NHS
Buckinghamshire
Clinical Commissioning Group

Integrated Risk Management Framework

Note: The CCG Integrated Risk Management framework is a generic document which covers the approach to be taken by the CCGs and its overall systems.

Author/s	Russell Carpenter
Date of Approval	September 2018
Review Date	September 2020
Policy Number	CHCCGPOL050

DOCUMENT CONTROL SUMMARY

Title	Integrated Risk Management Framework
Lead Officer	Robert Majilton, Deputy Chief Officer
Purpose of document	This document sets on the CCGs' approach to risk management and escalation.
Status	FINAL
Version No.	1.9
Date	September 2018
Author(s)	Russell Carpenter
Date of approval by Audit Committee	26/09/18
Date of ratification by Audit Committee	26/09/18
Review Date	Bi-annual

VERSION CONTROL SUMMARY

Date & Version	Author	Comment
November 2016 1.0	Russell Carpenter	Re-write and changes to reflect federation organisational arrangements; supersedes previous Aylesbury Vale Risk Management Framework Version 3 (December 2014) and Chiltern CCG Integrated Risk Management Framework April 2013.
1.1 - 1.6 November-December 2016	Russell Carpenter	Various iterations to reflect changes to internal risk management process
1.7 September 2017	Russell Carpenter	Amendments post risk management internal audit • Risk management threshold for corporate risk register escalation set at 12 • Changes to Programme Board titles
1.8 January 2018	Russell Carpenter	Change to version number to reflect final version post Audit Committee approval and ratification
1.9 September 2018	Russell Carpenter	September 2018 Change to logo 1.7 section 5 – revisions to programme board titles to reflect ICS Governance arrangements 3.9 Insertion of risk appetite statement

1.0 Introduction

1.1 This Framework outlines the purpose, reasons and the system of assurance for management of risk within Aylesbury Vale and Chiltern CCGs'. Every activity that the CCGs' undertake, or commissions others to undertake on their behalf, brings with it some element of risk that has the potential to undermine, or prevent the organisations achieving strategic aims/goals.

1.2 The CCGs' therefore recognises that risks must be taken in order to achieve strategic aims/goals and deliver beneficial outcomes to communities served. These risks must be taken in a controlled manner to reduce exposure to a level deemed acceptable by CCG Governing Bodies, relevant auditors and regulators.

1.3 The Governing Bodies of the CCGs' also need to be confident that all possible sources of risk to the achievement of strategic aims/goals have been considered and evaluated, paying particular attention to risks at the boundaries of their responsibilities.

1.4 To discharge both of these requirements, the CCGs have a responsibility to ensure proper governance in line with best practice in corporate, clinical and financial governance. This will in turn enable the CCGs to be compliant with statutory obligations and ensure aims/goals and objectives are met.

1.5 The Framework enables a clear view of the risks affecting each area of its activity; how these risks are being managed, the likelihood of occurrence and their potential impact on the successful achievement of the CCG objectives. This document sets out the framework for the identification and management of risk within the CCG and the system of assurance against that Framework.

1.6 The Governing Bodies of the CCGs are advocates of the principle that Risk Assurance is not just the responsibility of one role or person within an organisation. It is the responsibility of everyone (all CCG members and staff), whether clinical or non-clinical, and requires their commitment and collaboration.

1.6.1 The Framework is owned by CCG senior management (including Clinical Commissioning Directors and Clinical Leads), who support its implementation by ensuring a progressive, honest and open environment and where all types of risks can be identified and managed in a timely, positive and constructive way. More specifically, it is corporately owned by the Chief Finance Officer but management responsibility is with Robert Majilton, Deputy Chief Officer.

1.7 Other specifically related policies related to this framework and to be read in conjunction with it include the Information Governance Policy, Incident Reporting Policy and Procedure, Whistleblowing Policy, Disciplinary Policy, Training and Development Policy and Conflicts of Interest Policy.

1.8 Please refer to **Appendix 1** for a **list of definitions and roles and responsibilities** of individuals associated with this Framework. **Appendix 3** also

describes accountabilities in relation to CCG committees with responsibility for oversight and scrutiny of risk.

