Policy Document

Reference: RM01

Risk Management

Version:	**11**
Date Ratified:	**February 2021 by the Trust Board**
To Be Reviewed Before:	**February 2024**
Policy Author:	**Associate Director of Corporate Governance**
Executive Lead:	**Chief Executive**

Version Control Schedule

Version	Issue Date	Comments
1	March 2004	
2	October 2005	
3	September 2008	Updated to complement risk management initiatives within the Trust and to promote integration of risk.
4	November 2009	Updated to reflect changes in the reporting of the Assurance Framework and to reflect the governance structure within the Trust.
5	March 2011	Revised to align with new Board and Sub-Committee structure and SLM and Directorate arrangements.
6	October 2012	Updated policy to reflect changes in NHSLA standards and G01
7	December 2014	Review of process and outcome following internal audit review undertaken in 2014.
8	April 2015	Update to flowchart to use risk assessment proforma
9	November 2015	Update to the policy following recommendations identified from the risk management review
10	March 2017	Complete rewrite of the policy.
11	February 2021	3 yearly review. Policy amended to clarify roles and responsibilities and to incorporate Risk Appetite and Tolerance.

Statement on Trust Policies

The latest version of 'Statement on Trust Policies' applies to this policy and can be accessed here

Contents	Page

1. INTRODUCTION

What is 'risk'?
Risk is defined as an uncertain event or set of events, which should it occur, will have an effect upon (i.e. threaten) the achievement of objectives. Risk consists of a combination of the likelihood of the 'threat' happening and the impact of that threat happening.

What is 'Risk Management'?
Risk Management is the term used to describe the activities required to identify, understand and control exposure to uncertain events which may threaten the achievement of objectives.

Why do we do it?
Risk Management is a key component of general management practice as it aims to ensure that:

- Achievement of objectives is more likely
- Adverse (damaging) events are less likely
- Costly re-work and 'fire-fighting' is reduced
- Capital and resources are utilised more efficiently and effectively
- Performance is improved (including quality, finance for example)
- Decision-making is much better informed
- Positive outcomes for stakeholders are increased
- Our reputation is protected and enhanced

2. POLICY STATEMENT

The Trust is committed to ensuring that the highest standards of service are provided and recognises the fundamental role that risk management has in enabling this.

3. SCOPE

This policy identifies the lines of accountability for management of risk throughout the organisation and is applicable to all staff. In addition, this policy should be read alongside the Trust's Accountability Framework, in terms of the accountabilities associated with risk management.

4. DEFINITIONS

There are a number of terms used when describing risk management. However, the following table sets out the key terms which are featured within this policy and are therefore applicable to our risk management process.

Key Term	Definition
Risk Management	Risk Management is the term used to describe the activities required to identify, understand and control exposure to uncertain events which may threaten the achievement of objectives.
Risk	Risk is described as the combination of: • Cause (If…(something happens)) • Event (Then…(this may occur)) • Effect (Resulting in….(the impact))
Control	Actions which are in place to assist in the mitigation of the risk and the achievement of an objective, by reducing the likelihood or impact. For example, a policy or training programme.

Key Term	Definition
Assurance	Assurance is the evidence which describes how effective the controls are. For example, a report summary of incidents may tell us that we have very few patient falls, therefore suggesting that our controls to prevent falls are working effectively.
Risk Appetite	Sets out the levels and types of risk we are prepared to accept, tolerate, or be exposed to at any point in time, in pursuance of our objectives.
Risk Tolerance	The amount (risk level/score) we are prepared to take to achieve our strategic and operational goals.
Risk Register	A record of all identified risks relating to a set of objectives, including their history, status and risk score. The purpose of a risk register is to evidence and drive risk management activities and it is used as a source or means of risk reporting.
Project / Programme Risks	Project and programme risks are managed in the same way as other risks in the Trust but there are slight differences in the approach. Risk registers or logs will still be maintained for risks to programmes or projects but these are held as part of the project documentation held within the Programme Management Office. However, this project documentation may be referred to as a source of control and/or assurance, within related risks held on the Risk Register.
Strategic Risks	These are reported via the Board Assurance Framework. These include strategic risks which concern the Trust's main purpose and could impact the achievement of key objectives (e.g. data loss, leadership capability as well as big external events/perils and how the Trust can become more resilient e.g. economic downturn, terrorist attack, extreme weather or cyber-attacks).
Cross-cutting Operational Risks	These are reported via the Corporate Risk Register. These include big cross-cutting internal risks over which the Trust has full or partial control and/or that can be managed through internal controls e.g. fraud, health and safety, capacity and capability and data security.
Directorate / Divisional Risks	These are reported via the Divisional Risk Register. These include local/delivery risks that could impact the achievement of directorate business plans.
Three Lines Model	This approach highlights the levels of assurance that has been obtained both internally and externally and is used when articulating the assurances within the Board Assurance Framework.

5. ROLES AND RESPONSIBILITIES

All staff have a responsibility for risk management and compliance with this policy, including awareness of the risks within their working environment, how their role impacts on those risks and taking reasonable steps to reduce the risk if possible.

The following provides an overview of those with specific responsibilities to ensure the implementation of this policy.

The **Chief Executive** has overall responsibility for risk management. As Accounting Officer, the Chief Executive has responsibility for maintaining a sound system of internal control that supports the achievement of the Trust's policies, aims and objectives, whilst safeguarding public funds and departmental assets. Responsibilities in respect of risk management include:

- reviewing the strategic objectives of the organisation with the Board
- ensuring that the Trust has an effective structure and system in place to manage risks within the organisation
- ensuring that employees and the public are properly protected against exposure to risks arising out of or as a result of the Trust's activities
- signing the Annual Governance Statement in the annual report and accounts

Executive Directors are responsible for:

- ensuring delivery of the strategic objectives
- identification, control, monitoring and reporting of the risks which may threaten achievement of strategic objectives
- maintaining accurate and up to date risk registers, relevant to their objectives and report through the Board Assurance Framework
- providing oversight of operational risks which have been escalated to the Corporate Risk Register

The **Corporate Governance Department** is responsible for:

- development and review of the Risk Management Policy
- provision of education, support and expertise in relation to Risk Management
- provision of training on the Risk Management Policy
- monitoring and reporting compliance with the Risk Management Policy
- facilitating the reporting of appropriate risks to the Board, Committees and Executive Groups
- facilitating the provision of a Board Assurance Framework to the Board and Committees

The **Quality, Safety & Compliance Department** is responsible for:

- facilitating the reporting of appropriate risks to specialist corporate groups

Divisional Chairs, Associate Directors, Associate Chief Nurses (or equivalent for non-clinical divisions) and Clinical Governance Leads (medical) are jointly responsible for:

- leading and overseeing implementation of the Risk Management Policy at Divisional level which includes effective identification and ongoing review of, controls, monitoring and reporting of the risks which may threaten achievement of Divisional objectives
- facilitating the reporting and where necessary, escalation of appropriate risks to the Divisional Board and the Executive Groups

Clinical Directors and Directorate Managers (or equivalent for non-clinical divisions) are responsible for:

- leading and overseeing implementation of the Risk Management Policy at Directorate level which includes the effective identification and ongoing review of, control, monitoring and reporting of the risks which may threaten achievement of Directorate objectives
- facilitating the reporting and where necessary, escalation of appropriate risks to the Divisional Board from the Directorate
- maintaining accurate and up to date risk registers, relevant to their Directorate / service objectives

