NHS
Sunderland
Clinical Commissioning Group

Risk Management Policy and Framework

C014

Better health for Sunderland

Contents

Version Control

Version	Significant Changes	Approved by	Date approved	Lead
V1	First issue	Governing Body	24/07/12	D Cornell, CCG
V2	• Risk management policy merged with risk management framework to implement as a single document. • Introduction of low level risk register for monitoring of very low and low risks. • Section 3.6: new section on ways risk can be managed. • Section 37: updated • Section 3.9: new section on assurance framework • Section 4: duties and responsibilities updated • Section 7.3: best practice recommendations updated to include NHS England policies • Appendix 1 updated. • Appendix 2 updated. • Appendix 3 updated.	Quality, safety and risk committee Governing Body	April 2015 May 2015	K Watson, NECS D Cornell, CCG
V2.1	• Section 3.9 added: risk materialisation	Quality, Safety and Risk Committee Governing Body	16 August 2016 27 September 2016	D Cornell D Cornell
V2.2	• References to audit and risk committee and quality and safety committee updated	Governing Body	November 2017	D Cornell

V3	**Section 2.2** Added project risk to examples **Section 4** amended responsible committee sections and re-ordered **Section 6.2** amended details of training, removing reference to annual mandatory training **Section 7.2** updated reference to DPA **Section 7.3** updated Best Practice Recommendations **Section 8.3** updated reference to records management code of practice **Section 9** Removed - section (Equality Impact) and added new format Equality Analysis as Appendix 1 **Appendix 2** previously Appendix 1 – amended diagram **Appendix 3** – previously Appendix 2; removed previous consequence table and added new NHSE domains **Appendix 4** Removed new risk form to reflect guidance in updated standard operating procedure **Appendix 4** new appendix showing escalation/de-escalation of project risks	Audit and Risk Committee	October 2018	D Cornell
V3.1	Section 3.11 – new. Overview of management of fraud, bribery and corruption. Section 4 – AuditOne added to roles and responsibilities Appendix 1 – EIA template changed to current template version.	Audit and Risk Committee	3 September 2019	D Cornell
V3.2	3.2 Categories of risk – categories updated Appendix 3 – table 1 consequence score updated Step 3 – assigning a risk rating matrix updated Step 7 – align to corporate objective – objectives updated Table 5 – risk management action guide updated Appendix 5 – Escalation and de-escalation scores updated, and approval committee changed Section 7 – Documentation updated	Audit and Risk Committee	25 May 2021	D Cornell

1. Introduction

For the purposes of this policy, NHS Sunderland Clinical Commissioning Group will be referred to as 'the CCG'.

This policy and framework (the policy) sets out the CCG's approach to managing risk to ensure it meets 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;
- 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 are 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.

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

2.1 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 CCG objectives. It is measured in terms of likelihood (frequency or probability of the risk occurring) and severity (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.

2.2 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 QIPP programme.
- Environmental including health and safety – ensuring the well-being of staff and visitors whilst using our premises.
- Project risk – the Project Management Office risk management process mirrors the corporate approach. A process is set in place to escalate project risks with a residual risk score of 10 or above to the corporate risk register (see appendix 5).

3. Risk Management Framework

This policy sets out the CCG's risk management framework for how risk management will be implemented throughout the organisation to support the realisation of the strategic objectives.

This includes the processes and procedures adopted by the CCG to identify, assess and appropriately manage risks and detailed roles and responsibilities for risk management.

The CCG's risk management reporting structure is set out in appendix 1.

3.1 Risk assessment

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 2*,* guidance on risk assessment and action.

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.

Risks are assessed in terms of the likelihood of occurrence/re-occurrence and the consequences of impact, using a standardised 5x5 risk matrix (see appendix 2). For each risk that is not adequately controlled, an action plan to reduce or eliminate the risk is required. The implementation of the action plan and residual risk assessment must be kept under review, to assess whether planned actions have reduced or eliminated the risk as expected.

3.2 Categories of risk

There are four categories of risk:

- **extreme** – 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

- **high –** 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.

- **moderate –** 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 through reasonably practical measures, such as reviewing working arrangements, purchase of small pieces of new equipment, raising staff/patient awareness etc.

- **low –** these risks are deemed to be low level or minor risks which can be managed and monitored within the individual department, at operational level. These risks cause minimal or limited harm or concern.

Once the category of risk has been identified, this then needs to be entered onto the CCG's risk register in the Safeguard Incident and Risk Management System (SIRMS). Please refer to section 3.8 below for further guidance on risk registers.