2.0 Principles & Purpose

2.1 Principles:

- Risk management is captured as part of **business as usual**, rather than being viewed or practiced as a separate programme.
- **Delegated** to those that can mitigate and manage the risk but with clear accountability/assurance – e.g. Member Practices delegate risk management to the Executive Committee with assurance by the Governing Body on principal risks (through the Governing Body Assurance Framework) associated with strategic aims/goals, but will get assurance through the annual report and involvement in key groups such as the Audit Committee.
- **Appropriate** to the degree of risk – impact and likelihood and the risk acceptability/appetite in the area. The CCG recognises it needs to take calculated risks.
- **Focused on** – Clinical (Quality), Financial, Reputational and Operational delivery risks (for which there is a more specific list of risk categories contained within supporting procedure).

2.2 Purpose:

The purpose of this Framework is;

- To describe the arrangements for effective management of risk in support of AVCCG'S vision and strategic objectives and to meet relevant standards imposed by legislation and associated guidance;
- To encourage a culture where risk management is viewed within the organisation, and by key partners, as an essential process of the CCG's activity
- To ensure structures and processes are in place to support the assessment, management and monitoring of risks throughout the CCG.
- To assure the public, patients, staff and partner organisations that the CCG is committed to managing risk appropriately.

3.0 Risk management systems and risk appetite.

3.1 The CCG operates two major systems to facilitate the management of risk throughout the organisation. These are:

- Proactive risk management, via regular planning and management activities implemented through the 13 step risk assessment flowchart and guidance described in **Appendix 2**; and
- Reactive risk management, in response to inspections, alerts, incidents and complaints through the near-miss and incident reporting process described in detail within Incident Reporting Policy and Procedure.

3.2 The organisation's overall risk appetite is moderate. This means that the CCGs' remain guarded, but will take on (i.e. tolerate) low to modest levels of risk in order to achieve acceptable outcomes. The CCGs' recognise that this position

will moderately increase the potential for organisational exposure to risk, but that this exposure will potentially result in more positive outcomes for the CCG.

3.3 The Governing Body will set specific limits for the levels of risk they are comfortable to tolerate in the pursuit of its objectives on an annual basis. The impact of agreeing these limits on decision-making will be evaluated in-year to ensure decisions are in-line with the stated position.

3.4 The CCGs organisational risk appetite is currently set at **12** for risks aligned to the Corporate Risk Register and 15 for risks aligned to the Governing Body Assurance Framework, explaining why the threshold for escalation of risks to each of these documents is set to the levels that they are (appendix 2, step 11).

3.5 The CCG has no appetite for fraud and financial crime risk and a zero tolerance to regulatory breaches.

3.6 Both the risk appetite and risk tolerances for each risk aligned to a strategic aim/goal will be agreed by the Risk Owner and, when reviewed for escalation to the Corporate Risk Register, by the Programme Board or other CCG committee which is responsible for the risk.

3.7 Methods of controlling risk must be balanced in order to support advancement and the effective use of resources in order to achieve substantial benefit. As a general principle, the CCG will seek to control all highly probably risks which have the potential to:

- Cause significant harm to patients, the local community, staff, visitors and any other stakeholders
- Severely compromise the reputation of the CCG
- Result in financial loss that may endanger the viability of the CCG
- Significantly jeopardise the CCG's ability to carry out its core purpose and/or meet its strategic objectives
- Threaten the CCG's compliance with law and regulation

3.8 The CCGs' appetite for risk is also aligned to its four strategic aim/goals as follows:

Strategic aim/goal	Risk Appetite
Better Health for Bucks; to commission high quality services that are safe, accessible to all and achieve good patient outcomes for all	In order to ensure that the CCG invests in innovate methods of delivery and maintaining high quality of services, the CCG will is willing to accept moderate levels of risk which will ensure a good likelihood of return on investments in innovation and quality. These investments may include development in systems and technology, as well as improvements in management control and alternative ways of working towards achieving positive patient outcomes.
Better Care for Bucks; to ensure local people and stakeholders have a greater influence on the services we commission.	In order to ensure that the CCG maintains a positive reputation in the local and health communities, the CCG will accept low levels of risk, i.e. where there is little chance for negative repercussions.
Sustainability within Buckinghamshire; to contribute to the delivery of a financially sustainable health and care economy that achieves value for money and encourages innovation	In order effectively manage the CCG's financial position and ensure value for money, the CCG will take low risk options that limit financial loss, though this may mean limited return on financial investments.
Leadership across Buckinghamshire; to promote equity as an employer and as clinical commissioners.	In order to effectively manage the CCG's regulatory and compliance requirements, the CCG will take low risk options that will ensure compliance with regulatory requirements while maintaining openness around new methods for achieving and maintaining compliance.

