Surrey Heartlands CCGs' Joint Risk Management Strategy and Policy

Policy ID	SHCCGS-CORP02
Version	2.0
Owner	Executive Director of Communications and Corporate Affairs for the Surrey Heartlands CCGs
Approving Committee	Surrey Heartlands CCGs' Governing Bodies (following recommendation from Audit Committees)
Date agreed	July 2018
Next review date	July 2019

Working together as the Surrey Heartlands Clinical Commissioning Groups
Guildford and Waverley CCG | North West Surrey CCG | Surrey Downs CCG

Document Control			
Version	2.0	**Version date**	02/08/18
Contact details	Executive Director of Communications and Corporate Affairs for the Surrey Heartlands CCGs		
GPMS	OFFICIAL [Business in Confidence]		

Significant changes since last version			
Version	**Status**	**Who**	**Changes**
1.0	Final	Natasha Moore	Joint Policy written following feedback from the 3 CCGs and also comments incorporated following internal Audit review. Approved by 3 Audit Committees, 3 Governing Bodies in October/ November 2017.
1.1	Draft	Natasha Moore	Amendments reviewed by Audit Committee in Common meeting 20/07/18
2.0	Final	Elaine Newton	Approved by Governing Body meetings in July 2018

Equality statement
Surrey Heartlands Clinical Commissioning Groups aim to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the Human Rights Act 1998 and promotes equal opportunities for all. This document has been assessed to ensure that no-one receives less favourable treatment on grounds of their gender, sexual orientation, marital status, race, religion, age, ethnic origin, nationality, or disability. Members of staff, volunteers or members of the public may request assistance with this policy if they have particular needs. If the person requesting has language difficulties and difficulty in understanding this policy, the use of an interpreter will be considered.

Surrey Heartlands CCGs embrace the six staff pledges in the NHS Constitution. This policy is consistent with these pledges.

Equality analysis
Equality analysis is a way of considering the effect on different groups protected from discrimination by the Equality Act, such as people of different ages. There are two reasons for this:

- to consider if there are any unintended consequences for some groups
- to consider if the policy will be fully effective for all target groups

		Yes, No or N/A	Comments
1.	Does the document/ guidance affect one group less or more favourably than another on the basis of:	No	
	Age Where this is referred to, it refers to a person belonging to a particular age (e.g. 32 year olds) or range of ages (e.g. 18 - 30 year olds).	No	
	Disability A person has a disability if s/he has a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities.	No	
	Gender reassignment The process of transitioning from one gender to another.	No	
	Marriage and civil partnership In England and Wales marriage is no longer restricted to a union between a man and a woman but now includes a marriage between a same-sex couple. Same-sex couples can also have their relationships legally recognised as 'civil partnerships'. Civil partners must not be treated less favourably than married couples (except where permitted by the Equality Act).	No	
	Pregnancy and maternity Pregnancy is the condition of being pregnant or	No	

		Yes, No or N/A	Comments
	expecting a baby. Maternity refers to the period after the birth and is linked to maternity leave in the employment context. In the non- work context, protection against maternity discrimination is for 26 weeks after giving birth and this includes treating a woman unfavourably because she is breastfeeding.		
	Race Refers to the protected characteristic of Race. It refers to a group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins	No	
	Religion and belief Religion has the meaning usually given to it but belief includes religious and philosophical beliefs including lack of belief (e.g. Atheism). Generally, a belief should affect your life choices or the way you live for it to be included in the definition.	No	
	Sexual orientation Whether a person's sexual attraction is towards their own sex, the opposite sex or to both sexes	No	
2.	Is there any evidence that some groups are affected differently?	No	
3.	If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?	No	
4.	Is the impact of the document/guidance likely to be negative?	No	
5.	If so, can the impact be avoided?	N/A	
6.	What alternative is there to achieving the document/guidance without the impact?	N/A	
7.	Can we reduce the impact by taking different action?	N/A	

For advice in respect of answering the above questions, please contact Executive Director for Comms and Corporate Affairs for the Surrey Heartlands CCGs. If you have identified a potential discriminatory impact of this procedural document, please contact as above.

Names and Organisation of Individuals who carried out the Assessment	Date of the Assessment
Natasha Moore, Governance Manager	01/09/17

Executive Summary

This strategy sets out Surrey Heartlands CCGs' approach to identification, assessment, treatment and monitoring of risk, which enables informed management decisions within Surrey Heartlands CCGs. The policy covers all staff engaged in the business of Guildford and Waverley CCG, North West Surrey CCG and Surrey Downs CCG.

The policy defines what it means by risk and risk management, as well as levels of risks as follows:

System	Risks to the **organisations' functions/ strategic risks** are noted on the **Governing Body Assurance Framework** (GBAF) and are those that will usually be **pan year.**)
Local	**Operational risks** are those that affect the **day-to-day business** of the CCGs and are more likely to close in year. These are noted on the Corporate Risk Register and primarily managed by Joint Executive Team.
Project	**Project/ service are risks** are the subject of **local risk registers** and managed **within the project framework**.

The **risk appetite statement**, outlined in 3.7.2, drives the organisation's strategic objectives/ operational responses and gives Management clear expectations on how the Governing Bodies feel risks should be managed. There may be valid reasons for setting a level of tolerance outside the scope of the statement of risk appetite and where a risk score sits out of this range, the risk commentary of how effective the controls and assurances are for that risk will be detailed. This will allow the Governing Bodies to focus on the risks that are outside of the risk tolerance when reporting.

Risk tolerance is outlined with **tolerance levels being linked to outcomes** and themes, with each tolerance level having an associated target score range (see 3.7.7). This is to be reviewed on an annual basis and propose any changes to the Governing Bodies. Target scores will be recorded on the operational risk management system. An **example risk is used throughout** the policy to help readers apply concepts outlined.

Roles/ Responsibilities

Roles and responsibilities are outlined with the **Joint Accountable Officer having overall accountability** and responsibility for the management of risk across the Surrey Heartlands CCGs. **Executive Directors** within the Joint Executive Team have **delegated responsibility** for risk management within their areas but with **all staff having responsibility for identifying risks** within their areas of work and taking appropriate action to assess and manage risks and/ or report them to their line manager.

The policy also outlines responsibility for **partnership working** and governance between organisations, with the **relevant partnership lead taking responsibility** for ensuring that relevant risks are identified and follow the risk management process. **Risk Owners** need

to ensure that any **risks identified are shared** and are noted on risk registers of all organisations with a stakeholder interact/ impact.

Process and Approach to Risk Management

Section 6 of the policy outlines 6 stages to managing risks:

- **Step 1- Identify risk**- Risks can be identified from a variety of sources in the context of joint working and should be described so that anyone reading can understand. The risk management system will provide an opportunity for risks to be identified as being Surrey Heartlands CCG-wide or relating to a specific CCG.

- **Step 2- Analyse/ Score risks**- The grading matrix (outlined in appendix 3) gives equal weighting to consequence and likelihood of the risk. The inherent, current and target scores for a risk are recorded on the operational risk management system and it is expected that where there is a gap between current and target score, actions will be specified to close this gap. Once a risk has met target score, the risk can be recommended for closure by the relevant committee/ board.

- **Step 3- Assess risks**- Risk Handlers must review progress, design and adequacy; and Owners should assess overall effectiveness of controls. The 'three lines of defence' model should be adopted to assess nature of assurances and to identify any gaps.

- **Step 4- Take action**- The most appropriate treatment option for a risk will be selected using the 'Four Ts' methodology (see 6.7) and will be recorded on the operational risk management system by the Risk Handler. Once an option has been chosen, actions will be assigned to a risk. Once these have been completed, they may be assigned as controls and assessed for their effectiveness.

- **Step 5- Monitoring and Reviewing of Risks**- There will be a cycle of risk review where all risks are reviewed by the Risk Handler and Owner in line with Audit Committee and Governing Body meeting dates. Where the current risk remains higher than its target score, this process is repeated until the risk is either eliminated or reduced to its target.

- **Step 6- Communicate and Consult**- Specific training for risk management will be provided for the Governing Bodies at least every two years, with specific training provided to Risk Owners and Handlers in the use of the operational risk management system and principles of risk. Focused training is provided to teams as required.

Contents

1 Introduction

Purpose of the strategy and policy

1.1 This strategy sets out Surrey Heartlands CCGs' approach to strategic management of risk and the supporting infrastructure which enables informed management decisions in the identification, assessment, treatment and monitoring of risk.

1.2 Surrey Heartlands CCGs are committed to making risk management a core organisational and collaborative process and believe that good risk management will not only provide a safer environment, better care and ensure safety of patients but will also help fulfil their corporate and shared objectives in the short and longer term. They acknowledge that commissioning the delivery of health services carries inherent risk; however, managing these risks effectively can bring benefits and opportunities.

