NHS
Yorkshire
Ambulance Service
NHS Trust

Risk Management Policy

Document Author: Executive Director of Quality, Governance and Performance Assurance

Date Approved: May 2017

Document name	PO-Risk Management Policy – May 2020
Version	V2.1
Responsible Committee	Risk and Assurance Group
Responsible Director	Executive Director of Quality, Governance and Performance Assurance
Document Owner (title)	Risk Manager
Document Lead (title)	Executive Director of Quality, Governance and Performance Assurance
Approved By	Trust Management Group
Date Approved	10 May 2017
Review Date	10 May 2020
Equality Impact Assessed	Yes
Protective Marking	Not Protectively Marked

Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
0.1	December 2013	Mark Hall	D	This document has been updated and replaces all previous versions of the Incident Management Policy; Risk Escalation & Reporting Procedure; Investigation, analysis and Learning Policy.
1.0	15/01/2014	Mark Hall	A	Approved SMG 15/01/14
1.1			D	Minor amends
1.2	15/12/2016	Maxine Travis	D	Removed sections relating to incident reporting, SI investigation and learning – now covered in Investigations and learning policy. This document replaces all previous versions of the Risk Management Policy and procedures Added section on Actions module, risk scoping and framing, internal audit risk profiling.
1.3	27/02/2017	Maxine Travis	D	Added section 3.7 Risk owner and action owners (feedback from RAG 16.02.17) Section 3.10 add 3.10.1 completing actions to section on closing and archiving risks
2.0	10/05/2017	Maxine Travis	A	Approved at TMG 10/05/2017
2.1	Feb 18	Risk Team	A	Document formatted – New visual identity
A = Approved D = Draft				
Document Author = Risk Manager				
This document is controlled. If you would like to suggest amendments to this document please contact the document author.				
Associated Documentation: ▪ Risk Management and Assurance Strategy ▪ Health and Safety Policy ▪ Infection Prevention and Control Policy				

- Education and Development Policy
- Trust Statutory and Mandatory Training Workbook 2015-17
- Records Management Policy
- Complaints Policy
- Claims Handling Policy
- Information Governance Strategy

Staff Summary

Recognising or identifying sources of risk
Describing a risk
Identifying controls and gaps
Developing an action plan
Oversight of risk leads and key groups / committees
Responding to Datix auto-prompts
Completing actions and Closing/archiving risks
Management guidance is available to support risk and action owners with the practical application of this policy and in using risk and actions modules within the Datix system

1.0 Introduction

1.1 Yorkshire Ambulance Service NHS Trust is committed to identifying and managing all risks associated with the service it delivers and acknowledges that failure to recognise and address risk could lead to harm to patients, staff and others, damage to the Trusts reputation and adverse publicity, to financial or business loss, and to litigation.

1.2 Actively recognising risks associated with the services it provides and proposed business developments allows implementation of risk reduction strategies to mitigate the likelihood of the impact materialising.

1.3 Risk management is integral to corporate activities and embedded into routine business of the Trust in order that it can effectively support and identify risks associated with service change and external factors.

1.4 This policy underpins delivery of the Trust's Risk Management and Assurance Strategy and other associated documents, providing an overview of the process for identification and management of risks.

1.5 This policy is supported by Risk Management Guidance for Managers which provides a practical, step-by-step approach to using the Datix Risk Management system.

2.0 Purpose/Scope

2.1 The purpose of this document is to detail the process to be followed to identify and assess the impact and likelihood of risks, to explain the risk register process and to state responsibilities of individuals, groups and committees in the process.

2.2 The document applies to all Trust staff, volunteers and contractors engaged on Trust business.

3.0 Process

3.1 Recognising or identifying sources of risk: Set out below are examples of the potential sources by which risks can be identified. This list is not exhaustive.

3.1.1 Quality Impact Assessment

In the delivery of the Trust's strategic objectives there are a number of major service developments including Quality and Efficiency Savings Programmes and service transformation projects. The Quality Impact Assessment (QIA) process assesses the impact of change on quality of services. Output from this process is used to inform a view of Directorate and Corporate risk.

3.1.2 Incidents and near misses

Identifying recurrent near-miss incidents and monitoring levels of harm associated with particular categories of incidents is a mechanism whereby the Trust can be alerted to potential risks to patients, staff and the Trust.

3.1.3 Complaints and Concerns

Identification of themes and trends, particularly related to complaints and concerns can inform services of emerging risks to patient safety, organisational reputation and potential litigation.

