Castle Point and Rochford
Clinical Commissioning Group

RISK MANAGEMENT POLICY

CPRCCG CP16

2019-20

Version:	8.0
Ratified by:	Audit and Risk Committee
Date ratified by Governing Body:	28th November 2019
Name of Director Sponsor:	Director of Strategy and Planning
Name of originator/author:	Associate Director of Assurance
Name of responsible committee:	Audit and Risk Committee
Date issued:	November 2019
Review date:	November 2021
Target audience:	All CCG Staff

1. Introduction and Purpose

NHS Castle Point and Rochford CCG (hereafter referred to as "the CCG") has a responsibility to ensure that proper governance is in place and is in accordance with best practice in corporate, clinical and financial governance. Every activity that the CCG undertakes or commissions others to undertake on its behalf, brings with it some element of risk that has the potential to threaten or prevent the organisation from achieving its objectives.

This Risk Management Policy enables the organisation to have a clear view of the risks affecting each area of its activity; how those risks are being managed, the likelihood of occurrence and their potential impact on the successful achievement of the CCG's objectives. This document sets out the approach for the identification and management of risk within the CCG.

This Policy applies to all members of the CCG, the CCG Governing Body, CCG Executive team and all managers to ensure that risk management is a fundamental part of the CCG approach to governing the organisation and all of its activities.

The CCG recognises the importance of involving local stakeholders in its risk management processes and of working in partnership to identify, prioritise and control shared risks.

The five CCGs comprising the Mid and South Essex Sustainability and Transformation Partnership (STP) (Basildon and Brentwood, Castle Point and Rochford, Mid Essex, Southend and Thurrock CCGs) have formed a STP Joint Committee (STP JC). The Committee's primary purpose is to commission and manage the contacts for Acute services (NHS and independent sector), NHS 111 and Out of Hours services, ambulance services, Patient Transport services and acute Mental Health services. The STP Joint Committee will also play a role in decision making about Learning Disability services within the existing pan-Essex arrangements.

The CCGs within the STP JC will work to identify those risks which are specific to the work of the individual CCGs and STP JC and will implement risk management process to manage and reduce the level of risk.

1.2 Scope

The CCG is committed to a policy that minimises risks to all its stakeholders through a comprehensive system of internal control whilst providing maximum potential for flexibility, innovation and best practice in the delivery of its strategic objectives.

The Risk Management Policy underpins the CCG's objectives and enables the organisation to prioritise risks so as to direct resources for managing risks effectively.

This Risk Management Policy will apply across all parts of the organisation and include all CCG staff, localities and member practices. It relates to all of the CCG activities as a commissioner of NHS Services. Furthermore it applies to all CCG premises and persons engaged in business on behalf of the CCG.

2. Definitions

2.1 Risk

At is simplest, risk is the possibility that loss or harm will arise from a given situation. In the context of this Policy, this encompasses anything from the possibility of injury to an individual patient or member of staff to anything which impacts upon the CCG's ability to fulfil its aims and strategic objectives.

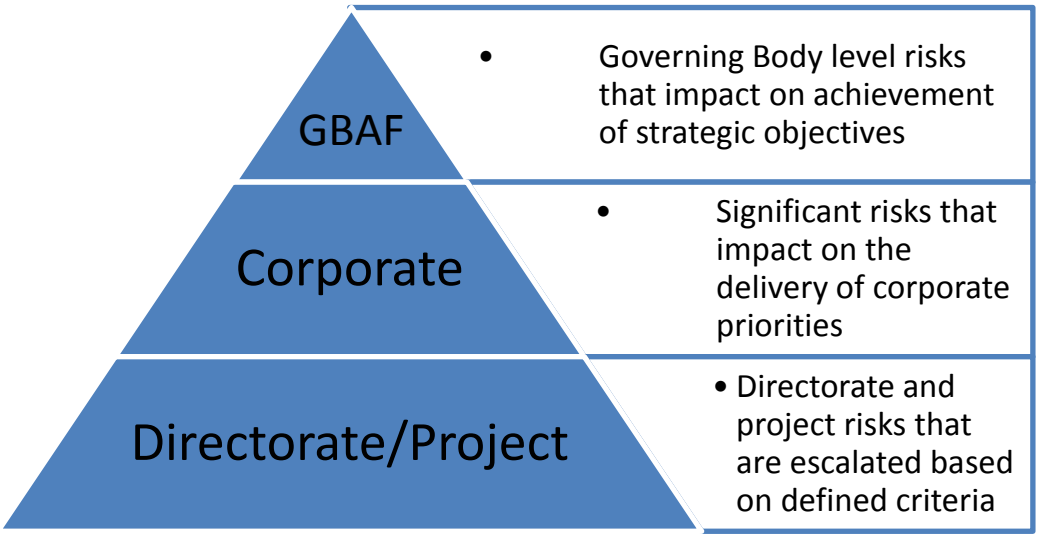
2.2 Risk Management

Risk Management may be defined as a proactive tool in the:

- Identification of risks;
- Analysis and assessment of the likelihood and potential impact of risks;
- Elimination of those risks that can be reasonably and practicably eliminated;
- Control of those risks that cannot be eliminated by reducing their effects to an acceptable level;
- Communication of risks; and
- Regular monitoring of risks to ensure that controls are effective in reducing the level of risk

2.3 Risk Management Approach

The diagram below reflects the overall approach that is to be taken to the management of risk within the CCG and forms the basis of this policy. The diagram outlines the hierarchy of registers which will record risks to the delivery of specific pieces of work or the overall position of the CCG.



2.4 Strategic Risks

Strategic risks are those related to the delivery of the CCG's strategic objectives. They have the highest potential for external impact including engagement with the wider health and social care community and with external stakeholders.