Divisional Governance & Quality Managers (or equivalent for non-clinical divisions) are responsible for:

- facilitating implementation of the Risk Management Policy at Divisional level which includes the effective identification and ongoing review of, control, monitoring and reporting of the risks which may threaten achievement of Divisional objectives, in accordance with the procedure set out within this policy
- monitoring and reporting compliance with the Risk Management Policy at a Divisional level, as identified by the Corporate Governance Department

'Risk Owners' including all Departmental / Ward / Service Managers are responsible for:

- identification and ongoing review of, control, monitoring and reporting of the risks which may threaten achievement of Directorate objectives, in accordance with the procedure set out within this policy
- maintaining accurate and up to date risk registers, relevant to Directorate objectives

Chairs of Specialist Corporate Groups (i.e. Safe Medications Group, Falls Steering Group etc.) are responsible for:

- identification, management and oversight of risks relevant to their specialist subject, ensuring appropriate action is taken
- reporting, where appropriate to the Executive Group

Organisational Responsibilities

Assurance Mechanism	Responsibilities
Trust Board	The Trust Board is ultimately accountable for ensuring that the Trust has effective governance and risk management processes in place. The Board identifies the strategic risks that it considers are the key risks likely to impact on the delivery of the Trust's objectives and overall strategy. Board Committees have responsibility for monitoring the effectiveness of the controls and assurances in place to manage these risks.
Quality Governance Committee	The Committee shall consider the Trust's strategic risks of a clinical nature, particularly in relation to the strategic objectives of providing safe, effective, caring and responsive services and achieving NHS constitutional patient access standards. The relevant Executive Director responsible for managing each respective strategic risk shall be accountable at the Committee for responding to challenge and scrutiny of the Committee.
Performance & Finance Committee	The Committee shall consider the Trust's strategic risks of a non-clinical nature particularly in relation to the strategic objective of ensure efficient use of resources. The relevant Executive Director responsible for each strategic risk shall be accountable at the Committee for responding to challenge and scrutiny of the Committee.
Transformation & People Committee	The Committee shall consider the Trust's strategic risks of a non-clinical nature particularly in relation to the strategic objectives of achieving excellence in employment, education, development and research and lead strategic change within Staffordshire and beyond. The relevant Executive Director responsible for each strategic risk shall be accountable at the Committee for responding to challenge and scrutiny of the Committee.
Audit Committee	The Committee's primary role is to provide the Trust Board with a means of independent and objective review of financial and corporate governance, assurance processes and risk management across the whole of the Trust's activities.
Executive Quality & Safety Oversight Group	The Group will provide assurance to the Quality Governance Committee on the delivery of the Risk Management Strategy and operational management of risks. It is responsible for escalating to the Quality Governance Committee risks which link to key strategic risks on the Board Assurance Framework. The Group will consider key risks in relation to: • Patient Safety • Effectiveness • Service User and Carer Experience • Statutory Regulation and Requirements • National Guidance and Best Practice

Assurance Mechanism	Responsibilities
Executive Health & Safety Group	The Group will provide assurance to the Quality Governance Committee on the delivery of the Risk Management Strategy and operational management of risks. It is responsible for escalating to the Quality Governance Committee risks which link to key strategic risks on the Board Assurance Framework. The Group will consider key risks in relation to: • Statutory Regulation and Requirements
Executive Infrastructure Group	The Group will provide assurance to the Performance and Finance Committee on the delivery of the Risk Management Strategy and operational management of risks. It is responsible for escalating to the Performance and Finance Committee risks which link to key strategic risks on the Board Assurance Framework. The Group will consider key risks in relation to: • Estates infrastructure • Control of IM&T Assets • Business continuity • Value for money and sustainability • Contracting • Standing Financial Instructions (SFI's) and financial control • Fraud and negligent conduct
Executive Business Intelligence Group	The Group will provide assurance to the Performance and Finance Committee on the delivery of the Risk Management Strategy and operational management of risks. It is responsible for escalating to the Performance and Finance Committee risks which link to key strategic risks on the Board Assurance Framework. The Group will consider key risks in relation to: • Data quality
Executive Data Security & Protection Group	The Group will provide assurance to the Performance and Finance Committee on the delivery of the Risk Management Strategy and operational management of risks. It is responsible for escalating to the Performance and Finance Committee risks which link to key strategic risks on the Board Assurance Framework. The Group will consider key risks in relation to: • IM&T security • Data security
Executive Research & Innovation Group	The Group will provide assurance to the Transformation and People Committee on the delivery of the Risk Management Strategy and operational management of risks. It is responsible for escalating to the Transformation and People Committee risks which link to key strategic risks on the Board Assurance Framework. The Group will consider key risks in relation to: • Research • Innovation
Executive Workforce Assurance Group	The Group will provide assurance to the Transformation and People Committee on the delivery of the Risk Management Strategy and operational management of risks. It is responsible for escalating to the Transformation and People Committee risks which link to key strategic risks on the Board Assurance Framework. The Group will consider key risks in relation to: • Staff recruitment • Employment practice • Staff retention

Assurance Mechanism	Responsibilities
Executive Strategy & Transformation Group	The Group will provide assurance to the Transformation and People Committee on the delivery of the Risk Management Strategy and operational management of risks. It is responsible for escalating to the Transformation and People Committee risks which link to key strategic risks on the Board Assurance Framework. The Group will consider key risks in relation to: • Partnerships
Divisional Boards	Divisional Boards are responsible for reviewing and controlling the risks within their Divisions as part of the development of divisional and directorate risk registers and escalating risks to the relevant Executive Groups. Divisions are able to escalate risks to the Corporate Risk Register for additional oversight by an Executive Director.

6. EDUCATION/TRAINING AND PLAN OF IMPLEMENTATION

Type of Training	How to Access Training	Who Requires Training
Risk Assessment Template completion	• Step by Step Instructions included on the Risk Assessment Template (appendix 4) • Additional support is available from the Corporate Governance Department	Any staff member identifying a risk for inclusion on the Risk Register.
Risk Management Policy Training	1-1 Training available via the Corporate Governance Department Face to face sessions	• Associate Chief Nurses • Divisional Chairs • Clinical Directors • Clinical Governance Leads (medical) • Divisional Governance and Quality Managers • Matrons • Directorate Managers • Central Functions and Estates, Facilities & PFI risk register leads as determined by the Division
Datix Risk Register completion	Quality, Safety and Compliance Department	As listed above, or any staff member with delegated authority from the above to input risks directly onto the risk register.

Training records are held centrally within the Corporate Governance Department.

7. MONITORING AND REVIEW ARRANGEMENTS

7.1 Monitoring Arrangements

In addition to individual roles and responsibilities for monitoring risks:

Committee Assurance

- The Audit Committee is responsible for oversight of the Risk Management Policy and will receive quarterly reports in the form of the Board Assurance Framework.
- In addition, the Performance and Finance Committee. Quality Governance Committee and Transformation and People Committee, will consider quarterly Board Assurance Framework Reports

Audit

- The Corporate Governance Department will undertake audits of compliance against this policy, including data quality elements, which will be reported to Divisional Performance Reviews
- An annual audit of compliance will take place as part of the Internal Audit Programme and will be reported to the Audit Committee.