1.3 Surrey Heartlands CCGs also recognise the importance of involving local stakeholders in their risk management processes and of working in partnership to identify, prioritise and control shared risks. It is paramount that a culture of openness and transparency is promoted and upheld so that risks can be effectively managed.

1.4 The **aim of this strategy** is to establish and maintain a framework for risk management which:

1.4.1 Integrates risk management across the CCGs and embeds practices into the day-to-day operation of the CCGs, ensuring sophisticated analysis of risk including understanding interdependencies and impact of risks being realised. This ensures that all Governing Body members and staff understand their risk management responsibilities through training and development.

1.4.2 Sets out a process for monitoring, reporting and updating risks across the CCGs based on best practice, national guidance and compliance with the Care Quality Commission (CQC) Standard's commissioner responsibilities.

1.4.3 Ensures that operational risk management system have the confidence of the Audit Committees and provides assurance to the Head of Internal Audit in framing the Annual Audit Opinion. This will assist the Governing Bodies in agreeing their Annual Governance Statements[1].

[1] Mandated Department of Health Annual Reporting processes as set out in the annually updated Department of Health Manual of Accounts

2 Scope

2.1 This strategy and policy provides an overarching framework for the management of risk within Surrey Heartlands CCGs to include Guildford and Waverley CCG, North West Surrey CCG and Surrey Downs CCG.

2.2 It applies across all parts of the organisations and includes all staff, Governing Body members and persons engaged in business on behalf of Surrey Heartlands CCGs, including those employed by other organisations and/ or working on behalf of Surrey Heartlands CCGs.

2.3 It covers risks identified at project, local and system-wide levels areas across all levels of the CCGs' activities.

3 Principles of the strategy

Definitions:

3.1 What is risk?

3.1.1 Risk is the possibility that loss or harm will arise from a given situation. This encompasses anything from the possibility of injury to an individual, patient or member of staff, to anything which impacts upon the CCGs' ability to fulfil its aims and objectives.

3.2 What is an issue?

3.2.1 An issue is something that has already happened, was unplanned and requires immediate management action. Ultimately, risks are different to issues.

3.3 What is risk management?

3.3.1 The process by which an organisation identifies and assesses risks, proposes controls and agreed actions which are then undertaken.

3.3.2 It is defined as a proactive approach to the:

- identification of risks;
- analysis and assessment of the likelihood and consequence of risks;
- treating those risks where mitigating actions, controls and are implemented with the aim to eliminate the risk; and
- tolerating risks that cannot be eliminated by reducing their likelihood or consequence to an acceptable level through an action plan

3.4 Issues management

3.4.1 Staff within each CCG should follow their own CCG process for managing issues. This policy exclusively focuses on risks and risk management.

3.5 This Risk Management Strategy and Policy will use the following example risk throughout the document to help readers apply concepts outlined:

3.5.1 "If the CCG does not have effective Health and Safety measures in place, then it will breach its statutory requirement to keep staff safe."

3.6 The strategy identifies three levels of risk (see section 6.4 for further details):

System Risks to the **organisations' functions/ strategic risks** are noted on the **Governing Body Assurance Framework** (GBAF) and are those that will usually be **pan year** and are **overarching** of those risks on the Corporate Risk Register (CRR).

Local **Operational risks** are those that affect the **day-to-day business** of the CCGs and are more likely to close in year. These are noted on the CRR and primarily managed by Joint Executive Team.

Project **Project/ service are risks** are the subject of **local risk registers** and managed **within the project framework**.

3.6.1 In the example of our Health and Safety risk (see 3.5.1), this would fall under an Operational risk as it affects the day-to-day business of the CCGs and is likely to be closed in year. Therefore this would be primarily managed by Joint Executive Team and be reported in the CRR.

3.7 Risk appetite and tolerance

What is risk appetite?

3.7.1 Risk appetite can be defined as "the amount and type of risk that an organisation is willing to take in order to meet their strategic objectives. Organisations will have different risk appetites depending on their sector, culture and objectives. A range of appetites exist for different risks and these may change over time"[2].

3.7.2 Risk appetite statement

- Surrey Heartlands CCGs are committed to the active management of risk within services they commission, seeking to minimise risks wherever possible to service users, staff, and members of the public.

[2] https://www.theirm.org/knowledge-and-resources/thought-leadership/risk-appetite-and-tolerance/

- The CCGs are committed to establishing an organisational culture that ensures risk management is an integral part of everything we do. This will be enabled and supported by a comprehensive system of internal controls aligned to management systems, corporate planning, clinically-led commissioning strategy development and objective setting, to assure the Governing Bodies that the CCGs are doing their *reasonable best* to protect their stakeholders against all kinds of risks.

- The CCGs recognise that it is sometimes necessary to take risks in order to achieve objectives and deliver beneficial outcomes to stakeholders. The CCGs must, however, take risks in a controlled manner, ensuring the long-term benefits outweigh any short-term losses and reduce exposure to a level deemed acceptable by the Governing Bodies and the statutory framework in which they operate.

- As a general principle the CCGs will seek to control all risks and minimise to a low risk level those which have the potential to:
  - Compromise patient safety, experience or clinical effectiveness;
  - Cause significant harm to staff, visitors and other stakeholders;
  - Compromise severely the reputation of the CCGs;
  - Have financial consequences that could endanger the CCGs' viability;
  - Jeopardise significantly the CCGs' ability to carry out their core purpose;
  - Threaten the CCGs' compliance with law and regulation or the delivery of good governance, including fraud, regulatory and governance breaches which should be mitigated to low risk level.

3.7.3 In the example of our Health and Safety risk (see 3.5.1), as per the Risk appetite statement, this risk would be minimised to a low level risk and it has the potential to cause harm to staff, visitors or other stakeholders.

3.7.4 The risk appetite statement drives both the organisation's strategic objectives and its operational responses in given situations. It gives the Executive and senior management clear expectations on how the Governing Bodies feel risks should be managed and contributes to a clear culture for the continuous management of risk across the organisation.

3.7.5 No statement of risk appetite can encompass every eventuality and there may be exceptions which mean that the CCGs have valid reasons for setting a level of tolerance outside the scope of the statement of risk appetite. Where a risk score sits out of this range, the risk commentary should reflect how effective the controls and assurances are for that risk will be detailed

along with the movement of the risk. This will allow the Governing Bodies to focus on the risks that are outside of the risk tolerance when reporting.

What is risk tolerance?

3.7.6 Risk tolerance is the amount of risk which is judged to be justifiable and is the amount of risk that any organisation is prepared to tolerate or be exposed to at any one point in time. Each risk tolerance level correspondences to outcomes and target score ranges. The expected target score for a risk supporting these outcomes should fall within the corresponding range. This target score will be recorded on the operational risk management system.

3.7.7 If a risk supports more than one of the below outcomes, the Risk Owner will determine the target score. The list below is not exhaustive.

Risk level	Supporting what outcomes?	Expected target score range:
Low risk tolerance	• Mitigation of unsafe services • Safe patient care • Serious incident avoidance • Long-term financial sustainability • Nationally defined expectations or regulatory compliance • Continued confidence of the public in the CCG • Health and Safety • Maintenance of critical systems	1-4
Moderate risk tolerance	• Stakeholder collaboration • In-year financial balance • Good workforce strategy and organisational change • Patient safety awaiting or following national direction	5-8
High risk tolerance	• Maintenance of non-critical systems • Decision making processes that may require reputation management • Effective management of delegated functions	9- 12
Significant risk tolerance	• Taking carefully described financial and clinical risks for long term benefit	15-20

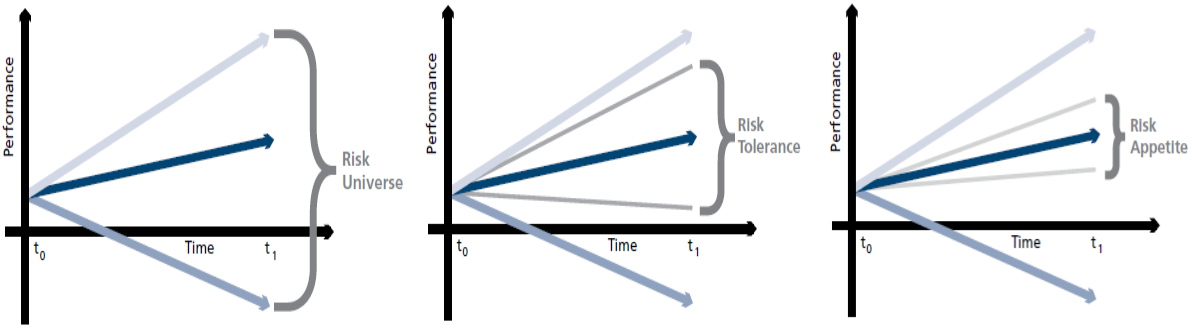
3.5.8 Using the above risk targets, our Health and Safety risk (see 3.5.1) would have a target score of between 1-4 within the 'low risk tolerance' range.

