Improving care together across Surrey Downs

NHS
Surrey Downs
Clinical Commissioning Group

Title of paper:	Risk Management Strategy		
Author:	Justin Dix, Governing Body Secretary		
Exec Lead:	Miles Freeman, Chief Officer		
Date:	24th April 2015		
Meeting:	Governing Body		
Agenda item:	07	**Attachment:**	04
For:	Information / Discussion / Decision		

Executive Summary:

The CCG is required to revise its risk management strategy on an annual basis in order to ensure that the risk element of the system of internal controls is up to date and ideally moving towards best practice.

This is the third iteration of the CCG’s risk management strategy and it has been substantially enhanced to reflect the substantial learning from the first two years of operation. It has been given positive assurance by Audit Committee members and by Internal Auditors.

Key changes are:

- Clearer layout and cross referencing
- More extended treatment of “Treat, Tolerate, Terminate or Transfer”
- Introduction of the concept of potential benefits matching risks
- Exposition of the three lines of defence model including suppliers as part of the first line
- Inclusion of the responsibilities of the two new committees (finance and performance, and primary care) in managing risk
- A clearer description and flowchart for risk process

- A full exposition of risk appetite
- Clearer description of how the strategy will be used and implemented

Compliance section

Please identify any significant issues relating to the following

Risk Register and Assurance Framework	Subject of the paper
Patient and Public Engagement	No specific issues
Patient Safety & Quality	There are particular sections on treatment of patient safety risk in the risk appetite statement
Financial implications	This strategy is particularly important as the CCG moves to manage the risks associated with financial recovery
Conflicts of interest	No specific issues
Information Governance	No specific issues
Equality and Diversity	No specific issues
Any other legal or compliance issues	None specific.

Accompanying papers (please list): Risk Management Strategy V3.1

Summary: What is the Governing Body being asked to do and why? AGREE the risk management strategy for 2015-16

NHS
Surrey Downs
Clinical Commissioning Group

RISK MANAGEMENT STRATEGY

Improving care together across Surrey Downs

Policy ID	CG02
Version:	3.1
Date ratified by Governing Body	Awaiting ratification
Author	J Dix
Last review date:	
Next review date:	

Version History

V.	**Date**	Status and/ or amendments
V1	**17/05/13**	First draft
V2	**29/04/14**	Revised on basis of first year of operations to reflect changes in structure and learning.
V3.1		Annual revision for April 2015 Governing Body

EQUALITY STATEMENT

Surrey Downs Clinical Commissioning Group (Surrey Downs CCG) aims 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 Downs CCG embraces the four staff pledges in the NHS Constitution. This policy is consistent with these pledges.

EQUALITY ANALYSIS

This policy has been subject to an Equality Analysis, the outcome of which is recorded on the following two pages.

		Yes, No or N/A	Comments
1.	Does the document/guidance affect one group less or more favourably than another on the basis of:		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Age	No	
	• Disability - learning disabilities, physical disability, sensory impairment and mental health problems	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?	N/A	
4.	Is the impact of the document/guidance likely to be negative?	N/A	
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 the Corporate Office, Surrey Downs CCG. 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
Mark Sanderson	20th June 2014
Justin Dix	

Contents

1 OBJECTIVES OF THE RISK MANAGEMENT STRATEGY *Page 6*
2 PRINCIPLES OF GOOD GOVERNANCE *Page 7*
3 APPROACH TO RISK MANAGEMENT *Page 7*
4 DEFINITIONS *Page 9*
5 ACCOUNTABILITY AND RESPONSIBILITIES IN RELATION TO RISK MANAGEMENT *Page 11*
6 RISK MANAGEMENT ORGANISATIONAL STRUCTURE *Page 13*
7 COLLABORATIVE ARRANGEMENTS AND COMMISSIONING SUPPORT *Page 15*
8 TYPES OF RISKS *Page 16*
9 RISK IDENTIFICATION *Page 18*
10 RISK ANALYSIS *Page 20*
11 THE “FOUR TS” METHODOLOGY *Page 21*
12 RISK MANAGEMENT AND RISK APPETITE *Page 22*
13 SURREY DOWNS CCG RISK DATABASE *Page 22*
14 MONITORING AND REVIEW OF RISK *Page 23*
15 THE GOVERNING BODY ASSURANCE FRAMEWORK *Page 24*
16 RELATIONSHIP BETWEEN THE ASSURANCE FRAMEWORK AND RISK DATABASE *Page 25*
17 LEARNING AND DEVELOPMENT *Page 25*
18 MONITORING AND REVIEW OF THE STRATEGY *Page 26*

Appendices

APPENDIX 1: RISK SCORING METHODOLOGY

APPENDIX 2: RISK APPETITE STATEMENT

APPENDIX 3: RISK IDENTIFICATION FLOWCHART

1. OBJECTIVES OF THE RISK MANAGEMENT STRATEGY

1.1. All of NHS Surrey Downs Clinical Commissioning Group's activities – from the strategic to the operational, and including both mandatory and optional area of work - carry some degree of risk.

1.2. Surrey Downs Clinical Commissioning Group (SDCCG) is therefore committed to ensuring that the Governing Body has a clear process for the management of risk and that it can communicate this to staff with delegated responsibilities, suppliers and to partner agencies it works with. The "Three Lines of Defence Model" set out in Section 3.1 makes it clear that the CCG can have a reasonable expectation that contracted suppliers, primary care contractors, local authority partners and others that it works with will form part of the overall risk management process, managing risk, communicating it and escalating it as appropriate.