3.9 Risk appetite statement

Zero Risk Appetite - Patient safety and quality, Governance, and compliance with legislation
We will continue to hold patient safety in the highest regard and *will not accept any risk* that may jeopardise it. We will continue to ensure we operate as an accountable and transparent organisation, complying with all relevant legislation and *will never accept risks* that if realised could result in us being non-compliant with legislation

Low Risk Appetite - Capacity & Capability and Financial Sustainability
We will continue to ensure that everyone's roles, responsibilities and objectives are aligned to the achievement of our plan and will *only accept risks in exceptional circumstances* that if realised would stop our management and staff working together effectively to deliver our vision. We will strive to deliver our services within the contracted income as laid out in the financial plan and *will not accept risks (except in very exceptional circumstances)* that if realised might cause us to exceed the financial plan.

Neutral Risk Appetite – Reputation
We will continue to maintain high standards of conduct and patient care and in doing so are *willing to accept some risks in certain circumstances* that may result in reputational damage to the organisation.

Moderate/High Risk Appetite – Maximising innovation and working with others
We will continue to encourage a culture of innovation within the organisation and are *willing to accept risks* associated with this approach. We will continue to work with other organisations to ensure we are delivering the best possible service to our patients and are *willing to accept risks* associated with this collaborative approach.

This statement is purely a guide to risk appetite; it does not in itself confirm the CCG's agreed risk appetite at any particular time.

4.0 Risk Management with partner organisations and other stakeholders

4.1 Risk is often at its highest at the interface between organisations and it is here that clarity on responsibilities and accountability can be most difficult to ascertain. The CCG must work with partner organisations (including other CCGs, NHS organisations and Local Authorities) to identify and manage risks and prioritise them, which may also lead to joint action plans.

4.2 Independent Contractors are also bound by statutory obligations in the same way as the CCG (Health and Safety at Work Act 1974, Environment Act, COSHH Regulations etc.). In addition all clinicians are responsible to their professional bodies for their clinical practice.

4.3 As such Independent Contractors need to ensure that they are managing clinical and non-clinical risks appropriately. Independent contractors need to comply with their regulatory bodies and respective standards of professional practice. For GPs this includes complying with incident investigation and reporting systems of their employing or contracting body. (GMC standards: Good Medical Practice).

4.4 General public awareness of the CCG Risk Management Framework will be achieved through the review by the CCG Governing Body at meetings held in public, reference in the annual reports, publication on the CCG websites and through public engagement and locality meetings where applicable.

5.0 Method/arrangements/process/procedure

5.1 Risk Registers are used to organise and manage risk at project/team and corporate risk levels, through a system called Verto. This contains a number of core Risk Registers on which risks may appear:

1. Governing Body Assurance Framework
2. Corporate Risk Register.
3. Quality and Performance
4. Primary Care
5. Continuing Healthcare

5.2 **Appendix 3** shows formal review of risk reports by committees – the Governing Body and its reporting committees. Where there are specific accountabilities for a committee, these are listed. Risk Reports to each committee will be derived from all the Risk Registers identified above unless otherwise specified.

5.3 The Governing Body needs to be confident that all possible sources of risk to the achievement of strategic aims/goals have been considered and evaluated, paying particular attention to risks at the boundaries of their responsibilities.

5.4 Staff members must also be familiar with this Framework and specifically in identifying, assessing, reporting and escalating risks, especially ensuring those emerging which are extreme are reported as soon as they become apparent and to take any reasonable steps to mitigate that risk. Staff will be supported to do this through systems for induction, training and reviews.