Strategic risks are reviewed and modified by the Governing Body on a quarterly basis and are to be managed as complex processes as opposed to discrete events. The Governing Body will ensure that strategic risks are properly identified and correctly managed, by review of the Governing Body Assurance Framework and performance management.

2.5 Operational Risks

Operational risks consist of risks to the CCG's ongoing day to day business delivery, such as clinical (patient safety), staff safety, security, information, financial and litigation. Whilst they may have some external impact, they mostly impact on the internal functioning and services of the CCG.

As an operational risk may be relevant to two or more Directorates, (e.g. management of conflicts of interest), a responsible Director will be identified for the management of each risk with responsibility for ensuring that appropriate processes are putting place to enable managers and staff to control the risk at Directorate level.

Operational risks will be managed within the local, directorate and committee structures, as appropriate, dependent on the level of risk identified. Significant operational risks, which are not effectively managed, may impact on the delivery of strategic objectives. Therefore managers are required to escalate operational risks to strategic level if and when they are risk rated as Red/Extreme.

3. Objectives

The CCG Governing Body recognises that robust risk management and assurance is an integral part of its governance responsibilities and part of Castle Point and Rochford CCG's culture. The Governing Body is, therefore, committed to ensuring that risk management forms an integral part of its philosophy, practices and business plans rather than viewed or practised as a separate programme, and that responsibility for implementation is accepted at all levels of the organisation.

The overall objective is to make the organisation more effective and able to meet national objectives and the local corporate, clinical and financial governance core objectives.

3.1 The specific Risk Management objectives are to:

- Maintain a risk management framework which provides assurances to the Governing Body.

- To develop the risk management infrastructure across CCG by ensuring that appropriate clinical and non-clinical connections are established and maintained in order to ensure a collaborative approach to risk management.
- To have systems in place to ensure that all staff receive relevant risk management training through corporate and local induction within three months of commencement of employment and on an ongoing basis.
- To ensure that the risk management process escalates both financial and quality of care risks to the Governing Body.
- Ensures processes are based on best practice and national guidance and compliance with any relevant standards;
- Assists the Governing Body in agreeing the Annual Governance Statement;
- Embeds risk management practices into the day-to-day functions of the CCG and within the role of every member of staff.

4. Responsibilities

All staff, Committees, Sub-Committees and groups that support the CCG's business have a responsibility for identifying, assessing and putting systems in place to mitigate any risks to the achievement of strategic objectives, and to ensure these are managed through the risk register system.

4.1 Responsibility of the CCG Governing Body

Castle Point and Rochford CCG Governing Body has a duty to assure itself that the organisation has properly identified the risks it faces, and that it has processes and controls in place to mitigate those risks and the impact they have on the organisation and its stakeholders. This is achieved via review of the Governing Body Assurance Framework and Risk Registers. In order to verify that risks are being managed appropriate and that the CCG can deliver its objectives, the Governing Body receives a copy of the Strategic and Operational Risk Registers and considers reports from Audit, Quality, Finance and Performance and Primary Care Committees. The Governing Body also receives a report from the Sustainability and Transformation Partnership Joint Committee.

The Governing Body is provided with a report on how the CCG is performing against the CCG Improvement and Assessment Framework and the NHS constitutional standards. In particular, the Governing Body monitors progress on action plans to reduce risk levels.

4.2 Responsibility of Governing Body Sub-Committees

4.2.1 Responsibility of the Audit and Risk Committee

The Audit and Risk Committee, in line with the NHS Audit and Risk Committee Handbook, is to ensure the CCG has an effective process in place with regard to risk management. The Audit and Risk Committee is "the Assurance Committee" and monitors the quality of the Assurance Framework and Risk Register and refers significant issues to the Governing Body. The Audit and Risk Committee is the central means by which the Governing Body ensures that effective internal control arrangements are in place. The Audit and Risk

Committee receives and considers the latest iteration of the Assurance Framework and Risk Register at every meeting, along with updates on significant developments.

The Audit and Risk Committee is responsible for providing independent assurance to the Governing Body on the effectiveness of the CCG's risk management systems and processes, including monitoring of compliance with the Risk Management Policy.

The Audit and Risk Committee will receive a copy of the Governing Body Assurance Framework/Strategic Risk Register and Operational Risk Registers at each meeting. The Committee will seek assurance from these documents on the adequacy of the CCG's risk management arrangements and prioritise any risks relating to the CCG's system of financial controls. The Audit and Risk Committee will also review the Risk Management Policy on an annual basis.

The Audit and Risk Committee will also have responsibility for agreeing the annual internal audit plan to ensure that the CCG receives assurance that controls are adequate and effective and will obtain assurance sufficient to enable the Governance Statement to be signed off by the Governing Body at the end of each financial year.

4.2.2 Responsibility of the Quality, Finance and Performance Committee (QFC)

The Quality, Finance and Performance Committee will ensure the CCG develops effective strategies and plans to maintain a sound system of risk management and quality assurance is in place across the CCG, in order to achieve its strategic objectives. The committee will also ensure appropriate recovery plans are in place where performance deviates and recommend approval of strategies to the CCG Governing Body. The sub-committee also serves to provide the CCG, with assurance that the budgets, as delegated, are being managed effectively and efficiently, and with due regard to the governance and financial procedures.

The committee will continuously assess financial and non-financial risks relating to the QIPP plans and ensure the CCG has in place measures and mitigation to manage risk.

The Committee will receive a copy of the Board Assurance Framework/Strategic Risk Register and Operational Risk Registers at each meting and will recommend to the Governing Body the escalation/de-escalation of risks, inclusion of new risks or closure of existing risk except those risks relating to the system of financial control which are within the remit of the Audit and Risk Committee.