1.3. The CCG specifically acknowledges the need for suppliers to have rigorous risk management systems in place as set out in Recommendation 91 of the Francis Report (May 2013).

1.4. The CCG will be able to systematically identify which areas of risk it is able to tolerate, and those which will require intervention or some other management.

1.5. Surrey Downs CCG seeks to be an innovative organisation that uses risk management not just to avoid or mitigate potentially adverse events, but to highlight potential opportunities through making risk and opportunity transparent. There is a recognition that innovation and collaboration in particular bring uncertainties that are both inevitable and desirable, and the CCG seeks to foster a culture that sees risk and risk management as positive aspects of change that can be used to bring about improvements in health and the delivery of health services.

1.6. Risk Management is therefore an integral component of the CCG's approach, in particular to:

- Ensuring the availability of health services and commissioning high standards of safe patient care
- Improving the health of the local population
- Having good relationships with the local community and managing change effectively
- Working collaboratively with other organisations and guaranteeing business continuity
- Ensuring the safety of its employees and others to whom it has a responsibility in the conduct of its business

2. PRINCIPLES OF GOOD GOVERNANCE

2.1. Governance in NHS Surrey Downs CCG is intended to be integrated and consistent, with systems and processes set by the Governing Body but used at all levels of the organisation, to provide assurance that the actions conducted in its name are sound.

2.2. Although the 33 member practices are ultimately accountable, the Governing Body is the core of the legal entity that controls and directs day to day activities and is responsible for its systems and processes. These are expected to be robust and stand up to legal and public scrutiny with the ultimate aim of ensuring probity in the conduct of all areas of its business.

2.3. The CCG owes a duty of care to its stakeholders and needs to observe the responsibilities that go with that. These include

- Patients and the local community
- The suppliers, both NHS and non-NHS, from whom it commissions and with whom it collaborates
- The taxpayer
- Other CCGs with whom it works collaboratively and in some cases formally
- Surrey County Council and local councils
- Its staff
- The voluntary sector

3. APPROACH TO RISK MANAGEMENT

3.1. In broad terms the CCG uses the In the Three Lines of Defence model, which is a sector standard approach and which is interpreted in Surrey Downs CCG as follows:

3.1.1. Management control is the first line of defence in risk management; the organisation's risks at a granular level are owned by managers who accept responsibility for managing a risk as part of "business as usual". Risk management is part of the day job and fully embedded in working practices. For a commissioning organisation, part of the first line of defence may be the supplier of healthcare or a service (i.e. from a Commissioning Support Unit) as the CCG should have specified reasonable expectations of first line defence at this level.

3.1.2. Control and compliance oversight functions established by management are the second line of defence, namely the existence of risk registers and an assurance framework, training for staff, and a systematic approach that ensures consistency and timeliness of reporting and action. These control and compliance regimes extend from the front line to the Governing Body.

3.1.3. Independent assurance is the third line of defence – independent audit and other mechanisms that give the organisation an impartial view.

3.1.4. Each of these three "lines" plays a distinct role within the organisation's wider governance framework as set out in Section 2 above.

3.2. The CCG's approach to risk management is based on the following principles:

3.2.1. Risk cannot usually be eliminated but it can be managed and decisions can be made which are reasonable and fair within the constraints of finite resources.

3.2.2. The organisation must identify both strategic and operational risks in a balanced way.

3.2.3. There must be clarity regarding ownership of and responsibility for risk at different levels of the organisation.

3.2.4. Risk takes many different forms, such as patient safety, financial, business continuity, information governance, reputation and so on. These must be seen in the specific context of each case and not generalised.

3.2.5. In defining risk appetite, the CCG seeks to guide itself and its staff on the process of risk assessment and defining what is and is not acceptable; however this is only guidance and ultimate ownership of risk sits with the Governing Body and accountable officers for each area.

3.2.6. Risk is increasingly shared with other organisations and the CCG's systems and processes will always seek to work with the different approaches of others without diluting accountability.

3.2.7. The risk strategy identifies three tiers of risk:

- Risks to the organisation’s principal objectives - these are high level and usually strategic and are managed through the Governing Body Assurance Framework. The Governing Body should take corporate responsibility for ensuring that it directs the Executive, where necessary, on the scale of mitigation and the willingness to accept risk (see “The Four T’s in Section 11).
- Significant risks that the Governing Body should be sighted on but which should be managed by the Executive.
- Project risks or service area risks which are the subject of local risk registers which the Executive should be sighted on.

3.3. The process for identifying and managing risk is set out in **APPENDIX 3**

4. DEFINITIONS

4.1. The following definitions are used throughout this document and in the operationalising of risk management in the CCG.

4.2. Risk and opportunity

4.2.1. A risk is an event that, should it occur, will have a an adverse effect on one of the CCG’s mandated responsibilities or chosen objectives.

4.2.2. It is quantified in terms of potential impact and likelihood. It consists of a combination of the probability of a perceived threat or opportunity occurring, and the magnitude of its impact on the objectives.

4.2.3. An opportunity is an uncertain event, often arising from the analysis of risk, that could have a favourable impact on both risk mitigation and the achievement of objectives.

4.3. Risk Assessment and Management

4.3.1. Risk assessment is the process used to evaluate a risk and to determine whether precautions are adequate or more should be done. The risk is compared against predetermined acceptable levels of risk.

4.3.2. Risk management is the systematic application of management policies, procedures and practices to the tasks of identifying, analysing, assessing, treating and monitoring risk.

4.4. Impact and likelihood

4.4.1. Impact is a measure of the effect that the predicted harm, loss or damage would have on the people, property or objectives affected.