6. TRAINING

6.1 Staff training on risk management is central to the successful implementation of this Framework.

6.2 The CCG will:

- Ensure all employees, committee members and stakeholders have access to a copy of this Risk Management Framework and appropriate advice, guidance and information to carry out their duties;
- Produce registers and reports of risk across the CCGs which will be subject to routine review through committees as specified in Table 1;
- Communicate to employees any action to be taken in respect of risks identified;
- Develop supporting policies, procedures and guidance based on the results of assessments and all identified risks to assist in the implementation of this Framework;
- Provide new employees with an induction and all employees with training on risk management systems. Statutory and Mandatory training also includes health and safety, fire and manual handling training; and the management of information.
- Ensure that training programmes raise awareness of the importance of identifying and managing risk; and
- Ensure that employees and other workers have the knowledge, skills, support and access to expert advice necessary to implement the policies, procedures and guidance associated with this Framework.
- Provide regular training to the Governing Body to ensure it can effectively discharge its duty in respect of oversight and scrutiny of the Governing Body Assurance Framework.

7. EQUALITY IMPACT ASSESSMENT

In relation to equality impact and the nine protected characteristics race, sex, disability, age, sexual orientation, religious or other belief, marriage and civil partnership, gender

reassignment and pregnancy and maternity, an assessment has not identified any detriment.

8. MONITORING, EVELUATION AND REVIEW

8.1 Review of the Framework

The Framework is subject to bi-annual review of its effectiveness through internal audit, or before if legislative, best practice, and/or procedural changes occur. Any recommendations for change will be submitted to the Audit Committee for review and agreement before submission to the Governing Body for ratification.

8.2 Assurance of the Framework

Several sources of assurance, both internal and external, on the effectiveness of the Risk Management Strategy and related internal control systems will be used, including:

- The CCG annual governance statement (which will also include risk management priorities).
- External Audit
- Review of risk management and board assurance framework related processes by Internal Audit
- Performance monitoring / regulatory review e.g. by the NHS Commissioning Board
- Compliance with the Integrated Risk Management Framework, and related policies and procedures, will also be monitored by:
  - The Executive Team through regular review of the Corporate Risk Register.
  - Audit Committee through the review of selected risks, and of reports received throughout the year.
  - The Audit Committee which approves the internal audit plan to ensure key organisational systems and controls are effective, and which reviews the full Governing Body Assurance Framework (GBAF)
  - The Governing Body through regular review of the Governing Body Assurance Framework (GBAF).
  - Other Programme Boards and CCG committees through review of risk reports and risk registers as described in **Appendix 3**.

References:

- Appendix 1 – list of definitions (including project and corporate risk) and roles and responsibilities' of individuals associated with this Framework.
- Appendix 2 – 13 step flowchart process with supporting guidance on risk management and escalation (also described in appendix 2).
- Appendix 3 – formal review of risk reports by committees – the Governing Body and its reporting committees.

Appendix 1 – definitions and roles and responsibilities of individuals

Term	Definition
Risk	An uncertain event or set of events which, should they occur, will have an effect upon the achievement of a strategic aim/goal.
Risk Management	A logical and systematic method of establishing the context, identification, analysis, evaluation, treatment and monitoring of risks associated with any activity, function or process.
Risk Register	A central repository for risks including information such as likelihood, impact, the actions to be taken to reduce impact/likelihood, the Risk Owner etc.
Project Risk Register	One for each project populated at the team level and managed by managers, project managers, risk owners or delegated risk owners.
Corporate Risk Register	Comprised of all risks from local risk registers beyond the risk appetite, reviewed by the Executive Team with executive accountability for each risk. This documents, for each risk included: • Risk Definition • Risk Cause • Risk Proximity • Risk rating (initial, current and acceptable) • Rationale for Current Score • Rationale for Acceptable Score • Controls/dependencies (internal and external) • Assurances (internal and external) • Gaps in controls and gaps in assurances • Mitigating actions – both controls and assurances It also documents owners for controls, assurances and actions, and also due dates for actions. More information is provided within the risk management flowchart and guidance.

