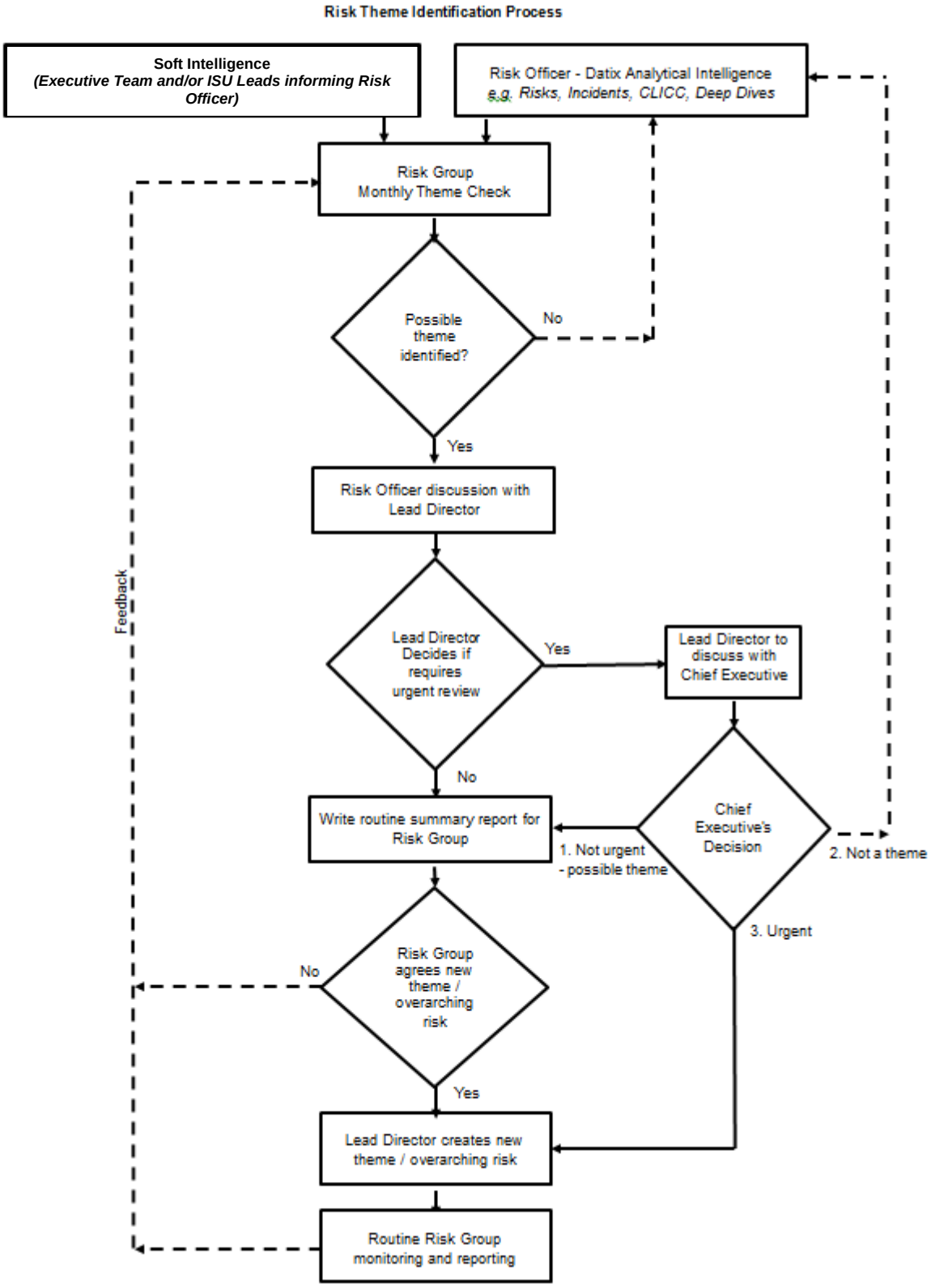
(Adapted from ISO 31000 Risk Management – Principles and Guidelines)



A risk can be any event that **might** occur or is occurring which **could or is** affecting the ability of the Trust/ISU to achieve its **objectives** – it is what could happen, how it could happen and who could be affected by it.



