South Tyneside
Clinical Commissioning Group

Risk Management Policy

Ratified	Audit & Risk Committee
Status	Final
Issued	3 June 2021
Consultation	Executive Committee
Equality Impact Assessment	Complete
Distribution	All Staff
Date Amended following initial ratification	June 2021
Implementation Date	June 2021
Planned Review Date	June 2023
Version	3
Author	Senior Governance Manager, Senior Governance Officer, North of England Commissioning Support Unit
Location	S:\Archive\Governance – Active\Policies\

Where this is an update to an existing policy:

Previous policy: CO14 Risk Management Policy

Issue date of previous policy: June 2019

Location of previous policy in policy archive: S:\Archive

Policy Validity Statement
This policy is due for review on the date shown above. After this date, policy and process documents may become invalid.

Policy users should ensure that they are consulting the currently valid version of the documentation.

Accessible Information Standards
If you require this document in an alternative format, such as easy read, large text, braille or an alternative language please contact stynccg.enquiries@nhs.net

Version Control

Version	Release Date	Author	Update comments
V1	28.02.13	Liane Cotterill	Policy provided to Clinical Commissioning Group (CCG) as part of policy suite
V1.1	28.08.14	Debra Elliott	Risk assessment and assessment guidance and associated changes regarding the management of risk including risk appetite. Safeguard Incident Risk Management (SIRMS) Risk Register Standard Operating Procedure (SOP) added.
V2	23.09.15	Debra Elliott	Policy updates & amendments - version 2 See Appendix D
V2 Extension	12/12/17	Debra Elliott	Extension to policy (version 2) Extension requested to enable NHS England Risk Management Policy 2017 Updates to be discussed across NE CCGs with NECS Governance team to promote a common and collective approach to risk reporting and management in line with NHS England guidance
V2.1	20/12/17	Jonathon Millington	Formatting changes and Reference to General Data Protection regulation (GDPR) and updated on best practice recommendations.
V2.2	23/05/17	Wendy Marley	Amended training section following Governance and Assurance Internal Audit report that highlighted that annual training no longer takes place. Removed 'Provider Management' from list of CCG delivery areas. Updated Archiving section to refer to NHS England Records Management Code of Practice for Health and Social Care 2016
V2.3	10/09/2018	Wendy Marley	Appendix A updated consequence descriptors in line with NHS England policy and tailored to South Tyneside CCG's finance limits.
V2.4	01/02/2019	Wendy Marley	Duties and responsibilities expanded following internal audit recommendations that the policy should clarify roles in the CCG's risk management structure.

Version	Release Date	Author	Update comments
V2.5	04/06/2019	Wendy Marley	Amended Audit and Risk Committee risk review cycle.
V2.6	26/06/2019	Liz Durham	New fraud, corruption and bribery wording included. Updated EIA template included. Policy review frequency changed to every two years.
V2.7	April 2021	Wendy Marley	Policy extended for 12 months in light of COVD 19
V3	June 2021	Madeleine Wilkinson	Policy updated to reflect change in risk assessment matrix

Approval

Role	Name	Date
Approval	Audit & Risk Committee	28.08.14 (1.1)
Approval	Audit & Risk Committee	23.09.15 (2)
Approval	Audit & Risk Committee	12/12/17 (2 Extension)
Approval	Audit & Risk Committee	March 2018 (2.1)
Approval	Audit & Risk Committee	May 2018 (2.2)
Approval	Audit & Risk Committee	September 2018 (2.3)
Approval	Audit & Risk Committee	March 2019 (2.4)
Approval	Audit & Risk Committee	June 2019 (2.5)
Approval	Audit & Risk Committee	September 2019 (2.6)
Approval	Virtual Executive Committee	April 2021 (2.7)
Approval	Audit & Risk Committee	June 2021 (3)

Review

This document will be reviewed every two years.

Contents

1. Introduction

For the purposes of this policy, NHS South Tyneside CCG's will be referred to as "the CCG". This policy aims to set out CCG approach to risk and the management of risk in fulfilment of its overall objective to commission high quality and safe services. In addition, the adoption and embedding within the organisation of an effective risk management policy and processes will ensure that the reputation of the CCG is maintained and enhanced, and its resources are used effectively to reform services through innovation, large-scale prevention, improved quality and greater productivity.

1.1 Status

This policy is a corporate policy.

1.2 Purpose and scope

The purpose of this policy is to provide a support document to enable staff to undertake effective identification, assessment, control and action to mitigate or manage the risks affecting the normal business. The policy will:

Set out an organisation wide approach to managing risk, in a simple, straightforward and clear manner the intentions of the CCG for timely, efficient and cost-effective management of risk at all levels within the organisation.

The aims of the Policy are summarised as follows;

- to ensure that risks to the achievement of the CCG's objectives are understood and effectively managed
- support for staff to understand their role and have a consistent approach to risk management
- to ensure that the risks to the quality of services that the organisation commissions from healthcare providers are understood and effectively managed
- to assure the public, patients, staff and partner organisations that the CCG is committed to managing risk appropriately
- to protect the services, staff, reputation and finances of the CCG through the process of early identification of risk, risk assessment, risk control and elimination

The principles are consistent with those within the NHS England's Risk Management Policy and Process Guidance issued January 2015.