Term	**Definition**
Governing Body Assurance Framework (GBAF)	Aggregate of risk profile with direct correlation to contributing risks, linkage to strategic aims/goals and reviewed by the Governing Body. This documents, for each risk included: • Risk Definition • Risk Cause • Risk Proximity • Risk rating (initial, current and acceptable) • Rationale for Current Score • Rationale for Acceptable Score • Controls/dependencies (internal and external) • Assurances (internal and external) • Gaps in controls and gaps in assurances • Mitigating actions – both controls and assurances It also documents owners for controls, assurances and actions, and also due dates for actions. More information is provided within the risk management flowchart and guidance.
Incident	An event that has occurred with effect on strategic aims/goals. Risks are frequently and mistakenly articulated as incidents (or issues) that have already happened.
Issue	A certain or on-going circumstance, which will have or is already having an effect upon the achievement of aims/goals.
Risk assessment /evaluation	Process used to evaluate the risk and to determine whether precautions are adequate or more should be done. The risk is compared against predetermined acceptable levels of risk.
Project Risk	Risks that impact on the delivery of key projects/ and are the responsibility of Senior Responsible Officers, Project Managers/Project Leads monitored by Project Boards, Steering Groups and Programme Board (see also definitions for Risk Owner and Delegated Risk Owners.
Corporate Risk	All high level strategic and operational risks *(12+)* identified as affecting strategic aims/goals.

Term	**Definition**
Strategic Risk	A derivative of corporate risk with potential to impact across the organisation and, if realised, could fundamentally affect the way in which it exists or commissions services in the next 1 to 5 years. These risks will have a detrimental effect on the achievement of aims/goals. Types of strategic risk: • **Patient / Public:** those associated with the failure to meet the current and changing needs and expectations of patients and citizens • **Political:** those associated with the failure to deliver government or local membership policy • **Economic:** those affecting the ability of the CCG to meet its financial targets • **Market:** those affecting the ability of the CCG to secure appropriate cost and quality of provision to deliver its commissioning priorities • **Legislative:** those associated with current or potential changes in national or European law • **Social:** those relating to the effects of changes in demographic, residential or socio-economic trends • **Technological:** those associated with the capacity of the CCG to deal with the pace or scale of technological change or effectively harness technology to deliver its objectives • **Environmental:** those relating to the environmental consequences of progressing the CCG's strategic objectives.
Operational Risk	A derivative or corporate risk with potential to impact operational achievement and, if realised, could affect the way in which the Group operates across its localities in the next 0-1 years. They will have a detrimental effect on the CCG's key processes, and activities that underpin the delivery of objectives. Types of operational risk: • **Clinical:** those related to the delivery of effective care and treatment • **Contractual:** those related to the failure of providers to deliver services • **Business:** those affecting the delivery of the CCG's operational business plans • **Health and Safety:** those related to accident prevention and securing the safety and welfare of patients, staff and visitors • **Financial:** those associated with financial management • **Workforce and recruitment:** those related to the ability to attract, develop and retain required capacity and skills • **Legal liability:** those related to possible breaches of legislation