Appendix 6a - Risk Theme Identification Process

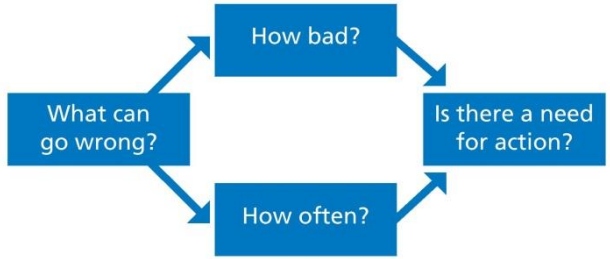


Appendix 7 - Key References

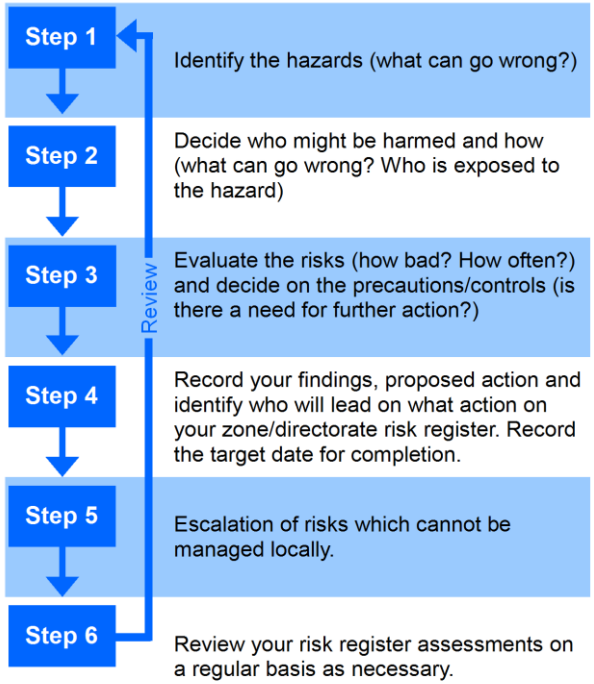
• NHS Providers Foundations of Good Governance • Health & Safety at Work Act 1974 • Management of Health & Safety at Work Regulations, (2006 Amendment & 1999) • Internal audit standards for the NHS	• DH: Information Security NHS Code of Practice (2007) • HFMA: Audit Publications

Appendix 8 - Risk Assessment Tools

What is risk assessment? A risk assessment seeks to answer four simple, related questions:



It is not usually possible to eliminate all risks but health and social care staff have a duty to protect patients/service users, themselves and the organisation as far as 'reasonably practical'. This means you must avoid any unnecessary risk. It is best to focus on the risks that really matter – those with the potential to cause harm either clinically, financially or to the organisation as a whole. Keep risk assessment simple – do not use techniques that are overly complex for the type of risk being assessed.



In a risk assessment we need to look at:

Hazards – A hazard is something with the potential to cause harm. The harm could be injury or illness, damage to equipment or premises or some other loss.

Risks – A risk is the likelihood that a hazard will cause actual harm, or effect the successful operation of the organisation, department or project. (i.e. the consequence)
For each hazard identified it is important to decide whether it is significant and whether appropriate and sufficient controls or contingencies are in place to ensure that the risk is properly controlled.

Controls – Controls are the arrangements made, or the precautions taken, to a reduce risk. (It is what is in place now)

Risk Score/Rating – A risk score or rating is the calculation of hazard consequence x likelihood, taking into account current controls.