3.1.4 Claims

Data relating to clinical (patient) and non-clinical (employer and public liability) claims is regularly analysed by the Legal Services Department in order to learn lessons and reduce the risks associated with claims.

3.1.5 Triangulation of information

Information from incidents, complaints and claims is collated to identify overarching themes and trends, to learn lessons and to recognise key risks to the organisation. These inputs are discussed collectively by the Incident Review Group which meets on a fortnightly basis. A Significant Event and Lessons

Learned Report is received bi-monthly by Quality Committee and twice yearly at Trust Board.

3.1.6 Central Alerting System (CAS) notifications

The Trust acknowledges and assesses the relevance of CAS alerts; these can relate to equipment failures, clinical patient safety, medication, or estate issues (list not exhaustive). Failure to implement the necessary actions to address these alerts would present a risk to the organisation both in terms of non-compliance with the required remedial actions to ensure patient and/or staff safety, and failure to comply with sign off which will be escalated by the Department of Health to our regulators. Any risk to achieving timely compliance with CAS alerts will be reported and managed as a risk.

3.1.7 Inspections for Improvement

The Inspections for Improvement process is led and coordinated by the Quality and Safety Team with engagement from Clinical Supervisors, Clinical Managers and Locality Directors. Each Ambulance station, standby point and Patient Reception Centre is inspected as part of a rolling programme by a small team or individual, depending on the size of the premises. The Health & Safety Manager, Local Security Management Specialist and Information Governance Manager provide expert input into the process. Action plans are created for each premise following inspection, and where actions cannot be addressed, a risk may be identified specific to one location or relating to a recognised issue collectively recognised in a number of locations.

3.1.8 New policies and procedures

New and revised policies and procedures are assessed to ensure that they do not introduce new risks, or where the emerging risk presents less of a threat than continuing the existing practice, a plan to mitigate these should be put in place alongside implementation of the policy.

3.1.9 Internal Audit

Failure to deliver recommendations of Internal Audits within agreed timescales should be risk assessed by the appropriate governance group, and any residual risk reported on the risk register

3.1.10 Business Continuity (BC) exercises

Recommendations from BC exercises are captured within the risk management process to ensure delivery of actions to reduce risk of failure in the event of an actual incident.

3.1.11 Risk Assessments

Where risk assessments are conducted these can be task-specific, dynamic (real-time presenting circumstances), person-specific (eg. pregnancy) or related to premises, equipment or vehicles. More detailed information on conducting risk assessments can be found in the Risk Assessment Procedures on the intranet. Themes and trends identified from risk assessments may be articulated on the Trust's risk register.

Line managers are responsible for ensuring risk assessments are undertaken in their areas. The Health and Safety Manager will support the line managers and provide training as appropriate. The management of risks identified through the risk assessment process will be determined by the risk rating:

High (15-25): The risk should be escalated to the Trust Risk Manager, recorded on the Trust's Datix Risk Management system risk module (as described below) and managed at a Directorate Level by the line manager. The risk and associated action plan to reduce it should be reviewed by local governance groups. Strategic and Operational risks will be reviewed by Risk and Assurance Group to determine whether it should be escalated to the Corporate Risk Register report.

Medium (8-12): The risk should be managed at a departmental level by the line manager. The risk should be considered for recording on the risk register on Datix. Strategic and Operational risks graded 12 and above will be reviewed by the Risk and Assurance Group to determine whether they should be escalated to the Corporate Risk Register report. Risks should be reviewed at least quarterly.

Low (1-6): The risk can be managed at a local level by the line manager. The risk assessment should be reviewed at least annually along with the local action plan.

3.1.12 Other sources of risks

The examples above are not exhaustive and potential risks recognised during day to day activities should be escalated by any member of YAS staff to their line manager.

3.2 Tool to scope the risk

3.2.1 A tool to support the risk owner in articulating the risk, controls, gaps and actions required to mitigate the risk is at appendix 2. This tool can be used by the individual or by a group to develop and discuss a risk prior to recording on Datix.

3.2.2 Support for this process is available from the nominated Directorate Risk Lead and/or the YAS Risk Manager.

3.3 Describing a risk

3.3.1 The risk description should convey the risk clearly and concisely. In describing a risk, the risk lead is defining three factors; the potential threat, what will happen if the threat materialises, and ultimately the impact.