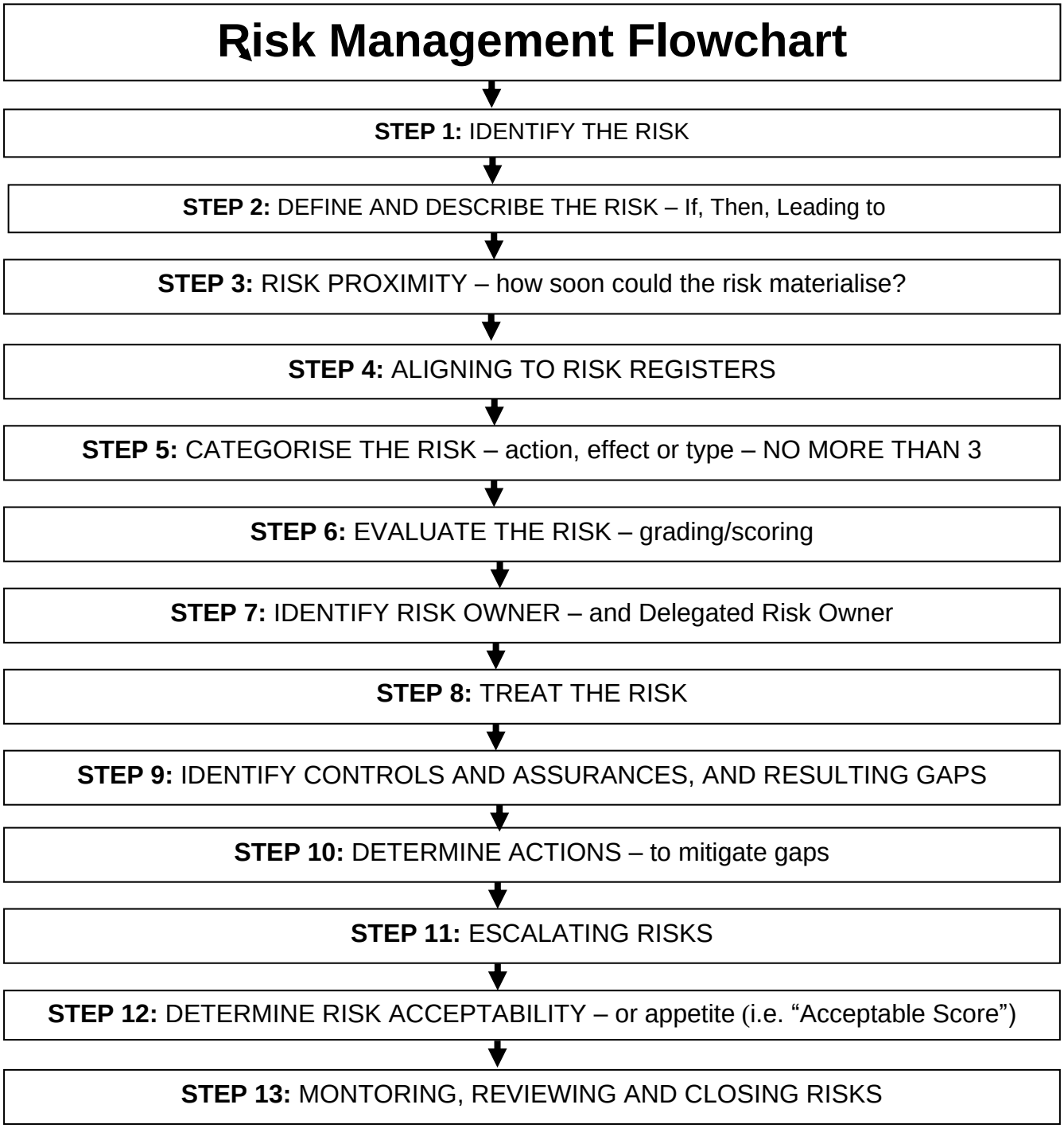
	• **Estate and technological:** those related to reliance on buildings and operational equipment.
Term	**Definition**
Strategic Aims/Goals (and objectives /priorities)	• Strategic aims/goals are high level and broad that do not relate to a specific target, frequently a 3-5 year timescale. A goal is a specific target, an end result or something to be desired. It is a major step in achieving a vision. • A Strategic Objective is a measure of change in order to achieve an aim/goal. Attainment of a goal may require a number of objectives to be reached. Strategic objectives are also defined over the same timescale as above. Strategic objectives should support the achievement of the primary purpose of the CCG. Each strategic objective should have tangible success measures i.e. those things that will tell you at the end of the year whether the strategic objective has been achieved. These should be easily understood by the Governing Body and CCG staff. • A Strategic Priority is a strategic objective ranked by their importance (at a point in time which may change) in achieving the strategic aims/goals. • Corporate Objectives are frequently annual in delivery.
Risk Acceptability /Appetite (i.e. Acceptable Score)	This is the level of risk that the CCG is prepared to accept or be exposed to at any point in time, post mitigation.
Risk Tolerance	This is the level of risk an organisation can actually cope with, which in turn influences the amount of risk considered acceptable (i.e. appetite). It is the level, amount or degree of risk that the CCG or a particular delegated authority is willing to accept and is a guide for staff on the limits of risk that they can take. E.g. a corporate risk scoring 16 for example would breach the threshold for risk reporting purposes, but the Governing Body may still accept it as a tolerable level of risk.
Zero tolerance risks	These are risks in areas which the Governing Body has agreed they would benefit from being aware of, regardless of risk rating, at any particular point in time. Recommendations for classification of zero based risks come from the Governing Body. The CCG will take a similar approach to identifying and managing such risks, monitored by the Audit Committee and Executive Committee.