4.4.2. Likelihood is a measure of the probability that the predicted harm, loss or damage will occur. The control of risk involves taking steps to reduce the risk from occurring such as application of policies or procedures.

4.5. The Assurance Framework

4.5.1. The assurance framework is the tool that the Governing Body uses to continually assess the risk of failure of its principal objectives.

4.5.2. It is an integral part of the system of internal control and defines the high-level potential risks. It also summarises the controls and assurances that are in place or are planned to mitigate them, and aligns principal risks, key controls, and assurances on controls alongside each objective.

4.6. Assurance and Controls

4.6.1. Assurance means a reliable source of information that clearly states the most recent position with regard to a risk. For example, prescribing data from national systems is a source of assurance regarding prescribing spend.

4.6.2. Gaps in assurance refers to a lack of reliable or timely information. The delay in getting information from the national prescribing system is a gap in assurance; similarly lack of real time data on prescriptions issued by local GPs could be said to be a gap in assurance.

4.6.3. A control is an action that can be taken that will have a measurable impact in mitigating a risk. For instance, issuing advice to GPs on how to substitute generic for branded drugs with the same level of effectiveness would be a control.

4.6.4. A gap in control would be the absence of actions, e.g. if no GP practice prescribing advice programme existed this could be seen as a gap in controls.

4.6.5. It should be noted that documents such as minutes of meetings and policies are secondary sources and are neither an assurance nor a control, although minutes might contain information or describe actions that demonstrate either or both. The risk database should be specific about assurance and actions and not see the existence of documents in themselves as providing evidence that risks are being accurately assessed and mitigated.

4.6.6. Independent assurance is external evidence that risks are being effectively managed (e.g. planned or received audit reviews).

4.7. Risk appetite and the Four Ts

4.7.1. Risk Appetite is the board defined level of risk that an organisation is prepared to accept or not. As well as being a risk management tool it represents a balance between the potential benefits of innovation and the threats that change inevitably brings.

4.7.2. The Four T's are the choice of Treat, Terminate, Tolerate or Transfer – these are the four fundamental choices in relation to an individual risk within the CCG's risk database (see section 11.)

5. ACCOUNTABILITY AND RESPONSIBILITIES IN RELATION TO RISK MANAGEMENT

5.1. The Governing Body is responsible for ensuring that risk management is in place, is effective, is regularly reviewed, and that there is adequate risk management capacity in terms of systems and staff training and development.

5.2. Principal Executive Roles

5.2.1. Risk Management forms an integral part of the normal management process for these Executive Leads within their areas of responsibility.

5.2.2. The Chief Officer in his or her accountable officer role has overall responsibility for ensuring an effective risk management system is in place within the CCG and for meeting all statutory requirements and adhering to guidance issued by NHS England in respect of governance. He or she will ensure that the system of internal controls is fully described and accounted for in the Annual Report, in particular through the Annual Governance Statement.

5.2.3. The Chief Officer will review the minutes of the Governing Body and all its principal committees and will, with the Governing Body and committee chairs, ensure that any risks identified in these forums are considered for inclusion in the assurance framework and risk register.

5.3. Principal Operational Roles

5.3.1. The Governing Body Secretary is responsible for the day to day co-ordination of the Assurance Framework and Corporate Risk Database, and for liaising with individual heads of service who manage any local risk registers.

5.3.2. The Chief Operating Officer is also the nominated director responsible for Health and Safety and Security.

5.3.3. The Chief Operating Officer has responsibility for the Patient Advice & Liaison Service (PALS), public engagement, managing the complaints, claims, freedom of Information requests, corporate responses, and for ensuring effective and responsive staff communication.

5.3.4. The Chief Finance Officer is the accounting officer for financial matters, and is responsible for ensuring the Governing Body has appropriate financial information, including taking responsibility for and reporting proposals to resolve any financial overspend. He / she is responsible for managing the strategic development and implementation of financial risk management including financial governance, financial management and investment advice. He / she is also responsible for ensuring that the CCG is fulfilling its statutory financial duties and legal obligations.

5.3.5. The Head of Quality is responsible for all aspects of clinical risk and risk to the quality of service in the CCG's commissioned services. This includes management of serious incidents and their potential consequences.

5.4. Senior Management and staff

5.4.1. Heads of Service are expected to operationalise risk management at its most fundamental level both through promoting a positive culture at team level throughout the organisation and through supplying leadership where a risk is identified and needs managing.

5.4.2. Senior Managers are responsible for ensuring appropriate and effective processes are in place for managing risk within their areas of responsibility. They are also responsible for implementing the specific agreed actions to reduce an identified risk and for advising their line manager if the risk is increasing to a level where escalation to the Corporate Risk Database needs to be considered.

5.4.3. All Staff – including agencies, contractors and employees of other statutory agencies working in SDCCG premises - have a responsibility to co-operate with managers in order to achieve the objectives set out in this strategy document.

5.5. Co-ordination of risk management

5.5.1. Risk Management processes are overseen on a day to day basis by the Governing Body Secretary who acts as a central reference point for all business risk issues within the CCG.

5.5.2. The Governing Body Secretary receives and collates information on risks, liaises with auditors, monitors new developments in risk management, develops knowledge and expertise and acts as liaison point for risk management issues, both within SDCCG and with external bodies. The role includes monitoring of proposed developments and initiatives and checking that they are likely to be compliant with good risk management processes.

6. RISK MANAGEMENT ORGANISATIONAL STRUCTURE

6.1. Responsibility for managing risk is vested at various levels throughout the organisation as set out in the Scheme of Reservation and Delegation and in Section 5 above.