3.5.9 The Governing Bodies will define and agree on risk appetite and tolerance for the CCGs so staff can work with the confidence of knowing the parameters in which they can work.

What is the difference between risk appetite and risk tolerance?

3.5.10 The diagrams below (taken from the Institute of Risk Management[3]) illustrate the differences between:

- all the risks that the organisation might face (the 'Risk Universe');
- risks that, if a situation should present, might be tolerable (the 'Risk Tolerance'); and
- those risks that they actively wish to engage with (the 'Risk Appetite').



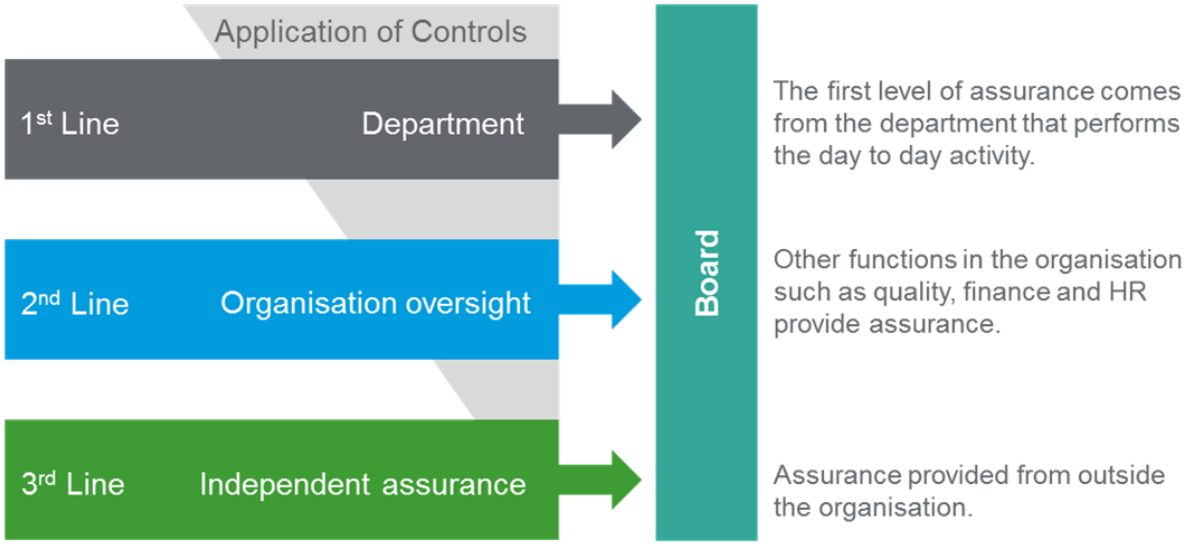
3.5.11 In practice, risk tolerance is the level of risk that the CCGs could accept whereas the risk appetite is the total level of risk that the CCGs could bear given their risk profile, i.e. their capacity, with consideration given to their longer term strategy of what they need to achieve and the resources available to do this.

3.5.12 Using the Health and Safety risk (see 3.5.1) as an example, the CCGs are mindful of the legislative requirements and their long-term capacity but ultimately the safety of staff is imperative. Therefore, using the principles of appetite and tolerance, the CCGs' appetite for this risk is smaller than risk tolerance windows as illustrated in the graphs in section 3.5.10.

3.6 Surrey Heartlands CCGs will have in place an assurance framework based on a **'three lines of defence' model** as table. This will be reported via the risks registers and will provide the committees and Governing Bodies with assurance on the effectiveness of the CCGs' risk management framework.

[3] Institute of Risk Management publication: 'Risk Appetite and Tolerance: Executive Summary'. Available via: https://www.theirm.org/knowledge-and-resources/thought-leadership/risk-appetite-and-tolerance.aspx

3.6.1 The diagram below distinguishes between 1st, 2nd and 3rd line lines of assurances.



3.6.2 Examples of the lines of defence could include the below:

Nature of Assurance	Definition	Examples
1st Line	Inter-departmental direct assurance from 'day-to-day' activity	• direct management monitoring • local management controls • financial regulations • contract standing orders • performance data • Key performance indicators (KPIs)
2nd Line	Risk assurance from other organisational mechanisms for reporting and monitoring	• compliance & legal mechanisms • corporate risk management • Equality Analysis • Internal Audit Review
3rd Line	Independent/ external assurance	• External Audit Review • External Inspectorate • NHS England assurance

3.6.3 In practice, the CCGs should aim to have assurance for the Health and Safety risk (see 3.5.1) in place based on this 'three lines of defence' model with front line/ business operations; corporate governance oversight; and third party review assurances all being in place. Any gaps should be noted under 'gaps in assurances' and can be targeted for future work, for example, indicate areas for future audits.

4. Legislative Framework/ Core Standards

4.1 The Surrey Heartlands CCGs' approach to risk management will be developed in line with good practice and the following legislative and regulatory requirements:

4.1.1 The National Health Service Litigation Authority administers the Clinical Negligence Scheme for Trusts and Risk Pooling Scheme for Trusts. This is used as a benchmark for good practice.

4.1.2 NHS England (NHSE), co-ordinates the reporting of and learning from adverse events occurring in the NHS. The CCGs will report all serious incidents to NHSE following good practice guidance from NHSE and promote and monitor compliance with Safety Alerts.

4.1.3 The Care Quality Commission (CQC) is the independent regulator of health and social care in England. CQC regulates care provided by the NHS, local authorities, private companies and voluntary organisations, with the aim of ensuring that better care is provided for everyone. Through assessment of their registration status, achievement of national priorities and quality of financial management, the Commission provides a quality rating for all NHS organisations. Providers' compliance with the Commission's registration requirements will be one of the means by which the CCGs assures themselves that high quality healthcare is being provided.

4.1.4 The Health and Safety Executive's (HSE) role is to protect people against health and safety risks arising out of work activities. The HSE achieves this by providing information and advice, promoting training and good practice, inspection, investigation and enforcement. The CCGs report all staff Health and Safety incidents to the HSE via the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR) reporting tool, which have resulted in an over three day absence from work. Assurance regarding the Health & Safety systems and processes in place in all contracted services will be sought to ensure patient, public, Governing Body member and staff safety remain a high priority when looking to commission services.

4.1.5 Information Governance (IG) and Cyber Security related incidents and near misses are reported in accordance with local reporting procedures as approved by the CCGs' Information Governance Sub Committee. Serious IG and Cyber Security related incidents will be handled in accordance with the Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation which is available from the NHS Digital website. Any serious IG or Cyber Security related incidents will be reported to the Information Commissioner's Office and NHS Digital via the NHS Information Governance Toolkit.

5 Roles and Responsibilities

5.1 Surrey Heartlands CCGs Governing Bodies

5.1.1 Ensure that the CCGs have:

- an effective risk management strategy and policy to best support their key aims;
- an effective risk management system in place; and
- an adequate risk management capacity, i.e. risk team, systems in place and staff training and development.
- They will also agree the risk tolerance for the organisation.

5.1.2 Seek assurance that the risk management strategy and policy is working effectively through their own activities, including development of systems and processes for financial and organisational control, clinical and information governance and risk management.

5.1.3 Receive regular reports on risk and using these registers, they will:

- consider the risks on the Governing Body Assurance Framework (GBAF) and assess how they have been identified, evaluated and managed;
- assess the effectiveness of the related system of internal control in managing the risks, having regard, in particular, to any significant failings or weakness in internal control that have been reported;
- have an informed consideration of risk which underpins the CCGs' organisational strategy, decision making and allocation of resources;
- consider whether necessary actions are being taken promptly to remedy any significant failings or weaknesses;
- consider whether the findings indicate a need for more extensive monitoring of the system of internal control; and
- escalate risks to the member practices as required.

5.1.4 The Governing Bodies will also be able to indicate the 'scope' of risks that they wish to review alongside GBAF risks, for example, risks that have not changed in current score over a certain period of time, risks with a current score above a specified threshold, risks that have increased in current score value since the last reporting period etc.

5.1.5 The operation of Governing Bodies are underpinned by the following internal controls:

- Governing Body Assurance Framework (GBAF);
- Corporate risk register (CRR);
- Audit Committee (responsible for review of internal controls system and risk management system through review of work of sub committees); and
- Annual Governance Statement. (The Governing Bodies are required to

approve Annual Governance Statements[4], for sign off by the Joint Accountable Officer, which provides assurance that each part of the organisation is doing its reasonable best to manage the CCGs' affairs efficiently and effectively through the implementation of internal controls to manage risk.)