Term	**Definition**
Risk Owner	Responsible for management, control, regular review and escalation of individual risks. They are responsible for taking a lead role in embedding risk management processes within their project/team. This is not necessarily the same as the action owner, as actions may be delegated to others. They are specifically responsible for: • Ensuring local risk registers are maintained and updated • Ensuring risks that meet the tolerance level of 8 or more are escalated to either the Corporate Risk Register or Governing Body Assurance Framework • Providing assurance on risk management activity through the relevant Programme Board or other CCG committee to which the project or team is ultimately accountable. Depending on the risk and the register to which it is assigned, a Risk Owner (at project level) should always be: • The Senior Responsible Officer (SRO) for the project • A managerial deputy to a Clinical Commissioning Director or Clinical Lead, • Deputy to a senior manager that is a member of the Governing Body and/or Executive Committee, • Another manager with risk responsibility as part of portfolio, e.g. Project Manager or Locality Business Support Manager.
Delegated Risk Owner	The individual often responsible for populating and updating project or team Risk Registers, Programme Board Risk Registers and those associated with Regulatory and Corporate Affairs through the Verto system. The roles and responsibilities of these individuals include: • Proactively engage in reviewing and quality checking risk reports/registers and update within their project/team. Manage risks on Verto system to enable production of Risk Reports for committees. • Report any concerns to their Director (as Corporate Risk Owner if the risk were escalated), and advise other directors, managers and other staff within their team of identified risks requiring attention. Depending on the risk and the register to which it is assigned, a delegated risk owner should always be: (1) A managerial deputy to a Senior Responsible Officer (SRO) for the project, managerial deputy to a Clinical Commissioning Director or managerial deputy to a Clinical Lead, (2) Deputy to a senior manager that is a member of the Governing Body and/or Executive Committee, (3) Another manager with risk responsibility as part of portfolio, e.g. Project Manager or Locality Business Support Manager. This

	individual may be responsible (as deputy to the risk owner) for reviewing and updating risks through the Verto system.
Term	**Definition**
Corporate Risk Owner	The individual who is responsible for the management and control of a risk which has been escalated by a programme board, CCG committee or individual to the Corporate Risk Register (CRR). The Corporate Risk Owner should always be: (1) A Clinical Commissioning Director (2) A Clinical Lead (3) A Senior manager that is a member of the Governing Body and/or Executive Committee. This individual is responsible for owning the risk (at corporate level) and providing assurance when it is discussed by the Executive Committee or Governing Body. This definition applies to risks on registers presented to the Governing Body (Assurance Framework), Executive Committee (Corporate Risk Register) and Programme Boards. A Risk Owner, Delegated Risk Owner and Corporate Risk Owner should not be the same person.
Senior Responsible Officers (SRO)	• Ensuring that project/programme risk registers have been challenged and scrutinised at each Programme Board meeting. • Ensuring risk is appropriately monitored by Project Managers and any actions identified will effectively mitigate the risks identified • Ensuring Corporate Risks are escalated to the Corporate Risk Register reported to the Executive Committee.
Managers	Managers must ensure that where they are employing or contracting agency and locum staff they are made aware of and adhere to, all relevant policies, procedures and guidance of the CCG, taking actions to prevent risks and escalating any risks for appropriate mitigation and subsequent action.
Accountable Officer	Has overall accountability for having in place an effective risk management system within the CCG and for meeting all statutory requirements and adhering to guidance issued by NHS England (or other relevant bodies) in respect of governance.
Chief Finance Officer	Is the senior responsible officer (SRO) for risk management in the CCG and is designated as the accountable and responsible officer for implementing the system of internal control including the Governing Body Assurance Framework (GBAF).
Director of Corporate Affairs	Risk Management Lead (supported by the Corporate Governance Lead and Programme Management Office) with overall management responsibility for risk management, function audit, and ensuring timely reporting of risk reports, the Corporate Risk Register and Governing Body Assurance Framework.

Term	**Definition**
Risk Grading/Scoring	The total risk score worked out by identifying the consequence and likelihood scores and cross referencing the scores on the risk matrix.
Consequence	A measure of the effect that the predicted harm, loss or damage would have on the people, property or objectives affected.
Likelihood	A measure of the probability that the predicted harm, loss or damage will occur.
Impact	Measure of the effect that the predicted harm, loss or damage would have on the people, property or objectives affected.
Control	Taking steps to reduce the risk from occurring such as application of policies or procedures.
Assurance	What we are doing to manage the risk and how this is evidenced – how and when will this be reported to the Governing Body. Independent assurance is any external evidence that risks are being effectively managed (e.g. planned or received audit reviews).
Action	How the identified gap is to be addressed and how the risk is to be diminished.
Gaps in controls or assurance	Where an additional system or process is needed, or evidence of effective management of the risk is lacking.
External Audit	The organisation appointed to fulfil the statutory functions in relation to providing an opinion on the annual accounts of the CCGs.
Internal Audit	The team, which may be part of the CCGs an outsourced provider, responsible for evaluating and forming an opinion of the robustness of the system of internal control, including risk management.