6.2. The Governing Body

6.2.1. The Governing Body is delegated by the group (the 33 member practices acting collectively) to take overall responsibility for the group's running and has overall responsibility for risk management.

6.2.2. The Governing Body Assurance Framework and Corporate Risk Database will normally be reviewed by the Governing Body at each Governing Body meeting.

6.3. The Executive Committee

6.3.1. The Executive Committee is the committee of the Governing Body that discharges the responsibilities for day to day operational management of SDCCG.

6.3.2. The Corporate Risk Database and Governing Body Assurance Framework will be reviewed by the Executive Committee at least quarterly.

6.4. The Quality Committee

6.4.1. This committee reviews all aspects of patient safety and quality including safeguarding, infection control and early warning systems.

6.4.2. The committee also monitors collaborative work on quality with other CCGs and partner bodies.

6.4.3. The committee will monitor risk at each meeting, focusing primarily on risks of a quality and patient safety nature.

6.5. The Audit Committee

6.5.1. The Committee's primary role is to provide assurance regarding the adequacy and effective operation of the organisation's overall internal control system and testing and support of this through programmes of audit, education, and challenging compliance.

6.5.2. Key components include the risk strategy; policies; the assurance framework and risk register; audit reports; reports from other committees and from the executive; and oversight of the annual report.

6.5.3. The Committee has a pivotal role to play in reviewing the disclosure statements that flow from the organisation's assurance processes. In particular these cover the Annual Governance Statement, included in the Annual Report and Accounts, and ensuring that the CCG operates in a way that enables it to remain authorised by NHS England.

6.5.4. The Audit Committee is in a position to focus proactively on the high risk areas for the organisation, either where the inherent risk is high and the level of dependency upon the operation of controls is critical, or where the residual risk is high and the situation needs monitoring. Part of this responsibility is discharged by commissioning programmes of audit that help to identify risks before they become critical and thus support the organisation in the achievement of its objectives.

6.6. The Remuneration, Nominations and Human Resources Committee

6.6.1. This is the committee of the Governing Body that reviews and agrees pay and performance of directors and clinical leads and sets the strategy for the Governing Body in relation to very senior managers. It also has overall responsibility for reviewing the organisation's HR strategy, talent management, and workforce risks.

6.6.2. The committee will review risk at each meeting, focusing primarily on risks relating to succession, leadership, talent management, and the workforce resilience of the organisation.

6.7. The Primary Care Committee

6.7.1. This is the committee of the Governing Body that oversees primary care development and signs off independently on decisions where clinical members of the CCG are conflicted because of their roles as primary care contractors.

6.7.2. The committee will review risk at each meeting, focusing primarily on risks relating to primary care provision and working with NHS England and other agencies.

6.8. The Finance and Performance Committee

6.8.1. This is the committee of the Governing Body that oversees the CCG's Financial Recovery Plan and ensures the accuracy of financial information provided to the Governing Body. It has a key role around financial risk and sustainability of the organisation in the long term.

6.8.2. The committee will review risk at each meeting, focusing primarily on risks relating to achieving control total, meeting performance requirements, and the long term sustainability of the CCG.

7. COLLABORATIVE ARRANGEMENTS AND COMMISSIONING SUPPORT

7.1. NHs Surrey Downs CCG is responsible for ensuring there is a robust system of governance within its contractual arrangements with the following outsourced services:

- South East Commissioning Support Unit (SECSU)
- Services provided under collaborative arrangements with other CCGs

7.2. The CCG is also responsible for ensuring there is a robust system of governance with respect to services that it hosts on behalf of other organisations specifically:

7.2.1. Individual Funding Requests (IFR)

7.2.2. Continuing Health Care (CHC)

7.2.3. Medicines Management

7.3. The CCG is also responsible for the provision of a Referral Support Service (RSS) to local GP practices

7.4. Where there are issues with agreeing the level or impact of risk in any given collaborative instance, the CCG will use the disputes procedures within that relationship to achieve a mutually acceptable description of the risk for inclusion on its risk register

8. TYPES OF RISKS

8.1. The CCG encounters a diverse range of risks. This section sets out in broad terms the types of risk that may occur. In many cases risks impact in more than one area; for instance, failure of a project may impact on patient safety, workforce and finance. The following is a broad guide rather than a detailed list of risks and their interrelationships. Responsibilities for each area are set out in the CCG's detailed scheme of delegation.

8.2. Strategic Risk

8.2.1. A strategy is a long term plan of action designed to achieve a particular goal, most often success in achieving corporate objectives. SDCCG is charged with delivering a number of strategies within the overall NHS planning framework; these include:

- Key targets such as improved access to healthcare
- Better quality of healthcare
- Financial Recovery
- Protection of the public from infectious diseases
- Long term and sustainable improvements in the nation's health
- Capacity changes or innovative ways of working that require system reform
- Emergency Preparedness Resilience and Response (EPRR) planning as a Category 2 responder under civil contingencies

8.2.2. Strategic risks may also occur outside of the CCG's remit, for instance:

- Change of policy with the election of a new government
- New policies made under central direction such as the Better Care Fund, Frances enquiry etc.

8.3. Financial and Resource Management Risk

8.3.1. Financial and Resource Management risks are those which may affect the ability of the organisation to achieve its business objectives whilst at the same time ensuring financial probity, public accountability and compliance with budgetary constraints.