5.2 Committees of the Governing Bodies

5.2.1 A key component of an effective GBAF is a clearly defined structure that makes explicit the scheme of delegation and clearly identifies the line of reporting. Appendix 1 shows the relationship with risks and the committee structure of each Surrey Heartlands CCG.

5.2.2 The committees are responsible for:

- Responsible for identifying, assessing and putting systems in place to mitigate any risks to the achievement of corporate objectives and to ensure these are managed through the Risk Registers.
- Will demonstrate commitment to board assurance through their endorsements and implementation of the GBAF, receiving regular updates as and when appropriate.
- Ensure that the terms of reference for the established committees references the requirement to consider risk and their mitigation and escalate as appropriate.

5.3 Joint Accountable Officer

5.3.1 Has overall accountability and responsibility for the management of risk across the Surrey Heartlands CCGs and is responsible for:

- Continually promoting risk management and demonstrating leadership, involvement and support.
- Ensuring an appropriate committee and reporting structure is in place to manage risk.
- Defining the duties of staff in relation to risk management.
- Ensuring appropriate procedural documents are embedded.
- Ensuring that Complaints; Claims; and Health and Safety Management inform the risk management process.

5.4 Joint Executive Team

5.4.1 Will review the risk registers ahead of Audit Committee and Governing Body meetings but discharges the responsibilities for day-to-day operational management of Surrey Heartlands CCGs' risks

5.4.2 Will ensure organisation-wide coordination and prioritisation of risk management issues. They will monitor in detail as often as required, individual high level risks including action plans and controls. This also includes ensuring that relevant staff within their organisation regularly attends

[4] part of the mandated Department of Health Annual Reporting processes as set out in the annually updated Department of Health Manual of Accounts

risk training as specified by the Risk Team.

5.5 Chief Finance Officer

5.5.1 Has delegated responsibility for financial risk management and will ensure:

- There are arrangements in place to identify risks associated with finance and performance, the mitigation measures necessary to control the risk and to monitor these measures.
- The effectiveness of the CCGs financial control systems.
- The Audit Committees and internal audit effectively perform their roles in assuring the CCGs system of internal control.
- Robust Counter Fraud and Local Security Management arrangements are in place.
- Ensuring that there is appropriate review of the CCGs' risk management system via internal audit and that these are reported to the Audit Committee.

5.6 Executive Director of Quality

5.6.1 Has delegated responsibility for clinical and quality risk management including:

- Ensuring that there are arrangements in place to identify, mitigate and monitor risks associated with clinical care and treatment within the CCGs commissioned services, this includes (but not exclusively), patient safety regarding commissioned services in line with local and national legislation and guidance.
- Managing and overseeing the performance management of serious incidents reported by the providers of health services commissioned by the CCGs.

5.7 Executive Director of Communications and Corporate Affairs

5.7.1 Is the executive management lead for risk management with delegated responsibility for ensuring that:

- Risk management systems are in place throughout the CCGs;
- risk registers present a balanced, accurate and representative reflection of the risk profile of the organisation;
- relevant emergency planning related risks, including input from the Community Risk Register, are identified through risk management processes in the organisation's risk register as required by the Civil Contingencies Act 2004[5];
- the Governing Body and its committees receive reports on the risk registers;
- timely and robust review of all risks takes place in line with the CCGs' requirements; and
- the Risk Management Strategy and Policy is updated on an annual basis and approved by the CCG Governing Bodies.

[5] The Surrey Community Risk Register takes into account risk identified in the National Risk Register that is owned by the Cabinet Office.

5.8 Executive Director of Strategic Commissioning

5.8.1 Has delegated responsibility for risks relating to strategic commissioning and is responsible for:

- Ensuring there are arrangements in place to identify risks associated with finance and performance, the mitigation measures necessary to control the risk and to monitor these measures.

5.9 CCG Managing Directors

5.9.1 Responsible for identifying and managing risks relevant to their locality and relevant local partnerships.

5.9.2 They are accountable for effective management of risk within their areas of responsibility.

5.10 Deputy Directors and Associate Directors

5.10.1 Operationally responsible for ensuring effective structures and systems for managing risks exist within their teams, departments and functional areas and for taking this policy into consideration in all areas of subsequent delegation and line management.

5.11 Risk Owners and Handlers

5.11.1 Risk Owners are accountable for the effective management of risk within their area of responsibility, ensuring that they are regularly reviewed and updated. They should delegate a senior member of staff to ensure that all their owned risks are reviewed and approved in the event of their absence.

5.11.2 Where a Risk Owner is not an Executive Director, they are responsible for maintaining oversight of risks and must advise the relevant Executive Director of any significant change to risks between cycles who will determine which committees will require an exception risk report having considered the causes and implications of any change in the risk rating.

5.11.3 Risk Handlers are responsible for identifying, assessing and mitigating risk and entering these onto the risk management system. They must ensure the monitoring of any identified and appropriate risk management control measures within their designated areas and scope of responsibility. In situations where high risks have been identified and where local control measures are considered inadequate, Risk Handlers are responsible for bringing these risks to the attention of the Risk Owner.

5.11.4 Risk Owners and Handlers must be of an appropriate level as stated below to ensure the appropriate level of management and oversight:

Risk Type	Owner	Handler
GBAF	Executive Director or Deputy Director	At least at Associate Director level

CRR	Executive Director, Deputy Director or Associate Director	Nominated person within the team
Project	Project Sponsor	Project Lead

5.11.5 It is recommended that different members of staff are allocated as the Handler and Owner for risks to ensure an additional level of oversight. However, in exceptional circumstances it is acknowledged that this may to be possible for project risks, for example the Project Sponsor may also be the Lead.

5.11.6 Risk Owners and Handlers must regularly attend risk training as specified by the Risk Team.

5.12 Risk System Champions

5.12.1 A Risk System Champion will be identified within each Team or Department by the appropriate senior manager. The Risk System Champion will:

- Receive additional specialist training on the operation risk management system;
- Support the relevant Risk Handlers in reviewing and updating risks;
- Be a point of contact where required between the Risk Administrator and their team; and
- Support their team/ directorate in reviewing their relevant risks at team meetings as required, including providing risk registers from the system for discussion.

5.13 All Staff

5.13.1 Have an individual responsibility for:

- Co-operating with managers in order to achieve the objectives of this policy and are accountable for their own working practice and behaviour. This is implicit in all contracts of employment.
- Identifying risks within their area of work and taking appropriate action to assess and manage such risks and/ or report them to their line manager.
- Contractors, voluntary and agency staff working for the CCG should ensure that any risks they identify are communicated to their relevant contract relationship manager who must then assess any risk that has been identified or reported to them and take action to mitigate where necessary.
- Maintaining safe working practices (in the case of clinical staff this requirement includes safe clinical practice in diagnosis and treatment).
- Being aware of their duty under legislation to take reasonable care of their own safety, the safety of others and of any emergency procedures relevant to their role and place of work, e.g. resuscitation, evacuation and fire precaution procedures.
- Attending training and development events to ensure a full understanding of their risk management responsibilities. Line managers are to provide adequate opportunities for staff attendance at risk management training

programmes, and effectiveness of risk management in appraisals.

5.14 Managers responsible for Contracts and Procurement

5.14.1 Ensuring that services commissioned by the CCGs are in line with best practice and national guidance and ensuring that assurance is provided to the CCGs on services commissioned.

5.14.2 Ensuring risk assessments are conducted and when awarding contracts for services and that risks and plans to mitigate them are assessed during the tender process. Providers must give adequate assurance that they manage risk appropriately.

5.14.3 Responsible for risks around procurement compliance.

5.15 Risk Management Team

5.15.1 Act as administrator for the operational risk management system and provide expert advice and training to staff and the CCGs on the operational risk management system.

5.16 Health and Safety

5.16.1 Health and Safety input is co-ordinated through the responsible manager. The CCGs will source specialist support and advice regarding Health and Safety risks as required.

5.17 Commissioning support for hosted services

5.17.1 CCGs may host services on behalf of other organisations; e.g. Individual Funding Requests (IFR), Continuing Health Care (CHC), Medicines Management. CCGs will use disputes procedures if there are issues with agreeing the level or impact of risk in any given situation with services provided to include on their risk register which is mutually acceptable.