3.3.2 The model for describing a risk adopted by YAS is the IF…THEN…RESULTING IN model.

3.3.3 The dependent relationship between the potential for something to happen (IF), the circumstances should this happen (THEN) and the impact (RESULTING IN) should clearly describe the risk. Examples of this are provided in one-to-one training and guidance can be sought from the Trusts Risk Manager where necessary.

3.4 Identifying Controls and Gaps

3.4.1 Controls are arrangements that are already in place to mitigate or manage the risk and these can include policies and procedures, monitoring and audit.

3.4.2 Every control should be relevant to the risk that has been described, it should be clear that the control directly impacts on managing the risk and the strength of the control should be considered when deciding the influence this will have on the risk rating.

3.4.3 Despite having identified controls, where the service has established that a risk exists, it is the uncontrolled issues that are articulated as Gaps.

3.4.4 Gaps are issues which are not controlled and directly affect our mitigation of the risk. Gaps require clear and proportionate actions to address them, as described below.

3.5 Developing an action plan

3.5.1 For each Gap identified, there should be at least one action to address it. The action should specifically address the gap, should be time-limited and have an owner responsible for completion, or for ensuring completion by delegation.

3.5.2 The Actions module in Datix sits alongside the Risk module and is used to capture all actions associated with risks. One gap in control may require multiple actions recorded against it. Actions are recorded individually to ensure an audit trail of implementation is captured against each action.

3.5.3 Action plans should have an identified owner for every action and a review date, i.e. a date upon which progress towards completing the actions will be reviewed. The review dates associated with new action plans should project forwards from the date that the risk register entry is completed. Review dates are important because they enable the organisation to monitor progress towards reducing the risk over time.

3.5.4 Where the risk owner is recording actions and these are to be allocated to another individual, the risk owner should discuss with the proposed action owner prior to allocating to ensure ownership is agreed.

3.5.5 The Datix Risk Management System will remind action owners by email when their specific actions are due for review.

3.6 Differentiating between controls, gaps and actions

3.6.1 To summarise:

- Controls are things that are already in place to manage or monitor the risk.
- Gaps are the issues that we need to address to control the risk fully
- Actions describe how you will address the gaps to reduce or eliminate the risk you have described

3.7 Risk Owner and Action Owners

3.7.1 Each recorded risk will have a designated Risk Owner. The Risk Owner takes oversight of the risk, ensuring the action plan is proportionate to addressing the gaps in control in order to mitigate the risk to the target level.

3.7.2 In addition to a designated Risk Owner, the risk will have one or more Action Owners. Action Owners are responsible for delivery of the specified actions that will mitigate the risk to his target level.

3.7.3 The Action Owner may be the same individual as the Risk Owner, or could be from a different service or directorate. As stated above often there are multiple actions recorded, each may have a different Action Owner.

3.7.4 When recording a risk, the Risk Owner should ALWAYS ensure that Action Owners are consulted prior to recording actions and allocating them responsible for delivery. It is courteous, and essentially ensures that the individual agrees to be responsible for ensuring delivery of the aforesaid action in the way described and in the timeframe stipulated.

3.7.5 There can be conflicts of ownership and subsequent failure to effectively manage a risk where actions are allocated to individuals who do not, or cannot, take ownership.

3.8 Risk Rating

3.8.1 The Trust's Risk Matrix is based upon the National Patient Safety Agency (NPSA) framework which is 5 x 5 model of consequence multiplied by likelihood to arrive at a RAG (Red, Amber, Green) rating, to which the Trust has then defined our approach to management.

3.8.2 Consequence: The YAS risk matrix has a number of 'domains' which are essentially categories of type of risk, for example financial, clinical, quality or reputational. Against each of these domains are consequence descriptors that are scored between 1 and 5, negligible to catastrophic.

3.8.3 Likelihood: The risk matrix describes a measure of frequency, or probability, of the risk occurring as the likelihood. This is scored between 1 and 5, Rare to Almost Certain, again with descriptions of these labels to support selection.

Likelihood should be assigned using the predicted frequency of occurrence of the adverse outcome. If it is not possible to determine a numerical probability then use the probability descriptions to determine the most appropriate score. The Risk Matrix gives a probability descriptor to describe the adverse outcome occurring within a given time frame, such as the lifetime of a project or a patient care episode.

3.8.4 The Trust's Risk Matrix should be applied as follows once the description of the risk has been agreed:

Step 1 Identify the appropriate Domain which describes the adverse consequence that might arise from the risk. This is the 'Resulting in' part of the description of the risk.

Step 2 Determine the consequence score (C) for the potential adverse outcome relevant to the risk being evaluated within that Domain.

Step 3 Determine the likelihood (L) of the adverse outcomes occurring using the descriptor.

Step 4 Calculate the risk score the risk multiplying the consequence by the likelihood: C (consequence) x L (likelihood) = R (risk score)

Step 5 Identify the level at which the risk will be managed in the organisation, assign priorities for remedial action, and determine whether risks are to be accepted on the basis of the colour bandings and risk ratings, and the organisation's risk management system. Include the risk in the organisation risk register on Datix at the appropriate level.

3.9 Responding to Datix auto-prompts

3.9.1 The Datix system automatically sends out a reminder to the Risk Lead recorded on the individual risk record when the review date is reached and not updated.

3.9.2 A notification is also received by any Action owner when the recorded action reaches its Due Date, when an update is expected. Progress can be updated at any point in relation to an overarching risk or an associated action and the owner should not wait to receive a notification if progress can be refreshed.

3.9.3 The overall Risk Review date and individual Action Due dates may differ as there may be a number of actions to be completed over a period of time in order to mitigate the overall risk.

3.10 Completing actions and Closing and Archiving Risks

3.10.1 When an action is complete, a completed date should be added, this allows an audit trial to demonstrate delivery of actions to mitigate the risk. When an action is completed, consideration should be given to the risk rating and whether the action has significant impact on the likelihood or consequence of the risk occurring, and whether the risk can be reduced.

3.10.2 There can be a number of completed actions recorded against a risk that remains open. The action owner is responsible for updating and closing actions when completed.

3.10.3 When a risk has been reduced or eliminated through the implementation of action plans, the risk can be closed and archived from the 'live' risk register.

3.10.2 Risks can be closed without reaching the target risk rating where the service recognises that residual risk will not or cannot be mitigated and accepts the outstanding low level of risk

3.10.3 Risks should be closed with approval of the appropriate Directorate Governance group or committee

3.10.4 The current risk rating should be amended to illustrate that the action plans have controlled the risk. That is to say, the current risk rating should be low green (1-6) prior to contemplating the removal of a risk from the risk register. The status of the risk should be 'Awaiting Final Approval', and the 'closed' date should be entered.

4.0 Managing and monitoring risks including oversight of risk leads and key groups / committees

4.1 Each Directorate, business / service area or CBU has a nominated risk 'champion' who is their Risk Lead. The role of this Risk Lead is to maintain oversight of all risks for their area, be the representative for their business area at Risk and Assurance Group (RAG) and provide updates to RAG on behalf of their service on existing and emerging risks.

4.1.1 The Risk Manager meets with Risk Leads as part of the Risk Management work plan to undertake periodic review of risks, dependent upon the area; this may be monthly or quarterly. In addition, the Risk Lead receives any Datix Risk Module training required to support them in their role.

4.1.2 The Risk Manager will support the Risk Lead to produce risk reports that will be reviewed by the Directorate/CBU Governance Group. The Risk Lead should lead this discussion as part of the Directorate/CBU Governance Group and update the risks on Datix following the meeting. The Risk Manager is available to support this process as required.

4.2 The Trust's Risk Management Strategy sets out the framework which enables implementation and promotes continuous improvement in the processes and cultures which are essential in delivery of effective risk management. The Risk Management Strategy articulates the Trust's risk appetite and is underpinned by this policy and documents detailed below:

4.2.1 The Board Assurance Framework is a high level document that sets out principal risks to delivery of the Trust's Strategic Objectives and identifies assurances in control of the risk and any gaps in assurance. An assurance is evidence that the controls/systems which are in place to control the risk are working effectively. Assurances can be both internal and external. Internal assurance can be provided by describing the key performance indicators and monitoring arrangements that are in place which evidence a control is working. For example, KPI's relating to audit activity, scorecard monitoring, self-audits which demonstrate policy compliance. External assurance provides independent evidence that a control is effective and therefore generally provides a stronger source of assurance to the Board. Examples of external assurance include external audits, Internal Audit reports. The BAF is reviewed through the quarterly cycle of corporate governance groups and committees

4.2.2 The Trusts Risk Matrix is based on the National Patient Safety Agency 5x5 matrix and allows for articulation of descriptors of risk types such as 'financial', 'staff safety', 'clinical' or 'information governance' alongside a likelihood of occurrence ranging from 'rare' to 'almost certain' in order to calculate a risk score. The risk score determines the level of reporting and scrutiny of the risk and associated action plan.

4.2.3 The Corporate Risk Register (CRR) presents Strategic and Operational Risks graded ≥12. The CRR is reviewed on a monthly basis at RAG and follows the quarterly cycle of corporate governance committees.

4.2.4 Local risk registers capture lower graded risks with action plans that can be managed at local level and are reviewed by the service risk lead.

4.2.5 Risk Registers are live records and are populated and updated through the organisation's risk management process and recorded on Datix. This process enables all risks to be quantified and graded, and escalated as necessary. It provides a structure for collecting information about risks that is consistent and will:

- Support the analysis of risk
- Support decisions about whether or how these risks could be mitigated and monitored
- Provide a framework for escalation for Board scrutiny and prioritisation of actions through the Board Assurance Framework (BAF) and Corporate Risk Report
- Support strategic analysis and organisational decision making

4.2.6 Risk Registers should be a regular agenda item for local business area governance meetings, directorate meetings and specialist groups to ensure risks are constantly identified, monitored and re-evaluated throughout the year.

5.0 Training expectations for staff

5.1 Training is delivered as specified within the Trust Training Needs Analysis (TNA). All staff receive Corporate Induction which provides a high level view of the Trust's governance structure, and how to identify and escalate potential risks or actual incidents.

5.2 Delivery of training is an integral part of the Risk Management annual work plan. Specific training is targeted at service area nominated risk leads and is predominantly delivered via 1:1 sessions with the Risk Manager. Small group awareness sessions are held with staff that are responsible for reviewing business area/departmental risk registers.

6.0 Implementation Plan

6.1 The latest version of this Policy will be posted on the Trust Intranet site for all members of staff to view. New members of staff will be signposted to how to find policies and procedures during Trust Induction.

7.0 Monitoring Compliance

7.1 For the Trust to be assured that the processes described within this policy are working, monitoring arrangements are shown in the table below.

Auditable Standards	Methodology	Frequency	Monitoring Committee
All Service / Business Areas should be represented at Risk and Assurance Group	Review of attendance register by the Risk Manager / Chair of RAG	6-monthly	Reported back to RAG and escalated to TMG where indicated
All risks should remain in date	Review of Corporate Risk Register at RAG Monthly risk review meetings with Risk Leads and Risk Manager	Monthly	RAG

8.0 References

National Patient Safety Agency: A Risk Matrix for Managers. Available online at: http://www.npsa.nhs.uk/nrls/improvingpatientsafety/patient-safety-tools-and-guidance/risk-assessment-guides/risk-matrix-for-risk-managers/

PLEASE NOTE YAS STAFF SHOULD REFER TO THE YAS RISK MATRIX AVAILABLE ON PULSE.

9.0 Appendices
Appendix 1 - Roles & Responsibilities

This section of the Procedure provides a brief synopsis of the roles and responsibilities of key groups and committees and key individuals.

Trust Board
The Trust Board adheres to the principles outlined in the UK Corporate Governance Code (2012). The Board recognises its accountabilities and provides leadership within a framework of practical and effective controls which enables risk to be assessed and managed. The Board sets the strategic aims and ensures that resources are in place to meet its objectives. It receives reports at each meeting on the highest principal risks and associated actions as detailed in the Trust's Board Assurance Framework.

Audit Committee
The Audit Committee is a formal Committee of the Trust Board. The Audit Committee provides overview and scrutiny of risk management. It meets quarterly and has an annual work plan which has been refined to reflect the increased focus on quality governance.

Quality Committee
The Committee undertakes scrutiny of the Trust's clinical governance and quality plans, compliance with external quality regulations and standards and key functions associated with this, including risks to delivery of plans that are related to these areas.

Trust Executive Group
Reporting to the Trust Board, the Trust Executive Group is accountable for the operational management of the Trust and the delivery of objectives set by the Board. It is also the formal route to support the Chief Executive Officer in effectively discharging his responsibilities as Accountable Officer.

Trust Management Group (TMG)
The Trust Management Group supports the operational management of the Trust and the delivery of objectives set by the Trust Board. The Group carries delegated responsibility from the Trust Executive Group.

Risk and Assurance Group
The Group receives reports on all directorate risk registers and specific risk issues from the members, including representatives from all other associated risk management groups.

Strategic Health & Safety Committee
This strategic Committee is responsible for the review and monitoring provision of a healthy, safe and secure environment for all employees, contractors and members of the public who may be affected by the activities of the Trust. The Committee is

responsible for instigating appropriate action to address risks identified from issues that may compromise the above.

Clinical Governance Group (CGG)
The Clinical Governance Group (CGG) provides a focus for clinical risk and quality issues. It receives reports by exception on clinical risk issues and is responsible for directing action to manage clinical risk.

Clinical Quality Development Forum (CQDF)
Clinical Quality Development Forum is a sub-group of CGG. The CQDF reviews clinical risks on a monthly basis, exception reporting to CGG.

Medicines Management Group (MMG)
The Medicines Management Group (MMG) reports directly into the CGG and is responsible for reviewing drug related incidents and serious incidents (SIs), instigating appropriate action to address issues identified.

Incident Review Group (IRG)
The Incident Review Group (IRG) is a working group that is responsible for reviewing and instigating appropriate action to address issues identified in relation to incidents, potential SIs and near misses, along with identifying themes and trends from the following specialty areas;-

- Formal Complaints/Concerns
- Claims
- Coroner's inquest
- Clinical Case Reviews
- Human Resources processes

Information Governance Working Group
Information Governance Working Group is responsible for advising upon and overseeing the management of all issues associated with confidentiality and information governance/security that have been highlighted by incident reports.

Executive Director of Quality, Governance and Performance Assurance
The Executive Director QGPA has overall lead responsibility for driving the direction, development, management and implementation of the Risk Management Strategy.

Executive Medical Director
The Executive Medical Director is responsible for working closely with the Executive Director QGPA for in relation to risk management and providing expert advice and guidance where necessary, particularly in relation to clinical risk.

Executive Directors
Directors have responsibility for ensuring that the Risk Management Policy is implemented within their directorates and that risk management is embedded within their governance arrangements.

Associate Director Performance, Assurance and Risk
The Associate Director of Performance, Assurance and Risk is responsible for promoting and supporting of embedding of effective risk management processes within the Trust.

Risk Manager
The Risk Manager is responsible for operational implementation of the Risk Management and Assurance Strategy and Risk Management Policy, including providing support, guidance and training to risk leads on implementation.

Managers
All managers are responsible for playing a part in identification and management of risk within the extent of their roles and responsibilities. They will be expected to comply with the systems and associated procedures, and ensure all efforts are made to encourage their teams to escalate potential risks they become aware of.

In addition, there are managers with specific interest and responsibility for oversight of risk management within their specialist area of work, these include;-

- Health and Safety Manager
- Local Security Management Specialist (LSMS)
- Information Governance Manager
- Caldicott Guardian
- Head of Safeguarding
- Head of Safety

All staff
All staff across the Trust have a responsibility to ensure they make themselves aware of and comply with the Risk Management Policy. Staff are responsible for reporting identified potential risks within their area of work. Staff will be required to participate in activities which are commensurate with the Trust's Risk Management Policy and statutory or legislative requirements.

Appendix 2 - Risk Register Assessment Form (template page 1)

Date risk identified	
Risk owner	
Risk title	
Risk description	IF THEN RESULTING IN
First Review date	
Risk source (how has this become apparent) **choose all that apply**	4Cs **/** BC **/** Claims **/** External Audit **/** Incidents **/** Internal Audit **/** Internal Business Review**/** Legislation **/** PRF **/** Project **/** Regulatory body **/** Risk assessment **/** Safety Alert **/** Self Audit
Risk type – select ONE	Strategic **/** Operational **/** Programme or project
Risk sub-type – select ONE	Adverse Publicity and reputation **/** Business Continuity **/** Capacity **/** CIP **/** Clinical **/** Equipment **/** Estates & Facilities **/** Financial **/** Health & Safety **/** Hillsborough **/** Human Resources **/** ICT **/** Information Governance **/** IPC **/** Patient experience **/** Patient harm **/** Regulatory Compliance **/** Safeguarding **/** Security **/** Staff safety **/** Supply&Procurement **/** Training & Education
Directorate	
Business area	
Existing controls	
Adequacy of controls	Adequate / inadequate / uncontrolled
Gaps in control	
Initial risk score	Consequence ( ) x Likelihood ( ) = ( )
Target risk score	Consequence ( ) x Likelihood ( ) = ( )

Risk Register number (generated by Datix)

Record actions overleaf

Risk Register Assessment Form (template page 2)

Action title	Due date	Owner	Action title	Action description