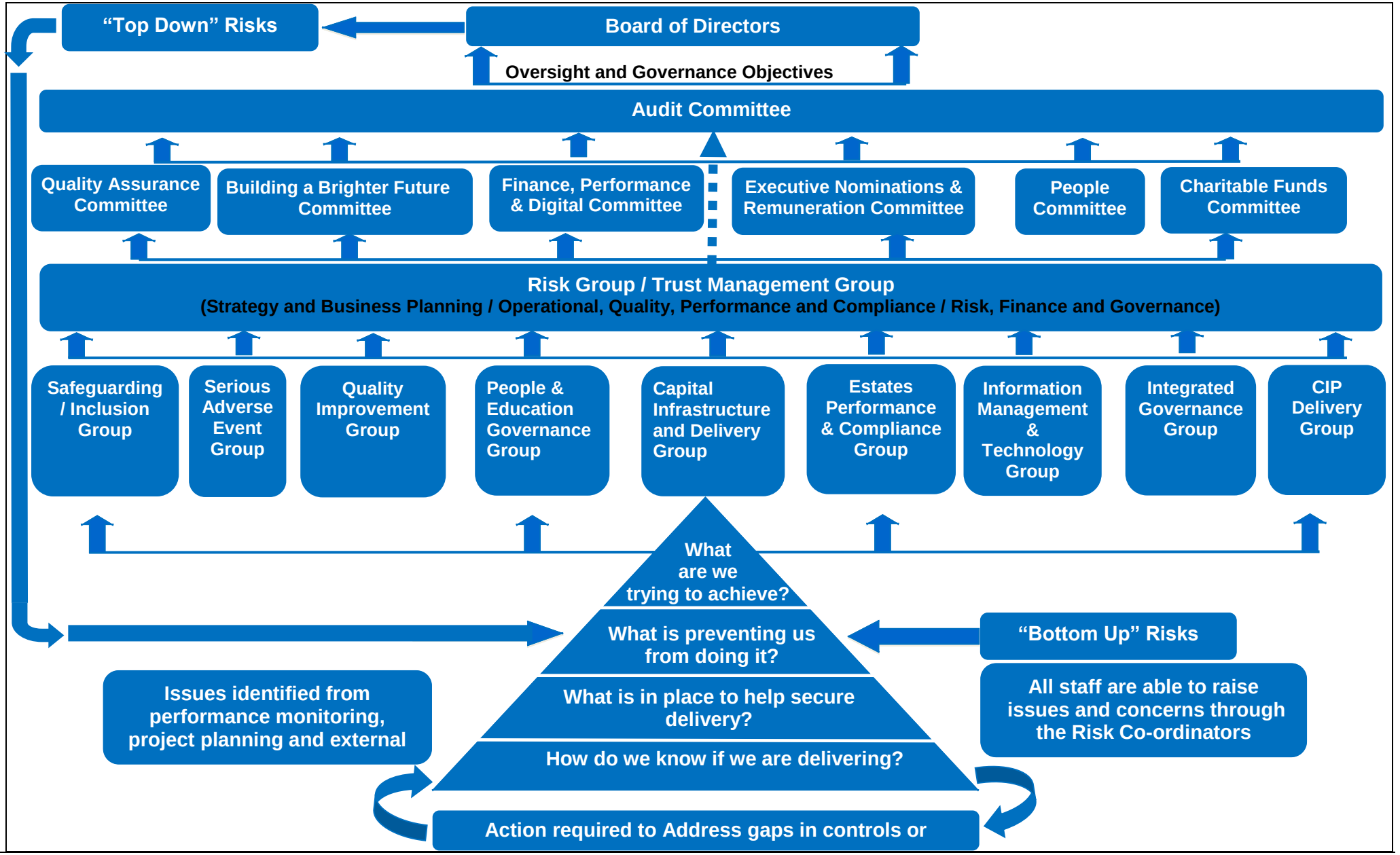
Risk Register – The Risk Register is where risks, once identified, are managed on a day to day basis.