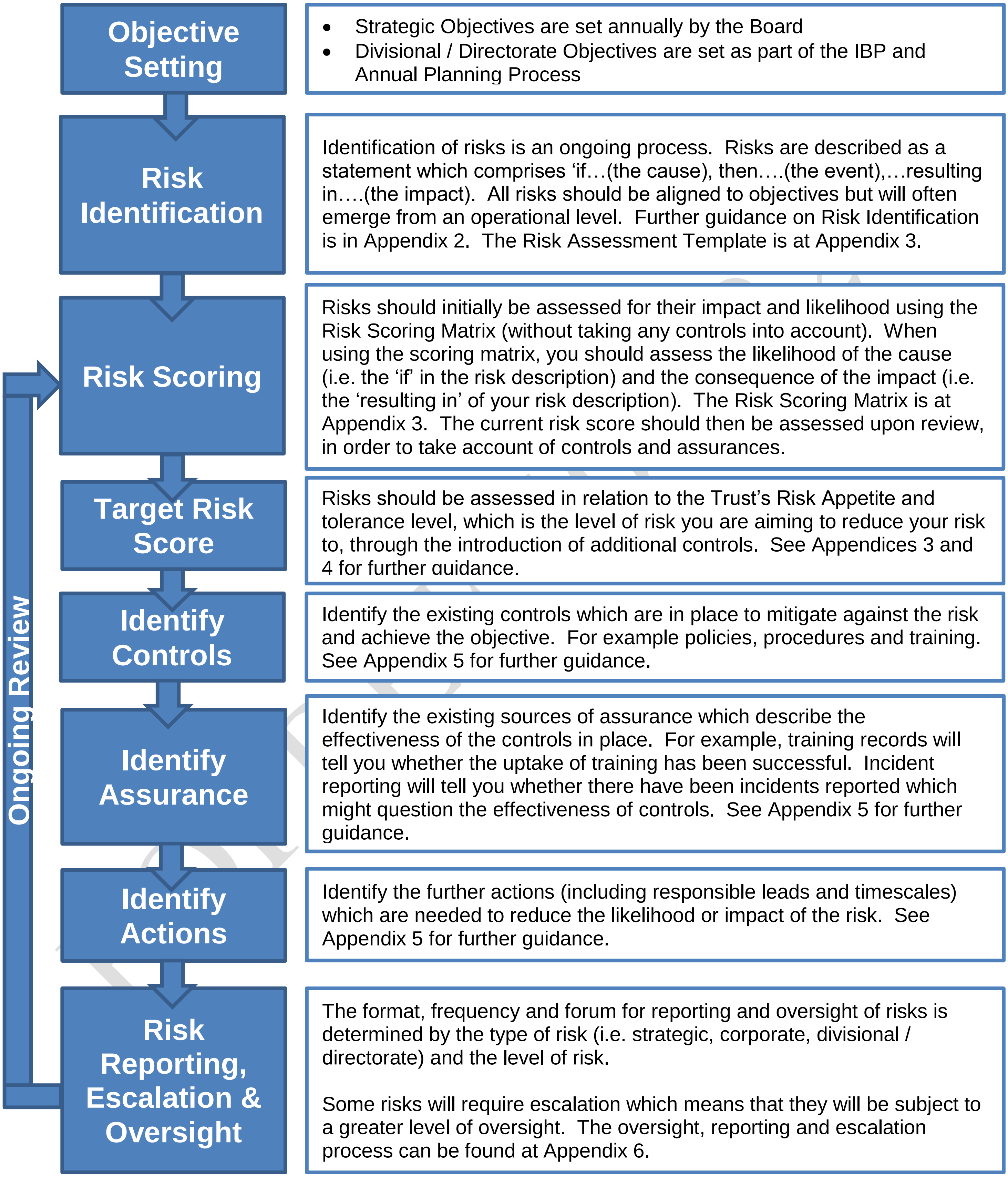
7.2 Review

This policy will be reviewed by the Corporate Governance Department at least every three years post ratification, unless it is deemed necessary to do so sooner.

8. REFERENCES

AmberWing Risk Management Training

Appendix 1: Risk Management Process



Objective Setting

- Strategic Objectives are set annually by the Board
- Divisional / Directorate Objectives are set as part of the IBP and Annual Planning Process

Risk Identification

Identification of risks is an ongoing process. Risks are described as a statement which comprises 'if…(the cause), then….(the event),…resulting in….(the impact). All risks should be aligned to objectives but will often emerge from an operational level. Further guidance on Risk Identification is in Appendix 2. The Risk Assessment Template is at Appendix 3.

Risk Scoring

Risks should initially be assessed for their impact and likelihood using the Risk Scoring Matrix (without taking any controls into account). When using the scoring matrix, you should assess the likelihood of the cause (i.e. the 'if' in the risk description) and the consequence of the impact (i.e. the 'resulting in' of your risk description). The Risk Scoring Matrix is at Appendix 3. The current risk score should then be assessed upon review, in order to take account of controls and assurances.

Target Risk Score

Risks should be assessed in relation to the Trust's Risk Appetite and tolerance level, which is the level of risk you are aiming to reduce your risk to, through the introduction of additional controls. See Appendices 3 and 4 for further guidance.

Identify Controls

Identify the existing controls which are in place to mitigate against the risk and achieve the objective. For example policies, procedures and training. See Appendix 5 for further guidance.

Identify Assurance

Identify the existing sources of assurance which describe the effectiveness of the controls in place. For example, training records will tell you whether the uptake of training has been successful. Incident reporting will tell you whether there have been incidents reported which might question the effectiveness of controls. See Appendix 5 for further guidance.

Identify Actions

Identify the further actions (including responsible leads and timescales) which are needed to reduce the likelihood or impact of the risk. See Appendix 5 for further guidance.

Risk Reporting, Escalation & Oversight

The format, frequency and forum for reporting and oversight of risks is determined by the type of risk (i.e. strategic, corporate, divisional / directorate) and the level of risk.

Some risks will require escalation which means that they will be subject to a greater level of oversight. The oversight, reporting and escalation process can be found at Appendix 6.

Appendix 2: Risk Identification

1. What is a risk and what is not a risk?

A risk is an **uncertain** event or set of events which, should it occur, will have an effect upon the achievement of objectives. Therefore:

Risk **is** 'uncertainty':	Risk **is not** 'certainty' which involves:
✓ an event that **might** happen	✗ an **incident**, which is an event which **has** happened an should be managed through RM07 Incident Reporting Policy. ✗ an **issue** which **will** or **is** happening.

2. How is a risk described?

A risk should be described with three components, articulating the **'future risk'**:

If…..	**Then…..**	**Resulting in…..**
This part of the description should capture the **cause**. *There should only be **one** cause.*	This part of the description should focus on the **event** which will occur if the cause happens. *There should only be **one** event.*	This part of the description should describe the **effect** of the event. For example, this may be: • Impact upon strategic objectives • financial loss • reputational damage • quality / patient is compromised • operational disruption • legal / regulatory action
Example		
If there is a fire	**then** patients may not be evacuated safely	**resulting in** legal / regulatory action, compromised patient safety, service disruption and financial loss.