This policy applies to all employees and contractors of the CCG. Managers at every level have an objective to ensure that risk management is a fundamental part of the approach to integrated governance. All staff at every level of the organisation are required to recognise that risk management is their personal responsibility.

Independent contractors are responsible for ensuring compliance with relevant legislation and best practice guidelines and for the development and management of their own procedural documents. Independent contractors are required to demonstrate compliance with risk management processes which are compatible with this policy.

2. Definitions

The following terms are used in this document:

- **Risk** is the chance that something will happen that will have an impact on the achievement of the CCG. It is measured in terms of likelihood (frequency or probability of the risk occurring) and consequence (impact or magnitude of the effect of the risk occurring)
- **Risk Appetite** the organisation's unique attitude towards risk taking that in turn dictates the amount of risk that it considers is acceptable
- **Risk Management** is the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects
- **Risk Assessment** is the process for identifying, analysing, evaluating, controlling, monitoring and communicating risk
- **Residual Risk** the risk remaining after the risk response has been applied

Examples of the types of risk that the CCG might encounter and need to mitigate against include:

- **Corporate risks** – operating within powers, fulfilling responsibilities, ensuring accountability to the public, governance issues
- **Clinical risks** – associated with our commissioning responsibilities and including service standards, competencies, complications, equipment, medicines, staffing, patient information
- **Reputational risks** – associated with quality of services, communication with public and staff, patient experience
- **Financial** – associated with achievement of financial targets, commissioning decisions, statutory issues and delivery of the Quality, Innovation, Productivity and Prevention (QIPP) programme
- **Environmental including health and safety** – ensuring the well-being of staff and visitors whilst using our premises

3. Risk Management Framework

3.1 Whenever risks to the achievement of CCG's objectives have been identified, it is important to assess the risk so that appropriate controls are put in place to eliminate the risk or mitigate its effect. To do this, a standard risk matrix is used, details of which are provided at Appendix A CCG Risk Assessment and Escalation Process. The matrix in the assessment guidance is based on current national guidance, but also adapted to suit the CCG risk appetite.

3.2 Using this standardised tool will ensure that risk assessments are undertaken in a consistent manner using agreed definitions and evaluation criteria. This will allow for comparisons to be made between different risk types and for decisions to be made on the resources needed to mitigate the risk.

3.3 Risks are assessed in terms of the **likelihood** of occurrence/re-occurrence and the **consequences** of impact. In order to arrive at an overall risk rating of the residual risk, the risk is rated to take account of the effectiveness of the controls, i.e. whether they are considered to be satisfactory, have some weaknesses or to be weak. This then provides the overall residual risk rating. Once the residual risk rating is determined an action plan identifying further mitigating action is put in place. An overview of five categories of risk (See Appendix A for full details):

- **Extreme 20 - 25** – the consequence of these risks could seriously impact upon the achievement of the organisation's objectives, its financial stability and its reputation. Examples include loss of life, extended cessation or closure of a service, significant harm to a patient(s), loss of stakeholder confidence, failure to meet national targets and loss of financial stability
- **Major 12 - 16** – these are significant risks that require prompt action. With a concerted effort and a challenging action plan, the risks could be realistically reduced within a realistic timescale
- **Moderate 8 - 10** – these risks can be realistically reduced within a realistic timescale through reasonably practical measures, such as reviewing working arrangements, purchase of small pieces of new equipment, raising staff/patient awareness etc. These risks should be managed through the existing line management arrangements
- **Low 1 - 6**– these risks are deemed to be low level or minor risks which can be managed and monitored within the individual department
- **Negligible** – these risks cause minimal or limited harm or concern

3.4 Once the category of risk has been identified, this then needs to be entered onto the CCG's risk register. Please refer to section 3.8 below for further guidance on risk registers.

3.5 Any risk that is identified through the risk assessment process (as well as the incident reporting system) and which the CCG is required legally to report will be reported accordingly to the appropriate statutory body, e.g. Health and Safety Executive or Information Commissioner.

3.6 There are a number of ways in which risks can be managed, including

- **Avoiding the risk** by not undertaking the activity generating the risk
- **Eliminating the risk** where this is possible and cost effective through the use of control measures
- **Reducing the risk** to an acceptable level if it can't be eliminated
- **Transferring the risk** either fully or in part to another body – this may not always be possible where the organisation retains statutory responsibility. Examples of transferred risk would be insurance arrangements, e.g. the NHS Litigation Authority, where the payment of premiums means that in the event of a claim arising it is the NHSLA that bears the financial risk, or through contractual arrangements, partnerships or joint working where there is shared risk etc.
- **Monitoring the risk** but taking no action, particularly where it is a relatively low risk or cannot be eliminated, reduced or transferred.

3.7 **Risk Appetite**

3.7.1 The CCG endeavours to reduce risks to the lowest possible level reasonably practicable. Where risks cannot reasonably be avoided, every effort will be made to mitigate the remaining risk. However there is the recognition that by understanding the organisation's 'risk appetite', this will ensure the CCG supports a varied and diverse approach to commissioning, particularly for practices to work proactively to improve efficiency and value.

3.7.2 Risk appetite is the amount of risk that the organisation is prepared to accept, tolerate or be exposed to at any point in time. It can be influenced by personal experience, political factors and external events. Risks need to be considered in terms of both opportunities and threats and should not be confined to money. They will also invariably impact on the capability of the CCG, its performance and its reputation.

3.7.3 The Governing Body will set boundaries to guide staff on the limits of risk they are able accept to in the pursuit of achieving its organisational objectives. The Governing Body will set these limits annually and review them as appropriate.

3.7.4 The Governing Body will set these limits based on whether the risk is:

- A threat: the level of exposure which is considered acceptable
- An opportunity: what the Governing Body is prepared to put 'at risk' in order to encourage innovation in creating changes

3.8 Risk Register

3.8.1 Current and potential risks are captured in CCG's Risk Registers and include actions and timescales identified to minimise such risks. The risk register is a log of risks that threaten the organisation's success in achieving its aims and objectives and is populated through the risk assessment and evaluation process.

3.8.2 If a risk materialises whilst it is being managed through the risk register, it should be recorded as an incident. Management of risks and incidents through SIRMS is interdependent since risks can be identified through the monitoring of incident themes and trends. If a particular type of incident continues to occur, this is an indication that there is a risk that requires management through the risk register.

3.8.3 If a risk materialises whilst it is being managed through the risk register, it should be considered whether it needs removing from the risk register. Reasons for occurrence should be analysed and evidence established as to whether a trend of similar incidents exists, that need to be managed through the risk register. If the risk is certain to materialise again or has the potential to re-occur, the risk should remain on the risk register for on-going management in order to ensure that underlying causes are addressed. If there is no chance it could happen again, the risk should be closed with an explanation that the incident management process is being followed in order to invoke actions to deal with consequences. A risk materialisation flowchart is attached at Appendix B.

3.8.4 The risk that has materialised should be recorded as an incident in SIRMS and the CCG's incident management process should be followed. See policy CO08 Incident Reporting and Management Policy.

3.8.5 Incident reports are reviewed at the CCG's committees, and this provides an opportunity for themes and trends to be picked up. The Audit and Risk Committee and Governing Body receive a report on a 6 monthly basis about non-clinical incidents. The Quality and Patient Safety Committee receives quality reports about clinical incidents reported by member practices. These reports might indicate that there is a strategic risk e.g. if a lot of practices are regularly reporting incidents around ambulance response times or referral problems. This is the most likely way that risks will be identified from incidents. It is highly unlikely that anything reported by CCG staff will become a risk e.g. information governance or health & safety incidents, although not impossible.

3.8.6 In addition to reports that are provided to the CCG's committees, the clinical quality team will share information with the governance team to allow them to assess whether there may be any risks that require management through the risk register. Information will be shared with the Director of Operations and Head of Corporate Affairs.

3.8.7 The register contains a local record of all current and potential risks for each area or function that the CCG is accountable for, as identified by the appropriate function lead(s). The Registers are updated by Risk Owners on a monthly basis and are reviewed by committees as per the frequencies set out in section 5.3 below.

NECS produce the monthly risk register/exception report the day after deadline for risk register updates if there are any outstanding issues or overdue risks an escalation process is implemented. The escalation process is outlined in Appendix C STCCG Risk register escalation of overdue risks process flow chart.

3.8.8 There is separate guidance which provides further detail and advice on the completion of risk registers, supported by a training programme for the leads involved in their completion. The Safeguard Incident & Risk Management System (SIRMS) Risk Register Standard Operating Procedure can be accessed via the CCGs internet.

4. Duties and Responsibilities

Council of Practices	The Council of Practices has delegated responsibility to the governing body (GB) for setting the strategic context in which organisational process documents are developed, and for establishing a scheme of governance for the formal review and approval of such documents.
Governing Body	The governing body has delegated responsibility from members for setting the strategic context in which organisational process documents are developed, and for establishing a scheme of governance for the formal review and approval of such documents.
Audit and Risk Committee	The audit and risk committee (ARC) has overall responsibility for assuring the governing body that the CCG has an effective system of internal control and risk management in place. The committee reviews the assurance framework and risk management systems and processes, which includes a review of the corporate risk register. It reports annually on its work in support of the annual governance statement, specifically commenting on the fitness for purpose of the governance and assurance arrangements, the extent to which it considers the application of risk management as a discipline to be embedded within the organisation. The ARC has overall responsibility for risk management, including reviewing the risk registers.

Joint Quality and Patient Safety Committee	The principal purpose of the joint quality and patient safety committee (Joint QPSC) is to exercise on behalf of the governing body those functions that are delegated to it in respect of the development, implementation and monitoring of clinical quality, patient safety and safeguarding risks and clinical governance. In particular, by providing assurance on the systems and processes by which the governing body leads, directs and controls its functions in order to achieve the organisation's objectives and ensure the commissioning of high quality, safe patient care.
Chief Officer	The Chief Officer has overall responsibility for the strategic direction and operational management, including ensuring that CCG process documents comply with all legal, statutory and good practice guidance requirements. In accordance with the Scheme of Delegation, the Director of Operations has responsibility for Strategic Risk Management including the Governing Body Assurance Framework.
Director of Operations	The Director of Operations is the Director lead with responsibility for the strategic risk management and will: • ensure the implementation of an effective risk management framework, supporting risk management systems and internal control; • continually promote risk management and demonstrate leadership, involvement and support; • ensure an appropriate committee structure is in place and develop the corporate governance and assurance framework; • ensure all directors and senior leads are aware of their managerial responsibility for risk management.
Head of Corporate Affairs	The operations manager is the lead for risk management and has a responsibility for: • ensuring risk management systems are in place throughout the CCG, co-ordinating risk management in accordance with this policy; • ensuring the assurance framework is regularly reviewed and updated; • ensuring that there is an appropriate external review of the CCG's risk management systems and that these are reported to the governing body; • overseeing the management of risks as identified by the audit and risk committee, ensuring risk action plans are put in place, regularly monitored and implemented; • incorporating risk management as a management technique within the performance management arrangements for the organisation; • ensuring that systems are place for assuring the commissioning of high quality and safe services, and

	the on-going monitoring of the same; • ensure incidents, claims and complaints are and managed used the appropriate procedures.
Senior leads	All senior leads have a responsibility to incorporate risk management within all aspects of their work and are responsible for ensuring the implementation of this policy by: • demonstrating personal involvement and support for the promotion of risk management; • ensuring staff under their management are aware of their risk management responsibilities in relation to this framework; • setting personal objectives for risk management and monitoring their achievement; • ensuring risks are identified, managed and mitigating actions are implemented in functions for which they are accountable; • ensuring a risk register is established and maintained that relates to their area of responsibility, ensuring risks are escalated where they are of a strategic in nature; • ensure incidents, claims and complaints are reported and managed used the appropriate procedures.
All Staff	All staff, including temporary and agency staff, are responsible for: • Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken. • Co-operating with the development and implementation of policies and procedures and as part of their normal duties and responsibilities. • Identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising their line manager accordingly. • Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager. • Attending training / awareness sessions when provided.
NECS	The senior governance manager and senior governance officer will provide risk management support and advice to the CCG as part of a service line agreement.
AuditOne	Manages fraud on behalf of NHS South Tyneside CCG.

5. Implementation

5.1 This policy will be available to all staff for use and be available through the intranet and public websites for the CCG.

5.2 The CCG has adopted a standardised framework for the assessment and analysis of all risks encountered in the organisation and which is set out in this policy. The implementation of this policy is achieved through the completion of the risk register. It is also supported by a detailed reporting structure through its various committees and which are described in the policy. Directors and senior leads will be responsible for ensuring the policy is implemented in their areas of responsibility and compliance with this policy may be monitored through a process of auditing as set out by the Governing Body.

5.3 The Governing Body has overall responsibility for governance, assurance and management of risk. The Governing Body has a duty to assure itself that the organisation has properly identified the risks it faces and that it has processes and controls in place to mitigate those risks and the impact they have on the organisation and its stakeholders. The Governing Body discharges this duty through the Audit and Risk Committee which:

- Identifies risks to achievement of its delivery areas.
- Identifies risks associated with transitional arrangements.
- Monitors these via the Assurance Framework.
- Ensures that there is a structure in place for the effective management of risk through the CCG.
- Approves and reviews risk management policy on a two yearly basis.

Risk registers are updated on a monthly basis and are reviewed as follows:

- Quarterly at **Audit and Risk Committee** (All risks which are EXTREME, HIGH and MODERATE).
- Three times per year by the **Governing Body** (All risks which are EXTREME, HIGH and MODERATE).
- Bi monthly at **Joint Quality and Patient Safety Committee** (quality and safeguarding risks which are EXTREME, HIGH and MODERATE).
- LOW risks are considered at **team level** under the guidance of the relevant Director.

5.4 The CCG will produce and maintain a Governing Body Assurance Framework (AF). The AF forms part of the overall governance arrangements of the CCG and is a key component of the organisation's internal control arrangements. The AF forms a significant part of the assurance given by the Chief Officer in the Annual Governance Statement. It will be prepared at the start of each financial year when the organisation's strategic objectives are known. It should be prepared with the involvement of senior leaders, reviewed by the Audit and Risk Committee. It will also be approved by the Governing Body and reviewed by it at least six monthly.

5.5 The CCG recognise the risk that fraud, bribery and corruption pose to its resources. This risk is included in the corporate (strategic) risk register with an appropriate internal risk owner identified. Operational management and recording of detailed fraud, bribery and corruption risks will be carried out by the CCG's counter fraud provider, AuditOne, as agreed in the counter fraud workplan and using their fraud risk planning tool.

Regular meetings will be held between key CCG staff (i.e. CFO, Head of Corporate Affairs, etc.) and the AuditOne counter fraud specialist to review existing and emerging risks. Regular reports will be provided to the Audit and Assurance Committee to ensure effective executive and non-executive level monitoring of fraud, bribery and corruption risks.

6. Training Implications

The Director of Operations will ensure that the necessary training or education needs and methods required to implement the policy and procedure(s) are identified and resourced or built into the delivery planning process. This may include identification of external training providers or development of an internal training process.

The training required to comply with this policy is key to the successful implementation of this policy and embedding a culture of risk management in the organisation. Through a training and education programme staff will have the opportunity to develop more detailed knowledge and appreciation of the role of risk management. Training and education in risk management will be offered through regular staff induction programmes and a rolling programme of risk management and training programmes.

7. Related Documents

7.1 Other related policy documents

This policy is also supported by the business continuity plan, incident reporting and management policy and health and safety policy.

7.2 Legislation and statutory requirements

The policy has been developed with reference to Department of Health publications and publications of expert bodies on governance and risk management as follows:

- Data Protection Act 2018
- Principles and framework contained in the legislation including:
- Health and Safety at Work Act 1974
- Data Security and Protection toolkit [replaced IG Toolkit]

7.3 Best practice recommendations

- NHS Audit Committee Handbook, 4th edition (2018)
- NHS Governance, 4th edition (2017)
- Building the Assurance Framework: A practical guide for NHS Boards March 2003. Gate log Reference1054
- New Integrated Governance Handbook (2016)
- Intelligent Commissioning Board (2006 & 2009)
- Taking it on Trust – Audit Commission (2009) Institute of Risk Management
- The Healthy NHS Board: principles for good governance (2010)
- Health and Safety Executive guidance
- NHS England's core standards for emergency preparedness, resilience and response

8. Monitoring, Review and Archiving

8.1 Monitoring

The Governing Body will agree a method for monitoring the dissemination and implementation of this policy. Monitoring information will be recorded in the policy database.

8.2 Review

8.2.1 The Governing Body will ensure that this policy document is reviewed in accordance with the timescale specified at the time of approval. No policy or procedure will remain operational for a period exceeding two years without a review taking place.

8.2.2 Staff who become aware of any change which may affect a policy should advise their line manager as soon as possible. The Governing Body will then consider the need to review the policy or procedure outside of the agreed timescale for revision.

8.2.3 For ease of reference for reviewers or approval bodies, changes should be noted in the 'document history' table on the front page of this document.

NB: If the review consists of a change to an appendix or procedure document, approval may be given by the sponsor director and a revised document may be issued. Review to the main body of the policy must always follow the original approval process.

8.3 Archiving

The Governing Body will ensure that archived copies of superseded policy documents are retained in accordance with Records Management: Code of Practice for Health and Social Care 2016.

Appendix A - Risk assessment and escalation process

Step 1: Determine the consequence score

This is offered as guidance when completing a risk assessment, either when an incident has occurred or if the consequence of potential risks is being considered.

Choose the most appropriate domain for the identified risk from the left hand side of the table. Then work along the columns in same row to assess the severity of the risk on the scale of 1 to 5 to determine the consequence score, which is the number given at the top of the column. Note consequence will either be negligible, minor, moderate, major or catastrophic.

Table 1: Consequence score

Impact	1. Very Low	2. Low	3. Moderate	4. High	5. Very High
A. Injury	Minor injury not requiring first aid.	Minor injury or illness, first aid treatment needed.	RIDDOR / Agency reportable.	Major injuries or long-term incapacity / disability.	Death or major permanent incapacity.
B. Patient experience	Unsatisfactory patient experience not directly related to patient care.	Unsatisfactory patient experience – readily resolvable.	Mismanagement of patient care.	Serious mismanagement of patient care.	Totally unsatisfactory patient outcome or experience.
C. Service / business interruption	Loss / interruption>1 hour.	Loss / interruption>8 hours.	Loss / interruption>1 day.	Loss / interruption>1 week.	Prolonged loss of service or facility.
D. Staffing and skill mix	Short term low staffing level temporarily reducing service quality	Ongoing low staffing level reducing service quality.	Late delivery of key objective / service due to lack of staff. Ongoing unsafe staffing	Uncertain delivery of key objective / service due to lack of staff.	Non-delivery of key objective / service due of lack of staff.
E. Financial / asset	Funded/partially funded between £0 and £10k. Unfunded between £0 and £10k	Funded/partially funded between £10k and £50k. Unfunded between £10k and £25k	Funded/partially funded between £50k and £100k. Unfunded between £25k and £50k	Funded/partially funded between £100k and £1m. Unfunded between £50k and £500k	Funded/partially funded over £1m. Unfunded over £500k
F. Inspection / audit	Minor recommendations. Minor noncompliance with standards and/or policies.	Recommendations given. Non-compliance with standards and/or policies.	Reduced rating. Challenging recommendations. Non-compliance with core standards and/or policies.	Enforcement action. Critical report and Low rating. Major noncompliance with core standards and/or policies.	Prosecution. Zero rating Severely critical report.
G. Adverse publicity / reputation	Rumours.	Short term damage with stakeholders Minor effect on staff morale.	Longer term damage with individual stakeholders Significant effect on staff morale.	Widespread stakeholder damage Local media > 3 days	Sustained and widespread stakeholder damage National media > 3 days
H. Data Security and Protection	There is absolute certainty that no adverse effect can arise from the breach	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be: The cancellation of a procedure but does not involve any additional suffering. Disruption to those who need the data to do their job.	An adverse effect may be: Release of confidential information into the public domain leading to embarrassment. Unavailability of information leading to the cancellation of a procedure that has the potential of prolonging suffering but does not lead to a decline in health. Prevention of someone doing their job such as cancelling a procedure that has the potential of prolonging suffering but does not lead to a decline in health.	Potential pain and suffering / financial loss: Reported suffering and decline in health arising from the breach. Some financial detriment occurred. Loss of bank details leading to loss of funds. Loss of employment.	Death / catastrophic event: A person dies or suffers a catastrophic occurrence.

Step 2: Determine the likelihood score

Now determine what is the likelihood of the impact occurring.
The frequency-based score is appropriate in most circumstances and is easier to identify. It should be used whenever it is possible to identify a frequency. The frequency-based score will either be classed as rare, unlikely, possible, likely or almost certain.

Table 2: Likelihood score

Likelihood score	**1**	**2**	**3**	**4**	**5**
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost certain**
Frequency **How often might it/does it happen**	Only occurs in exceptional circumstances, > 5-year period	Could occur at sometime within 1 to 5 years	Could occur in the next 12 months	Will probably occur in the next 6 months	Expected to occur in the next 3 – 6 months

Step 3: Assigning a risk rating

Now apply the consequence and likelihood ratings to give you a risk rating for each of the risks you have identified. Calculate the risk rating by multiplying the consequence by the likelihood: C (consequence) x L (likelihood) = R (risk score)

Table 3: Risk rating = consequence x likelihood (C x L)

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

For grading risk, the scores obtained from the risk matrix are assigned grades as follows:

	1 - 6	Low risk
	8 - 10	Moderate risk
	12 - 16	High risk
	20 - 25	Extreme risk

Step 4: Control measures

Consider the control measures that should be in place to mitigate the risk. Identify and record any gaps in controls.

Step 5: Assessing the effectiveness of control(s)

For each of the risks (and especially extreme and high risks) identify the controls that are in place. For example, in an operational setting and where an incident may have occurred, the controls may take the form of a policy, guideline, procedure or process, etc. For risks that have been identified as preventing achievement of organisational objectives then the control is likely to be a management action plan.

Table 4: Assessing the effectiveness of control(s)

Review the control(s) for each of the risks and apply the following criteria:

Satisfactory:	Controls are strong and operating properly, providing a reasonable level of assurance that objectives are being delivered.
Some Weaknesses:	Some control weaknesses/inefficiencies have been identified. Although these are not considered to present a serious risk exposure, improvements are required to provide reasonable assurance that objectives will be delivered.
Weak:	Controls do not meet any acceptable standard, as many weaknesses/inefficiencies exist. Controls do not provide reasonable assurance that objectives will be achieved.

Step 6: Align the risk to corporate objective/delivery area

The risk should be aligned to the delivery area that it will impact on.
South Tyneside delivery areas are:

1. Performance
2. Finance & QIPP
3. Organisational
4. Quality and Safeguarding

Step 7: Align to objective

The risk should be aligned to the current organisational objective that it will impact on. The CCG's objectives are:

1. Developing and delivering the CCGs key strategic priorities.
2. Making the best use of resources.
3. Improving patient experience and wellbeing
4. Ensuring the CCG is a well-led organisation.

Step 8: Developing an action plan
An action plan must be developed for all risks with a score of 15 or above. However, it is useful to develop an action plan regardless of risk score in order to record progress on control measures and who is responsible for carrying them out.

Step 9: Determine the frequency of review
The frequency of review should also be specified as this will need to be added to SIRMS 'Review Details' section by choosing the appropriate option from the drop down list.

Risk Updates

Risks should be reviewed and updated on a regular basis.

Please follow the guidance below:

- Before entering your update, ensure you have created a new version by clicking on 'New Version'.

- Scroll down to 'Controls and Assurances', click on each control measure in turn and edit to enter the assurance against each control. You will also need to alter the control effectiveness accordingly. You can also enter any new controls. *NB: As long as you have created a new version you can overwrite the assurance from the previous version as this will be archived in the previous version, and will provide an audit trail of progress. This will ensure that only the current position is seen on the printed risk register.*

- Scroll down to 'Action Plan', add any 'New' actions and update any existing actions by clicking on each action in turn and edit to provide an update on progress where possible. *NB: Please ensure you provide your update in the 'Progress' section.*

- Scroll down to 'Review Details', click on 'New' and enter the actual 'Review Date' (you can use the calendar for this). Please also enter the name of the person the risk was 'Reviewed By'. Then, in 'Details of Review' please describe what has been updated, e.g. controls and assurances; action plan; changes to residual risk rating. This section can also be used to highlight where (i.e. which committee) the risk will be discussed and also if closure is recommended.

- Scroll down to 'Residual Risk Rating' and where appropriate enter/amend the residual consequence and likelihood scores. Remember, this should correspond with the 'Risk Level' at the top of the form.

Residual risk rating

This is the consequence and likelihood after the control measures have been applied and actions on the action plan have been implemented. Taking into account the initial risk rating and the assessment of the effectiveness of the control together, you can now assess the residual risk that needs to be managed. The consequence and likelihood ratings should be applied, as in table 3 above.

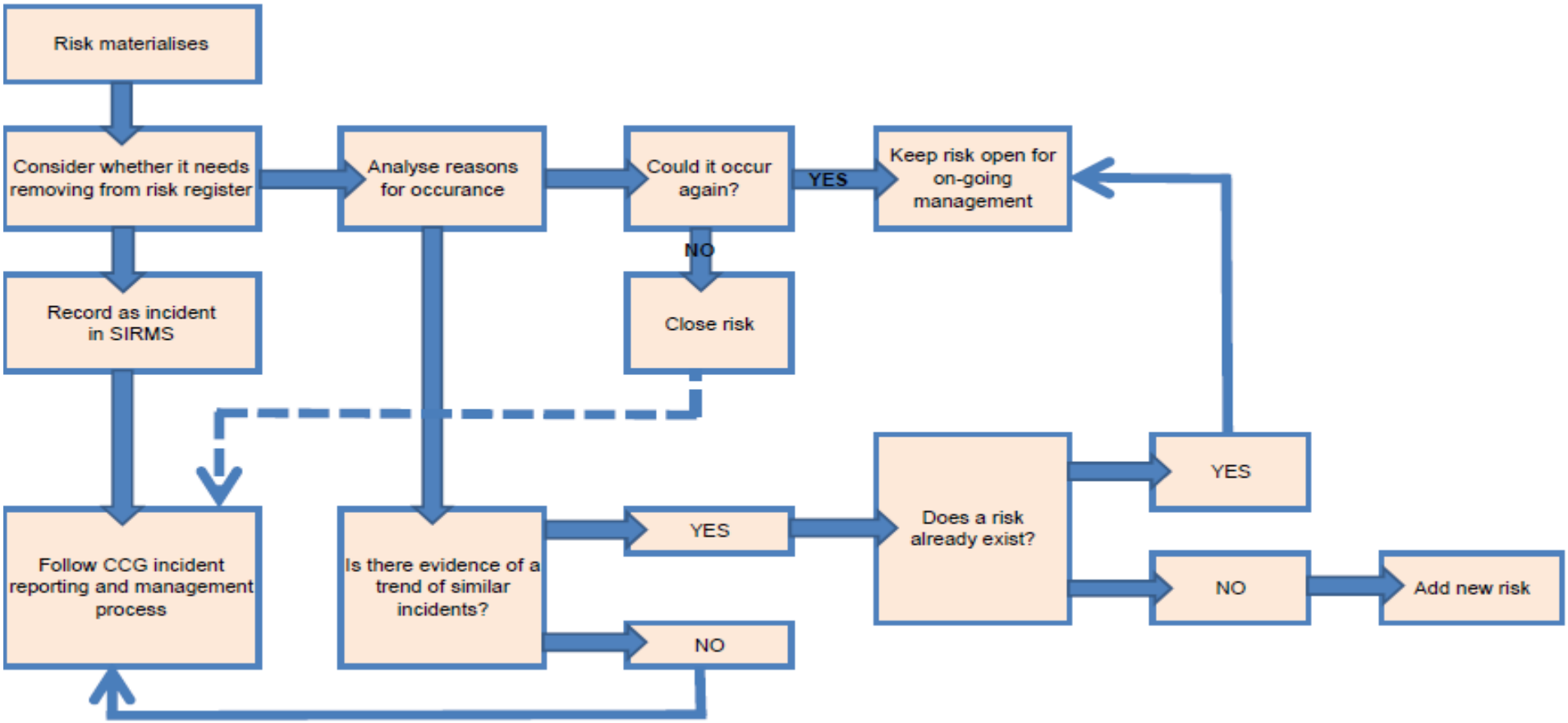
Risk Management Action Guide

Where risks have been identified and scored, then the following escalation arrangements should be used.

The table below provides a suggested action guide for the management of a risk:

Risk Rating	RAG Rating	Action	Level of Authority
20-25	Red	Significant probability that major harm will occur if control measures are not implemented URGENT action required. Director may consider limiting or halting activity	Warrants Chief Officer attention
12-16	Amber	Unacceptable level of risk exposure which requires constant monitoring and controls at Directorate level	Warrants Director attention
8-10	Yellow	Moderate probability of moderate harm if control measures are not implemented. Action in mediate term	Warrants Head of Service/Senior Lead Attention
1-6	Green	The majority of control measures are in place. Harm severity is small. Action may be long term	Warrants manager attention

Appendix B - Risk Materialisation Flowchart



Appendix C - STCCG Risk Register Escalation of Overdue Risks Process Flowchart

NECS produce risk register/exception report the day after deadline for risk register updates