Appendix 8 - Risk Assessment Tools *Continued*

Understanding the difference between a hazard and a risk – examples

A trailing PC cable lying across the floor is a **hazard**.
The **risk** is that someone trips over it.
If the cable is noticed and cleared by a member of staff, it was a **near miss**
If someone trips up and injures themselves before it is cleared away, this is an **incident**

Appendix 9 - Board Assurance Framework (BAF) Process



(E)quality Impact Assessment (EqIA) *(for use when writing policies)*

Policy Title (and number)	Risk Management Policy	**Version and Date**	V5.0 September 2022
Policy Author	Risk Officer		

An (e)quality impact assessment is a process designed to ensure that policies do not discriminate or disadvantage people whilst advancing equality. Consider the nature and extent of the impact, not the number of people affected.

Who may be affected by this document?

Patients/ Service Users ☐	Staff ☒	Other, please state… ☐

Could the policy treat people from protected groups less favorably than the general population?
PLEASE NOTE: Any 'Yes' answers may trigger a full EIA and must be referred to the equality leads below

Age	Yes ☐ No☒	Gender Reassignment	Yes ☐ No☒	Sexual Orientation	Yes ☐ No☒
Race	Yes ☐ No☒	Disability	Yes ☐ No☒	Religion/Belief (non)	Yes ☐ No☒
Gender	Yes ☐ No☒	Pregnancy/Maternity	Yes ☐ No☒	Marriage/ Civil Partnership	Yes ☐ No☒

Is it likely that the policy could affect particular 'Inclusion Health' groups less favorably than the general population? (substance misuse; teenage mums; carers[1]; travellers[2]; homeless[3]; convictions; social isolation[4]; refugees)	Yes ☐ No☒

Please provide details for each protected group where you have indicated 'Yes'.

VISION AND VALUES: Policies must aim to remove unintentional barriers and promote inclusion

Is inclusive language[5] used throughout?	Yes ☒ No☐ NA ☐
Are the services outlined in the policy fully accessible[6]?	Yes ☒ No☐ NA ☐
Does the policy encourage individualised and person-centered care?	Yes ☐ No☐ NA ☒
Could there be an adverse impact on an individual's independence or autonomy[7]?	Yes ☐ No☒ NA ☐

EXTERNAL FACTORS

Is the policy a result of national legislation which cannot be modified in any way?	Yes ☐ No☒

What is the reason for writing this policy? (Is it a result in a change of legislation/ national research?)

To set out Torbay and South Devon NHS Foundation Trust's expectations and procedures on Risk Management.

Who was consulted when drafting this policy?
Members of Risk Group and Audit Committee

Does this document require a service redesign or substantial amendments to an existing process? *PLEASE NOTE: 'Yes' may trigger a full EIA, please refer to the equality leads below*	Yes ☐ No☒

ACTION PLAN: Please list all actions identified to address any impacts

Action	Person responsible	Completion date

AUTHORISATION:
By signing below, I confirm that the named person responsible above is aware of the actions assigned to them

Name of person completing the form	Risk Officer	**Signature**	AA
Validated by (line manager)	Corporate Governance Manager	**Signature**	SF

Please contact the Equalities team for guidance:
For South Devon & Torbay CCG, please call 01803 652476
For Torbay and South Devon NHS Trusts, please call 01803 656676 or email pfd.sdhct@nhs.net
This form should be published with the policy and a signed copy sent to your relevant organisation.

[1] Consider any additional needs of carers/ parents/ advocates etc, in addition to the service user
[2] Travelers may not be registered with a GP - consider how they may access/ be aware of services available to them
[3] Consider any provisions for those with no fixed abode, particularly relating to impact on discharge
[4] Consider how someone will be aware of (or access) a service if socially or geographically isolated
[5] Language must be relevant and appropriate, for example referring to partners, not husbands or wives
[6] Consider both physical access to services and how information/ communication in available in an accessible format
[7] Example: a telephone-based service may discriminate against people who are d/Deaf. Whilst someone may be able to act on their behalf, this does not promote independence or autonomy