3. How risks should not be described

Failure of the Objective	Objective: To expand into more geographical territories Risk: Failure to expand into new territories
Questioning the Objective	Expanding into more geographical territories could place us in competition with other providers in those areas.
Composite Risks (i.e. using 'or')	Appropriate facilities may not be available **or** there may be resistance **or** we may not be able to recruit sufficient staff.
One-word risks	'Fraud', 'Fire', 'Reputation'
Statement of fact	There is a risk that projects may fail
Incident	Due to the computer system crashing
Issue	Because we don't have enough staff…. / when the new legislation is introduced…
Whinge	We've been told that a new computer system is being introduced, but nothing has been done to provide training to the staff
Essay	When the computer service centre was moved three years ago, various changes were made to working practices. Break times were extended, section leaders were appointed, cross training was provided as a back-up for absence. Now more changes are underway, so we are likely to have short term additional staffing costs. We are also spending more than planned on support for the new IT system, which may necessitate us to cut back in other areas, leading to an adverse impact on staff morale, lower service levels and damage to our reputation.

Appendix 3: Risk Assessment Template

Risk assessments should be entered onto the Datix Risk Management Module. This includes identifying up to date controls and assurances, and identifying future actions.

A. RISK DESCRIPTION

Remember: risk is uncertain. There should only be one cause and one event but the risk may have multiple effects.

Cause: **(the trigger leading to the event)**	*If…..*
Event: **(which might happen i.e. what are you worried about)**	*Then…..*
Effect*:	*Resulting in…...*

*when describing the 'effect', consider the following:

- Impact on the safety of patients, staff or public (physical / psychological harm)
- Impact on Quality / Complaints / Audit
- Impact on Human Resources / Organisational Development / Staffing / Competence
- Impact on Statutory Duty / Inspections
- Impact on Adverse Publicity / Reputation
- Impact on Business Objectives / Projects
- Impact on Finance including Claims
- Impact on Service / Business Interruption / Environment

B. LIKELIHOOD AND IMPACT ASSESSMENT

Step 1: To assess the likelihood of your risk, you must focus on the 'if…' section of your risk description.

Likelihood Descriptions		Likelihood Score	✓
Rare	This will probably never happen / recur.	**1**	
Unlikely	Do not expect it to happen / recur but it is possible it may do so.	**2**	
Possible	Might happen or recur occasionally.	**3**	
Likely	Will probably happen / recur but it is not a persisting issue.	**4**	
Almost Certain	Will undoubtedly happen / recur, possibly frequently.	**5**	

Step 2: To assess the impact of your risk, you must focus on the 'resulting in…' section of your risk description, using the Impact Score Matrix below

It is possible that your risk may have more than one impact, for example financial loss, service disruption and patient safety. You should use this table to impact score each of these categories separately and then select the one that has the **highest impact.**

Impact Domains	Risk Management Matrix - Impact Score and Examples of Descriptions				
	1	2	3	4	5
	Negligible	Minor	Moderate	Major	Catastrophic
Impact on the safety of patients, staff or public (physical / psychological harm)	Minimal injury requiring no/minimal intervention or treatment. No time off work	Minor injury or illness, requiring minor intervention Requiring time off work for >3 days Increase in length of hospital stay by 1-3 days	Moderate injury requiring professional intervention Requiring time off work for 4-14 days Increase in length of hospital stay by 4-15 days RIDDOR/agency reportable incident An event which impacts on a small number of patients	Major injury leading to long-term incapacity/disability Requiring time off work for >14 days Increase in length of hospital stay by >15 days Mismanagement of patient care with long-term effects	Incident leading to death Multiple permanent injuries or irreversible health effects An event which impacts on a large number of patients
Quality / Equality / Complaints / Audit	Peripheral element of treatment or service suboptimal Informal complaint/inquiry	Overall treatment or service suboptimal Formal complaint (stage 1) Local resolution Single failure to meet internal standards Minor implications for patient safety if unresolved Reduced performance rating if unresolved	Treatment or service has significantly reduced effectiveness Formal complaint (stage 2) complaint Local resolution (with potential to go to independent review) Repeated failure to meet internal standards Major patient safety implications if findings are not acted on	Non-compliance with national standards with significant risk to patients if unresolved Multiple complaints/ independent review Low performance rating Critical report	Totally unacceptable level or quality of treatment/service Gross failure of patient safety if findings not acted on Inquest/ombudsman inquiry Gross failure to meet national standards
Human Resources / Organisational Development / Staffing / Competence	Short-term low staffing level that temporarily reduces service quality (< 1 day)	Low staffing level that reduces the service quality	Late delivery of key objective/ service due to lack of staff Unsafe staffing level or competence (>1 day) Low staff morale Poor staff attendance for mandatory/key training	Uncertain delivery of key objective/service due to lack of staff Unsafe staffing level or competence (>5 days) Loss of key staff Very low staff morale No staff attending mandatory/ key training	Non-delivery of key objective/service due to lack of staff Ongoing unsafe staffing levels or competence Loss of several key staff No staff attending mandatory training /key training on an ongoing basis
Statutory Duty / Inspections / PFI Contracting	No or minimal impact or breech of guidance/ statutory duty	Breech of statutory legislation Reduced performance rating if unresolved	Single breech in statutory duty Challenging external recommendations/ improvement notice	Enforcement action Multiple breeches in statutory duty Improvement notices Low performance rating Critical report	Multiple breeches in statutory duty Prosecution Complete systems change required Zero performance rating Severely critical report
Adverse Publicity / Reputation	Rumours Potential for public concern	Local media coverage – short-term reduction in public confidence Elements of public expectation not being met	Local media coverage – long-term reduction in public confidence	National media coverage with <3 days service well below reasonable public expectation	National media coverage with >3 days service well below reasonable public expectation. MP concerned (questions in the House) Total loss of public confidence
Business Objectives / Projects	Insignificant cost increase/ schedule slippage	<5 per cent over project budget Schedule slippage	5–10 per cent over project budget Schedule slippage	Non-compliance with national 10–25 per cent over project budget Schedule slippage Key objectives not met	Incident leading >25 per cent over project budget Schedule slippage Key objectives not met
Finance including Claims	Small loss Risk of claim remote	Loss of 0.1–0.25 per cent of budget Claim less than £10,000	Loss of 0.25–0.5 per cent of budget Claim(s) between £10,000 and £100,000	Uncertain delivery of key objective/Loss of 0.5–1.0 per cent of budget Claim(s) between £100,000 and £1 million Purchasers failing to pay on time	Non-delivery of key objective/ Loss of >1 per cent of budget Failure to meet specification/ slippage Loss of contract / payment by results Claim(s) >£1 million
Service / Business Interruption / Environmental Impact	Loss/interruption of >1 hour Minimal or no impact on the environment No impact on other services	Loss/interruption of >8 hours Minor impact on environment Impact on other services within the Division	Loss/interruption of >1 day Moderate impact on environment Impact on services within other Divisions	Loss/interruption of >1 week Major impact on environment Impact on all Divisions	Permanent loss of service or facility Catastrophic impact on environment Impact on services external to the organisation
Information Security / Data Protection	Potential breach of confidentiality with less than 5 people affected Encrypted files	Serious potential breach of confidentiality with 6 – 20 people affected Unencrypted clinical records lost	Serious breach of confidentiality with 21 – 100 people affected Inadequately protected PCs, laptops and remote device	Serious breach of confidentiality with 101 – 1000 people affected Particularly sensitive details (i.e. sexual health)	Serious breach of confidentiality with over 1001 people affected Potential for ID theft

Step 3: To identify your <u>initial</u> risk score, you must take the result of your likelihood assessment and the result of your impact assessment and use the multiplication table below. This score is to be calculated before the introduction of any controls, and remains unchanged once calculated.