5.18 Partnership working and governance between organisations

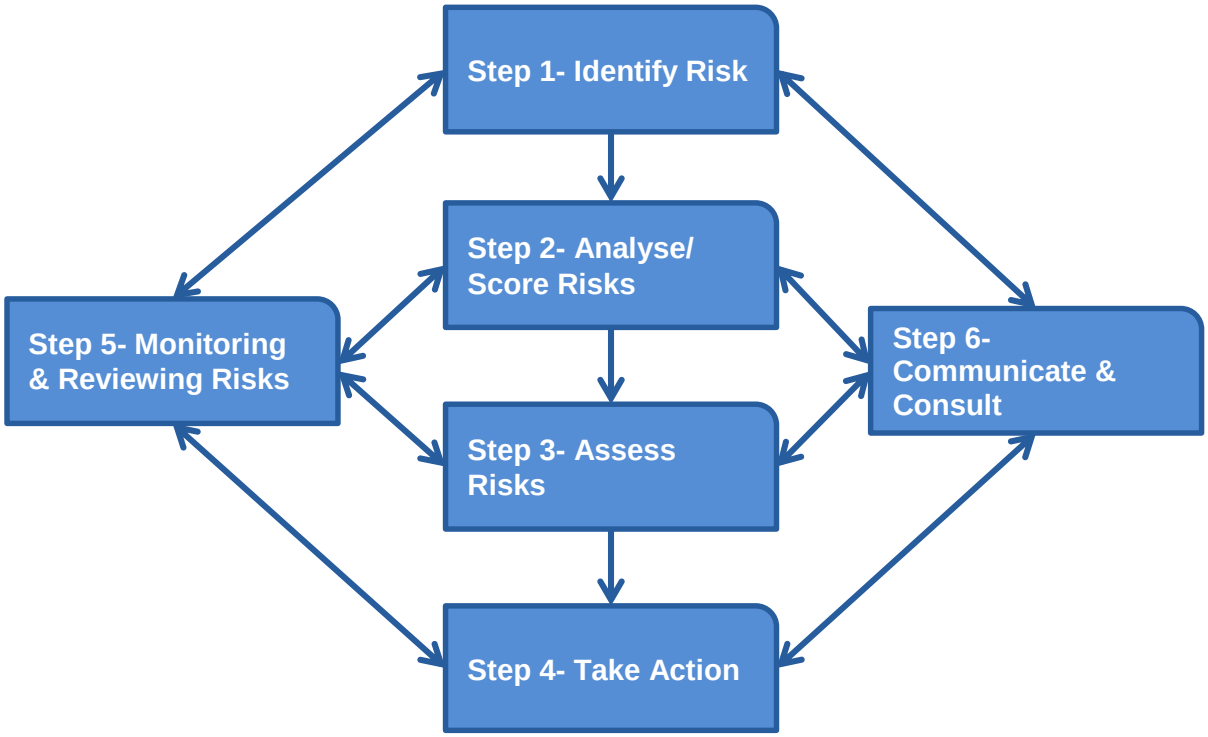
5.18.1 The CCGs work closely with key stakeholders around areas of identified risk and there are a number of joint structures that exist between agencies. It is often at the interface between organisations that the highest risks exist and clarity about responsibilities and accountabilities for those risks are most difficult to ascertain. Only by working closely and collaboratively with a wide range of partner organisations can these risks be identified and properly managed.

5.18.2 Given the collaborative and complex nature of commissioning, with lead and associate commissioner roles for specific areas, the CCGs will endeavour to involve partner organisations in all aspects of risk management as appropriate. Risk Handlers and Owners need to ensure that any risks identified are shared and noted on risk registers of all organisations with a stakeholder interest or impact. The Partnership Lead will take responsibility for ensuring that relevant risks are identified and follow the risk management

process (see section 6). The operational risk management system will provide a platform to identify risks as being Surrey Heartlands CCG-wide or only relating to one CCG. This should be reviewed in line with the risk management process.

6 Process and approach to Risk Management

6.1 This widely accepted model provides a generic approach for identifying, prioritising and dealing with risks in any situation – whether at local or corporate level. There are 6 stages to managing risk in this model (see below).



6.2 At the core of the risk management process is the CCGs' operational risk management system. This is the repository for all risk information and the management tool through which risk registers are produced to enable the organisation to understand its comprehensive risk profile.

6.3 Each stage of the risk management process should be documented by Risk Handlers on the operational risk management system in order to:

- Demonstrate the process is conducted properly;
- Provide evidence of systematic approach;
- Provide a record of risk and to develop the CCGs' knowledge of risk;
- Provide relevant decision makers with a risk management plan for approval;
- Provide an accountability mechanism and tool;
- Facilitate review and monitoring;
- Provide an audit trail; and
- Share and communicate information.

6.4 Step 1- Identify Risk

- Risk identification sets out to identify the exposure to uncertainty and should be approached in a methodical way to ensure that all significant activities within the CCGs have been identified and the risks flowing from these activities defined.

- Risks can be identified from a variety of sources, including those below outlining sources for potential risk identification. This may include:
  - Internal, external, past and future
  - Simple trigger lists
  - Objectives, targets and plans
  - Standards frameworks (NHS Resolution, Essential Standards of Quality and Safety)
  - Professional guidance
  - Care guidelines and standards
  - Process mapping, patient journey, care pathway
  - Literature
  - Own experience and knowledge
  - Complaints
  - Incidents

- The risk should be described so that anyone reading the description can understand it and should be framed in a way that clearly defines the cause and the effect, e.g. 'If…then…'. The source of the risk should also be identified on the operational risk management system, i.e. where the risk has arisen from.

- Risks should also be identified in the context of joint working across Surrey Heartlands and the risk management systems will provide an opportunity for risks to be identified as being Surrey Heartlands CCG-wide or relating to a specific CCG. These can either be GBAF or CRR risks.

- The Risk Handler should identify whether the risk should be noted on the GBAF, the CRR or whether the risk relates to a project/ programme.

System	**Risk to the organisations' functions/ strategic risks are noted on the Governing Body Assurance Framework (GBAF).**	• The GBAF is a report to the Governing Body about the effectiveness of the organisation's system of internal control and will form the key document for the Governing Body in ensuring all significant risks are controlled, that the effectiveness of these key controls has been assured and that there is sufficient evidence to support the Annual Governance Statement. • The GBAF includes risks that will be normally pan year, i.e. unlikely to be closed in year (although not all GBAF will be pan-year).

		• GBAF risks may have 'component' CRR risks sitting underneath on the CRR. • GBAF risks are reported to the Governing Bodies and other Governing Bodies Committees as appropriate. • GBAF risks can only be closed with the approval of the relevant Audit Committee (subject to the target score being reached and all associated actions marked as closed).
Local	**Operational risks are noted on the Corporate Risk Register (CRR).**	• The CRR is a vehicle for risks to be captured and reported. These risks affect the day-to-day business of the CCGs and are more likely to close in year. • These risks should be primarily managed by the Joint Executive Team but are reported to Governing Body, by exception, if they have a current score of 15 or above. All CRR risks are reported to Audit Committees. • CRR risks can be closed subsequent to local control by the Risk Owner (subject to the target score being reached and all associated actions complete).
Project	**Project/ programme/ team risks**	• Project or programme risks are the subject of local risk registers and managed within the project or programme framework. • These are not routinely reported on the GBAF or CRR but are escalated as appropriate either through the Joint Executive Team, relevant Committee with the remit for monitoring and assurance or through the relevant programme board. • Projects relating to a particular team would also fall in to this category.

- How do GBAF and CRR risks relate to each other?
  - Risks on the GBAF will have a more overarching significance than the more operational risks that sit on the CRR. Therefore, if the current score of a risk on the CRR changes, a review of the related GBAF risk, if applicable, will be undertaken by the Risk Handler. This may affect the current score of the GBAF risk and should be reflected in the risk commentary.

  - Risk Handlers and Owners should examine risk holistically and understood that a change in rating of one risk, may impact on another. Any impact should be

recorded and reflected accordingly.

- An increase or decrease in risk score above or below a certain threshold would not mean a change in risk type. For example, there may be risks on the GBAF with a 'low' score, such as below 10. Likewise, there may be 'higher' rated risks on the CRR.

- The Risk Handlers should undertake an equality impact assessment to identify if the risk impacts on any of the protected characteristics.

6.5 Step 2- Analyse/ Score Risks

- Surrey Heartlands CCGs use the NPSA (National Patient Safety Agency) 5x5 risk grading matrix (see appendix 2) giving equal weighting to both the consequence and the likelihood of the risk. This risk tool provides both a qualitative and quantitative analysis of the risk and is used to assess the severity of the risk for all events.

- When a risk is first assessed, the following risk scores are recorded on the operational risk management system:

Inherent score	Current score	Target score
Risk without any controls or mitigations. This does not change and shows how dangerous a risk might be without mitigating actions or controls implemented.	Risk with controls applied and planned actions. In many cases, there will be existing controls already in place which reduce the likelihood of risks, such as policies and procedures, monitoring and reporting mechanisms and audits. This is updated when controls or mitigations change.	The target score of the risk (based on section 3.7) and will reflect the associated risk tolerance. When a risk reaches target score, it is expected that it be put forward for closure (provided that all actions have been completed.).