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

3.6 Managing risk

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 if the CCG retains statutory responsibility. An example would be insurance arrangements, e.g. the NHS Litigation Authority, where the payment of premiums means that in the event of a claim arising, the NHSLA bears the financial risk, or through contractual arrangements, partnerships or joint working where there is shared risk.
- **Monitoring of 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

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 organisations 'risk appetite', this will ensure the CCG support a varied and diverse approach to commissioning, particularly for practices to work proactively to improve efficiency and value.

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.

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.

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 registers

The CCG maintains a risk register, which is a management tool used by CCG to provide it an overview of all significant 'live' risks facing the organisation and the action being taken to reduce them. The risks included within the register are varied and cover the entirety of the CCG's activities, from health and safety risks to risks around the delivery of services and achieving financial balance. The register is used by managers to monitor and manage risks at all levels within the organisation.

Current and potential risks are recorded on the risk register 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.

All risks will be managed by the risk management group as part of the director and senior team meetings. The risk management function will be overseen by the audit and risk committee to obtain assurances that there is an effective system operating across the CCG. This approach provides greater focus on moderate and high-level risks which the CCG faces and allows further challenge and scrutiny of actions taken to mitigate risks through the input of all directors and senior team members.

Strategic risks will be monitored by the governing body on a six-monthly basis as part of the governing body assurance framework. In addition, the audit and risk committee will make recommendations to the governing body on any high risks that require a more detailed focus as appropriate.

Risks categorised as low are reported on a low level risk register. Ongoing review and management of these risks will take place on a quarterly basis by the RMG as part of the director and senior team meeting.

A risk register standard operating procedure is available and provides further detail and advice on the completion of risk register in the SIRMS system. This is further supported by a robust training programme for all identified risk leads.

3.9 Risk Materialisation

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.

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 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.

Incident reports are reviewed at the executive and quality and safety committees as appropriate and this provides an opportunity for themes and trends to be picked up. The executive committee receives a report on a quarterly basis about non-clinical incidents and the quality and safety committee receive quality reports about clinical incidents reported by member practices. These reports may 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 and safety incidents, although not impossible.

3.10 Assurance Framework

All government departments, including NHS organisations, are required to provide an annual assurance that they have robust systems in place across their organisation to manage risk. This assurance comes in the form of an annual governance statement[1] (AGS) which must form part of the organisation's statutory accounts and annual report.

[1] Formerly called the Statement on Internal Control

In order to produce an AGS, the governing body must be able to demonstrate that they have been kept properly informed about the risks facing the organisation and has received assurances that these risks are being managed in practice, including that gaps in controls intended to manage risks have been identified and action taken to address them. The governing body will be able to demonstrate that it has met this requirement through the establishment of a robust and formal assurance framework.

Together with this policy and the risk register, the assurance framework is the key document used by the governing body to monitor the position in relation to risk management, providing it with a sound understanding of not only the key risks facing the organisation but also the action being taken to manage and reduce them.

The assurance framework is firmly connected to the organisation's principal objectives as set by the governing body, and is a live document, maintained on an on-going basis by the head of corporate affairs. The assurance framework is monitored by the audit committee and governing body on a six monthly basis.

The assurance framework sets out:

- the organisation's principal objectives;
- any significant risks that may threaten the achievement of those objectives (detailed in the supporting strategic risk register);
- the key controls intended to manage these risks;
- the assurance available to demonstrate that controls are working effectively in practice to manage risks together with the source of that assurance. any areas where there are gaps in controls and/or assurances; and how the organisation plans to take corrective action where gaps have been identified in either controls or the assurances available.

3.11 Fraud, Bribery and Corruption Risks

The CCG recognises the risk that fraud, bribery and corruption can pose to its resources. As a result, a risk has been included on the risk register to reflect this, with an appropriate risk owner and lead 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 work plan and through its fraud risk planning tool.

Regular meetings will be held between key CCG staff (i.e. Chief Finance Officer and Head of Corporate Affairs) and the AuditOne counter fraud specialist to review existing and any emerging risks. Regular reports will be provided to the Audit and Risk Committee as part of the risk register review process and counter fraud updates to ensure effective executive and lay member monitoring of fraud, bribery and corruption risks.