4.2.3 Responsibility of the CCG Chair

The role of the Chair is to:

- Lead the Governing Body, ensuring its effectiveness on all aspects of its role

and setting the Governing Body agenda;

- Ensure the provision of accurate, timely and clear information to the Governing Body members;
- Ensure that there is rigorous scrutiny on the organisation's risk management framework and processes;
- Ensure effective communication with staff, patients; public and key stakeholders;
- Arrange regular evaluation of the performance of the Governing Body; to review the actions of its committees and individual directors;
- Facilitate the effective contribution of lay members and to ensure constructive relationships between executives and lay members

4.2.4 Responsibilities of Lay members

Lay members have a role to ensure that the CCG has sound and robust risk management systems in place to monitor the contractual and performance management responsibilities of commissioned services by applying due diligence and scrutiny to test the effectiveness of controls in place to manage risks. Their focus will be strategic and impartial, providing an external view of the work of the CCG that is removed from the day-to-day running of the organisation. They hold the CCG's directors and the Clinical Leads to account on the management of both strategic and operational risks.

The lay members have a lead role in ensuring that the governing body and the wider CCG behaves with the utmost probity at all times.

4.2.5 CCG Accountable Officer (AO)

The Accountable Officer has overall responsibility for ensuring there is an effective risk management system in place within the CCG, for meeting statutory requirements and adhering to guidance issues by NHS England in respect of governance.

4.2.6 Responsibility of the Director of Strategy and Planning

The Director of Strategy and Planning has delegated responsibility for managing strategic development and implementation of organisational risk management and corporate governance and has corporate responsibility for Health and Safety, security management and the Public Sector Equality Duty.

The Director of Strategy and Planning also has corporate responsibility for Emergency Preparedness, Resilience and Response and is accountable for ensuring that appropriate measures are in place to support the CCG to respond to an incident in and outside of working hours.

4.2.7 Responsibility of the Chief Finance Officer

The Chief Finance Officer will report annually to the Governing Body on the adequacy of internal financial control and risk management as part of the

Governing Body's overall responsibility to prepare a statement of internal control for inclusion in the NHS body's annual report.

The Chief Finance Officer will also monitor the work of the Local Counter Fraud Specialist and be responsible for the organisation's overall compliance with the NHS standards in relation to counter fraud.

The Chief Finance Officer also performs the role of Senior Information Risk Officer (SIRO) and Security Management Director and has specific responsibilities in relation to the management of information and security risks, as well.

4.2.8 Responsibility of the Chief Nurse

The Chief Nurse has lead officer responsibility and accountability for safeguarding children and adults for the organisation. They work in partnership with the Local Authority and other key agencies to ensure that the CCG statutory duties in relation to safeguarding children and adults are met. The Chief Nurse also acts as the CCG's Caldicott Guardian.

4.2.9 Executives within the CCG

Executive Directors are responsible for the direct management of strategic and operational risks within their Directorate's area of responsibility, including development and implementation of associated risk management processes. Executive Directors must ensure that all risks within their area of responsibility are recorded and reviewed at least quarterly at Directorate meetings to ensure that controls are adequate and agree further action required to reduce the level of risk. Updates are to be provided to the AD of Assurance prior to each quarterly Audit and Risk Committee and Governing Body review.

4.2.10 Associate Director of Assurance

The Associate Director of Assurance has operational responsibility for the development and implementation and review of the CCG's Risk Management Policy and Assurance Framework and has responsibility for ensuring that comprehensive registers of all significant risks that may impact upon achievement of the CCG's strategic objectives are maintained, updated and reported regularly to relevant Committees and the Governing Body

4.2.11 Responsibility of Senior Managers

All Senior Managers are responsible for ensuring that appropriate and effective risk management processes are in place within their designated areas and scope of responsibility. They are also responsible for ensuring that all members of their staff are aware of the risks within their work environment and of their personal responsibilities, and that all their staff receives appropriate information, instruction and training to enable them to work safely. These responsibilities extend to anyone affected by the CCG's operations, including contractors, members of the public and visitors.

Senior Managers are responsible for ensuring that all necessary risk assessments are carried out within their directorate/department in liaison with relevant advisors where necessary, e.g. Health and Safety, Information Governance.

Senior Managers are responsible for ensuring the identification and mitigation of risk within all investment plans, business cases, and new projects initiated by the CCG.

Senior Managers are responsible for implementing and monitoring any identified and appropriate risk management control measures within their designated areas and scope of responsibility. In situations where Red/Extreme operational risks have been identified and where local control measures are considered inadequate, Directors/Managers are responsible for escalating these risks for the attention of the Quality, Finance and Performance Committee or where relating to the system of financial control, the Audit and Risk Committee.

4.2.12 All CCG Staff

All staff working for the CCG are responsible for:

- Being aware that they have a duty under legislation to take reasonable care of their own safety and the safety of others who may be affected by the CCG's business and to comply with appropriate CCG rules, regulations, instructions, policies, procedures and guidelines;
- Taking action to protect themselves and others from risks;
- Identifying and reporting risks to their line manager;
- Ensuring incidents, claims and complaints are reported using the appropriate procedures and channels of communication;
- Co-operating with others in the management of the CCG's risks;
- Attending mandatory and statutory training as determined by the CCG or their line manager;
- Being aware of emergency procedures relating to their particular locations;
- Reading the CCG's Risk Management Policy and comply with the procedures;
- Ensuring they are aware of the risk management policy;
- Having an understanding of the key risks faced by the CCG, particularly those relevant to the area in which they operate for reporting issues; either concerns or opportunities; that they identify in connection with CCG activities to their line manager for escalation into the formal risk management process as appropriate; and
- Ensuring all contractors, partners and visitors are made aware of the importance of risk management and the mechanisms for feeding concerns into the formal processes.