- If there is a gap between the current and target rating, it is expected that actions will be specified with a view to closing the gap between the current and target ratings.

- If a risk has met its target score and all associated actions are marked as closed, the risk can either be recommended for closure by Audit Committee if noted on the GBAF or closed locally by the Risk Owner if noted on CRR. If a risk has met its target score but cannot be closed, the commentary should reflect this position and explain the reasons for the risk not being recommended for closure. Any closed risks will be noted on the next relevant risk report.

- The rating of risks enables them to be prioritised and ensures that risks are brought to the attention of the most appropriate staff, i.e. the highest risks are notified at the most senior management level.

- Reducing a risk may have an adverse impact on another aspect of the CCGs' business, prevent the taking up of an important opportunity or stifle innovation. The risk prioritisation must consider these broader considerations. For this reason, the responsibility for prioritising risks lies at Governing Body, committee and executive level.

6.6 Step 3- Assess Risks

- An agreed risk is one which has been accepted after proper evaluation and is one where appropriate controls have been implemented. For a risk to be identified it will be:
    - Identified and entered on the operational risk management systems;
    - analysed in the context of the current controls in place;
    - an expected date for target score to be reached;
    - escalated to the appropriate level of management for action; and
    - actions planned recorded to reduce the risk and then kept under review.

<u>Controls and gaps in controls</u>

- Controls are measures or systems that are currently in place to mitigate either the likelihood or consequence of risk.

- As an example, a well phrased control will not only state what is in place, but when it was approved and by whom.

- Gaps in controls, or in other words what more can be done to mitigate the risk, should also be recorded on the operational risk management system.

- The effectiveness of controls should reflect not just their ability to manage a risk but also their actual effectiveness in terms of their consistent, complete, reliable and timely operation. An effectiveness rating for controls will be recorded on the operational risk management system. The effectiveness of controls will be assessed by Risk Owners reviewing the input from handlers and periodically reviewing the effectiveness of controls over time.

<u>Assurances and gaps in assurances</u>

- The 'three lines of defence' model will be adopted to assess the nature of assurances and to identify any gaps (see section 3.6.1).
- All assurances should be within the last financial year.
- Any gaps in assurances should also be identified, i.e. what more evidence do we need that systems and process in place are effective. For example, no 3rd line of defence assurances. Associated actions may aim to fill any gaps.

6.7 Step 4- Take Action

- The most appropriate treatment option will be selected for the management of each risk using the 'Four Ts' methodology, The Four Ts are four fundamental choices in relation to dealing with individual risks and are designed to help to bring current scores within target range as defined by the appropriate tolerance (see 3.7).

- The 'T' choice will be recorded on the operational risk management system by the Risk Handler and reviewed and approved by the risk.

Treat

- Treat (or in other words mitigate) is in practice the most common response, achieved by taking action to reduce either the consequence or likelihood of the risk.
- This enables the organisation to continue with the activity/ objective but with controls and actions in place to maintain the risk at an acceptable level.

Transfer

- This option is normally taken to transfer a financial risk or pass the risk to an insurer.
- Although there is also the opportunity to agree to transfer risks to a partner organisation in a joint project, it is important that all parties are clear to the exact extent of each partner's liability and responsibility for the risk.

Tolerate

- It may be appropriate to tolerate the risk without any further action for example due to either a limited ability to mitigate the risk or the cost of mitigation may be disproportionate to the benefit gained.
- The decision to tolerate would ideally be supported by a contingency plan to prevent the risk escalating.
- The risk may reach a "tolerate" level having been "treated" through an action plan that identifies a target risk score.
- If the risk cannot be tolerated, the Risk Owner must identify a target risk score and set out the actions that will be taken to achieve the agreed level of tolerance.

Terminate

- Some risks can only be managed by terminating the activity. However the capacity to address risks in the NHS in this way is limited (although it may apply to some projects that are no longer considered viable due to the resources required to manage the risks being disproportionate to the potential outcomes or benefits). An example would be terminating a contract that is unsafe or unsustainable.
- The decision to terminate may close the original risk but may mean that other more manageable or strategically acceptable risks have to then be described and managed in the short-term.

- It may be that more than one option could be applied to a risk to reduce its score; however the Risk Owner will decide which approach is taken.

- The approach taken will be recorded on the relevant risk register and the risk's controls will follow this approach.

Actions

- Once the options have been considered and the most appropriate way forward identified, a risk action plan will be drawn up with the aim to bring the risk score down to meet target level.
- Actions are a specific process that once completed, will help to bring the risk down to target score and therefore within its tolerance range and will be recorded on the operational risk management system and implemented along with an action owner identified with a deadline for completion.
- Once actions have been completed, they may be assigned as controls and will be assessed for their effectiveness.

6.8 Step 5- Monitoring & Reviewing Risks

- All risks, including development of controls and completion of actions, will be reviewed at least bi-monthly and reported in line with the cycle of meetings for the committees and Governing Bodies. Risk cycles will be set by the Risk Team and Risk Handlers and Owners will be required to review and approve their risk(s) by the given deadline. This will enable the preparation of risk reports to meet committee deadlines.

- Where the current risk remains outside the risk tolerance set by the Governing Body, the risk management process will be repeated until the risk is either eliminated or reduced to an acceptable level (see section 3.5.8). This does not detract from the responsibility of directorates to continually assess, manage and mitigate their risks and ensure that the process of escalating any issues to Joint Executive Team is followed to ensure that key persons are informed and involved appropriately and that the organisation is maintaining good risk management practices.

- Reporting of complaints/ patient experience and incidents (including information governance) will be reported through delegated authority from Governing Bodies to the Quality Committees. An annual complaints report will also be presented to the Governing Bodies.

- The Audit Committees may review specific risks through a deep dive report over a given timeline to track progress of risks and in doing so whether controls have had the outcome that was intended.

Risk Commentary

- Alongside each risk review, commentary should be noted on the operational risk management system which should reflect the 'gap' between current and target scores. The commentary should include:
  - A summary of the 'risk trend', e.g. if the risk score has increased, decreased or remained the same since last reporting cycle and reasons for this;
  - How effective the current controls and assurances in place are;
  - What more can be done to bring the current score down to target through future work planned, i.e. the 'journey' that the risk still has to go on to reach its target score;
  - Future work/ actions planned; and
  - If the risk target score is out of appetite (see section 3.7), then rationale for this.

Risk statues

- During review, the risk status should be reviewed and categorised as follows. A risk may not occupy all these statuses in sequence, nor may it occupy every status during a risk cycle.

Risk Status	Action/ definition
In holding area, awaiting review	Risk has been logged on the operational risk management system.
Being reviewed	Additional information has been included by the Risk Handler and risk awaiting review by Risk Owner.
Approved by owner	Risk has been reviewed and approved by the Risk Owner.
Proposed for closure	Once risk has met its target score and all actions are closed, Risk Handler can put the risk forward for closure.
Closed	When a risk is approved for closure.
Rejected	Occasionally a risk may be added to the system erroneously, e.g. if it is a duplicate risk, is an issue etc.

Closure of risks

- If after review a risk has met the target score and all associated actions have been closed, then the risk can be put forward for closure.

- The Risk Handler should indicate if a risk should be proposed for closure on the operational risk management system, which the Risk Owner should review.

- If the Risk Owner is in agreement, the risk commentary should reflect why the risk can be closed to provide assurance to the relevant committee(s) and Governing

Bodies. They should then action as follows:

GBAF	CRR	Project
• GBAF risks can be proposed for closure by the Risk Owner and approved by the Audit Committee at the next meeting. • Once in agreement, the risk can then be noted as closed on the operational risk management system, noting Audit Committee approval. • These risks will be noted at the next Governing Body meeting as having closed since the last meeting subject to Audit Committee agreement.	• Risks noted on the CRR can be closed subject to local control by the Risk Owner and should be marked as such on the operational risk management system. • However, the closure of these risks would be noted at the next Audit Committee meeting and Governing Body meeting as having closed since the last meeting.	• Project risks can be closed subject to local control by the Risk Owner and should be marked as such on the operational risk management system.

- It may be that in exceptional circumstances a risk has met target score but is not yet being proposed for closure. In these cases, the risk commentary should reflect why the risk is not being put forward for closure and what controls or mitigations need to be in place for it then be closed.

- Alternatively, in exceptional circumstances a risk may be put forward for closure before it has met target score, for example, if a risk has been realised earlier than expected. In these situations, the risk commentary must reflect the circumstances by which this risk should be closed prior to it having reached target score. Following this risk having been realised, it may be that additional new risks should be raised to reflect the change in situation; if so, the risk commentary should reference these new risks.