For example, if the likelihood score is '3' and the impact score is '4', when multiplied together, these you will give you a risk score of '12'.

		Impact Score				
		1	2	3	4	5
Likelihood Score	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

The numerical risk score will fall within a range as shown below, this will determine whether the risk is either, 'low, 'moderate', 'high' or 'extreme'.

Risk Score	
1 – 3	Low
4 – 6	Moderate
8 – 12	High
15 – 25	Extreme

<u>Initial</u> Risk Score (Likelihood x Impact)					
Likelihood:		Impact:		Score:	

C. EXISTING CONTROLS AND ASSURANCES

Step 4: Consider what existing controls and assurances are in place. Guidance on describing controls and assurances can be found at appendix 5.

Existing Controls (Controls should make a risk less likely to happen and/or reduce the impact if it does happen. Controls can also be a contingency to be enacted should the risk happen)	Existing Assurances (Assurances provide us with information or evidence about the effectiveness of our controls. An assurance description needs to state what the <u>source</u> of assurance is and more importantly <u>what the assurance is telling you</u> and if possible, the <u>time period</u> to which it relates)

Step 5: Identify your current risk score, taking into account existing controls and assurances and whether the controls have reduced the likelihood or impact of the risk.

Current Risk Score (Likelihood x Impact)					
Likelihood:		Impact:		Score:	

Step 6: To identify the target risk score, you must first identify the Trust's Risk Appetite, using the Risk Appetite Matrix (overleaf).

Consider the different sub-categories of risk and choose the most appropriate for your risk.

Depending on the tolerance assigned to that sub-category, consider the target likelihood and impact which would achieve a score within that range.

For example, if the risk score tolerance is between 4 and 6, the likelihood of the risk could be reduced to 2 and the impact to 3, achieving a score of 6. NB. It may not always be possible to reduce the impact of your risk therefore you should consider what actions could be taken to reduce the likelihood, before deciding on your target likelihood score.

Target Risk Score (Likelihood x Impact)					
Likelihood:		Impact:		Score:	

D. FURTHER ACTIONS

Step 7: If your assurance demonstrates that the controls are not working as effectively as planned, or you have not reached the target risk score, you need to identify future actions which could be put in place, in order to reduce the likelihood and/or impact and reduce the risk score to the acceptable range.

Action	Person Responsible	Due Date

E. REVIEW

Step 8: Review your risk assessment, in order to close any actions, articulate new controls and up to date assurances. Recalculate the risk score, taking these into account. If the assurance is negative, or if the risk score has not yet been reduced to a 'tolerable' level, in line with the Trust's Risk Appetite, identify further actions. See Appendix 7 for further details.

Risk Appetite Matrix

If the organisation's collective appetite for risk is unknown, it may lead to erratic or inopportune risk taking, exposing the organisation to a risk it cannot tolerate.

Sub Category of Risk		Risk Appetite	Risk Score Tolerance
Impact on Quality	Patient Safety (e.g. patient harm, infection control, pressure sores, learning lessons)	Cautious	Mod 4 – Mod 6
	Effectiveness (e.g. outcomes, delays, cancellations or operational targets and performance)	Open	High 8 – High 12
	Service User and Carer Experience and the ability to manage quality (e.g. complaints, audit, surveys, clinical governance and internal systems)	Open	High 8 – High 12
Impact on Regulation & Compliance	Statutory Regulation and Requirements (e.g. Information Commissioner, Care Quality Commission, Health and Safety Executive, Professional Regulatory Bodies such as General Medical Council, Nursing & Midwifery Council, external certifications such as JAG and ISO).	Cautious	Mod 4 – Mod 6
	National Guidance and Best Practice (e.g. National Institute for Health and Care Excellence, GIRFT)	Open	High 8 – High 12
Impact on Reputation	Day to day activity (e.g. standards of conduct, ethics and professionalism and delivery of services)	Cautious	Mod 4 – Mod 6
	Risk as a result of protecting and improving the safety of patients	Seek	Ext 15 – Ext 25
Impact on Workforce	Staff recruitment (e.g. compliance with regulations such as visa requirements, Equal Opportunities and Diversity, that ensure staff are recruited fairly and competent to deliver services)	Cautious	Mod 4 – Mod 6
	Employment practice	Cautious	Mod 4 – Mod 6
	Staff retention (e.g. attractiveness of Trust as an employer of choice)	Open	High 8 – High 12
Impact on Infrastructure	Estates Infrastructure	Cautious	Mod 4 – Mod 6
	Security (e.g. access and permissions to systems and networks)	Cautious	Mod 4 – Mod 6
	Control of Assets (e.g. purchase, movement and disposal of ICT equipment)	Cautious	Mod 4 – Mod 6
	Business continuity (e.g. cyber-attack, maintenance of networks, alternative solutions)	Cautious	Mod 4 – Mod 6
	Data (e.g. integrity, availability, confidentiality and security, unintended release)	Cautious	Mod 4 – Mod 6
Impact on Finance & Efficiency	Value for money and sustainability (including cost saving)	Cautious	Mod 4 – Mod 6
	Standing Financial Instructions (SFI's) and financial control	Cautious	Mod 4 – Mod 6
	Fraud and negligent conduct	Minimal	Low 1 – Low 3
	Contracting	Seek	Ext 15 – Ext 25
Impact on Partnerships / Collaboration	Partnerships	Open	High 8 – High 12
Impact on Innovation	Innovation (e.g. new ways of working, new products, new and realigned services, new models of staffing and realignment of services, international recruitment, new ICT systems and improvements)	Seek	Ext 15 – Ext 25
	Financial Innovation (e.g. new ways of working, new products, new and realigned services)	Open	High 8 – High 12

Appendix 4: Risk Appetite Statement

1. INTRODUCTION

The following Risk Appetite Statement makes clear the Trust Board's expectations in relation to the category of risks they expect management to identify and the level of such risk that is acceptable. If the organisation's collective appetite for risk is unknown, it may lead to erratic or inopportune risk taking, exposing the organisation to a risk it cannot tolerate.

The statement is based on the premise that the lower the risk appetite, the less the Board is willing to accept in terms of risk and consequently the higher levels of controls that must be put into place to manage the risk.

The higher the appetite for risk, the more the Board is willing to accept in terms of risk and consequently the Board will accept business as usual activity for established systems of internal control and will not necessarily seek to strengthen those controls. Risk appetite will therefore be set at one of the following levels:

LEVELS OF RISK APPETITE	
Avoid **Risk Score Tolerance 0**	We are not prepared to accept any risk.
Minimal **Risk Score Tolerance 1 – 3**	We accept that risks will not be able to be eliminated, therefore these should be reduced to the lowest levels, with ultra-safe delivery options, recognising that these may have little or no potential for reward/return.
Cautious **Risk Score Tolerance 4 – 6**	We are willing to accept some low levels of risk, while maintaining overall performance of safe delivery options, recognising that these may have restricted potential for reward/return.
Open **Risk Score Tolerance 8 – 12**	We are willing to accept all potential delivery options, recognising that these may provide an acceptable level of reward.
Seek **Risk Score Tolerance 15 - 25**	We are eager to be innovative, choosing options with the potential to offer higher business rewards.

2. CATEGORIES OF RISK

Risks at an operational level will be considered under the following categories:

- Quality – Safety, Effectiveness & Experience
- Regulation and Compliance
- Reputation
- Workforce
- Infrastructure (Estates & IM&T)
- Finance and Efficiency
- Partnerships/Collaboration
- Innovation

3. APPETITE FOR RISKS THAT MAY IMPACT UPON QUALITY

OUR STATEMENT ON QUALITY

Patient safety is our number one priority. While we aim to find a balance in our approach to achieve the best value for money in order to achieve financial sustainability for the future, we will not hesitate to spend money and apply resources to situations that present unacceptable risks to the safety of our patients.

We will protect patients from harm, giving them treatment that provides the best possible outcomes and make sure that they have a good experience of the treatment and care we provide. We have a moderate appetite to risks that may have an impact on any aspect of safety.

We will collect useful information on quality and share this information quickly with the people who are best placed to improve care. We will empower our staff to get things done and will be constantly vigilant in keeping quality standards high. We will take every opportunity to compare ourselves with other providers so that we continue to strive for excellence.

Sub Category of Risk	Risk Appetite	Risk Score Tolerance
Patient Safety (e.g. patient harm, infection control, pressure sores, learning lessons)	**Cautious**	**Mod 4 - Mod 6**
Effectiveness (e.g. outcomes, delays, cancellations or operational targets and performance)	**Open**	**High 8 – High 12**
Service User and Carer Experience and the ability to manage quality (e.g. complaints, audit, surveys, clinical governance and internal systems)	**Open**	**High 8 – High 12**

4. APPETITE FOR RISKS THAT MAY IMPACT UPON REGULATION AND COMPLIANCE

OUR STATEMENT ON REGULATION AND COMPLIANCE

We provide services within a highly regulated environment that must meet high levels of compliance expectations from a large number of regulatory sources. We will endeavour to meet those expectations within a framework of prudent controls, balancing the prospect of risk elimination against pragmatic operational imperatives.

Non-compliance with legal and statutory requirements undermines public and stakeholder confidence in the Trust, has the potential for harm and legal consequences and therefore the Trust has a moderate appetite in relation to those risks.

Sub Category of Risk	Risk Appetite	Risk Score Tolerance
Statutory Regulation and Requirements (e.g. Information Commissioner, Care Quality Commission, Health and Safety Executive, Professional Regulatory Bodies such as General Medical Council, Nursing & Midwifery Council, external certifications such as JAG and ISO).	**Cautious**	**Mod 4 – Mod 6**
National Guidance and Best Practice (e.g. National Institute for Health and Care Excellence, GIRFT)	**Open**	**High 8 – High 12**

5. APPETITE FOR RISKS THAT MAY IMPACT UPON REPUTATION

OUR STATEMENT ON REPUTATION

We accept that a level of reputational risk is inherent in all of our activities which include the effect of factors such as regulatory intervention; employee conduct, human resource practices, legal, licensing, policy decisions; fiscal responsibility and information security. Negative perceptions by patients, staff and other stakeholders may jeopardise our credibility and impede the achievement of delivering our strategic objectives.

We expect high standards of conduct, ethics and professionalism to be maintained at all times and we have a moderate appetite for risks that could cause reputational damage to the Trust or a loss in public confidence in our ability to deliver a quality service.

We will accept a significant level of risk to our reputation (where for instance we may spend above planned levels) in protecting and improving the safety of our patients, as this is the Board's highest priority.

Sub Category of Risk	Risk Appetite	Risk Score Tolerance
Day to day activity (e.g. standards of conduct, ethics and professionalism and delivery of services)	**Cautious**	**Mod 4 – Mod 6**
Risk as a result of protecting and improving the safety of patients	**Seek**	**Ext 15 – Ext 25**

6. APPETITE FOR RISKS THAT MAY IMPACT UPON WORKFORCE

OUR STATEMENT ON WORKFORCE

We believe that patient outcomes, safety and the quality of care we provide is influenced by the experiences and engagement of staff and the support they receive from colleagues and the Trust more widely. We will endeavour to ensure that the right numbers of properly qualified staff are in the right place at the right time.

As our greatest area of expenditure we expect that staff potential and performance is efficiently maximised while balancing this against opportunities for professional development, flexible working practices and the implementation of national agreements regarding terms and conditions. We have a moderate risk appetite for compliance risks relating to staff recruitment and the controls applied while in work.

We have high risk appetite to explore innovative solutions to future staffing requirements, our ability to retain staff and to ensure that the Trust remains as an employer of choice.

Sub Category of Risk	Risk Appetite	Risk Score Tolerance
Staff recruitment (e.g. compliance with regulations such as visa requirements, Equal Opportunities and Diversity, that ensure staff are recruited fairly and competent to deliver services)	**Cautious**	**Mod 4 - Mod 6**
Employment practice	**Cautious**	**Mod 4 - Mod 6**
Staff retention (e.g. attractiveness of Trust as an employer of choice)	**Open**	**High 8 – High 12**

7. APPETITE FOR RISKS THAT MAY IMPACT UPON INFRASTRUCTURE

OUR STATEMENT ON INFRASTRUCTURE

We are committed to providing patient care in a therapeutic environment and providing staff with an environment and supporting infrastructure in which to perform their duties. However, we have a moderate appetite for some risks related to our infrastructure and estate except where these adversely impact on patient safety, care quality and regulatory compliance.

Information Management and Technology (IM&T) plays an ever increasing role in supporting staff to deliver high quality services to patients. IM&T must support core Trust functions with sufficient capability, capacity, resilience and security from internal and external threats. The Trust relies on an increasingly mobile and technologically dependent workforce to carry out its core functions; we therefore expect that full business continuity plans are in place should services become unavailable.

We will collect personal and sensitive information to help us deliver services and improve their quality, ensuring that only those who have a legitimate purpose are given access to this data. We have a low risk appetite for IM&T risks relating to security, control of assets, business continuity and data.

Sub Category of Risk	Risk Appetite	Risk Score Tolerance
Estates infrastructure	**Cautious**	**Mod 4 – Mod 6**
Security (e.g. access and permissions to systems and networks)	**Cautious**	**Mod 4 – Mod 6**
Control of Assets (e.g. purchase, movement and disposal of ICT equipment)	**Cautious**	**Mod 4 – Mod 6**
Business continuity (e.g. cyber-attack, maintenance of networks, alternative solutions)	**Cautious**	**Mod 4 – Mod 6**
Data (e.g. integrity, availability, confidentiality and security, unintended release)	**Cautious**	**Mod 4 – Mod 6**

8. APPETITE FOR RISKS THAT MAY IMPACT UPON FINANCE AND EFFICIENCY

OUR STATEMENT ON FINANCE AND EFFICIENCY

To achieve the best value for money and to ensure our future financial sustainability we expect appropriate stewardship over our financial resources. This means that decisions regarding the pursuit of our strategic objectives must be balanced against the expectations of our regulators in meeting our financial plans and statutory duties.

We expect robust internal controls to be maintained which ensure compliance with applicable government and accounting standards. We will not tolerate risks that may lead to financial losses from fraud and negligent conduct as this represents a corporate failure to safeguard public resources.

Sub Category of Risk	Risk Appetite	Risk Score Tolerance
Value for money and sustainability (including cost saving)	**Cautious**	**Mod 4 – Mod 6**

Standing Financial Instructions (SFI's) and financial control	**Cautious**	**Mod 4 – Mod 6**
Fraud and negligent conduct	**Minimal**	**Low 1 – Low 3**
Contracting	**Seek**	**Ext 15 – Ext 25**

9. APPETITE FOR RISKS THAT MAY IMPACT UPON PARTNERSHIPS/COLLABORATION

OUR STATEMENT ON PARTNERSHIPS & COLLABORATION

We are committed to collaborating with our stakeholder organisations to bring value and opportunities across current and future services, through system-wide partnerships. We have a high risk appetite in developing partnerships with organisations who are responsible and have similar values, maintaining the required level of compliance with our statutory duties.

Sub Category of Risk	Risk Appetite	Risk Score Tolerance
Partnerships	**Open**	**High 8 – High 12**

10. APPETITE FOR RISKS THAT MAY IMPACT UPON INNOVATION

OUR STATEMENT ON INNOVATION

We have a significant appetite to pursue innovation in the delivery of services and challenge current working practices. The potential rewards in pursuing new solutions that may improve quality and provide business efficiencies must be balanced against the safety and wellbeing of our patients and staff.

We have a significant appetite to pursue innovation and challenge current working practices in support of the use of systems and technology developments, as well as new service design within the services it manages. We will therefore pursue options where innovation can provide higher rewards (despite greater inherent risks), but only where quality and compliance are not affected.

Although we cannot control or predict external factors that may affect our financial resources, we have a duty to protect cost saving through efficiencies and innovation. We are therefore willing to accept a high level of risk in pursuit of such activities but we expect prudent decisions to be made to mitigate the financial impact while providing optimal value for money.

Sub Category of Risk	Risk Appetite	Risk Score Tolerance
Innovation (e.g. new ways of working, new products, new and realigned services, new models of staffing and realignment of services, international recruitment, new ICT systems and improvements)	**Seek**	**Ext 15 – Ext 25**
Financial Innovation (e.g. new ways of working, new products, new and realigned services)	**Open**	**High 8 – High 12**

Appendix 5: Identifying Controls, Assurances and Actions

1. Identifying Controls

Generally speaking the purpose of control is to constrain risk rather than to eliminate it. Control relates to any **action** taken to manage risk. These actions may be taken to manage the impact if the risk is realised, or to reduce the likelihood of the risk occurring. When you are identifying controls, these must already be in place. Any controls to further to constrain risk which are not in place should be addressed within your action plan. Once these additional actions are in place, they become a control.

Examples of controls can include:

- Policies and procedures
- People, for example, a person who may have a specific role in delivery of an objective
- Training programmes
- Processes / practices, for example, a specific process which ensures the delivery of an objective

2. Identifying Assurances

Assurances provide us with information or evidence about the effectiveness of our controls. Assurances can be from a range of sources and will include internal assurances (for example a clinical audit) and / or external assurance (for example a report from a regulatory body).

Assurances can be positive or negative, meaning that the assurance can indicate whether our controls are working well or whether we need to make further improvements.

For example:

- A report on training uptake statistics will tell us whether our training uptake is reaching those intended
- A report on adverse incident reports will tell us whether our policies, procedures and processes are working effectively and without incident
- An audit will tell us whether we are compliant with relevant requirements (which could be our local policies or a national mandate)

3. Describing Assurances

How to describe assurances:	**How not to describe assurances:**
An assurance description needs to state what the source of assurance is and more importantly what the assurance is telling you and if possible, the time period to which it relates. For example: • Incident report monitoring during Quarter 1 20/21 has confirmed that there have been very few adverse incidents of pressure ulcers.	An assurance description should not simply feature a list of documents, as this does not provide sufficient information on the effectiveness of your controls. For example: • Adverse incident reports • Minutes of meetings • Report to Patient Safety Forum

4. Identifying Actions

Once you have identified your controls and assurances, you will need to identify what further actions need to be taken to achieve your objective / reduce the risk if possible. These actions are sometimes referred to as risk control and usually fall under the following categories:

Types of Risk Control (the 4 'T's)	
Terminate	Eliminates the risk completely.
Transfer	Passes the risk to a third party, who bears or shares the impact.
Treat	**Containment:** Reduces the likelihood and / or the impact
	Contingent: Establishes a contingency to be enacted should the risk happen.
Tolerate	Accepts the risk if it has reached the target risk score, subject to monitoring.

When identifying actions, you must ensure that each action also has a designated person responsible for completing the action and a due date by which the action will be completed.

Appendix 6: Risk Reporting, Oversight and Escalation

1. Risk Reporting

The majority of risks should be reported in the form of a Risk Register. A risk register is simply a record of all identified risks relating to a set of objectives, including their history and their status. For the purposes of the Board Assurance Framework, strategic risks will be reported in a standalone format and presented to Boards and Committees. Operational risks which are linked to any of the strategic risks will be taken from the Datix Risk Register.

A risk register is a tool designed to help managers achieve their objectives and to drive and provide evidence of risk management activities.

To ensure risk reporting is meaningful and effective, a Risk Register Report should include the following fields (all of which should be accurately completed within Datix).

ID	The unique identifier for your risk assessment, automatically generated by Datix.
Risk Owner	The person responsible for identification and management of the risk.
Primary Risk Subject	To identify the main category of risk i.e. Quality – Safety, Effectiveness & Experience, Regulation and Compliance, Reputation, Workforce, Infrastructure (Estates & IM&T), Finance and Efficiency, Partnerships/Collaboration, Innovation.
Strategic Objective	To identify which of the Trust's Strategic Objectives the risk will have an impact upon.
Title	The short title which describes the subject of the risk.
Risk Description	The risk description should include a risk description in line with the guidance set out within appendix 5. The risk description should include a composition of 'if…then…resulting in…'
Controls	To identify the actions being taken to manage the risk and achieve the objective (as set out within appendix 5).
Assurances	To describe the sources of assurance and what those assurances say in terms of the effectiveness of the actions taken (as set out within appendix 5).
Initial Risk Score	To confirm the risk score which was calculated when the risk assessment is first completed, without any controls/assurances in place. This remains unchanged once calculated.
Current Risk Score	To confirm the risk score which was calculated when reviewing the risk assessment taking into account controls and assurances. This is recalculated each time the risk assessment is reviewed.
Target Risk Score	To confirm the target risk score in line with the Trust's Risk Appetite Statement which should reflect the level of risk reduction required by introducing additional controls.
Actions	To identify the further action required.
Person Responsible	To identify who is responsible for carrying out the action.
Due Date	To identify when the action will be completed.
Completed Date	To confirm the date that the action has been completed.

2. Risk Oversight Framework

Risks are overseen at various levels throughout the organisation. The table below sets out the levels at which risks must be reported and overseen:

Level of Escalation / Oversight		Level / Types of Risk	Role and Purpose of Oversight	Style of Report
CORPORATE OVERSIGHT	**Board**	Risks identified against Strategic Objectives	• Scrutiny of the risks identified and holding responsible persons to account for the action being taken. • Assurance from the Audit Committee that the process is working effectively	Board Assurance Framework (BAF)
	Performance & Finance Committee / Quality Governance Committee / Transformation & People Committee	Risks identified against Strategic Objectives – relevant to their area of focus	Scrutiny of the risks identified and holding responsible persons to account for the action being taken.	Board Assurance Framework (BAF)
	Audit Committee	Risks identified against Strategic Objectives	Assurance from the Quality Governance Committee, Performance & Finance Committee and Transformation and People Committee that the process is working effectively	Board Assurance Framework (BAF)
	Performance Management Reviews	• Risks for escalation • Outcome of audit results	Holding responsible persons to account for the action being taken	Divisional Performance Management Review Presentation
	Executive Groups	All risks scoring 12 or above from Divisional or Corporate Risk Register	• Scrutiny, challenge of risks scoring 12 or above. • Referral to and assurance from key specialist corporate groups as appropriate. • Agreement of risks to be escalated to the Corporate risk Register	Risk Oversight Report (taken from Risk Registers)
	Specialist Corporate Groups	All 'corporate' risks relevant to their area of specialism.	Identification, management and oversight of risks relevant to their specialist subject, ensuring appropriate action is taken.	Corporate Risk Register
DIVISIONAL OVERSIGHT	**Divisional Boards**	All risks scoring 8 or above	• Challenge, review and monitoring of all risks scoring 8 or above. • Escalation of risks to Executive Groups.	Risk Register
	Divisional Governance Group	All risks	• Scrutiny, challenge, review and monitoring of all Divisional risks • Escalation of risks to Divisional Board	Risk Register
	Directorate / Operational Groups	All relevant risks	• Scrutiny, challenge, review and monitoring of all Directorate risks	Risk Register

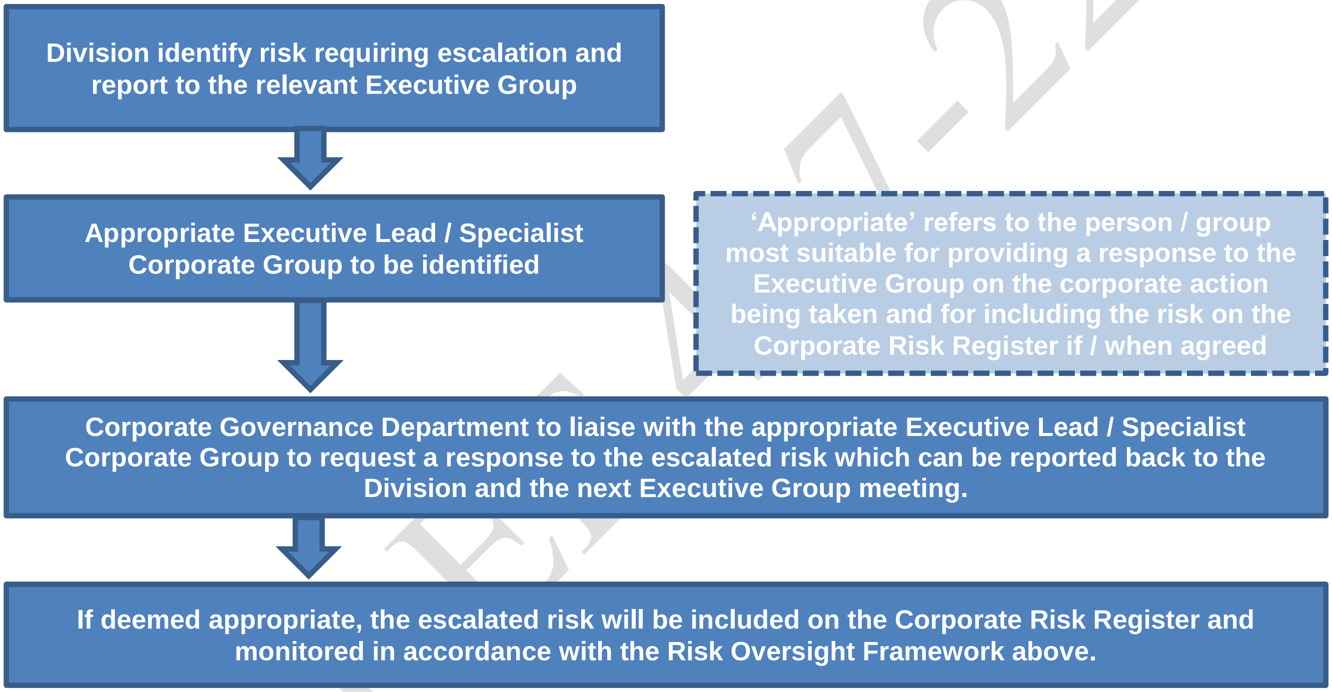
3. Risk Escalation to the Corporate Risk Register

Risk escalation to the Corporate Risk Register is where a risk is specifically drawn to the attention of an Executive Group for inclusion on the Corporate Risk Register.

Although the Executive Group will make a decision on those risks which will be included on the Corporate Risk Register, these will, in most circumstances be:

- Emergent risks which span across multiple divisions and are not already subject to corporate oversight
- Risks where the action required does not fall within the full control of the Division
- Risks which are overseen by the Specialist Corporate Groups due to their nature

4. Corporate Risk Register Escalation Process



Division identify risk requiring escalation and report to the relevant Executive Group

Appropriate Executive Lead / Specialist Corporate Group to be identified

'Appropriate' refers to the person / group most suitable for providing a response to the Executive Group on the corporate action being taken and for including the risk on the Corporate Risk Register if / when agreed

Corporate Governance Department to liaise with the appropriate Executive Lead / Specialist Corporate Group to request a response to the escalated risk which can be reported back to the Division and the next Executive Group meeting.

If deemed appropriate, the escalated risk will be included on the Corporate Risk Register and monitored in accordance with the Risk Oversight Framework above.

Appendix 7: Review of Risk

1. Risk Review

The Trust recognises that risk management should be embedded throughout the organisation. The review of risk should be an ongoing and iterative process which is part of day to day work. Risks should be reviewed by the Risk Owner, in order to:

- Enable key controls to be identified
- Identify whether the risk score is increasing, by articulating current assurance regarding the effectiveness of the controls
- Identify and implement actions for further mitigation
- Enable the opportunity to escalate risks
- Monitor implementation of actions and whether additional controls have had an impact on reducing the likelihood and/or impact
- Identify whether the actions taken have reduced the risk to a 'tolerable' level

2. Frequency of Reviews

Risks should be reviewed on a basis that is proportionate to the current risk rating. All risks should be reviewed by the Risk Owner and discussed at an appropriate governance meeting. Reviews should consider the risk description, current and target scores, identification of new controls, assurances and further actions. Updates should be made to the risk assessment on Datix in the respective fields.

NB. It is recognised that Progress Notes are utilised in some areas for providing updates on risks. It is imperative that information in relation to actions taken and current assurances are included within the controls, assurances and action planning fields. Progress Notes should therefore only be utilised to contain information not able to be provided within an existing field.

Risk Rating	Frequency of Review
Risks that have been closed but have a recurring theme	Annually
Risks scoring 3 or below	Six monthly
Risks scoring between 4 and 6	Quarterly
Risks scoring between 8 and 12	Bi-monthly
Risks scoring 15 or above	Monthly