4.2.13 Contractors, Agency and Locum Staff

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, including:

- The CCG Incident Reporting Policy and the Health and Safety Policy.
- Take action to protect themselves and others from risks.
- Bring to the attention of others the nature of risks which they are facing in order to ensure that they are taking appropriate protective action.

4.2.14 Responsibilities delegated to a Commissioning Support Unit (CSU)

The management of the following functions has been delegated to the ArdenGem CSU:

- HR services
- Business Intelligence
- Financial services including accounts receivable and payable, cash management and production of the year end statutory accounts
- IMT services including GP IT.

There are policies that govern the management of the above functions but it is the responsibility of the CSU to inform the CCG of any significant risks to the strategic objectives of the CCG.

5.0 Risk Management Process

Risk Identification/Internal Control - The CCG has established and maintains, via the Audit and Risk Committee and Quality, Finance & Performance Committee, continual reporting, auditing and monitoring to ensure standards are being implemented, and therefore, risk is controlled to the lowest reasonably practicable levels.

5.1.1 Methods for identifying and managing levels of risk would include:

- **Internal methods,** such as: incidents, complaints, claims and serious incident reporting and identification of trends, audits, QIPP related risks, project risks based on the achievement of project objectives, patient satisfaction surveys, risk assessments, surveys including staff surveys, whistle-blowing. Contract quality monitoring of commissioned services.
- **External methods,** such as: HM Coroner reports, media, national reports, new legislation, patient safety surveys, reports from assessments/inspections by external bodies, reviews of partnership working.

All incidents will be categorised to indicate severity using the risk matrix (Appendix A, Table 3). Details of all incidents are reported to the Quality, Finance and Performance Committee. The Quality, Finance and Performance Committee oversees the management of clinical incidents and management of health and safety incidents.

5.1.2 Quantifying and Scoring Risk

Once a risk is identified it is important to establish the likelihood of it

occurring and the potential impact if it did occur. This is called the original or inherent risk and is measured by using a risk assessment matrix found at Appendix A, Table 3. At this stage an acceptable or target risk level should be established for achievement through mitigating actions.

The risk assessment is a systematic and common approach to quantifying all categories of risk. The matrix assigns values between 1 and 5 to both the likelihood of the risk being realised and the possible consequences of this. These are then multiplied together to give a risk rating.

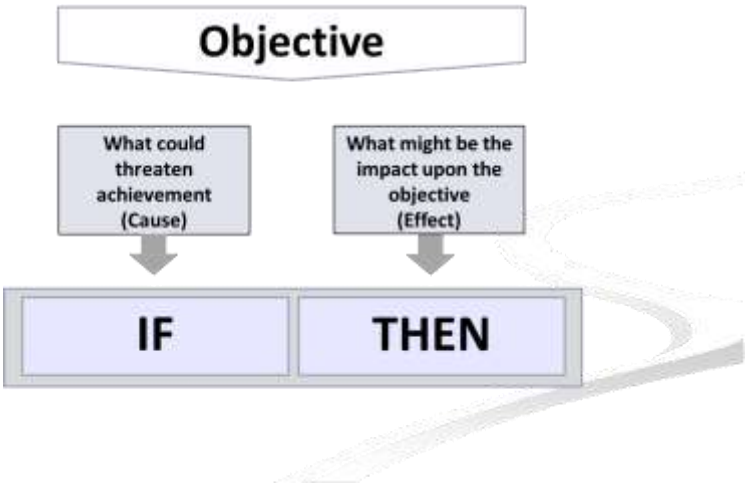
Risk is measured in two dimensions: the *impact* (what the outcome would be should the risk occur) and the *likelihood* (how probably it is that the risk will occur). The matrix that the CCG will use for rating risks is attached at Appendix A and will result in risks being rated in one of the following four categories:

- Extreme risk (red)
- High risk (orange)
- Moderate risk (yellow)
- Low risk (green)

Risk quantifying and scoring should be recalculated at each assessment after mitigating factors to establish a residual or current risk value.

The risk description needs to clearly summarise the potential cause and effect of the risk identified and it is therefore best practice to ensure that risks are described using the following model.

Fig. 1



5.1.3 Definitions of an Acceptable Risk and Risk Appetite

An acceptable risk may be defined as a potential hazard that is either small enough to have an immaterial effect on the achievement of organisational objectives, or is a significant risk that has been mitigated by the establishment of effective controls to minimise the likelihood of the risk occurring, or to minimise the adverse consequences should the risk identified occur.

'Risk appetite' is a threshold – the amount of risk that an organisation is prepared to accept before it takes action or the reducing amount of risk after certain actions, that the organisation finds acceptable to function alongside, with no further action thereafter. The CCG will express its risk appetite by using Risk Appetite Matrix (see Appendix B).

5.1.4 Evaluation of Risk

Risks are identified and managed by all teams across the CCG and are recorded in the Risk Register. Risks are escalated to the Governing Body Assurance Framework (GBAF) if it is considered that they would impact on the strategic objectives of the CCG. Risk escalation (or de-escalation) is reported to and reviewed by the Audit and Risk Committee.

Actions identified to minimise a potential risk are recorded on the Risk Register and include a time scale for expected completion of that action. When actions are complete they form part of the controls within the system.

5.1.5 Treatment of Risk

The following treatment options will be assessed and the most appropriate option selected for the management of each risk.

- **Avoid risk** – not proceeding with the activity likely to generate the risk;
- **Reduce risk** – reducing or controlling the likelihood of the occurrence;
- **Transfer of risk** – arranging for another party to bear or share some part of the risk, through contracts, partnerships, joint working, etc;
- **Accept risk** – some risks may be minimal and retention of them is therefore acceptable.

Once the above options have been considered and the most appropriate way forward identified, a risk option action plan will be drawn up and implemented. The rating and prioritisation of the risk will determine the speed with which the risk action plan should be implemented and at which level of the organisation the risk needs to be reported.