6.9 Step 6- Communicate & Consult

- Effective implementation of the strategy requires staff to be both aware of Surrey Heartlands CCGs' approach to risk management and to be clear about their roles and responsibilities within the process.

- Specific training in risk management will be provided for the Governing Bodies at least every two years.

- Focused training will be provided to teams and groups of staff which could include workshops.

- Specific training will be provided to Risk Owners and Handlers in the use of the CCGs' operational risk management systems and the wider principles of risk management and how they are applied within the CCGs.

- Support and guidance will be given to all staff to implement the strategy. To support the implementation of the strategy, risk management must be incorporated into the performance objectives for all staff on an annual basis and part of the induction programme for all new staff.

7 Monitoring and review of effectiveness

7.1 This Strategy and Policy will be available to all staff, the public and other stakeholders on the Surrey Heartlands CCGs' websites and will be communicated to all staff.

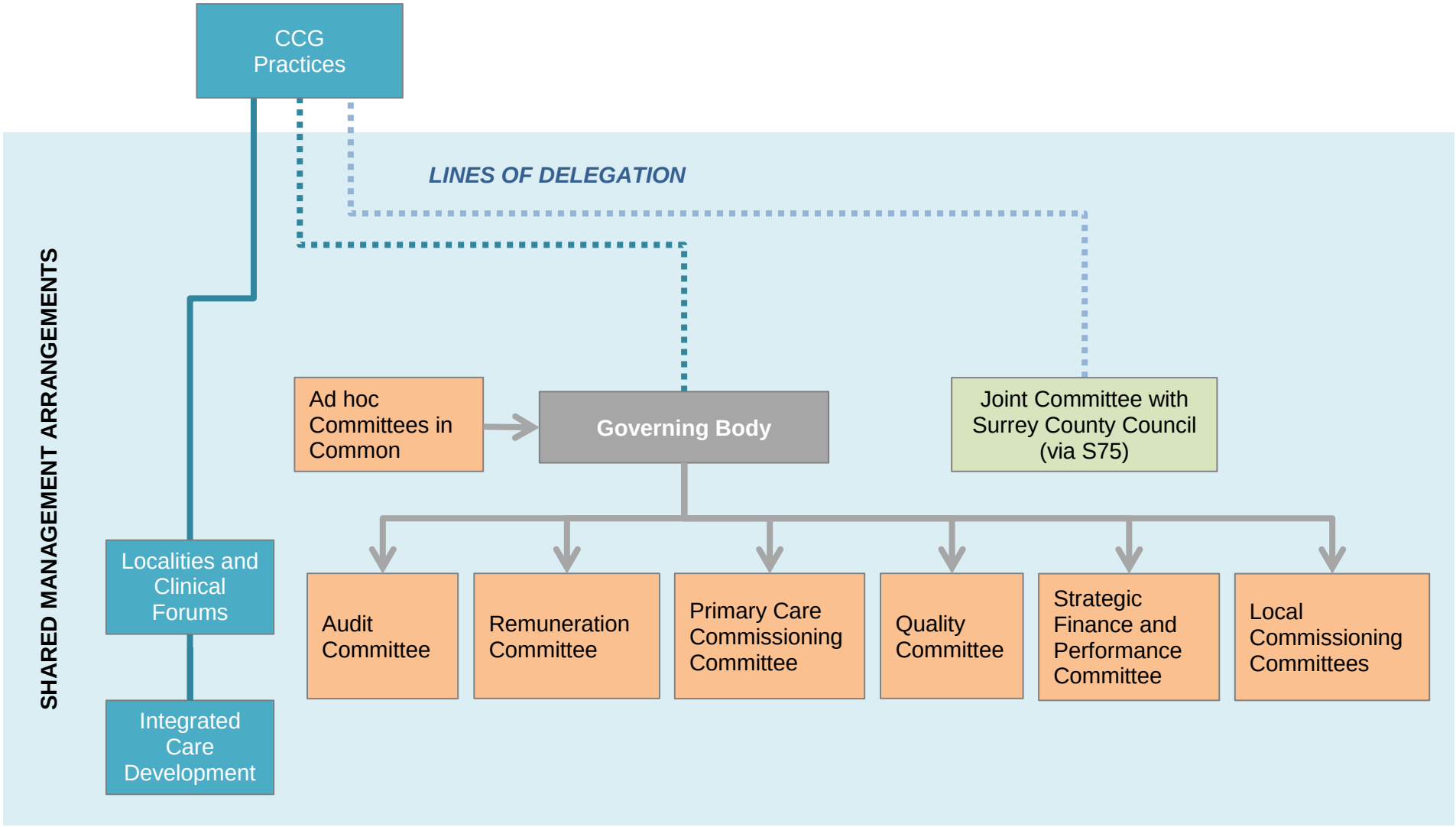
7.2 Please see Appendix 1 for Joint Governance and Committees in Common arrangements for Surrey Heartlands CCGs.

7.3 Review of the policy

7.3.1 The Audit Committees may include reviewing the effectiveness of the strategy as a part of the internal audit plan.

7.3.2 This Strategy and Policy will be reviewed annually by the Audit Committees and approved by the Governing Bodies and more frequently where circumstances demand, e.g. when procedural, legislative or best practice changes arise.

Appendix 1: Governance arrangements for Surrey Heartlands CCGs



Appendix 2: Risk Matrix & Scoring Methodology

These tables have been taken from the National Patient Safety Agency[6] and have been adapted for Surrey Heartlands CCGs' use.

Table 1: Consequence (C) score (severity levels) and examples of descriptors

Domains	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
Impact on the safety of patients, staff or public (physical/ psychological harm)	Minimal injury requiring no/ minimal intervention or treatment. No time off work	Minor injury or illness, requiring minor intervention Requiring time off work for >3 days Increase in length of hospital stay by 1-3 days	Moderate injury requiring professional intervention Requiring time off work for 4-14 days Increase in length of hospital stay by 4-15 days RIDDOR/ agency reportable incident An event which impacts on a small number of patients	Major injury leading to long-term incapacity/ disability Requiring time off work for >14 days Increase in length of hospital stay by >15 days Mismanagement of patient care with long-term effects	Incident leading to death Multiple permanent injuries or irreversible health effects An event which impacts on a large number of patients
Quality/ complaints/ audit	Peripheral element of treatment or service suboptimal Informal complaint/ inquiry	Overall treatment or service suboptimal Formal complaint stage 1 Local resolution Single failure to meet internal standards Minor implications for patient safety if unresolved Reduced performance rating if unresolved	Treatment or service has significantly reduced effectiveness Formal complaint stage 2 Local resolution (with potential to go to independent review) Repeated failure to meet internal standards Major patient safety implications if findings are not acted on	Non-compliance with national standards with significant risk to patients if unresolved Multiple complaints/ independent review Low performance rating Critical report	Totally unacceptable level or quality of treatment/ service Gross failure of patient safety if findings not acted on Inquest/ ombudsman inquiry Gross failure to meet national standards
Human resources/ organisational development/ staffing/	Short-term low staffing level that temporarily reduces service quality (< 1 day)	Low staffing level that reduces the service quality	Late delivery of key objective/ service due to lack of staff Unsafe staffing level or competence (>1 day)	Uncertain delivery of key objective/ service due to lack of staff Unsafe staffing level or competence (>5 days)	Non-delivery of key objective/ service due to lack of staff Ongoing unsafe staffing levels or competence

[6] http://www.npsa.nhs.uk/nrls/improvingpatientsafety/patient-safety-tools-and-guidance/risk-assessment-guides/risk-matrix-for-risk-managers/

competence			Low staff morale Poor staff attendance for mandatory/key training	Loss of key staff Very low staff morale No staff attending mandatory/ key training	Loss of several key staff No staff attending mandatory training /key training on an ongoing basis
Statutory duty/ inspections	No or minimal impact or breach of guidance/ statutory duty	Breach of statutory legislation Reduced performance rating if unresolved	Single breach in statutory duty Challenging external recommendations/ improvement notice	Enforcement action Multiple breaches in statutory duty Improvement notices Low performance rating Critical report	Multiple breaches in statutory duty Prosecution Complete systems change required Zero performance rating Severely critical report
Adverse publicity/ reputation	Rumours Potential for public concern	Local media coverage – short-term reduction in public confidence Elements of public expectation not being met	Local media coverage – long-term reduction in public confidence	National media coverage with <3 days service well below reasonable public expectation	National media coverage with >3 days service well below reasonable public expectation. MP concerned (questions in the House) Total loss of public confidence
Business Projects/ Objectives	Insignificant cost increase/ schedule slippage Key 'political' target is being achieved and impact prevents improvement	<5 per cent over project budget Schedule slippage Key 'political' target is being achieved but impact reduces performance marginally below target in the near future or performance currently on target, but there is no agreed plan to meet the target	5–10 per cent over project budget Schedule slippage Key 'political' goal is marginally below target or is soon projected to deteriorate beyond acceptable limits or there is an agreed plan but it does not yet meet the rising target	Non-compliance with national 10–25 per cent over project budget Schedule slippage Key 'political' target not being achieved and impact prevents improvement, or substantial decline in performance trend	Incident leading >25 per cent over project budget Schedule slippage Key objectives not met Key 'political' target is not being achieved and the impact further deteriorates the position
Finance including claims	Small loss Risk of claim remote	Loss of 0.1–0.25 per cent of budget Claim less than £10,000	Loss of 0.25–0.5 per cent of budget Claim(s) between £10,000 and £100,000	Uncertain delivery of key objective/ Loss of 0.5–1.0 per cent of budget Claim(s) between £100,000 and £1 million	Non-delivery of key objective/ Loss of >1 per cent of budget Failure to meet specification/ slippage