8.3.2. The following key areas are considered when managing financial risks:

- Clarity of financial objectives
- Financial accountability
- Responsibilities for financial management
- Auditing
- Governance of financial and resource management arrangements
- Standing Financial Instructions
- Training
- Monitoring the effectiveness of the Risk Management process
- Leadership
- Resources

8.4. Clinical and Quality Risk

8.4.1. Quality and clinical Risks are those which may directly affect patients. The Clinical Governance agenda directs the focus on these risks but the following key areas are considered when managing clinical risks (this list applies both to commissioning and to areas where the CCG is effectively a provider e.g. CHC):

- Patient safety
- Clinical effectiveness and best practice
- Clinical Audit
- Information Governance including Records management
- Integrated Care
- Managing and learning from incidents
- Staff Training and Development

8.5. Organisational and operational Risk

8.5.1. Organisational Risks are those which relate to the functioning and management of the CCG's operational areas.

8.5.2. The following key areas are considered when managing organisational risks:

- Organisational structure
- Human Resources / recruitment and retention of staff
- Reputation and any issues that affect the public's confidence in the organisation
- Use of technology and information
- Change Management
- Equality and Diversity
- Operational delivery such as managing referrals, continuing health care, and individual funding requests

9. RISK IDENTIFICATION

9.1. The CCG will take all reasonable steps to manage risk by a process of risk identification and risk assessment. In broad terms a risk, when identified, should normally be raised in a team meeting or with a line manager and then the risk should be described an drafted using the CCG's current template, with the support of the Governing Body Secretary if necessary.

9.2. The risk is draft until it has been agreed by the appropriate Executive Director, at which point it is "Awaiting Approval".

9.3. The approval of risks is reserved to the Executive Committee who may delegate this task to individual members of the Executive.

9.4. Risks are either identified as part of a structured assessment process, for instance quality reviews or through performance monitoring, or through incidents or near misses.

9.5. Programmed assessments are more likely to identify risks before they have materialised and all projects and programmes should create a local risk register and seek to reasonably identify the most likely risks to the success of the programme or project.

9.6. Risk identification processes seek to determine the nature of risks and their underlying causes. Assessments also seek to gauge the severity of the impact to the organisation in the event the risk materialises. The likelihood of the risk materialising is also assessed and is determined from an assessment of the internal controls in place.

9.7. Internal Sources of Risk Identification

9.7.1. These include risks identified through business processes

- Commissioning Decisions
- Research and Development
- Performance Management
- Provider led initiatives

1.2.

9.7.2. Risks identified through horizon scanning

- NHS News
- Legal intelligence
- Best practice reports
- National audit reports

9.7.3. Risks identified through clinical processes:

- Clinical Audit
- Serious Incidents
- Incident Reporting

9.7.4. Risks identified through patient and public engagement:

- Complaints
- PALS
- Feedback i.e. through engagement events or meetings in public

9.7.5. Risks identified through regulatory process:

- Care Quality Commission inspections
- Meetings with NHS England
- Compliance notices

9.7.6. Risks identified through proactive processes:

- Internal audit work programmes
- External audit work programmes
- Environmental Inspections

- CSU IG
- Finance
- Service redesign
- Performance
- Corporate
- Continuing Health Care
- Referral support Service
- Medicines Management

9.7.7. Risks identified through the CCG's governance structures:

- Council of Members
- Governing Body
- Committees and sub-committees
- Programme Boards

10. RISK ANALYSIS

10.1. The CCG's preferred approach to risk management is to seek to structure and quantify risk whilst acknowledging that there are strong subjective and operational factors involved. The key aim is to keep risk live and transparent and to embed risk awareness in the organisation at every level through awareness and training.

10.2. Likelihood and impact

10.2.1. The Risk Management system in place conforms to the principles that a risk factor is established by multiplying the probability of harm occurring (Likelihood) by the likely consequences (Impact). A copy of the Risk Scoring Matrix is attached in appendix 1.

10.2.2. It should be noted that any judgement where the likelihood is 5 (certain to happen) should involve contingency planning for managing up to the point at which the issue ceases to be a risk and becomes an incident. An example would be provider failure where the provider will be ceasing to trade on a specified future date and the impact will be catastrophic to patients if unmanaged. At this point the risk can be scored as 25 but the contingency planning should seek to reduce the impact by steps so that at the time the closure takes place the impact on patients is negligible. Once the provider ceases trading the issue can be removed from the risk register altogether.

10.2.3. Executives and managers will assess risks and devise action plans on the above basis using the generic risk assessment form, risk scoring matrix, local risk registers (see methodology set out in Risk Assessment Policy and Procedures). Directors and service / local managers will regularly review and monitor their local risk registers.

11. THE "FOUR TS" METHODOLOGY

11.1. The CCG articulates the principles of risk appetite through the use of the "Four Ts" methodology as follows.

11.1.1. Treat - treat or mitigate is in practice the most common response, achieved by taking action to reduce the probability of the risk occurring or by reducing the impact. 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.

11.1.2. 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 in the event that the risk escalated. The risk may reach a "tolerate" level having been "treated" through an action plan that identifies a target risk score (see 12.3.5).

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

11.1.4. Terminate - some risks can only be managed by terminating the activity. 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. The decision to terminate may mean that other more manageable or strategically acceptable risks have to then be described. An example would be terminating a contract that is unsafe or unsustainable. Terminating it may eliminate the risk but may mean that other risks have to be described and managed in the short term.

11.1.5. It is the responsibility of the Executive owner of the risk to agree the above prior to it being approved in the Executive.

12. RISK MANAGEMENT AND RISK APPETITE

12.1. It is not possible to eliminate all risk and it is the responsibility of the Governing Body to ensure that there are systems and controls in place to manage some risks at an acceptable level. A risk may be untreatable or the cost of treatment or control may be prohibitive. Where the decision is taken to accept a risk action needs to be put in place to minimise as far as possible the effects of risk exposure.