4. Duties and responsibilities

The following table sets out the duties and responsibilities for the CCG:

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.
Chief Officer (as Accountable Officer)	The chief officer, as accountable 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. • ensuring 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; • ensuring an appropriate committee structure is in place and developing the corporate governance and assurance framework; • ensuring all directors and senior leads are appointed with managerial responsibility for risk management.
Chief Finance Officer	The chief finance officer has a responsibility for: • providing expert professional advice to the CCG governing body on the effective, efficient and economic use of the CCG's allocation to remain within that allocation and identify risks to the delivery of required financial targets and duties; • ensuring robust risk management and audit arrangements are in place to make appropriate use of the CCG's financial resources; • ensuring appropriate arrangements are in identify risks and mitigating actions to the delivery of QIPP and resource releasing initiatives; • incorporating risk management as a management technique within the financial performance management arrangements for the organisation;
Head of Corporate Affairs	The head of corporate affairs 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 quality, safety 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.
Audit and Risk Committee (ARC)	The 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.
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 risk 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: • complying 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 • Highlighting any changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising their line manager accordingly, that could impact on this framework • identifying risks in relation to their working environment and role, and take appropriate action to assess them, take action and/or report them to their line manager • identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager

	• attending training / awareness sessions as appropriate.
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 counter fraud activities on behalf of Sunderland CCG.

5. Implementation

5.1 This policy will be available to all staff for use and be available through the intranet and public website for the CCG. It will also be available from the head of corporate affairs, NECS senior governance manager and all line managers.

5.2 All directors and managers are responsible for ensuring that relevant staff within their own teams and directorates have read and understood this document and are competent to carry out their duties in accordance with the procedures described.

5.3 The CCG has adopted a standardised approach for the assessment and analysis of all risks encountered in the organisation and which is set out in this framework. The implementation of this policy is supported through the completion of the risk register and the reporting arrangements to the various committees of the CCG. Directors and senior leads are also responsible for ensuring the policy is implemented in their areas of responsibility and compliance may be monitored through the audit programme set by the governing body.

5.4 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 as follows:

- identifies risks to achievement of its strategic objectives.
- 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 strategies for risk management on an annual basis.
- receives regular reports from the relevant quality and safety committee identifying significant clinical risks and mitigating actions.
- receives regular reports from the relevant quality and safety committee on significant risks to delivering financial balance and the delivery of the quality, innovation, productivity and prevention programme.
- demonstrates leadership, active involvement and support risk management.

6. Training

6.1 The chief officer (supported by the head of corporate affairs) will ensure that the necessary training or education needs and methods needed to implement

this policy and supporting procedure(s)are identified and resourced as required. This may include identification of external training providers or development of an internal training process.

6.2 Regular training is key to the successful implementation of this policy and embedding a culture of risk management in the organisation. Through a robust training and education programme staff will have the opportunity to develop more detailed knowledge and appreciation of the role of risk management.

6.3 Staff are expected to undertake training every two years as a minimum requirement. 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. Documentation

7.1 Other policies

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. Dissemination, monitoring and review and archiving

8.1 Dissemination

8.1.1 The policy will be available to all staff via the CCG's intranet or from the corporate affairs support officer.

8.2 Monitoring and review

8.2.1 The Audit and Risk Committee (on behalf of the governing body) will ensure the policy is reviewed on a bi-annual basis.

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.

Note: 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 head of corporate affairs 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 1 - Equality Analysis

necs 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:

Sunderland 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**

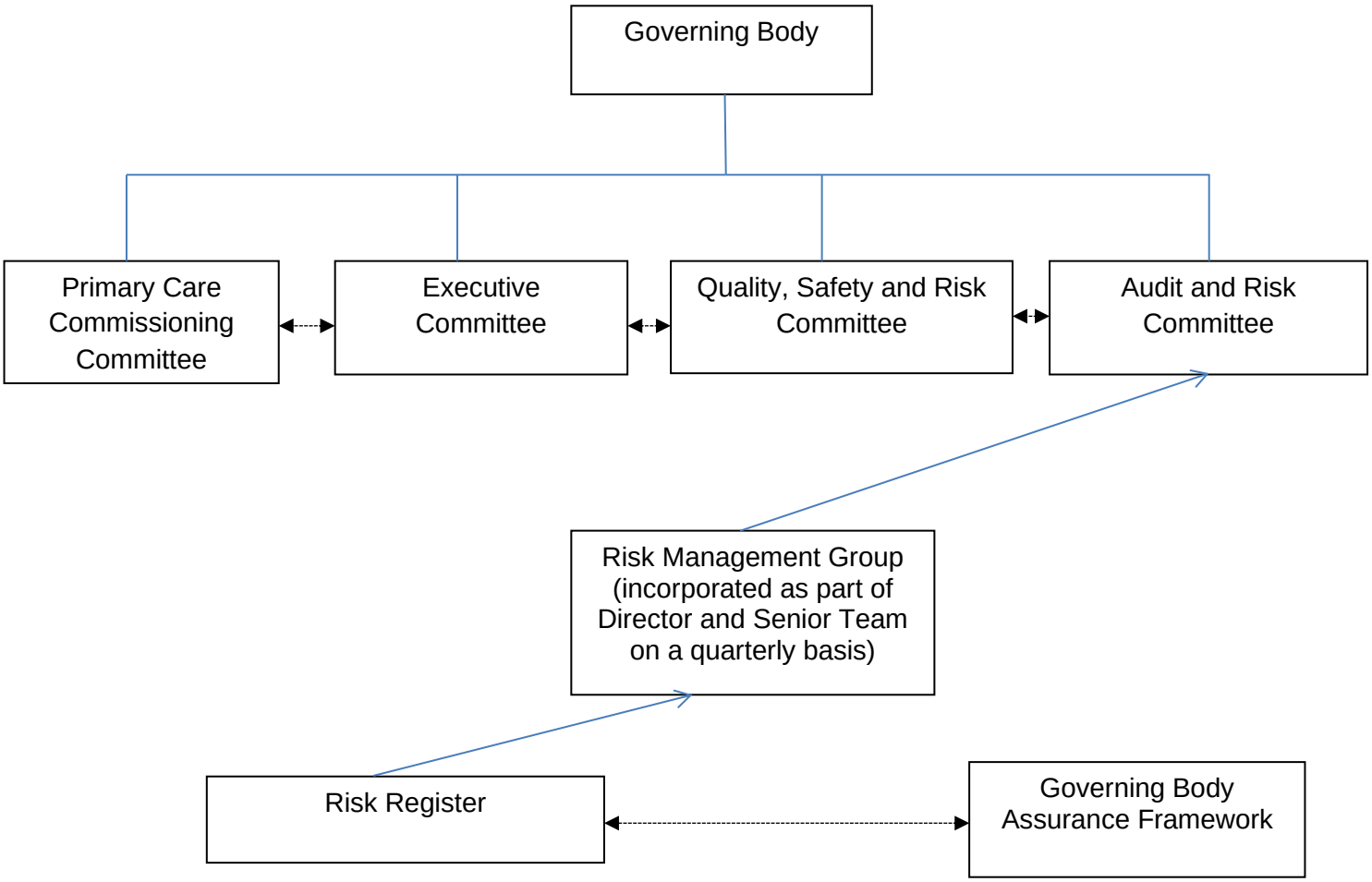
Publishing

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.

Appendix 2 - CCG's Risk Management Reporting Structure



Appendix 3

Guidance for Risk Assessment and Action

1. Risk Assessment

The following steps are intended to help guide staff when undertaking an assessment of a risk.

Step 1: determine the consequence score

Use the tables below 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 to 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 £100k.	Funded / partially funded over £1m. Unfunded over £500k.
F. Inspection / audit	Minor recommendations. Minor noncompliance with standards and/or policies.	Recommendations given. Noncompliance with standards and/or policies.	Reduced rating. Challenging recommendations. Noncompliance 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 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.	An adverse effect may be: Release of confidential information into the public domain leading to embarrassment.	Potential pain and suffering / financial loss: Reported suffering and decline in	Death / catastrophic event. A person dies or suffers a catastrophic occurrence.

		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.	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.	health arising from the breach. Some financial detriment occurred. Loss of bank details leading to loss of employment. Loss of funds.	

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

Table 3: risk assessment matrix, scoring = 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 will be put into 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.

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

Table 4: Assessing the effectiveness of control(s)

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: determine the risk type

The risk type should be specified into one of the following categories:

- strategic
- operational

Step 7: align to corporate objective

The risk should be aligned to the corporate objective it could/will impact on. The CCG's corporate objectives are:

CO1. Develop and support system transformation and ensure a well-led organisation.
CO2. Maintain financial control and performance.
CO3. Maintain and improve the quality of commissioned services.
CO4. Identify and deliver the CCG's strategic priorities
CO5. COVID-19 response and recovery

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: 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.

Step 10: Residual risk rating

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.

Please note: remember when describing to include the risk cause, event and effect. There is a mandatory field within the SIRMS system for you to complete.