Appendix 2 – a 13 step process flowchart with supporting guidance on risk management and escalation.



Appendix 3 – formal review of risk reports by committees – the Governing Body and its reporting committees.

Table 3a – formal review by CCG committees accountable to the Governing Body (a separate procedure describes the scoring process for corporate risks)

Note: this table refers to the Governing Body and committees that are directly accountable to it, where there is a specific Risk Register source for the risk report on Verto.

Committee	Summary of accountabilities	Risk Report Title	Report Owner	Report prepared by	Report Content	Frequency
Governing Body	Monitors GBAF (at least 4 times annually) with delegation from members, ratifies the Framework, and receives risk escalations from its committees, ratifies annual governance statement to member practices. GBAF content described in appendix 1.	Governing Body Assurance Framework (GBAF) /Heatmap	Chief Finance Officer	Corporate Governance Lead	Corporate Risks rated **15** and above. Quarterly deep dive with monthly update (for information) of any major changes. Escalations from other committees and programme boards as necessary across all Verto Risk Registers.	Quarterly (following month after Corporate Risk Register has circulated to the Executive)
Executive Committee	Regular review of the Corporate Risk Register and escalation to the GBAF. Ensuring Risk Owners are clearly identified. Corporate Risk Register described in appendix 1.	Corporate Risk Register	Chief Finance Officer	Corporate Governance Lead/Risk Assurance Manager SCWCSU	Corporate Risks rated **12** and above. Quarterly deep dive but monthly update (for information) of major changes. Includes escalations from committees and programme boards as necessary across all other Verto Risk Registers.	Quarterly

Committee	Summary of accountabilities	Risk Report Title	Register Owner	Report prepared by	Report Content	Frequency
Quality and Performance Committee	Reviews a quality and safety risk register advising on and managing clinical risk and receives reports from sub-groups on safeguarding etc.	Quality and Performance	Director of Commissioning and Delivery	Associate Director of Nursing and Quality	Corporate risks across all registers (at all scores) in patient experience, quality, safety, safeguarding, best clinical practice (e.g. NICE), clinical governance and performance /contracts and constitutional targets categories. Any further risks that the Quality Team add to Regulatory Affairs, Corporate Affairs or Business as Usual identifiers.	Every meeting (bi-monthly)
Primary Care Commissioning Committee	The Primary Care Operational Group will review the primary care risks on the Corporate Risk Register and report any risks scoring 12 or above to PCCC	Primary Care	Head of Primary Care	Primary Care Manager	Programme Board risks in Primary Care/delegated responsibility category. And additional risks that the Primary Care Team adds using Regulatory Affairs, Corporate Affairs or Business as Usual identifiers.	Every meeting (quarterly)

Table 3b – formal review by CCG committees accountable or reporting to the Governing Body, but which do not have a separate risk register on Verto

Note: this table refers to other committees accountable or reporting to the Governing Body which have risk report based on one or more risk categories (for information or assurance), which do not come from a Verto Risk Register source.

Committee	Summary of accountabilities	Risk Report Title	Report Owner	Report prepared by	Report Content	Frequency
Audit	Assurances the Governing Body on risk through approval of Risk Management Framework incorporating systems of internal control. Scrutinises framework and its operation.	n/a	Chief Finance Officer (Senior Information Risk Owner)	Head of Governance/ Risk Assurance Manager SCWCSU	Corporate risks across all registers in corporate governance and procurement categories (at all scores). Corporate Risk Register as also provided to the Executive Committee. Random selection of project risks to ensure risk grading/scoring methodology is being applied appropriately and consistently. The Audit Committee also approves the internal audit plan and integrated risk management framework to ensure key organisational systems and controls are effective. Any additional risks from the register reviewed by the Quality and Performance or Finance Committees.	Twice annually