				Purchasers failing to pay on time Claim(s) >£1 million	Loss of contract/ payment by results
Service/ business interruption Environmental impact	Loss/ interruption of >1 hour Minimal or no impact on the environment	Loss/ interruption of >8 hours Minor impact on environment	Loss/ interruption of >1 day Moderate impact on environment	Loss/ interruption of >1 week Major impact on environment	Permanent loss of service or facility Catastrophic impact on environment

Table 2: Likelihood score (L)

What is the likelihood of the consequence 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.

Likelihood score	**1 Rare**	**2 Unlikely**	**3 Possible**	**4 Likely**	**5 Almost certain**
Frequency How often might it/ does it happen	This will probably never happen/ recur	Do not expect it to happen/ recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/ recur but it is not a persisting issue	Will undoubtedly happen/ recur, possibly frequently

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

Likelihood score		**1 Rare**	**2 Unlikely**	**3 Possible**	**4 Likely**	**5 Almost certain**
Consequence score	**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 Negligible	1	2	3	4	5

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

1 - 4	**Low risk**
5 - 8	**Moderate risk**
9 - 12	**High risk**
15 - 25	**Significant risk**

Appendix 3: Glossary of definitions and acronyms

Term	Explanation/ definition
Actions	Actions are a specific process that once completed, will help to bring the risk down to target score and therefore within its tolerance range. See section 6.7.
Action owner	An owner of an action as assigned by the Risk Handler.
Appetite	Risk appetite can be defined as 'the amount and type of risk that an organisation is willing to take in order to meet their strategic objectives. See section 3.7.
Assurances	Assurances are where we can obtain demonstrable evidence that our controls and systems are effectives. 'Strong' assurances would follow 3 lines of defence model. See section 3.6.1 and 6.6.
CCG	Clinical Commissioning Group
Commentary	Risk Commentary should be noted on the operational risk management system which should reflect the 'gap' between current and target scores. See section 6.8.
Consequence	The results should the risk materialise.
Controls	Controls are measures or systems that are currently in place to mitigate either the likelihood or consequence of a risk. See section 6.6.
CQC	Care Quality Commission
CRR	Corporate Risk Register. See section 6.4.
Current score	The measurement in terms of likelihood and impact on a risk after controls and assurances are considered to mitigate the risk. See section 6.5.
Descriptor	A good risk descriptor talks about the likelihood and consequence, e.g. if this happens, then this might happen. A good risk description is important so there is clarity when a risk is put forward for closure and under what conditions the risk can be proposed for closure.
Gaps in Assurances	Where there is not enough evidence or information to be able to assess the risk and make effective judgments about risk mitigation. See section 3.6.1 and 6.6.
Gaps in Controls	Aspects of a risk that may be beyond the CCGs control. See section 3.6.1 and 6.6.
GBAF	Governing Body Assurance Framework. See section 6.4.
HSE	Health and Safety Executive
IG	Information Governance
Impact	A measurement of the effect the risk will have if it will materialise.
Inherent Score	Risk score is without any controls, actions or mitigations in place and shows how dangerous the risk could be if not managed. This does not change through the life of a risk. See section 6.5.
Likelihood	A measurement of the chance that a risk will materialise.
Mitigation	An action that will control a risk. See 'T' values'.
NHSE	NHS England
NPSA	National Patient Safety Agency

Term	Explanation/ definition
Objective	The context in which risks are assessed i.e. the CCG's corporate objectives
RIDDOR	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013
Risk	Risk is the possibility that loss or harm will arise from a given situation. This encompasses anything from the possibility of injury to an individual, patient or member of staff, to anything which impacts upon the CCGs' ability to fulfil its aims and objectives.
Risk Handler	See section 5.11.
Risk Management Process	Risk management is a corporate and systematic process for identifying risks of any severity or scale, evaluating their potential consequences, determining the most cost- effective means of risk control and acting on this information. The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying and analysing, evaluating, treating, monitoring and communicating risk. It describes the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.
Risk Matrix	The tool used to as accurately as possible identify the measurement of likelihood and consequence of the risk identified.
Risk Owner	See section 5.11.
Risk registers	The Risk Registers are a tool to capture and report on the risks identified at Project, Committee or Corporate level. See section 6.4
Risk System Champion	An individual with specialist knowledge in the operational risk management system to assist Risk Handlers and owners on operationally managing their risks. See section 5.12.
SHP	Surrey Heartlands Health and Care Partnership
Scoring	Three scores are recorded on the operational risk management system: inherent, current and target. The CCGs use a 5x5 matrix (as in appendix 2) which gives equal weighting to consequence and likelihood. See section 6.5.
Source of a risk	Source of a risk would be where or how this risk has arisen
'T' values/ '4 Ts'	The Four Ts are four fundamental choices in relation to dealing with individual risks and are designed to help to bring current scores within target range as defined by the appropriate tolerance. See section 6.7.
Target score	The target score of the risk (based on section 3.7) and will reflect the associated risk tolerance. See section 6.5.
Tolerance	Risk tolerance is about what an organisation can actually cope with. Risk tolerance levels are linked to outcomes with each level having a corresponding target score range which the risk's target score must fall within. See section 3.7.

Appendix 3: Procedural Document Checklist for Approval

	Title of document being reviewed:	Yes/No/ Unsure	Comments/ Details
A	**Is there a sponsoring director?**	Yes	
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3.	**Development Process**		
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	Yes	
	Is there evidence of consultation with stakeholders and users?	N/A	
4.	**Content**		
	Is the objective of the document clear?	Yes	Section 1.4
	Is the target group clear and unambiguous?	Yes	Section 2
	Are the intended outcomes described?	Yes	Section 1.4
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
6.	**Approval**		
	Does the document identify which committee/ group will approve it?	Yes	Section 7.3.2
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how the document will be disseminated and implemented amongst the target group? Please provide details.	Yes	Section 7.1
8.	**Process for Monitoring Compliance**		
	Have specific, measurable, achievable, realistic and time-specific standards been detailed to monitor compliance with the document? Complete Compliance & Audit Table.		Appendix 4
9.	**Review Date**		
	Is the review date identified?	Yes	
10.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for implementing and reviewing the documentation i.e. who is the document owner?	Yes	

Director Approval			
On approval, please sign and date it and forward to the chair of the committee/group where it will receive final approval.			
Name		Date	
Signature			
Committee Approval			
On approval, Chair to sign and date.			
Name		Date	
Signature			

Appendix 4: Compliance & Audit Table

NHS Resolution Monitoring Table				
Criteria	**Measurable**	**Frequency**	**Reporting to**	**Action Plan/ Monitoring**
Appropriate management of risks	BAF and CRR risk >15 Clinical risk register All Risk Owners and Handlers to attend risk training.	Every quarter 3 times per annum On appointment and subsequently every 2 years (more often if changes to the Risk Management Strategy and Policy).	Governing Bodies Quality Committees Joint Executive Team	Recommendations from the committees implemented and reflected in the risk registers Training records to be kept by the Risk Team
Assurance for a suitable system of risk management	Risk management Strategy and Policy GBAF and CRR	Annually Quarterly	Audit Committees/ Governing Bodies Audit Committees	Statement of assurance and recommendations from Internal Auditors
Assurance for risk associated with financial controls	Annual Governance statement	Annually	Audit Committees	Recommendations from Internal Auditors
Action for improvement of risk mitigation	Risk Register	Before each Audit Committee or Governing Body meeting	Joint Executive Team	Recommendations from the committee implemented and reflected in the risk registers
Progress in implementing risk actions	GBAF and CRR Clinical Risk Register Attendance at corporate induction	Every quarter 3 times per annum Quarterly	Audit Committees Quality Committees Joint Executive Team	Recommendations from the committees implemented and reflected in the risk registers