- Extreme (Red) risk – immediate action required. A Director must be informed and s/he will take responsibility for development and implementation of an appropriate risk action plan. Risk and proposed action plan to be reported at Quality, Finance and Performance Committee and Audit and Risk Committee and Governing Body level.

- High (Amber) risk – urgent senior management attention required. Within

one month an appropriate action point must be agreed, usually with a deadline for completion of no more than 6 months. Risk and proposed action plan to be reported at Quality, Finance and Performance Committee and Audit and risk Committee and Governing Body level.

- Moderate (Yellow) risk – specific responsibility for risk assessment and action planning must be allocated to a named person. Usual deadline for completion will be within 6 to 24 months and will depend on resource availability. Risk and proposed action plan to be reported to Quality, Finance and Performance Committee and Audit and Risk Committee and Governing Body level.

- Low (Green) risk – acceptable risk. Periodic monitoring and review may be undertaken at Directorate/departmental level to ensure that risk has not escalated and controls are still effective.

5.2 The CCG Governing Body Assurance Framework and Risk Register

The Governing Body Assurance Framework (GBAF) is a tool for the Governing Body to satisfy itself that risks are being managed and objectives are being achieved. A Governing Body Assurance Framework is also a requirement established by the Department of Health in *Assurance: the Board Agenda* in July 2002. The GBAF must set out:

- Strategic objectives
- Principal risks
- Key controls
- Assurances on controls, including Governing Body reports
- Gaps in control
- Gaps in assurance
- Action plans
- Lead Director

The CCG has established a clear GBAF so that it can confidently sign its Annual Governance Statement. The CCG GBAF reflects significant risks impacting on the CCG's strategic objectives. Significant risks would usually have a score of 15 and above and potentially threaten the achievement of the CCG's strategic objectives. However there are some risks that would not have an inherent risk of 15 and above but are sensitive and would greatly impact the reputation and the strategic objectives of the CCG. Any such risks will be presented to the Executive Team Management by the relevant Director for agreement and inclusion onto the GBAF.

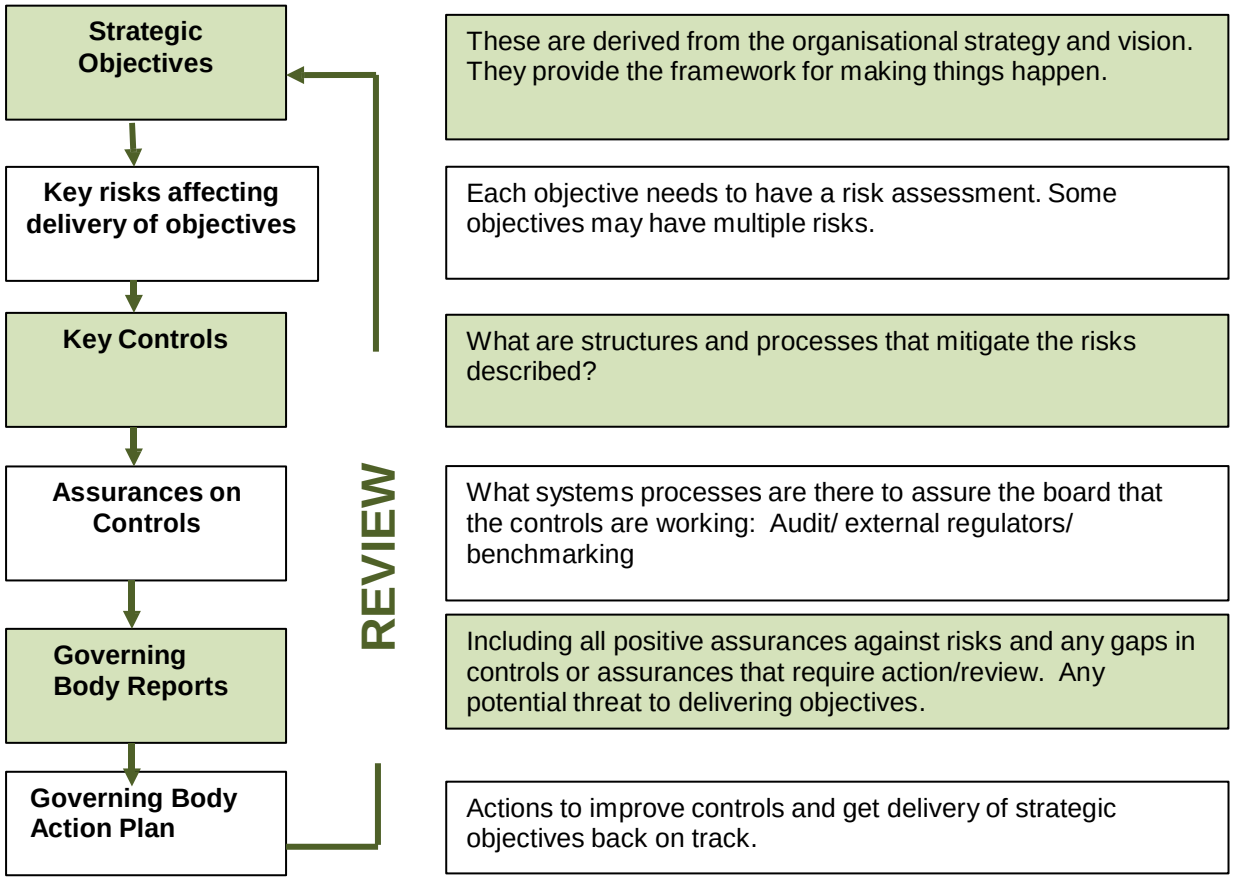
When a GBAF risk has been mitigated and the risk score is reduced the risks will stay on the GBAF for monitoring purposes until the Executive Team Management have agreed that it is no longer a risk to the CCG's strategic objectives. The proposal to remove the risk from the GBAF will then be submitted to the Governing Body as part of the GBAF report. The Governing Body will be the one body within the governance structure to decide whether a risk should be removed from the GBAF.