Head of Corporate Affairs will review above to identify any risks with review overdue or missing information

If there are any issues Head of Corporate Affairs to contact risk owners and lead directors to ask that risks are again reviewed and updated with a deadline of two working days

NECS produce a further risk register following day

Risk register reviewed again and any outstanding issues escalated to Director of Operations

Appendix D - Risk Management Policy version June 2021

Updates and Amendments summary

Page & section	Updates & amendments	Reason
p. 7 3.4	**Updated –** Reference to section corrected to 3.8 (previously referred to section 7.7)	Updated following internal audit recommendations.
P. 9 3.8.7	**Updated –** risk register review schedule amended from quarterly to bi-monthly	Updated following internal audit recommendations.
p. 10-12	**Updated –** Duties and Responsibilities section expanded to include roles of: Governing Body, Audit and Risk Committee, Quality and Patient Safety Committee, Director of Operations, Operations Manager, Senior Leads, NECS in risk management structure and hierarchy.	Updated following internal audit recommendations.
p. 12-13 5.3	**Updated -** clarifies role of the Audit and Risk Committee in the implementation of the risk management policy and corrects the frequency of the policy review. Sets out committee responsibility for risk register reviews.	Updated following internal audit recommendations.
p. 14 7.2	**Updated –** references to legislation and statutory requirements	Updated to reflect new Data Protection Act 2018 and new Data Security and Protection Toolkit
p. 13 5.3	**Updated –** frequency of review of risks at Audit and Risk Committee	Amended from bi-monthly to quarterly
p.14 5.5	Counter Fraud update at the request of AuditOne	Requested by AuditOne following release of guidance.
Pg 3, and para 5.3 and 8.2.1	Policy review frequency changed from every three years to two years.	Recommended by NECS as good corporate governance practice and aligned to other CCG's

Appendix E - Equality Impact Assessment

Partners in improving local health

NHS North of England Commissioning Support Unit

Equality Analysis
Initial Screening Assessment

May 2019

Step 1

As a public body organisation we need to ensure that all our strategies, policies, services and functions, both current and proposed have given proper consideration to equality and diversity, do not aid barriers to access or generate discrimination against any protected groups under the Equality Act 2010 (Age, Disability, Gender Reassignment, Pregnancy and Maternity, Race, Religion/Belief, Sex, Sexual Orientation, Marriage and Civil Partnership, Carers and Health Inequalities).

A screening process can help judge relevance and provides a record of both the process and decisions made.

This screening determines relevance for all new and revised strategies, policies, projects, service reviews and functions.

Completed at the earliest opportunity it will help to determine:

- The relevance of proposals and decisions to equality, diversity, cohesion and integration.
- Whether or not equality and diversity is being/has already been considered for due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED).
- Whether or not it is necessary to carry out a full Equality Impact Assessment.

Name(s) and role(s) of person completing this assessment:

Name: Elizabeth Durham
Role: Senior Governance Officer (NECS)

Title of the service/project or policy:

South Tyneside CCG Risk Management Policy

Is this a:

x	Strategy / Policy		Service Review		Project

If other, please specify:

What are the aim(s) and objectives of the service, project or policy:

This policy aims to set out the CCG's approach to risk and the management of risk in fulfilment of its overall objective to commission high quality and safe services

Who will the project/service /policy / decision impact?

Consider the actual and potential impacts:

- [x] Staff
- [ ] service users/patients
- [ ] other public sector organisations
- [ ] voluntary / community groups / trade unions
- [ ] others, please specify:

Questions	Yes	No
Could there be an existing or potential impact on any of the protected characteristic groups?		**No**
Has there been or likely to be any staff/patient/public concerns?		**No**
Could this piece of work affect how our services, commissioning or procurement activities are organised, provided, located and by whom?		**No**
Could this piece of work affect the workforce or employment practices?		**No**
Does the piece of work involve or have an impact on: • Eliminating unlawful discrimination, victimisation and harassment • Advancing equality of opportunity • Fostering good relations		**No**

If you have answered no to the above and conclude that there will not be a detrimental impact on any equality group caused by the proposed policy/project/service change, please state how you have reached that conclusion below:

This is an overarching policy which defines the risk framework (e.g. how to identify, assess and report risks). Separate policies exist which provide more detail how to manage specific types of risk and processes (e.g Health and Safety, Complaints, Safeguarding etc) and these will have more detailed consideration how to manage specific equality and diversity risks.

If you have answered yes to any of the above, please now complete the 'STEP 2 Equality Impact Assessment' document.

Governance, ownership and approval

Please state here who has approved the actions and outcomes of the screening		
Name	**Job title**	**Date**

Publishing

This screening document will act as evidence that due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED) has been given.

If you are not completing 'STEP 2 - Equality Impact Assessment' this screening document will need to be approved and published alongside your documentation.

A copy of all screening documentation should be sent to: **NECSU.Equality@nhs.net** for audit purposes.

If you have any queries in relation to this document or require further guidance please contact: **necsu.equality@nhs.net.**