12.2. "Risk appetite" is a phrase used to describe how an organisation perceives risk and its willingness to respond to it. Surrey Downs has a statement of risk appetite agreed at Governing Body level. This can be found in Appendix 2.

12.3. For each risk on its risk register the risk owner must:

12.3.1. Score the risk

12.3.2. Agree if the risk should be terminated or transferred

12.3.3. If not capable of being transferred or terminated, he / she should review the corporate statement of risk appetite and identify the best fit with the risk in question, seeking advice if required.

12.3.4. If the risk is currently scored at a level consistent with the statement of risk appetite then the risk can be tolerated

12.3.5. 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.

13. SURREY DOWNS CCG RISK DATABASE

13.1. A Risk Database is a tool to enable the CCG to record how it is managing its risks and improving its performance in areas where a risk has been identified. It provides a mechanism for the recording, review and prioritisation of the CCG's risks and associated action plans so that control measures can be implemented most effectively.

13.2. The Risk Database is a record of all forms of risks. It describes the risk in enough detail for it to be understood and assesses the impact and likelihood of realisation of the risk as well as the action necessary to manage or remove the risk.

13.3. Details of the responsible officer for implementing the action and the expected completion date are also included in the Risk Database.

13.4. The Executive Committee will review the Corporate Risk Database on a regular basis. It will be responsible for approving any additions, changes and closures on the Risk Database.

13.5. In situations where significant risks (those scoring 15 and over using the risk scoring matrix) have been identified within the Risk Database and where local control measures are considered to be potentially inadequate, departmental and service managers are responsible for bringing these to the attention of their Executive Lead. Risks are mapped to the Assurance Framework, and the principal objectives of the organisation.

13.6. The Risk Database will be used within the business planning process to inform the allocation of resources to the highest risks.

14. MONITORING AND REVIEW OF RISK

14.1. Effectiveness

14.1.1.The effectiveness of the Risk Management process will be monitored by:

- A programme of audits of systems and controls by internal audit
- Monitoring of the process by the Audit Committee
- Review of the effectiveness of the system of internal controls in line with annual reporting requirements.

14.2. Closure of risks

14.2.1.Risks will only be closed with the agreement of the Executive Committee and closure will be noted at the relevant Governing Body meeting

14.2.2. Closed risks will be kept on the CCG Risk Database but not normally visible in reporting. They can be re-activated as required should a risk re-emerge.

14.2.3.Some risks will be routinely closed at year end and a new risk raised from the 1st April, e.g. the risk to achieving the financial control total in any specific year.

15. THE GOVERNING BODY ASSURANCE FRAMEWORK

15.1. The Governing Body's Assurance Framework process has two main purposes:

15.1.1. It correlates directly to the CCG's operational plan and is a high level management assessment process and record of the primary risks relating to the delivery of key objectives. It demonstrates clearly the strength of internal controls to minimise the likelihood of these risks occurring and it identifies sources of assurance and evaluates them for suitability. It then receives and reviews actual assurances (i.e. published reports) and uses the findings to confirm or modify management's opinion of the adequacy of internal control.

15.1.2. In order for the Assurance Framework to be able to assess the ability of internal controls to ensure the delivery of key objectives it must record details of high level risk and control. It therefore cannot be an exception report relating to residual risks. In addition, it must be complete so as to allow assurance sources to confirm the accuracy of management assessments of risk and controls.

15.2. The high level risk identification process driving the Assurance Framework will take into account the need to manage potential risks rather than react to the consequences of risk exposure. Any gaps in control and assurance with regard to these potential risks need to be assessed by the Governing Body in terms of the impact they may have on objectives and performance.

15.3. The Assurance Framework for the CCG therefore refers to:

15.3.1. The Principal business objectives of the organisation

15.3.2. The significant risks that impact on the achievement of those objectives

15.4. The internal and external controls that have been put in place to provide assurance to the Governing Body give assurance of:

15.4.1. the adequacy of those controls

15.4.2. further work that needs to be undertaken

16. RELATIONSHIP BETWEEN THE ASSURANCE FRAMEWORK AND RISK DATABASE

16.1. The Assurance Framework sets out at the beginning of each year to proactively determine the risks that might emerge to the delivery of its principal objectives and its overall strategy.

16.2. The Risk Database will contain material risks for the organisation that may not otherwise be brought to the attention of the Governing Body and which are essentially more detailed and operational in nature.

16.3. Maintenance of the Assurance Framework and Risk Database will be monitored and facilitated by the Governing Body Secretary. This includes ensuring consistency between the documents and providing the Governing Body with regular position reports.

17. LEARNING AND DEVELOPMENT

17.1. Staff education and training will be addressed through a systematic approach by ensuring all new staff receive induction training in Risk Management and relevant existing staff receive regular update training in line with requirements outlined within the CCG's Statutory and Mandatory Training Guidance, which outlines the type of risk management training required, relevant staff groups and frequency of training.

17.2. Risk management training for managers provides them with an outline of their responsibilities in relation to the management of risk within their areas of responsibility. Specific Risk Management training seminars will be provided where required for the Governing body, Committees, and Senior Managers.

17.3. Case studies based on examples drawn from the CCG's risk database will be developed to assist staff in developing their risk management skills and capacity.

17.4. The CCG will take positive action where there is identified low uptake of Learning & Development opportunities, in any staff groups.

18. MONITORING AND REVIEW OF THE STRATEGY

18.1. The Risk Strategy will be reviewed on an annual basis and its effectiveness assessed by reviewing its implementation and application across the organisation. This will be done through the work of internal audit in reviewing the systems of internal control on an annual basis, and by other means if necessary as determined by the Executive Committee.

18.2. The terms of reference of all the Governing Body’s principal committees will be reviewed annually to ensure they are updated to reflect best practice in the management of risk in each area.

18.3. This strategy will be approved by the Governing Body in line with the requirement that it has ultimate responsibility for managing risk in the organisation.

APPENDIX 1: RISK SCORING METHODOLOGY

The methodology for scoring risks is adapted from the **NPSA Risk Matrix for Managers** and prioritises the risks faced by the organisation by severity. Each risk is scored against the likelihood of it occurring (between 1 and 5) and the impact the risk will have should it occur (between 1 and 5). These scores are multiplied together and the result determines the severity of the risk. A full guide to the scoring criteria is available in the NPSA document.

		Likelihood				
		1	**2**	**3**	**4**	**5**
		Rare	**Unlikely**	**Possible**	**Likely**	**Certain**
Impact	**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**

APPENDIX 2: RISK APPETITE STATEMENT

NHS
Surrey Downs
Clinical Commissioning Group

STATEMENT OF RISK APPETITE

March 2015

1) What are risk appetite and risk tolerance?

1.1 Risk appetite is the amount of risk that an organisation is prepared to take when pursing its aims. No two organisations will have exactly the same objectives and therefore all organisations need to define their risk appetite accordingly, and ensure this is agreed at Board level. The rest of the organisation – Executives, Heads of Service and individual staff - can then work with the confidence of knowing the parameters that constrain and enable them.

1.2 Risk tolerance is the amount of uncertainty an organization is prepared to accept in total or more narrowly within a certain business unit, a particular risk category or for a specific initiative.

2) Why do we need to define risk appetite at Governing Body level?

3.1 Policy in the UK has developed partly in response to international failings in corporate governance, for instance Barings Bank and Exon, where small groups of managers and in some cases individuals can cause significant losses in complex organisations.

3.2 The UK corporate governance code clearly states that The board of any enterprise is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives, and should maintain sound risk management and internal control systems. Risk management can therefore only be effective if (in the CCG's case) the Governing Body has set out its expectations.

3) Parameters of risk appetite

3.3 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 Body feel risks should be managed and contributes to a clear culture for the continuous management of risk across the organisation.

3.4 However, whilst the statement of risk appetite enables the rapid development of ideas and proposals it does not give individuals or teams the right to act unilaterally. Whether innovation, development or response to an incident, the usual internal controls still apply and in setting out a proposal or framing a risk, senior managers should scope specific risks and benefits using the statement of risk appetite for context.

4) Outcomes – controlled and developed

4.1 In setting its risk appetite the CCG is mindful of the need to distinguish between what it has a duty to control and what it has a duty to develop. For instance, the CCG is expected to control Health Care Associated Infections (HCAIs) and its risk appetite in this area will be low. However, an innovative project to improve outcomes and quality of life for sufferers of dementia may be worth pursuing even if there is a risk of a financial loss, since without testing innovative new approaches the possibility of health gain does not exist.

5) Risk appetite as a subjective function of leadership

5.1 Following the changes to the NHS in April 2013, new leadership structures have been put in place and are continuing to evolve. More than ever risk management is operating in a fast moving environment in which leaders are expected to define risk appetite, and sometimes redefine it on a regular basis, based on their individual and collective experience. Political factors and responding to external events will form part of this but it is important for leaders to avoid becoming risk averse.

5.2 Risks need to be considered in terms of their broader impact and not the dominance of a single factor such as finance. The overall capability of the CCG – which has statutory duties relating to money, quality, the NHS constitution and its own staff – needs to be factored in. It is therefore acknowledged that the statement of risk appetite is a broad one which enables better internal control and does not offer definitive answers to any specific risk management issue.

6) Risk appetite within the overall approach to internal controls

6.1 Risk appetite operates within the overall system of controls. The process model for this is as follows.

i. All the CCGs activities should be subject to risk management as set out in the risk strategy. These fall into three broad categories:

1. Risk managing the organisations principal objectives (via the assurance framework).

2. Risk managing specific projects or service areas

3. Risk managing the response to external events in-year

ii. In all three cases the lead manager should frame the risk using the accepted methodology in the risk strategy and the template for the corporate risk register. When determining the risk tolerance (target score) and setting out the mitigating actions the manager should review the statement on risk appetite below.

6.2 The risk score should be moderated by the appropriate Committee and agreed by the Executive before submission to the Governing Body for approval.

7) Risk appetite, risk tolerance and exceptions

7.1 It should be noted that in defining a broad area as zero tolerance, this does not mean that the target score for risk tolerance purposes is automatically a 1 as it can still fall into a range of scores between 2 and 5.

7.2 The expected score ranges are set out in the statement on risk appetite below.

7.3 No statement of risk appetite can encompass every eventuality and there may be exceptions which mean that the CCG has valid reasons for setting a level of tolerance outside of the scope of the statement of risk appetite.

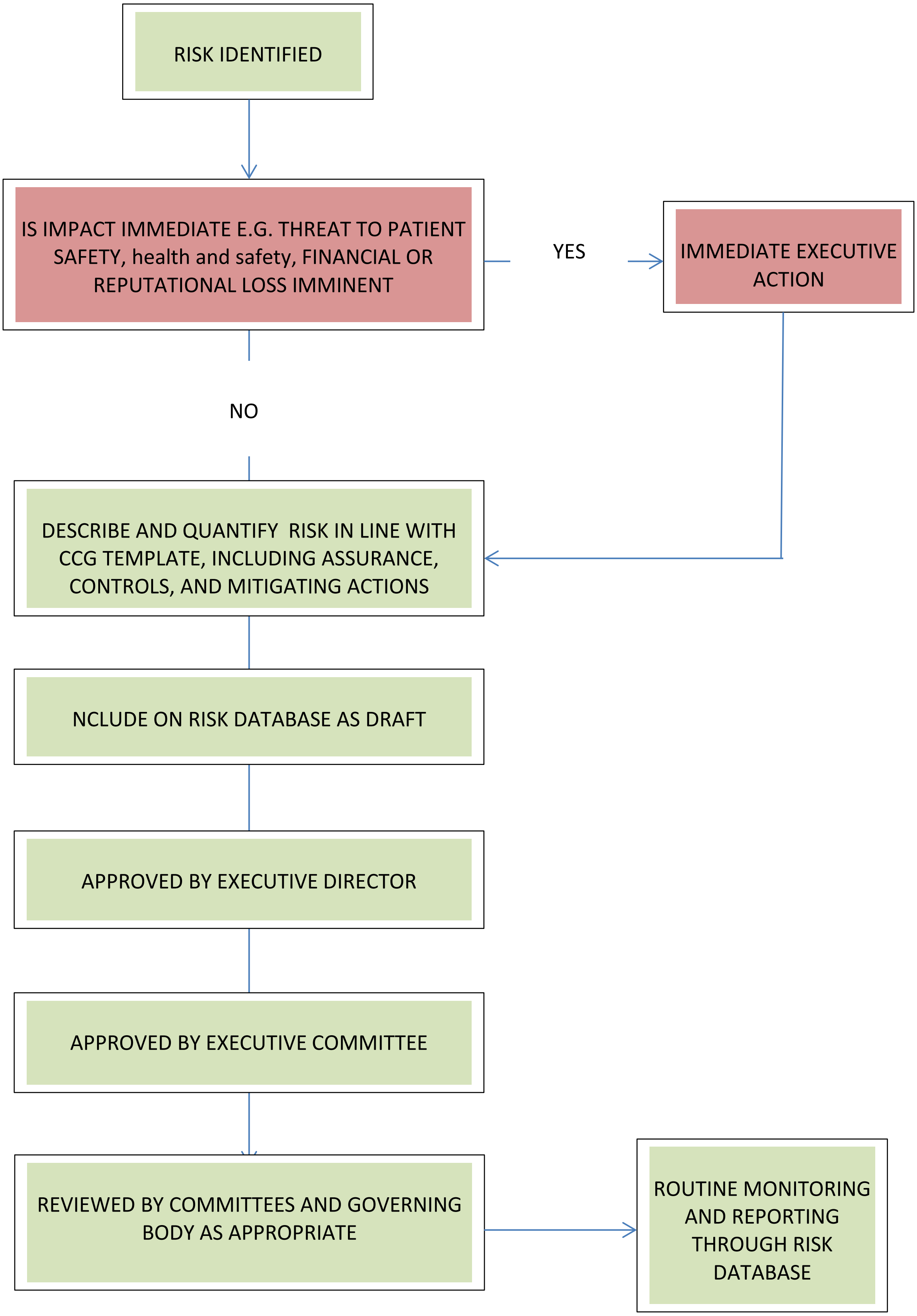
7.4 In this case the rationale will be formally documented and lessons learnt for a revised statement of risk appetite will be put in place.

8) Surrey Downs CCG statement of risk appetite.

The following is a statement of the CCG's current parameters for risk appetite (last updated September 2014). This was approved by the Governing Body on the 10th October 2014.

RISK LEVEL	SUPPORTING WHAT OUTCOMES?	SCORES
Minimal risk appetite	• Safe patient care • Disaster avoidance • Financial sustainability • Nationally defined expectations • Continued confidence of the public in the CCG	Expected target score range for specific risks: 1-5
Low risk appetite	• Mitigation of unsafe services • Stakeholder collaboration • In-year financial balance • Maintenance of critical systems • Regulatory compliance • Health and Safety	Expected target score range for specific risks: 6-8
Medium risk appetite	• Integrity of specific budgets and service areas • Patient safety awaiting national direction • Maintenance of non-critical systems • Decision making processes that may require reputation management • Good workforce strategy and organisational change • Effective management of delegated functions	Expected target score range for specific risks: 9-12
High risk appetite	• Taking carefully described financial and clinical risks for long term benefit • Management action to avoid a service becoming a high risk clinically or financially	Expected target score range for specific risks: 15-20

APPENDIX 3: RISK IDENTIFICATION FLOWCHART


RISK IDENTIFIED
IS IMPACT IMMEDIATE E.G. THREAT TO PATIENT SAFETY, health and safety, FINANCIAL OR REPUTATIONAL LOSS IMMINENT
YES
IMMEDIATE EXECUTIVE ACTION
NO
DESCRIBE AND QUANTIFY RISK IN LINE WITH CCG TEMPLATE, INCLUDING ASSURANCE, CONTROLS, AND MITIGATING ACTIONS
NCLUDE ON RISK DATABASE AS DRAFT
APPROVED BY EXECUTIVE DIRECTOR
APPROVED BY EXECUTIVE COMMITTEE
REVIEWED BY COMMITTEES AND GOVERNING BODY AS APPROPRIATE
ROUTINE MONITORING AND REPORTING THROUGH RISK DATABASE