A Risk Register is a management tool that enables an organisation to understand its comprehensive risk profile. It is a repository for all risk information. It records dependencies between risks and links between risks on the GBAF and risks on the risk register.

The risk register will be used to manage lower level and operational risks. The risk register will be forwarded monthly to Executive team and quarterly to the Quality, Finance & Performance Committee, and Audit and Risk Committee

All significant risks regardless of score should be notified to the Executive Team Management by the relevant Executive for agreement and inclusion on the GBAF. Any risk will be prepared in the same generic format to facilitate collation of information into a single CCG wide Risk Register.

5.3 The Governing Body Assurance Process



5.4 Risk Register

The organisation maintains a risk register. This will be populated by:

- high level risks identified in relation to corporate objectives;
- risks identified through internal or external assessments or reviews;
- risks identified through external compliance assessments (including self-assessments);
- risks identified through evaluation of incident and complaints reporting;
- risks identified through the evaluation of national/ high level 'incident' reports or inquiries;
- risks identified by relevant Committees and
- risks identified proactively through comprehensive risk assessments.

The risk register provides the framework for reporting risks. It is essential that all risks that have been identified by staff are recorded, scored and that they have the appropriate action in place to reduce risk where appropriate.

6.0 Risk Management Information, Training and Support

All staff will be made aware of the CCG's Risk Management Policy, what their role is and the forms of support available to them. Line Managers will be responsible for ensuring that employees' risk management training needs are assessed via local induction and reviewed annually via the CCG's individual performance review procedure.

The AD of Assurance will provide ongoing risk management support to relevant staff and will offer quarterly one to one meetings with all Risk Owners to assist in the review of their risks.

Specific training in risk management will be provided for the Governing Body on an annual basis.

7. Monitoring, Reviewing and Auditing

The Director of Strategy and Planning, as Executive Sponsor of this Policy, will be accountable for monitoring ongoing compliance with this policy.

The Audit and Risk Committee will ensure that the Annual Internal Audit Plan incorporates periodic assurance to the Governing Body on the robustness of CCG's risk management arrangements to support completion of the Governance Statement.

8. Approval and Review Mechanisms

This policy has been developed in light of currently available information, guidance and legislation that may be subject to review. The policy will be reviewed annually by the Quality, Finance and Performance and Audit and Risk Committees and the Governing Body.

9. Equality and Diversity

The 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. All policies and procedures should be developed in line with the CCG's Equality and Diversity policies and need to take into account the diverse needs of the community that is served. The equality impact assessment for this **policy** will be published on the CCG website.

10 Associated Policies and Guidance

- Health and Safety Handbook
- Conflicts of Interest Policy
- Information Governance Policy
- Anti-Fraud and Bribery Policy
- Freedom to Speak Up (Whistleblowing Policy)
- Claims Handling Policy
- Emergency Preparedness, Responsibility and Resilience Policy
- Business Continuity Policy
- Security Policy

11. Version Control

Version	**Date Issued** **Date of Review**	**Author** **Name and Title**	**Comments**
2.0	December 2012	Michelle Angell AD of Assurance	Michelle Angell, Head of Performance and Corporate Services
3.0	May 2014	Michelle Angell AD of Assurance	Policy review and refresh
4.0	December 2014	Michelle Angell AD of Assurance	Policy review and refresh
5.0	December 2016	Michelle Angell AD of Assurance	Policy review and refresh
6.0	October 2017	Michelle Angell AD of Assurance	Reviewed by the Policy Assurance Committee who approved the refreshed Policy in October 2017
7.0	November 2018	Michelle Angell AD of Assurance	Full re-write of policy.
8.0	November 2019	Michelle Angell AD of Assurance	Update

APPENDIX A - CCG Risk Assessment Scoring Guidelines

Introduction

Risk management is a systematic and effective method of identifying risks and determining the most cost effective means to minimise or remove them. It is an essential part of any risk management programme and it encompasses the processes of risk analysis and risk evaluation.

The Castle Point and Rochford CCG Governing Body ensures that the effort and resource that is spent on managing risk is proportionate to the risk itself. Castle Point and Rochford CCG has in place efficient assessment processes covering all areas of risk.

To separate those risks that are unacceptable from those that are tolerable risks should be evaluated in a consistent manner. Risks are usually analysed by combining estimates of consequence and likelihood in the context of existing control measures. The rating of a given risk is established using a two dimensional grid or matrix with consequence as one axis and likelihood as the other.

The following properties are essential for a risk assessment matrix:

- simple to use
- provides consistent results when used by staff from a variety of roles or professions
- capable of assessing a broad range of risks including clinical, health and safety, financial risk or reputation

This guidance can be used on its own as a tool for introducing risk assessment or for improving consistency or scope of risk assessments already in place within the organisation and for training purposes.

Guidance on Consequence Scoring

When undertaking a risk assessment the consequence or how bad the risk being assessed is must be measured. In this context consequence is defined as the outcome or potential outcome of an event. Clearly there may be more than one consequence of a single event.

Consequences can be assessed and scored using qualitative data. Whenever possible, consequences should be assessed against objective definitions across different domains to ensure consistency in the risk assessment process. Despite defining consequence as objectively as possible it is inevitable that scoring the consequences of some risk will involve a degree of subjectivity. It is important that effective, practical based training, and use of relevant examples form part of the implementation of any assessment system to maximise

consistency of scoring across the organisation.

The information in Table 1 should be used to obtain a consequence score. First define the risk explicitly in terms of the adverse consequence that might arise from the risk being assessed (see example 1 for cause and effect methodology). Then use Table 1 to determine the consequence score of the potential adverse outcomes relevant to the risk being evaluated. The examples given in Table 1 are not exhaustive.

How to Use Consequence Table 1:
Choose the most appropriate domain for the identified risk from the left hand side of the table. Then work along the columns in the same row to assess the severity of the risk on the scale of 1-5 to determine the consequence score which is the number given at the top of the column.

Consequence scoring:

1. Negligible
2. Minor
3. Moderate
4. Major
5. Catastrophic

Many issues need to be factored into the assessment of consequence. Some of these are:

- Does the organisation have a clear definition of what constitutes a minor injury?
- What measures are in place to determine psychological impact on individuals?
- What is defined as an adverse event and how many individuals may be affected?

A single risk area may have multiple potential consequences and these may require separate assessment. It is also important to consider from whose perspective the risk is being assessed because this may affect the assessment of the risk itself, its consequences and the subsequent action taken.

By implementing these guidelines the CCG will garner and benefit from more detailed definitions or samples for each consequence score.

Table 1 Assessment Of The Severity Of The Consequence Of An Identified Risk:
Domains, Consequence Scores (severity levels) and Examples of the Score Descriptors

	1	2	3	4	5
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Impact on the safety of patients, staff or public (physical / psychological harm)	Minimal injury regarding no / minimal intervention or treatment	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	Incident leading to death Multiple permanent injuries or irrevocable health effects An event which impacts on a large number of patients
Quality / complaints / audit	Peripheral element of treatment or service suboptimal Informal complaint / injury	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) complaint 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

	1	2	3	4	5
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Human resources / organisational development / staffing / competence	Short-tern 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) Low staff morale Poor staff attendance for mandatory / key training	Uncertain delivery of key objective / service due to lack of staff Unsafe staffing level or competence (>5 days) Loss of key staff Very low morale No staff attending mandatory / key training	Non-delivery of key objectives / service due to lack of staff Ongoing unsafe staffing levels or competence Loss of several key staff No staff attending mandatory training / key training on an ongoing basis
Statutory duty / inspections	No or minimal impact or breech of guidance / statutory duty	Breech of statutory legislation Reduced performance rating unresolved	Single breech in statutory duty Challenging external recommendations / improvement notice	Enforcement action Multiple breeches in statutory duty Improvement notices Low performance rating Critical report	Multiple breeches 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	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.

	1	2	3	4	5
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
		Elements of public expectation not being met			MP concerned (questions in the House) Total loss of public confidence
Business objectives / projects	Insignificant cost increase / schedule slippage	<5 per cent over project budget Schedule slippage	5–10 per cent over project budget Schedule slippage	Non-compliance with national 10–25 per cent over project budget Schedule slippage Key objectives not met	Incident leading >25 per cent over project budget Schedule slippage Key objectives not met
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 Purchasers failing to pay on time	Non-delivery of key objective / Loss of >1 per cent of budget Failure to meet specification / slippage Loss of contract / payment by Results Claim(s) >£1 million
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

Guidelines on Likelihood Scoring

Once a specific area of risk has been assessed and its consequences score agreed, the likelihood of that consequence occurring can be identified by using Table 2 below which includes probability and frequency descriptions. As with the assessment of consequence the likelihood of a risk occurring is assigned a number from 1 to 5 the higher the number the more likely it is the consequence will occur:

Likelihood scoring:

1 Rare
2 Unlikely
3 Possible
4 Likely
5 Almost certain

When assessing likelihood it is important to take into consideration the controls already in place. The likelihood score is a reflection of how likely it is that the adverse consequence described will occur. Likelihood can be scored by considering:

- Frequency (how many times will the adverse consequence being accessed actually be realised?; or
- Probability (what is the chance the adverse consequence will occur in a given reference period?)

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.

Table 2 Likelihood Scores

Frequency and Probability Descriptors

Likelihood Score	1	2	3	4	5
Descriptor	Rare	Unlikely	Possible	Likely	Almost Certain
Frequency How often might it/does it happen	Can't believe the risk will ever happen	Do not expect the risk to happen but it is possible	The event may occur occasionally	The event will probably occur but is not a	The event will undoubtedly occur, possibly
Probability Will it happen or not?	<0.1 per cent	0.1-1 per cent	1-10 per cent	10-50 per cent	>50 per cent

It is possible to use more quantitative descriptions for frequency by considering how often the adverse consequence being assessed will be realised. A simple set of time framed definition for frequency is shown above in Table 2.

However frequency is not a useful way of scoring certain risks, especially those associated with the success of time limited or one off projects such as a new IT system that is being delivered as part of a three year programme or business objective. For these risks the likelihood score cannot be based on how often the consequence will materialise. Instead it must be based on the probability that it will occur at all in a given period. In other words a

three year IT project cannot be expected to fail once a month and the likelihood score will need to be assessed on the probability of adverse consequences occurring within the project's time frame.

With regard to achieving a national target the risk of missing the target will be based on the time left during which the target is measured. The CCG might have assessed the probability of missing a key target as being quite high at the beginning of the year but nine months later if all the control measures have been effective there is a much reduced probability of the target not being met.

This is why specific "probability" scores have been developed for projects and business objectives. Likelihood scores based on probability have been developed from project risk assessment tools from across industry. The vast majority of these agree that any project which is more likely to fail than succeed (that is, the chance of failing is greater than 50 per cent) should be assigned a score of 5.

Risk Scoring and grading

Risk scoring and grading as follows:

Define the risk(s) explicitly in terms of the adverse consequence(s) that might arise from the risk.

Use Table 1 to determine the consequence score(s) (C) for the potential adverse outcome(s) relevant to the risk being evaluated.

Use Table 2 to determine the likelihood score(s) (L) for those adverse outcomes. If possible, score the likelihood by assigning a predicted frequency of occurrence of the adverse outcome. If this is not possible, assign a probability to the adverse outcome occurring within a given time frame, such as the lifetime of a project or a patient care episode. If a numerical probability cannot be determined, use the probability descriptions to determine the most appropriate score.

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

The five by five risk matrix in Table 3 below shows both numerical scoring and colour bandings. The CCG Risk Management Policy is used to identify the level at which the risk will be managed in the CCG, assign priorities for remedial action, and determine whether risks are to be accepted, on the basis of the colour bandings and/or risk score.

Table 3 Risk Matrix

Define the risk(s) explicitly in terms of the adverse consequence(s) that might arise from the risk. Integrate the likelihood score to the matrix.

	Most Likely Consequence				
Likelihood of occurrence	1)None - No obvious injury or harm Loss of 0.1–0.25 per cent of budget Claim less than £10,000	2) Minor - More than 3 days off sick due to injury. Loss of 0.25–0.5 per cent of budget Claim(s) between £10,000 and £100,000.	3) Moderate Hospitalised or medium term injury. Major financial loss (£20K to £100K) including litigation settlement.	4) Major - Significant / permanent harm. Uncertain delivery of key objective/Loss of 0.5– 1.0 per cent of budget. Claim(s) between £100,000 and £1 million Purchasers failing to pay on time.	5) Catastrophic - Death or major disaster / loss Non-delivery of key objective/ Loss of >1 per cent of budget Failure to meet specification/ slippage Loss of contract / payment by results Claim(s) >£1 million
1) Rare - Can't believe the risk will ever happen <0.1 %	1	2	3	4	5
2) Unlikely - Do not expect the risk to happen but it is possible 0.1-1 %	2	4	6	8	10
3) Possible - The event may occur occasionally 1-10 %	3	6	9	12	15
4) Likely - The event will probably occur but is not a persistent issue 10-50 %	4	8	12	16	20
5) Almost certain - The event will undoubtedly occur, possibly frequently >50 %	5	10	15	20	25

Following risk scoring and mapping onto the risk matrix, the risks are assigned grades as follows:

Red (15-25)	**Extreme risk**
Amber (8–12)	**High risk**
Yellow (4–6)	**Moderate risk**
Green (1-3)	**low risk**

The above model risk matrix has the following advantages:

- Most NHS organisations are familiar with the five by five matrix.
- It is simple yet flexible and therefore lends itself to adaptability
- It is based on simple mathematical formulae and is ideal for use in spreadsheets
- Equal weighting of consequence and likelihood prevents disproportionate effort directed at highly unlikely but high consequence risks. This should clearly illustrate the effectiveness of risk treatment
- There are four colour bandings for categorising risk. Even if the boundaries of risk categorisation change we are able to compare "scores" to monitor whether risks are being evaluated in a similar manner

Source: A risk matrix for risk managers – NPSA January 2008

Example of a risk identification and management with the Cause and Effect methodology:

Risk description:

- Concern about the CCG's adherence to the Data Protection Act
- Risk of breaching the DPA

Causes:

- Lack of understanding of the Act by staff
- Low completion rate by staff of IG and data protection e-learning modules
- Line managers do not encourage staff to read and be aware of CCG policies

Effects:

- Patient and/or staff data may be incorrectly processed and shared with 3rd parties
- CCG may incur financial penalties if investigated by the Information Commissioners Office
- CCG may receive adverse publicity and reputational damage
- Level of complaints and litigation claims received may increase

With the knowledge of our individual 'causes', we now know where to concentrate our controls and actions to mitigate or at least reduce the risk.

If we can eliminate or at least reduce the likelihood of each cause occurring then we can reduce the overall likelihood (L) score.

However the chance of us being able to actually reduce the consequence (C) score is low because should the risk be realised the outcome is still likely to be the same (in most cases but probably not all) – so it is the likelihood we are essentially trying to reduce which in turn will of course reduce the overall risk score.

Appendix B Risk Appetite Matrix

Risk Score (tolerance range)	Risk Appetite assessment	Description
1 – 3	Zero/ low risk appetite	The CCG is not willing to accept any risk under any circumstances
4 – 8	Moderate risk appetite	The CCG is willing to accept some risks in certain circumstances
9 – 12	High risk appetite	The CCG is willing to accept risks that may result in identified impact.
15 – 25	Extreme/ very high risk appetite	The CCG accepts risks in this category that are likely to result in identified impact.

Risk Category	Risk Appetite	Rationale
Quality	**6** Moderate	We will ensure the provision of high quality services to our patients and will only rarely accept risks which threaten that goal
Safety	**3** Low	We hold patient and staff safety in the highest regard and will seek to minimise any risks that threatens either
Regulatory	**1** Low	We will comply with all legislation relevant to the CCG and will not accept any risk which, if realised, would result in non-compliance
Reputation	**6** Moderate	We will maintain high standards of conduct and will accept risks that may cause reputational damage only in certain circumstances and where the benefits merit the risk
Innovation	**12** High	We encourage a culture of innovation within the CCG and are willing to accept risks associated with this approach
Finance	**6** Moderate	We will stay within set financial limits and will accept risks that may cause financial loss only in certain circumstances and where the benefits merit the risk
Partnerships	**9** High	We will work with other organisations to ensure the best outcome for patients and are willing to accept the risks associated with a collaborative approach

If a risk's residual score is higher than the risk appetite for that particular category of risk, more will need to be done to manage the risk and this may require additional resources.

If the risk's residual score is the same as or lower than the risk appetite for that particular category of risk, the risk will be considered tolerable (although it will continue to be monitored if risk-rated at a 4 or above).