Risk cause: As a result of…. (the trigger)

Risk event:	There is a risk that….(what might happen)
Risk effect:	Which will result in….(the impact on the achievement of objectives)

2. Risk management action guide

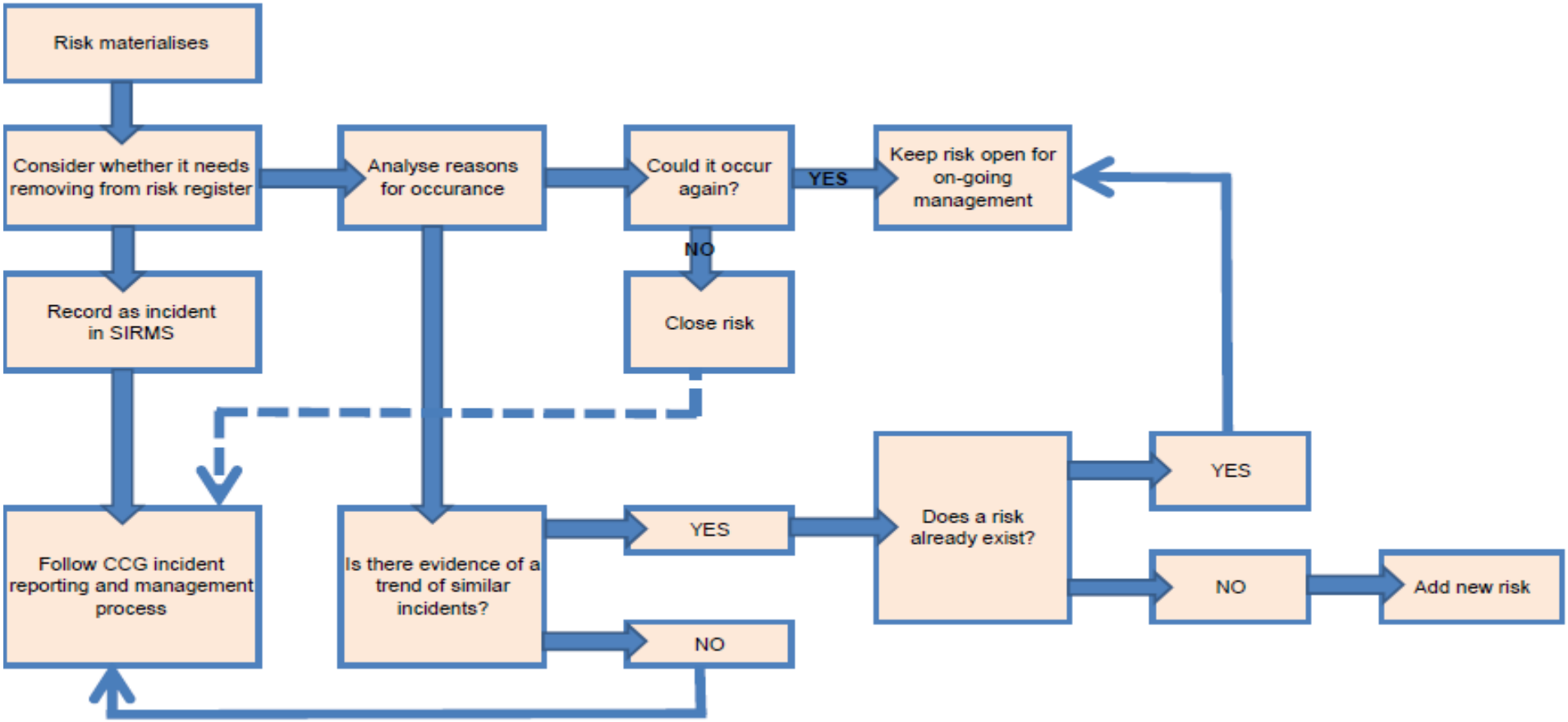
Where risks have been identified and scored, the following escalation arrangements should be used. The table below provides a suggested action guide for the management of a risk.

Table 5: 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 Operating 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 4

Risk Materialisation Flowchart



Appendix 5

Escalation and de-escalation of project risks

To escalate a project risk to the corporate risk register:

Step 1
- PMO and project lead identify risk and rate using the CCG risk matrix

Step 2
- If risk scores 12 or above (residual rating), inform programme lead

Step 3
- Programme lead to review and agree risk rating

Step 4
- If rating still 12 or above, programme lead to raise with Head of Corporate Affairs

Step 5
- Does the risk potentially have an impact on the delivery of the CCG's corporate objectives?

Step 6
- **If yes, programme lead (risk owner) to add to corporate risk register.** The risk will then be managed in line with the corporate risk management process, with updates provided by the project lead.

Step 7
- If no, risk continues to be monitored by the programme lead as part of the project risk register process

To de-escalate a risk from the corporate risk register to project risk register: