NHS
Somerset
Clinical Commissioning Group

RISK MANAGEMENT STRATEGY

APPROVED for Silver Phase

November 2019

CONTENTS

APPROVED for Silver Phase

APPROVED for Silver Phase

RISK MANAGEMENT STRATEGY

VERSION CONTROL

Document Status:	APPROVED
Version:	1.6 v0.13

DOCUMENT CHANGE HISTORY		
Version	**Date**	**Comments**
1.0	June 2012	Draft document in preparation for authorisation April 2013
1.1	June 2012	Draft amended to reflect published structure for the Somerset CCG
1.2	21 June 2012	Draft amended to reflect comments
1.3	5 May 2013	Amended to include comments from CCG Governing Body
1.4	10 Feb 2016	Revised version recommended to the Governance Committee: • General refresh to reflect organisational change Risk scoring matrix revised, Appendix 1, section 4.2 • Project risk management added in section 1.7 • Removal of requirement to produce annual risk management report, which will be covered instead by an annual review of the Risk Management Strategy
1.5	Feb 2016	Final
1.6	2019	Revised version for Board Assurance review

APPROVED for Silver Phase

Equality Impact Assessment (EIA) Form OR EIA Screening Form completed. Date:	25 November 2019

Sponsoring Director:	David Freeman, Chief Operating Officer, Somerset Clinical Commissioning Group
Reviewer(s):	Somerset Clinical Commissioning Group Chief Executive, Somerset Clinical Commissioning Group Directors, Somerset Clinical Commissioning Group Deputy and Associate Directors, Chair of the Somerset Clinical Commissioning Group Governing Body, Somerset Clinical Commissioning Group Audit provider.
Approval	Somerset Clinical Commissioning Group Audit Committee, Somerset Clinical Commissioning Group Clinical Executive Committee and Somerset Clinical Commissioning Group Governing Body.
Author:	Claire Miller Interim Risk and Assurance Manager

APPROVED for Silver Phase

1 RISK MANAGEMENT STRATEGY

Introduction

1.1 Risk is an inherent part of the commissioning and provision of primary and acute (planned or emergency) healthcare, with the successful achievement of these objectives being subject to uncertainty of either an opportunity or threat with an associated impact.

1.2 The risk management strategy (RMS) encompasses identifying, assessing and monitoring risk, controls, assurance, accountability, reporting, roles and responsibility, tolerance, appetite, acceptable/unacceptable risk and escalation.

1.3 Definitions for terms used in this policy to describe any risk management function are included within Appendix 6.

Scope

1.4 This strategy applies to Somerset Clinical Commissioning Group (CCG) as an individual organisation and as a partner in the Sustainability and Transformation Partnership (STP), and to the 'risk stakeholders' associated to the CCG.

1.5 'Risk stakeholders' applies to all CCG staff (permanent, temporary, fixed term employment), volunteers; all committee members of committees within the CCG governance structure.

1.6 Risk management is the responsibility of all risk stakeholders and is defined within Appendix 1.

1.7 Incident reporting, management and learning is outside of the scope of this policy.

1.8 The management and submission of risks in relation to national risk registers are outside of the scope of this policy.

Purpose

1.9 The purpose of this strategy is to provide a structured, integrated and coherent approach for the management of CCG risk to minimise threats, and maximise opportunities. The strategy seeks to ensure:

- CCG risks in relation to the delivery of its strategic objectives are minimised where a threat exists.

- CCG risks in relation to the delivery of its strategic objectives are maximised where an opportunity exists.

APPROVED for Silver Phase

- That the wellbeing of the health population of Somerset and CCG staff is optimised.

- That the assets, business systems and CCG finances are protected.

- The implementation and ongoing improvement, together with the management of a comprehensive, integrated and standardised approach to the management of risk.

- Standardised processes are in place for updating and reviewing risks based on new developments or actions taken.

- Alignment to CCG governance, control, risk and assurance to support the Governing Body Assurance Framework (GBAF).

- To outline roles, responsibilities, authority and accountability for risk management as defined in Appendix 1 embedded within the CCG governance structure with the inclusion of the Sustainability and Transformation Partnership (STP).

- To identify a standard process and model for risk assessment.

- To ensure that its risk management strategy supports CCG's governance and leadership.

1.10 This policy will inform the CCG's Statement of Internal Control.

2 RISK MANAGEMENT STATEMENT

2.1 Risk management is a process based on best governance practice, designed to ensure that NHS organisations are doing their 'reasonable best' to manage themselves in order to meet their objectives and protect patients, staff, the public and other stakeholders against risks of all kinds.

2.2 As part of the CCG's governance arrangements, this strategy outlines risk management, emphasising the way that the CCG can implement its strategic objectives having formulated and designed a risk management system. A clear understanding of the key strategic objectives and a commitment to corporate governance will ensure that risk analysis and management are applied throughout the organisation.

2.3 The CCG will ensure that this policy will be compliant with all relevant legislation and regulation.

APPROVED for Silver Phase

2.4 The CCG will ensure that risk management is established throughout the organisation with guidance on roles, responsibilities, processes and procedures.

2.5 The management of clinical and non-clinical risk is accepted as a key organisational responsibility and an integral part of management and governance processes.

2.6 The Governing Body (GB) has the overall responsibility for the CCG's risk management. CCG committees will have the responsibility for overseeing and monitoring risks together with individual role based responsibilities as outlined in Appendix 1.

2.7 This policy will be communicated to the risk stakeholders as defined in section 6 of this policy.

2.8 The strategy will seek to support CCG clinical leads, directly employed staff and commissioned providers in managing risk through safe systems of practice, including the identification of risk and the use of clinical guidelines and protocols to minimise risk.

2.9 The CCG Audit Committee will ensure, on behalf of the CCG Governing Body that safe systems and robust risk management arrangements are in place for the commissioning of health services by the CCG.

2.10 Integrated risk management is the identification and assessment of the collective risks (strategic, corporate and clinical) that affects the value, and the implementation of the organisation's strategic objectives. This risk management strategy aims to maximise the value of an integrated risk management approach by demonstrating the CCG's risk profile and investigating mitigating actions and controls.

2.11 Integrated risk management is strategic and operational. It addresses fluctuations that can occur in the wider environment. Using a risk management approach means that risks are not seen in isolation and by following the strategy the organisation responds to all the risks faced by the CCG in delivery of its objectives.

2.12 Integrated risk management evaluates the organisation's total risk exposure and ensures that the organisation has the ability to achieve its strategic objectives, to provide sustainable, high quality, safe and effective care and treatment services for the people of Somerset.

2.13 In future the scope of the CCG organisation's responsibilities for risk management within the commissioning and health community may alter, and this policy may need to be altered to reflect these changes. Consequently, the risk management strategy and policy will be reviewed regularly to incorporate any modifications required due to unforeseen factors and new policies that may impact on delivery of the CCG's strategic objectives.

APPROVED for Silver Phase

2.14 CCG is committed to delivering a risk management culture that underpins the successful achievement of the organisation's strategic objectives by ensuring no unduly negative behaviors for those identifying risks exists and the adoption of a fair blame culture, supporting staff to raise concerns, Being Open and listening and operating the Duty of Candour.

2.15 Clinical risk will be subject to this policy and will be the responsibility of CCG Quality and Nursing directorate in addition to the clinical incident management process. The Risk Management Strategy also endeavors to promote a culture whereby patient safety is at the heart of all clinical practice and where staff are open to sharing learning from the experiences related to the management of risk.

2.16 CCG is committed to continuously improving the management of risk throughout the organisation.

2.17 The CCG seeks to ensure that through its governance structure (as outlined in the CCG constitution) and for those identified as accountable that:

- Wherever possible, risks that could and should have been identified are.
- Wherever possible, any negative effect from realised risks fall outside of the impact defined against the risk.

2.18 Considered risk taking is defined through the CCG risk appetite as described in Appendix 5.

2.19 The CCG is committed to competent risk management by providing access to comprehensive risk training, guidance and advice.

2.20 The CCG has statutory obligations to ensure that risks arising from its undertaking are assessed through a standard risk assessment process as detailed within Appendix 7.

2.21 The CCG seeks to ensure that the outcomes from risk management are incorporated into policy development.

2.22 The CCG seeks to ensure that the principles of successful risk management outlined in this policy are implemented and sustained.

2.23 The CCG uses a computer application to record and monitor risk entries and activities to support effective risk management and reporting. This risk system is Datix.

APPROVED for Silver Phase

3 ARRANGEMENTS FOR RISK MANAGEMENT

Definitions

3.1 Appendix 6 sets out the definitions relating to this policy.

Principles of successful Risk Management

3.2 The principles of successful risk management are fundamental to the management of the direction, control and decision making of an organisation. The principles are:

- Ensuring risk management is not a compliance activity, instead being utilised and sighted across the whole organisation as an everyday discipline to successfully deliver objectives.
- A process that follows risk identification, assessment, treatment, monitoring, reporting, learning and improving.
- A culture where risk management is considered an essential and positive element in the provision of healthcare.
- Honest and open communication about the risks to achieving the organisation's objectives and the resources needed to reduce them.
- Recognition of effective risk management and learning from error.
- Collaborative working using accurate, timely and credible information (internal and external working).
- Using collaborative working to manage and plan risk.
- High quality and relevant risk data.
- Clarity of business realities and threats from market forces.
- Clarity on risk appetite and risk appetite review.
- Standardised check and challenge to ensure robust accountability and action focused conversation.
- Integration of risk with strategic objective setting and review.
- Integration of performance measures to risk appetite and tolerance.

APPROVED for Silver Phase

- Continuous improvement of risk management and assurance to support the organisation’s objectives together with the health and care system’s strategic objectives.

- Awareness and planning for the resources required to deliver risk management and risk controls.

- Integration with an organisation’s ambition to be high performing.

- Integration with an organisation’s workforce appraisals.

- Organisational wide, continuous communication of risk.

- Enterprise risk management applied for 1st, 2nd and 3rd tier defence.

- Management of issues which stem from a risk which has realised.

APPROVED for Silver Phase

Roles and Responsibilities for Risk Management

3.3 Appendix 1 sets out the responsibilities and accountabilities of specific roles and forums within the CCG governance structure (as defined within the CCG Constitution and CCG Governance Handbook).

Risk Management Process

3.4 Appendix 2 sets out the risk management process relating to this policy including tolerance, escalation and risk monitoring, which has been founded on the UK standard ISO 31000.

Notification of a serious or urgent risk

3.5 If a serious or urgent risk arises in the CCG, this must be reported immediately to a CCG Director or if out of hours the CCG Director on call.

Significant Risk

3.6 A significant risk is defined in Appendix 6.

Acceptable Risk

3.7 An acceptable risk is defined in Appendix 6.

Risks and risk assessments from suppliers or third parties

3.8 If a risk assessment has been carried out by a supplier, contractor or third party who are providing services to the CCG the outcome of the assessment must adhere to the process defined in this policy.

Impact Assessments

3.9 Impact assessments may exist before a risk is initiated. Additionally, impact assessments may be used as part of the analysis carried out for the risk assessment at the request of the Risk Owner or a CCG manager.

3.10 The General Data Protection Regulations 2016 and Data Protection Act 2018 mandates that a Data Protection Impact Assessment (DPIA) is completed before actions likely to result in high risk to individuals' rights and freedoms occur. DPIAs are risk assessments that are concerned with the use of personal data within an organisation. They are designed to assist organisations to consider whether data is secure, whether there is or could be any risk to individuals' privacy, and whether organisations are meeting their obligations. The focus is on the potential for harm – to individuals or to society at large, whether it is physical, material or non-material. To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. DPIA must comply with the CCG's DPIA Policy.

Risks registers

3.11 Datix provides the function of a risk register for the CCG; apart from project plan risk registers, risk registers must not exist or be created outside of Datix.

3.12 Projects and programmes will hold their own risk registers and manage those risks in accordance to their chosen risk management strategy (which should be agreed at the preliminary stages of the project). Any project or programme that identifies a risk with a current risk rating score greater or equal to the CCG significant risk tolerance and if the risk is in relation to time, cost, outcome (agreed outcomes of the project/programme) or workforce, must enter the risk into the CCG risk management process

3.13 Partnerships will hold their own risk registers and manage those risks in accordance to their chosen risk management strategy (which should be agreed at the preliminary stages of the partnership formation). The CCG representative in the partnership must follow the risk management process as defined within this policy for any partnership risk. If the partnership does not undertake a risk assessment, the risk must be assessed using the risk assessment as defined within this policy. The

APPROVED for Silver Phase

CCG risk exposure of any partnership risk must be treated as a separate risk and follow the risk management process as defined within this policy. The CCG representative is responsible for upholding the continuous management of that risk between the CCG and partnership.

Transferring Risk

3.14 The guidance with regard to the transferring of risk is defined within the CCG Scheme of Reservation and Delegation.

Minimising Risk

3.15 Risk stakeholders have an important role in minimising risk.

3.16 The CCG will ensure that learning takes place from the outcomes of risk management which will be shared with risk stakeholders through the CCG's governance arrangements, raising awareness and training.

Risk Blueprint

3.17 The CCG Risk Blueprint will enable the CCG to map the hierarchy of the interrelationships between risks and to ensure that changes within interrelated risks are reflected throughout.

Risk Plan

3.18 As part of the risk assessment process, a risk plan must be created to address any gaps in controls or assurance in addition to any tasks required to continue to deliver the controls and/or assurance to an effective level. The requirement for risk plans are outlined in appendix 3.

The Governing Body Assurance Framework (GBAF)

3.19 The GBAF provides an evidence based 'mechanism' that supports the successful delivery of strategic & regulatory objectives of the CCG. It provides this by:

- Triangulating in a standardised way, the right information (accurate, relevant, and timely) to provide assurance across the governance structure of the CCG.

- Being a tool to support the functions of the CCG for a tool for improvement, not performance management.

- Supporting action focused conversations for those who have responsibilities in risk management.

APPROVED for Silver Phase

- Providing evidence that our controls for risk and delivery are working and are effective.

- Providing the ability to clearly identify, challenge and mitigate when they are not.

- Providing evidence of assurance for risk/controls.

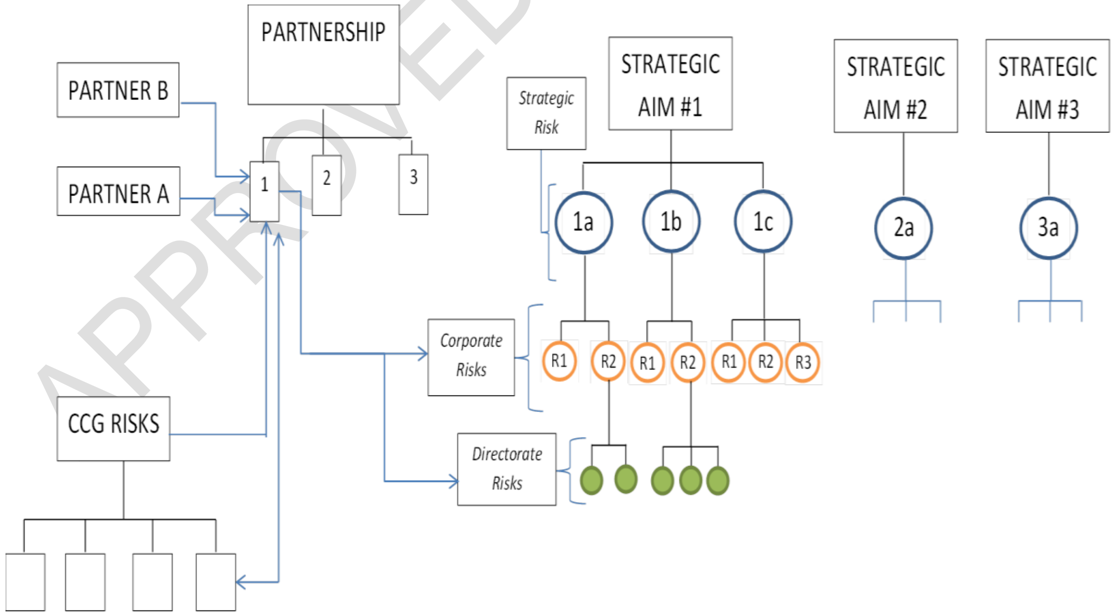
3.20 The GBAF will be presented at Governing Body meetings (excluding development sessions) and at CCG committee meetings in relation to the risks and responsibilities of those committees.

Reporting Risk to external organisations

3.21 The CCG may be required to report risk to organisations external to the CCG. Reporting requirements to such organisations will be defined by and managed by the Risk Management Group.

Risk Structure

3.22 The structure of risks will comprise of directorate risks, corporate risks and strategic risks as shown in the diagram below.



APPROVED for Silver Phase

Realisation of risks to become risk-issues

3.23 A risk-issue plan should be included within a risk plan, outlining the actions that would be taken to address any risk-issue that occurs as a result of a risk realising.

3.24 The risk-issue plan should be communicated to the necessary audience in respect of the risk.

3.25 The prioritisation of risk-issues for action or escalation should be communicated to the subsequent forum (as defined in A11.12) to identify the affect upon the CCG and/or existing risk.

APPROVED for Silver Phase

4 MONITORING AND COMPLIANCE

4.1 An annual review of this policy to reflect any improvements and /or changes in the requirements for risk management will be undertaken by a resource identified by the CCG's Chief Operating Officer.

4.2 An annual review of this policy for compliance will be produced by an audit team assigned by the CCG every three years as a minimum.

4.3 All documents in existence at the time of the issue of this policy will remain in effect until such time as they are reviewed, replaced or cancelled.

4.4 The Audit Committee will ensure, on behalf of the CCG Governing Body that a robust and effective risk management process is in place for the commissioning of health services by the CCG.

5 IMPLEMENTATION, TRAINING AND SUPPORT

5.1 The effective implementation of this policy will facilitate the delivery of high quality service and, alongside stakeholder training and support, will provide an awareness of the measures needed to prevent, control and contain risk.

5.2 The CCG will:

- Ensure that the policy is reviewed and ratified according to the CCG Scheme of Reservation and Delegation.

- Ensure risk stakeholders have access to a copy of this policy.

- Ensure that risk stakeholders have the knowledge, skills, support and access to expert advice necessary to implement policies, procedures and guidelines associated with this policy.

- Monitor and review the performance of the organisation in relation to the management of risk and the continuing suitability and effectiveness of the systems and processes in place to manage risk.

5.3 The CCG Head of Governance is responsible for archiving all previous versions of this policy and supporting evidence of review, ratification and approval of this policy.

APPROVED for Silver Phase

Training

5.4 Awareness and compliance to this policy must be undertaken through training.

5.5 Training for all risk stakeholders in respect of this policy is vital to ensure that stakeholders are able to comply with this policy and the obligations to the Health and Safety at Work Act 1974.

5.6 Risk stakeholders staff will receive training through staff induction and through the CCGs mandatory training system.

5.7 Risk stakeholders will be supported with any additional training that is requested or identified through appraisals and CCG training needs analysis.

5.8 The process for recording attendance to training and the follow up of non-attendance for all risk stakeholders is defined within the CCG's Mandatory Training Policy.

6 COMMUNICATION WITH RISK STAKEHOLDERS

6.1 This policy is available on the designated CCG policy sharing location.

6.2 This information can be provided in other formats or languages on request.

6.3 Following approval of this policy, risk stakeholders will be notified through the CCG extranet.

APPROVED for Silver Phase

7 REFERENCES

7.1 The Functions of Clinical Commissioning Groups, Department of Health, 2012.

7.2 Risk Management ISO 31000, International Organization for Standardization, 2018

7.3 NHS Audit Committee Handbook: HFMA practical guide. 4th Edition, Healthcare Financial Management Association, 2018.

7.4 Audit and risk assurance committee handbook, HM Treasury, 2016.

7.5 Building a Framework for Board/Governing Body Assurance 360 Assurance, Good Governance Institute, 2014.

7.6 The Health Quality Improvement Partnership Good Governance Handbook, Good Governance Institute, 2015.

7.7 The UK Corporate Governance Code, Financial Reporting Council, 2018

7.8 The new Integrated Governance Handbook 2016, Good Governance Institute, 2016.

7.9 Risk Management Strategy, Oxford University Hospitals, 2015.

7.10 Health and Safety at Work Act, Health and Safety Executive, 1974.

7.11 The Statement on Internal Control: A Guide for Audit Committees, National Audit Office, 2010.

7.12 Core Competencies in Public Service Risk Management, CFA and Alarm, 2011.

7.13 Health and Social Care Integrated Joint Boards: Risk Appetite, Good Governance Institute, 2017.

7.14 Risk Guidance Paper Appetite & Tolerance, Institute of Risk Management, 2011.

7.15 A Risk Practitioners Guide to ISO 31000: 2018, Institute of Risk Management, 2018.

7.16 Risk Control Effectiveness, Paladin Risk Management Services, 2017.

7.17 Terms of reference for the risk committee, ICSA, 2019.

7.18 The Orange Book, Management of Risk - Principles and Concepts, HM Government, 2019.

APPROVED for Silver Phase

7.19 A risk matrix for risk managers, National Patient Safety Agency, 2008.

7.20 IFRS 7 Financial Instruments: Disclosures, International Financial Reporting Standards, 2018.

7.21 Data Security Standard 1 Personal confidential data, Health and Social Care Information Centre, 2019.

7.22 National Cyber Security Centre, Risk management guidance V0.1, August 2016.

8 ASSOCIATED DOCUMENTATION

8.1 All documents in the CCG Library of Procedural documents are relevant but in particular this policy should be read in conjunction with the following policies and documents:

- Risk Management Process Standard Operating Procedure
- Risk Management Strategy – FAQs
- Risk Management Risk Assessment Standard Operating Procedure
- Records Management Policy
- Infection Prevention and Control Policy
- Serious Incident Policy
- Incident Reporting Policy
- 'Being Open' Policy
- Whistle Blowing Policy
- Complaints Policy
- Health and Safety Policy
- Data Protection Policy
- Scheme of Reservation and Delegation
- Data Protection Impact Assessment Policy
- CCG Constitution

APPROVED for Silver Phase

9 CONCLUSION

9.1 The CCG has embedded risk management into its governance arrangements. It is essential that risks can be rated in a common currency within the NHS and other organisations, allowing financial, operational and clinical risks to be compared against each other and prioritised. The tools included in this strategy provide a system for risk assessment that can be used easily and consistently by staff working within the organisation and our key partners.

APPROVED for Silver Phase

10 EQUALITY IMPACT ASSESSMENT

SOMERSET County Council

NHS Somerset Clinical Commissioning Group

EQUALITY IMPACT ASSESSMENT FORM

INITIAL INFORMATION

Name of policy/service: Risk Management Strategy Version number (if relevant): 1.6	Directorate/Service: Corporate
Assessor's Name and Job Title: Claire Miller, Interim Risk and Assurance Manager. Telephone: 01935 384006	Date: 25.11.19
Sponsoring Director/Council Officer: David Freemen, Chief Operating Officer, Somerset CCG	Date: 02.12.19

Please refer to the Equality Impact Assessment Guidance to complete this form.

OUTCOMES
Briefly describe the aim of the policy / service and state the intended outcomes for patients and / or staff?
The aim of this policy is define the risk management strategy of the Somerset CCG. It is intended to ensure that risk management is used as a business tool to enable the successful delivery of the CCG's strategic, corporate and directorate objectives. Additionally, this policy aims to add value to staff by providing the guidance to proactively manage risk and therefore to reduce the impact of risk to patients and services commissioned by the CCG.
EVIDENCE
What data / information have you used to assess how this policy / service might impact on protected groups?
• A risk management survey was issued in November 2019. • The CCG Risk Management Group's terms of reference includes monitoring for risk management which does not comply with The Equality Act 2010 (the Act) which prohibits direct or indirect discrimination, harassment or the victimisation of people with the following 'protected characteristics' • Using the CCG staff forum to identify and concerns in respect of this policy and people with protected characteristics.
Who have you consulted with to assess possible impact on protected groups? If you have not consulted other people, please explain why?

APPROVED for Silver Phase

The Quality & Equality Officer, Somerset Clinical Commissioning Group has been consulted (November 2019)

ANALYSIS OF IMPACT ON EQUALITY

The Public Sector Equality Duty requires us to **eliminate** discrimination, **advance** equality of opportunity and **foster** good relations with protected groups. Consider how this policy / service will achieve these aims.

Please read ‘Questions to Ask’ in the EIA guidance.
Note: in some cases it is legal to treat people differently (objective justification).[1]

- ***Positive outcome*** *– the policy/service eliminates discrimination, advances equality of opportunity and fosters good relations with protected groups*
- ***Negative outcome*** *– protected group(s) could be disadvantaged or discriminated against*
- ***Neutral outcome*** *– there is no effect currently on protected groups*

Please tick to show if outcome is likely to be positive, negative or neutral. Consider direct and indirect discrimination, harassment and victimisation.

APPROVED for Silver Phase

Protected Group	Positive outcome	Negative outcome	Neutral outcome	Reason(s) for outcome
Age	✓			Risks in relation to this group are not restricted.
Disability[2]	✓			Risks in relation to this group are not restricted.
Religion or belief	✓			Risks in relation to this group are not restricted.
Sex	✓			Risks in relation to this group are not restricted.
Sexual Orientation	✓			Risks in relation to this group are not restricted.
Gender Reassignment	✓			Risks in relation to this group are not restricted.

[1] See definition of ‘objective justification’ in guidance
[2] Includes mental impairment, learning difficulty (dyslexia). Full definition in guidance.

Protected Group	Positive outcome	Negative outcome	Neutral outcome	Reason(s) for outcome
Race and ethnicity	✓			Risks in relation to this group are not restricted.
Pregnancy and maternity	✓			Risks in relation to this group are not restricted.
If applicable, Other Disadvantaged Groups (for example carers, veterans and military staff, homeless, rurality, low income, etc.)[3]	✓			Risks in relation to this group are not restricted.

MONITORING OUTCOMES Monitoring is an ongoing process to check outcomes. It is different from a formal review which takes place at pre-agreed intervals.
What methods will you use to monitor outcomes on protected groups?
The CCG Risk Management Group will provide the CCG Audit Committee with an annual statement regarding the outcomes on protected groups in respect of this policy.

APPROVED for Silver Phase

REVIEW
How often will you review this policy / service? (Minimum every three years)
This policy aims to be reviewed annually.
If a review process is not in place, what plans do you have to establish one?
N/A

IMPLEMENTING THE POLICY / SERVICE

Negative outcomes – action plan

An Equality Impact Assessment **cannot be signed off** until negative outcomes are addressed. What actions you have taken / plan to take to remove / reduce negative outcomes?

Action taken / Action to be taken	Date	Person

[3] These groups are not protected groups under the Equality Act 2010 but should be considered alongside the protected groups where applicable.

		responsible
N/A	N/A	N/A
If a negative outcome(s) remain explain why you think implementation is justified.		
N/A		

Lead organisation	
NHS	**Somerset County Council**
Equality Impact Assessment forms must be authorised by the sponsoring Director Send completed form to the Patient Engagement Team at: somccg.eia@nhs.net.	**Equality Impact Assessment forms must be authorised by the sponsoring Council Officer** Send completed form to: txrutland@somserset.gov.uk
The EIA form and guidance are currently available on NHS Somerset CCG website: http://www.somerset.nhs.uk/welcome/about-us/equality-and-diversity/equality-impact-assessments/	

APPROVED for Silver Phase

APPENDIX 1: RESPONSIBILITIES AND ACCOUNTABILITY

CCG Role Based Responsibilities

A11.1 CCG Chief Executive: As the Accountable officer for the CCG, the Chief Executive (CEO) has overall responsibility for the CCG and for the effective delivery of risk management in order to protect all persons who may be affected by the CCG's business.

A11.2 The CEO is supported by members of the Governing Body in discharging those responsibilities and these are referred to in the CCG Constitution which includes a scheme of delegation.

A11.3 The CEO has overall responsibility for the CCG's risk management strategy and provides assurance to the CCG Governing Body of the effectiveness and continuous improvement of:

- Governance.
- The risk management process.
- The GBAF.
- Assessment of risk.
- Audit of risk.
- Setting risk tolerance for corporate risks.
- Quality of risk management.
- Approval of any risk management statements within the CCG Annual Report and annual Governance Statement.

A11.4 CCG Chief Operating Officer is responsible for:

- Implementing and maintaining effective governance and risk management arrangements in the CCG in accordance to this policy.

- Information governance, health and safety, security management and liaison with the Local Security Management Specialist to ensure robust security management.

- Setting risk tolerance for their directorate risks.

- Provision and approval of papers in relation to risk for the Clinical Executive Committee (CEC).

- Delegated responsibility for the provision of the risk management services on behalf of all CCG Directors excluding those responsibilities which are directly outlined in this policy.

A11.5 CCG Director of Quality & Nursing: Is responsible for:

- Progressing patient safety and clinical governance, clinical risk and assurance for the CCG.

- The system administration of the CCG risk system.

APPROVED for Silver Phase

- Setting risk tolerance for their directorate risks.

- Provision and approval of papers in relation to risk for the Patient Safety & Quality Assurance Committee.

- The assurance that quality impact assessments, clinical incidents or complaints are identified and where necessary reflected in risks within the risk management process.

A11.6 CCG Director of Finance, Performance and Contracting: Is responsible for:

- Progressing financial and performance risk management and for ensuring that effective risk management is in place as part of commissioning arrangements.

- Setting risk tolerance for their directorate risks.

- Provision and approval of papers in relation to risk for the Finance and Performance Committee.

- The assurance that financial impact assessments are identified and where necessary reflected in risks within the risk management process.

- The assurance to the Audit Committee for the processes and management of International Financial Reporting Standards.

A11.7 The Caldicott Guardian is responsible for ensuring that the CCG satisfies the highest practical standards for managing patient information and governance risks. The Caldicott Guardian will act as the conscience of the organisation in this respect, and will actively support work to manage risks relating to patient information.

A11.8 All Directors and Senior Managers: are responsible for:

- Compliance with this policy and are accountable for the risk management (clinical, operational and financial) performance within their areas of authority.

- Ensuring staff accountable to them understand their responsibilities in respect of this policy.

- Ensuring that there are people designated to fulfil the risk management roles as defined in Appendix 1 and that these people are aware, trained and are providing the requirements of this role to comply with this policy.

- Ensuring that risks are captured in relation to their area of responsibility in accordance with this policy.

APPROVED for Silver Phase

- Using the CCG risk system in accordance to this policy for capturing risk data and ensuring that risk registers are not held outside of the CCG risk system or do not comply with the CCG Records Management Policy.

- Disseminate to their service/department for implementation and to ensure that the policy is implemented within their areas of authority.

- Where risk assessments identify a need for additional resources, this is incorporated into an action plan and, if under their control, is implemented.

- Ensuring that the resources and effort in delivering the risk are proportionate to the risk and where they are not, it is identified within the risk assessment and escalated in compliance with this policy.

- The approval and management for risk assessments as identified within this policy.

- Allow sufficient time for Risk Assessors to conduct adequate risk assessment and risk management.

- Ensuring that learning from events and risk assessments is disseminated throughout the organisation.

- Identifying and recording any problems relating to this policy and ensuring that this is communicated to their line manager and the CCG Risk Manager.

- Receive risks from teams/specialties within their directorate to assess against directorate objectives, directing actions, timescales and ownership where necessary.

- Approve directorate level risk within the agreed committee and/or GB meeting papers schedule.

A11.9 Risk stakeholders are responsible for:

- Adherence to this policy.

- To provide further information in relation to risks as necessary.

- Using the CCG risk system as and when directed by their line manager in accordance to this policy.

- Where there is responsibility for the assignment of contractors, adherence to risk management arrangements as defined in the CCG Health and Safety Policy and in particular the ‘Health & Safety at Work Act 1974’.

APPROVED for Silver Phase

- Ensuring that their personal practice at work is safe and effective as possible, and that it complies with the provisions laid down in CCG, Standing Orders and Standing Financial Instructions.

- Adhering to a positive culture of risk management to support compliance with this policy.

A11.10 CCG Risk Manager is responsible for and accountable to the Chief Operating Officer for:

- Developing, implementing, monitoring and continuous improvement of the CCG's Risk Management Strategy and Risk Management process.

- Leading and coordinating risk management activities to support the delivery of the CCG Risk Management Strategy.

- Leading and coordinating risk management activities to support risk.

- Leading and coordinating risk training and induction.

- Leading and coordinating development of risk management programmes to enable the CCG to meet legal obligations.

- Leading and coordinating a risk awareness culture within the CCG.

- Leading and coordinating the provision of the GBAF, assurance framework reporting and any risk management reports.

A11.11 CCG Specialist Advisors are responsible for advising and performing risk management in respect of specialist areas being:

- Health and Safety.

- Manual Handling and ergonomic safety.

- Fire Safety.

- Information Governance.

- Finance.

- Patient quality and safety.

- Safeguarding.

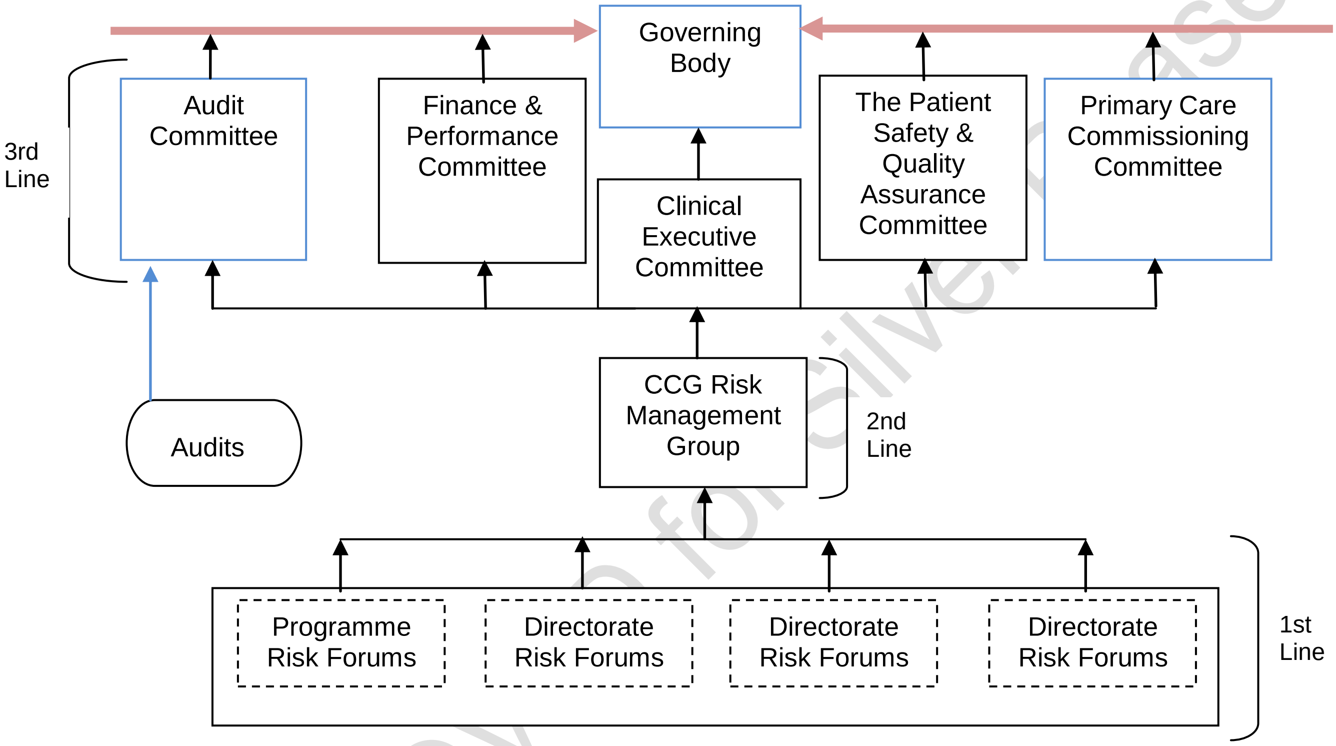
- Public Health.

- Criminal/Legal.

APPROVED for Silver Phase

CCG and Sustainability & Transformation Partnership Forum Responsibilities

A11.12 The diagram below shows the forums that have responsibility for risk management in the monitoring and oversight of risk within the CCG. It details the process flow of verification and validation of risk to ensure that all necessary actions have been completed and that the risk information triangulates appropriately. This will support high quality risk reporting and enable action focused conversations within the forums. This diagram does not indicate risk management accountability or assurance.


Governing Body
3rd Line
Audit Committee
Finance & Performance Committee
Clinical Executive Committee
The Patient Safety & Quality Assurance Committee
Primary Care Commissioning Committee
Audits
CCG Risk Management Group
2nd Line
Programme Risk Forums
Directorate Risk Forums
Directorate Risk Forums
Directorate Risk Forums
1st Line

APPROVED for Silver Release

A11.13 The CCG Governing Body is ultimately responsible and accountable for the comprehensive and effective management and governance of risks faced by the CCG. The CCG Governing Body will:

- Agree the CCG's strategic aims and objectives, and review these on an annual or biannual basis.

- Identify the strategic risks that may prevent the CCG from achieving its strategic objectives.

- Agree that where strategic risks have realised, where change to the CCG strategy is required.

- Receive the GBAF to assess strategic risks against strategic objectives and agree further actions, ownership and deadlines in respect of strategic risks controls and assurances.

- Receive corporate risks which are identified for the Governing Body's attention in accordance to this policy and agree further actions, ownership and deadlines in respect of strategic risks controls and assurances.

- Review risk compliance metrics as identified by the GBAF in order to agree further actions, ownership and deadlines with regards to assurance or risk control.

- Review and approve the Risk Management Strategy policy.

- Approve the recommendations of any audit in respect of this policy.

- Ratify changes to this policy when required.

- Define and review the CCG's risk appetite.

- Ensure that the risk management process operates successfully to deliver and the risk appetite.

- Set the tolerance for risk capacity against CCG strategic aims.

- Set the tolerance for risk appetite against CCG strategic aims.

- Set the tolerance for the significant risk definition.

- Set the risk tolerance for strategic risks.

- Evaluating the organisational capacity to handle risk.

- Ensure they are adequately equipped with the knowledge and skills to fulfil their risk management duties.

- Ensure the effectiveness of its internal control system and risk management arrangements protect patients, staff, the public, and other stakeholders against risks of all kinds.

- Receive support from the Audit Committee in respect risk management to comply with the Public Sector Internal Audit standards.

A11.14 The Clinical Executive Committee will:

- Receive the GBAF to assess strategic risks against strategic objectives and agree further actions, ownership and deadlines in respect of strategic risks; agree risks for escalation to the Governing Body.

APPROVED for Silver Phase

- Receive the risk assurance framework reporting to assess corporate risks and agree further actions, ownership and deadlines with regards to assurance or risk control; agree risks for escalation to the Governing Body.

- Receive actions for risks that have been identified for escalation by the Risk Management Group and agree further actions, ownership and deadlines with regards to assurance or risk control.

- Review risk compliance metrics as identified by the assurance framework reporting in order to agree further actions, ownership and deadlines with regards to assurance or risk control.

- Submit any changes to this policy to the CCG Governing Body when required for ratification.

- Review and approve the recommendations of any audit in respect of this policy.

- Approve the Risk Management Group's terms of reference.

- Provide the clinical leadership in relation to risks identified within this committee's responsibilities.

- Instruct risk reassessment where necessary.

A11.15 The Patient Safety & Quality Assurance Committee will:

- Receive the GBAF to assess Quality and Nursing risks and agree further actions, ownership and deadlines with regards to assurance or risk control; agree risks for escalation to the Governing Body.

- Receive actions for risks that have been identified for escalation by the Risk Management Group and agree further actions, ownership and deadlines with regards to the Corporate Risk Register, assurance or risk control.

- Review risk compliance metrics as identified by the GBAF in order to agree further actions, ownership and deadlines with regards to assurance or risk control.

- Instruct risk reassessment where necessary.

A11.16 The Remuneration Committee will not undertake any roles and responsibility in regard to risk management.

APPROVED for Silver Phase

A11.17 The Primary Care Committee will:

- Receive the GBAF to assess Primary Care risks and agree further actions, ownership and deadlines with regards to assurance or risk control; agree risks for escalation to the Governing Body.

- Receive actions for risks that have been identified for escalation by the Risk Management Group and agree further actions, ownership and deadlines with regards to the Corporate Risk Register, assurance or risk control.

- Review risk compliance metrics as identified by the GBAF in order to agree further actions, ownership and deadlines with regards to assurance or risk control.

- Instruct risk reassessment where necessary.

A11.18 The Finance and Performance Committee will:

- Receive the GBAF to assess Finance risks and agree further actions, ownership and deadlines with regards to assurance or risk control; agree risks for escalation to the Governing Body.

- Receive actions for risks that have been identified for escalation by the Risk Management Group and agree further actions, ownership and deadlines with regards to the Corporate Risk Register, assurance or risk control.

- Review risk compliance metrics as identified by the GBAF in order to agree further actions, ownership and deadlines with regards to assurance or risk control.

- Instruct risk reassessment where necessary.

A11.19 CCG Director's Monday meeting
The Executive Directors will meet jointly on a weekly basis and will undertake the following:

- Receive risks in accordance to the assigned risk monitoring activities defined in Appendix 4 to agree further actions, ownership and deadlines with regards to assurance or risk control.

- Instruct risk reassessment where necessary.

A11.20 The scope of the Risk Management Group's work is defined in the terms of reference for this committee (Appendix 8). This group is not a delegated forum from the Governing Body. This group is an internal risk management forum to facilitate effective management of risk.

APPROVED for Silver Phase

A11.21 The work undertaken by the Risk Management Group should be described in a separate section of the CCG's annual report and the Risk Management Group chair should attend the AGM to respond to any relevant questions relating to the committee's responsibilities.

A11.22 The Risk Management Group will:

- Ensure that the integrity of interrelated risks is maintained with any change and/or impact cascaded throughout the risk blueprint.

- Ensure that the risks they receive provide triangulation of risk information for each risk or aggregation of risk for the recipient committees.

- Escalate matters of concern or attention to the relevant risk overseeing and or monitoring forum.

- Recommend the undertaking of a risk assessment or risk reassessment where necessary.

- Oversee the provision and submission of risks to external organisations including any in relation to the CCG Specialist Advisors.

- Ensure that the risk plans which underpin the delivery of the effectiveness of the controls and the effectiveness of the assurance and delivering to the timescales identified within the risk assessment.

- Use performance data or other information sources identified within the risk assessment to scrutinize the risk data to ensure the triangulation of the risk data.

APPROVED for Silver Phase

Audit Committee

A11.23 The role of the Audit Committee is to:

- Review the findings of internal (and external) audits in relation to the policy, the GBAF and Corporate Risk Register and any agreed management action.

- Seek assurance that the risk management process is robust and fit for purpose and report the outcome to the CCG Governing Body.

- Review the Risk Management Strategy prior to Governing Body ratification.

Internal Audit

A11.24 The risk management strategy and GBAF will be subject to periodic review by internal audit to assess the design and effectiveness of the risk management controls and any specific requirements that the CCG specify within their terms of reference for internal audit.

Risk Management Process

A11.25 Third Party: a person or organisation outside of the CCG who may identify or produce work that identifies a potential risk.

A11.26 Risk Identifier: any person identified as a risk stakeholder (as defined within section 1.6) may identify risk.

A11.27 Risk Assessor: a CCG member of staff with the employment grade of band 7 or above that has been given the authority to perform CCG risk assessments by their line manager.

A11.28 Risk Owner: a CCG member of staff with the employment grade of band 7 or above that has been given the authority to approve CCG risk assessments by their line manager within the tolerance and escalation detailed within this policy and is accountable for the management of the risk. Risk plans can be approved by the risk owner to support the risk assessment.

A11.29 Monitoring Forum: is the forum responsible for the risks related to their area of work in line with the risk monitoring activities and roles and responsibilities as defined in this policy. They will approve or identify actions in respect of those risks to be completed before the risks are subsequently reported to the overseeing committee. They may also request actions of other committees in relation to risks.

A11.30 Overseeing Committee: is an executive level forum that is accountable for risks in line with the risk monitoring activities defined in this policy. For strategic risks and corporate risks, the Governing Body is the overseeing committee; for directorate risks the committees established for the directorates are the overseeing committees. They may also request actions of other committees in relation to risks.

APPROVED for Silver Phase

APPENDIX 2: RISK MANAGEMENT PROCESS

A21.1 The risk management process is a list of coordinated and standardised activities that enable the stakeholders to comply with this policy and to provide the necessary risk data for the GBAF and assurance framework reporting.

Initiation, Assessment and Creating a Risk

A21.2 The risk management process is defined within the Risk Management Process Standard Operating Procedure.

Updating and Monitoring Risk

A21.3 The responsibilities for risk monitoring activities are defined in Appendix 4.

A21.4 Throughout the lifecycle of a risk, risk data can become obsolete or antiquated over time.

A21.5 Any update of risk data attributed to the uncontrolled risk, risk controls or target risk post the risk assessment, then approval will be at the request of the Risk Owner, CCG Director, monitoring forum, Risk Management Group and/or overseeing committee.

A21.6 If any risk data relating to the uncontrolled or target controlled risk is updated post risk assessment approval, the risk assessment for the risk must be updated and saved as an updated version (to ensure audit trail integrity) and follow the risk assessment process (Appendix 7) and risk management process (Appendix 2).

A21.7 The monitoring of new, closed, increased risk score and decreased risk score will be monitored as part of the risk monitoring activities are defined in Appendix 4.

Tolerance

A21.8 Tolerance reflects the boundaries upon which certain levels of responsibility being individual and/or forum within the governance structure can operate before escalation and/or any formal instruction.

A21.9 Tolerance can be set for qualitative and quantitative measures.

A21.10 The CCG should aims to review tolerance levels annually or during periods of increased uncertainty or adverse change.

A21.11 The responsibility for setting risk tolerance is defined in Appendix 1 which defines the setting of risk tolerances at the different levels of the

APPROVED for Silver Phase

organisation, thresholds for escalation and authority to act, and evaluating the organisational capacity to handle risk.

A21.12 The responsibility for setting tolerance for the risk significant risk is defined in Appendix 1.

A21.13 Qualitative tolerance is defined through the risk appetite as in Appendix 5.

A21.14 Quantitative tolerance is defined through risk exposure as defined in Appendix 1.

APPROVED for Silver Phase

Escalation

A21.15 Escalation is required within risk management in order to safeguard the risk against future difficulty and to ensure that the correct approval, awareness and decision making can occur from the appropriate audience within the CCG governance structure.

A21.16 Uncontrolled risk tolerance: If the risk’s monetary exposure exceeds the risk tolerance, the Risk Assessor will need to verify the tolerance is correct and is not required to escalate. The Risk Owner will be required to seek a counter approval of this risk from their line manager.

A21.17 Uncontrolled risk appetite: If the risk appetite is “OUT OF RANGE”, the Risk Assessor will not need to escalate.

A21.18 Target controlled risk: Where the controls have been assigned to the risk (within the risk assessment) and the total impact of the controls against is less than the risk exposure, the dates by which the controls or assurance are outside the timescales of the risk and/or the risk exposure is outside of the tolerance and/or the risk appetite is “OUT OF RANGE”, no escalation is required from the Risk Assessor as the Risk Owner will take these elements into consideration when assigning a “yes” or “no” to the “Is the risk acceptable as a target controlled risk” question within the risk assessment. The Risk Owner may assign a “no” to the “Is the risk acceptable as a target controlled risk” question if they have identified any of the following:

- That the controls do not balance the risk exposure.
- The dates by which the controls or assurance are outside the timescales of the risk.
- The risk exposure is outside of the tolerance and/or the risk appetite is “OUT OF RANGE”.

The Risk Owner must complete their rational for this choice and then seek a counter approval from their line manager.

A21.19 Target controlled risk appetite: Where the target controlled risk appetite is “OUT OF RANGE”, the Risk Owner will need to ensure that all possible considerations for potential additional controls have been applied. The Risk Owner will be required ensure that the target risk appetite is “IN RANGE”.

A21.20 Whenever the exposure of a risk is increased from the exposure stated when the risk was initially assessed, this should be escalated to the risk owner for permission and action to reassess.

A21.21 Whenever the current controlled risk score, likelihood or severity is over the uncontrolled risk score, likelihood or severity this should be escalated to the risk owner for permission and action to reassess.

A21.22 Whenever the effectiveness of controls or the effectiveness of assurance delivery dates breach the deadline date specified within the risk assessment, this should not be a reason to reassess.

Closing a Risk

A21.23 A risk can be closed once it has reached its target risk rating and/or when the risk can no longer happen (perhaps it already has occurred, or maybe it can no longer occur.) If it’s a project risk, then it’s when the project has closed. Closed risks are highlighted to committees for approval of closure.

A21.24 When there is a change to the CCG strategy, any associated strategic, corporate or directorate risks may need to be closed in order to create the new or revised risks which align to the strategic aims. Closed risks are highlighted to committees for approval of closure.

APPROVED for Silver Phase

APPENDIX 3: RISK MATRIX AND RISK GRADING

A31.1 Choose the most appropriate domain for the identified risk from the Risk Severity Matrix (based on the '*A risk matrix for risk managers, National Patient Safety Agency, 2008)* table below along 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 based on the consequences described. Next, refer to the Risk Likelihood Matrix as shown below. When selecting the likelihood take into consideration the controls currently in place. The likelihood score is a reflection of how likely it that the consequence described in your selection will occur either by 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?). Likelihood cannot be based on how often the consequence will materialize. It must be based on the probability that it will occur at all in a given period e.g. likelihood of consequences occurring within the project's time frame, or a patient care episode or within a national target's remaining time during which the target is measured.

Risk Severity Matrix

	1	**2**	**3**	**4**	**5**
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
A. Impact on the safety of patient, staff or public (physical / psychological harm)	Minimal injury requiring no / minimal intervention or treatment. No time off work required.	Minor injury or illness requiring minor intervention. Requiring time off work for <3 days. Increase in length of hospital stay by 1-3 days.	Moderate injury requiring professional intervention. Requiring time off work for 4-14 days. Increase in length of hospital stay by 4-15 days. RIDDOR/agency reportable incident. An event which impacts on a small number of patients.	Major injury leading to long-term incapacity / disability. Requiring time off work for >14 days. Increase in length of hospital stay by >15 days. Mismanagement of patient care with long-term effects.	Incident leading to death. Multiple permanent injuries or irreversible health effects. An event which impacts on a large number of patients.

AP for Silver Phase

	1	2	3	4	5
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
	Incorrect medication dispensed but not taken. Incident resulting in a bruise / graze. Delay in routine transport for patient.	Wrong drug or dosage administered, with no adverse effects. Physical attach such as pushing, shoving or pinching, causing minor injury. Self-harm resulting in minor injuries. Grade 1 pressure ulcer. Laceration, sprain, anxiety requiring occupational health counselling (no time off work required).	Wrong drug or dosage administered with potential adverse effects. Physical attack causing moderate injury. Self harm requiring medical attention. Grade 2/3 pressure ulcer. Healthcare – acquired infection (HCAI). Incorrect or inadequate information / communication on transfer of care. Vehicle carrying patient involved in a road traffic accident. Slip / fall resulting in injury such as a sprain.	Wrong drug or dosage administered with adverse effects. Physical attack resulting in serious injury. Grade 4 pressure ulcer. Long-term HCAI. Retained instruments / material after surgery requiring further intervention. Haemolytic transfusion reaction. Slip / fall resulting in injury such as dislocation / fracture / blow to the head. Loss of a limb. Post-traumatic stress disorder. Failure to follow up and administer vaccine to baby born to a mother with hepatitis B.	Unexpected death. Suicide of a patient known to the service in the past 12 months. Homicide committed by a mental health patient. Large-scale cervical screening errors. Removal of wrong body part leading to death or permanent incapacity. Incident leading to paralysis. Incident leading to long-term mental health problem. Rape / serious sexual assault.
B. Quality / complaints / audit	Peripheral element of treatment or service sub-optimal. Informal complaint / inquiry.	Overall treatment or service sub-optimal. Formal complaint (stage 1). Local resolution. Single failure to meet internal standards. Minor implications for patient safety if unresolved. Reduced performance rating if unresolved.	Treatment or service has significantly reduced effectiveness. Formal complaint (stage 2). Local resolution (with potential to go to independent review). Repeated failure to meet internal standards. Major patient safety implications if findings are not acted on.	Non-compliance with national standards with significant risk to patients if unresolved. Multiple complaints / independent review. Low performance rating. Critical report.	Incident leading to 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.

AP

	1	2	3	4	5
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
C. Human resources / organisational development / staffing / competence	Short-term low staffing levels that temporarily reduces service quality <1 day	Low staffing level that reduces service quality.	Late delivery of key objectives / 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 objectives / service due to lack of staff. Unsafe staffing level or competence (>5 days). Loss of key staff. Very low staff morale. No staff attendance for 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.
D. Statutory duty / inspections	No or minimal impact or breech of guidance / statutory duty	Breech of statutory legislation. Reduced performance rating if unresolved.	Single breech of 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.
E. Adverse publicity / reputation	Rumours. Potential for public concern.	Local media coverage – short-term reduction in public confidence. Elements of public expectation not being met.	Local media coverage – long-term reduction in public confidence.	National media coverage with <3 days service well below reasonable public expectation.	National media coverage with >3 days service well below reasonable public expectation. MP concerned (questions in the House). Total loss of public confidence.
F. 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.
G. 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.

AP

	1	2	3	4	5
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
H. 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.

APPROVED for Silver Pl

Risk Likelihood Matrix

Likelihood Score	1	2	3	4	5
Descriptor	Rare	Unlikely	Possible	Likely	Almost Certain
Probability	This will probably never happen / recur. Not expected to occur for years	Do not expect it to happen / recur but it is possible it may do so. Expected to occur at least annually.	Might happen or recur occasionally. Expected to occur at least monthly.	Will probably happen / recur, but it is not a persisting issue / circumstances. Expected to occur at least weekly.	Will undoubtedly happen / recur, possibly frequently. Expected to occur at least daily.
Probability	<0.1 % probability. of failing is <0.1 %	0.1-1 % probability. of failing is between 0.1-1%	1-10 per cent probability; of failing is between 1-10 %	10-50 per cent probability; of failing is between 10-50 %	>50 % probability; of failing is greater than 50 %
Control completeness	All controls are strong with no control gaps – if risk was to materialise, it may be likely as a result of external circumstances outside of our control or external factors not known to the organisation.	The controls have <10% of their control gaps outstanding - if risk was to materialise, it may be likely to be caused by external factors not known to the organisation.	The controls have 10% to 50% of their control gaps outstanding.	The controls have 51% to 70% of their control gaps outstanding.	The controls have 71% to 100% of their control gaps outstanding.
Strength of controls	All controls are effective	Majority of controls are effective.	Majority of controls are mostly effective.	Majority of controls are partially effective.	Majority of controls are not effective

APPR ce

Risk RAG Rating

A31.2 The table x below shows the 5 x 5 numerical and colour coded grading which form a RAG rating.

	Likelihood				
Severity	**1**	**2**	**3**	**4**	**5**
	Rare	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
5 Catastrophic	5	10	15	20	25
4 Major	4	8	12	16	20
3 Moderate	3	6	9	12	15
2 Minor	2	4	6	8	10
1 Negligible	1	2	3	4	5

Risk Grading

A31.3 For grading risk, the scores obtained from the risk matrix are assigned grades as follows:

1-3 Low	Lowest level of threat, no risk plan required but monitoring required.
4-6 Moderate	Enough threat for a risk plan to be required and risk monitoring required.
8-12 High	Pronounced threat with a mandatory risk plan to be required and risk monitoring required.
15-25 Extreme	Excessive a mandatory risk plan to be required and risk monitoring required.

Risk Assurance RAG

A31.4 For selecting the assurance RAG:

GREEN - Full assurance provided over the effectiveness and delivery:

- Complete listed for assurance
- KPIs defined against the risk and are being populated.
- Actions to deliver the gaps in assurance are on time and within budget
- List of assurances are fit for purpose.

AMBER

- Some gaps in list for assurance
- Some KPIs defined against the risk and are being populated.
- Some actions to deliver the gaps in assurance are on time and within budget
- List of assurances are partially fit for purpose.

APPROVED for Silver Phas

RED

- incomplete item listed for assurance i.e. item identified for assurance is not in place or is antiquated (may not be something that the CCG provides so may not be on the action list)
- no KPIs defined against the risk
- actions to deliver the gaps in assurance are 2 months over timescale, >20% over budget
- List of assurances are not fit for purpose.

Control Effectiveness RAG

A31.4 For selecting the effectiveness of controls, the RAG status is shown below. The criterion of measure within each RAG is defined within the risk assessment:

Effective
Mostly Effective
Partially Effective
Not Effective

APPROVED for Silver Phase

APPENDIX 4: RISK MONITORING ACTIVITIES

A44.1 Significant risk tolerance is set at the current controlled risk score equal to twelve and above (>=12).

A44.2 Directorate risks that are considered for corporate risks are: directorate risks with a current controlled risk score equal to twelve and above (>=12).

A44.3 Directorate risks: The table below shows the monitoring activities that should be undertaken to manage directorate risks. The overseeing committees for directorate risks are:

- Quality & Nursing risks within Patient Safety & Quality Assurance Committee.
- Finance & Performance risks within Finance & Performance Committee.
- Primary Care risks within Primary Care Committee.
- Operations risks within Clinical Executive Committee.

for Silver Phase

UC	CC	**Monitoring activities – Directorate risks** (UC = Uncontrolled risk RAG, CC = Current Controlled risk RAG)
🟥	🟥	**Ensure activities to reduce risk are urgently prioritised and proximity, exposure, KPIs, control & assurance is verified with Director.** Immediate Director awareness. Monitoring Forum: Directorate - weekly. Director's weekly meeting. Risk Management Group: Monthly. Overseeing committee – quarterly.
🟥	🟧	**Ensure activities to reduce risk are on track and affect from proximity, exposure KPIs, control & assurance.** Monitoring Forum: Directorate - weekly. Director's weekly meeting where proximity is within the next 2 weeks and/or risks with a controlled current risk score greater or equal to the significant risk tolerance which may generate a corporate risk. Risk Management Group: Monthly. Overseeing committees: quarterly for controlled current risk score greater or equal to the significant risk tolerance.
🟥	🟨	**Ensure activities to reduce risk are on track and affect from proximity, exposure KPIs, control & assurance.** Monitoring Forum: Directorate - monthly. Risk Management Group: Monthly. Overseeing committees: quarterly for controlled current risk score greater or equal to the significant risk tolerance.
🟥	🟩	**Ensure controls are effective as high reliance on controls to mitigate risk.** Monitoring Forum: Directorate - monthly.
🟧	🟥	**Ensure activities to reduce risk are urgently prioritised and proximity, exposure, KPIs, control & assurance is verified with Director.** Immediate Director awareness. Monitoring Forum: Directorate - weekly. Director's weekly meeting. Risk Management Group: Monthly. Overseeing committee – quarterly.
🟧	🟧	**Ensure activities to reduce risk are on track and inside proximity and with no increase in exposure, effectiveness or assurance.** Monitoring Forum: Directorate - weekly. Risk Management Group: Monthly

🟧	🟧	Overseeing committees quarterly for controlled current risk score greater or equal to the significant risk tolerance.
	🟨	**Ensure risks are monitored for changes within the risk that could affect risk score.** Monitoring Forum: Directorate - monthly. Risk Management Group: Monthly
	🟩	**Ensure risks are monitored for changes within the risk that could affect risk score.** Monitoring Forum: Directorate: quarterly reviews inside proximity and with no downturn in exposure, KPIs, control and assurance. Risk Management Group in month if proximity is within 4 weeks and/or downturn in exposure, KPIs, control and assurance.
🟨	🟥	**Ensure activities to reduce risk are urgently prioritised and proximity, exposure, KPIs, control & assurance is verified with Director.** Immediate Director awareness. Monitoring Forum: Directorate - weekly. Director’s weekly meeting. Risk Management Group: Monthly. Overseeing committee – quarterly.
🟨	🟧	**Ensure activities to reduce risk are on track and inside proximity and with no increase in exposure, effectiveness or assurance**. Monitoring Forum: Directorate - weekly. Risk Management Group: Monthly Overseeing committees quarterly for controlled current risk score greater or equal to the significant risk tolerance.
🟨	🟨	**Ensure risks are monitored for changes within the risk that could affect risk score.** Monitoring Forum: Directorate - monthly. Risk Management Group: Monthly
🟨	🟩	**Ensure risks are monitored for changes within the risk that could affect risk score.** Monitoring Forum: Directorate: quarterly reviews inside proximity and with no downturn in exposure, KPIs, control and assurance. Risk Management Group in month if proximity is within 4 weeks and/or downturn in exposure, KPIs, control and assurance.
🟩	🟥	**Ensure activities to reduce risk are urgently prioritised and proximity, exposure, KPIs, control & assurance is verified with Director.** Immediate Director awareness. Monitoring Forum: Directorate - weekly. Director’s weekly meeting. Risk Management Group: Monthly. Overseeing committee – quarterly.
🟩	🟧	**Ensure activities to reduce risk are on track and inside proximity and with no increase in exposure, effectiveness or assurance**. Monitoring Forum: Directorate - weekly. Risk Management Group: Monthly Overseeing committees quarterly for controlled current risk score greater or equal to the significant risk tolerance.
🟩	🟨	**Ensure risks are monitored for changes within the risk that could affect risk score.** Monitoring Forum: Directorate: quarterly reviews inside proximity and with no downturn in exposure, KPIs, control and assurance. Risk Management Group in month if proximity is within 4 weeks and/or downturn in exposure, KPIs, control and assurance.
🟩	🟩	**Ensure risks are monitored for changes within the risk that could affect risk score.** Monitoring Forum: Directorate: quarterly reviews inside proximity and with no downturn in exposure, KPIs, control and assurance. Risk Management Group in month if proximity is within 4 weeks and/or downturn in exposure, KPIs, control and assurance.

APPROVED for Silver Phase

A41.4 Corporate risks: The table below shows the monitoring activities that should be undertaken to manage corporate risks.

A44.5 Corporate risks that are considered for strategic risks are: corporate risks with a current controlled risk score equal to twelve and above (>=12).

UC	CC	**Monitoring activities – corporate risks** (UC = Uncontrolled risk RAG, CC = Current Controlled risk RAG)
🟥	🟥	**Ensure activities to reduce controlled risk are prioritised and are on track and proximity, exposure, KPIs, control & assurance is verified with CEO.** Immediate Chief Executive Officer awareness. Monitoring Forum: Director's weekly meeting. Directorate - monthly where risk domain is within directorate. Risk Management Group: Monthly. Overseeing committee: CEC - Monthly. GB - bimonthly.
🟥	🟧	**Ensure activities to reduce controlled risk are on track and affect from proximity, exposure KPIs, control & assurance.** Monitoring Forum: Director's weekly meeting where proximity is within the next 2 weeks. Directorate - monthly where risk domain is within directorate. Risk Management Group: Monthly Overseeing committee: CEC - Monthly. GB - bimonthly for controlled current risk score greater or equal to the significant risk tolerance.
🟥	🟨	**Ensure activities to reduce controlled risk are on track and affect from proximity, exposure KPIs, control & assurance.** Monitoring forum: Directorate - monthly where risk domain is within directorate. Risk Management Group: Monthly Overseeing committee: CEC - Monthly. GB – bimonthly where proximity is within the quarter.
🟥	🟩	**Ensure controls are effective as high reliance on controls to mitigate risk.** Monitoring forum: Director's weekly meeting where proximity is within the next 2 weeks. Risk Management Group: Monthly
🟧	🟥	**Ensure activities to reduce controlled risk are prioritised and are on track and proximity, exposure, KPIs, control & assurance is verified with CEO.** Immediate Chief Executive Officer awareness. Monitoring Forum: Director's weekly meeting. Directorate - monthly where risk domain is within directorate. Risk Management Group: Monthly. Overseeing committee: CEC - Monthly. GB - bimonthly.
🟧	🟧	**Ensure activities to reduce controlled risk are on track and inside proximity and with no increase in exposure, effectiveness or assurance**. Monitoring forum: Director's weekly meeting where proximity is within the next 2 weeks. Risk Management Group: Monthly. Directorate - monthly where risk domain is within directorate. Overseeing committee: CEC - Monthly. GB - bimonthly for controlled current risk score greater or equal to the significant risk tolerance.
🟧	🟨	**Ensure activities to reduce controlled risk are on track and inside proximity and with no increase in exposure, effectiveness or assurance**. Monitoring forum: Directorate - monthly where risk domain is within directorate. Risk Management Group: Monthly Overseeing committee: CEC - Monthly. GB – bimonthly where proximity in the quarter.
🟧	🟩	**Ensure risks are monitored for changes within the risk that could affect risk score.** Monitoring forum: Director's weekly meeting: quarterly reviews inside proximity and with no downturn in exposure, KPIs, control and assurance. Risk Management Group in month if

🟧	🟩	proximity is within 4 weeks and/or downturn in exposure, KPIs, control and assurance.
🟨	🟥	**Ensure activities to reduce controlled risk are prioritised and are on track and proximity, exposure, KPIs, control & assurance is verified with CEO.** Immediate Chief Executive Officer awareness. Monitoring Forum: Director's weekly meeting. Directorate - monthly where risk domain is within directorate. Risk Management Group: Monthly. Overseeing committee: CEC - Monthly. GB - bimonthly.
🟨	🟧	**Ensure activities to reduce controlled risk are on track and inside proximity and with no increase in exposure, effectiveness or assurance**. Monitoring forum: Director's weekly meeting where proximity is within the next 2 weeks. Risk Management Group: Monthly. Directorate - monthly where risk domain is within directorate. Overseeing committee: CEC - Monthly. GB - bimonthly for controlled current risk score greater or equal to the significant risk tolerance.
🟨	🟨	**Ensure activities to reduce controlled risk are on track and inside proximity and with no increase in exposure, effectiveness or assurance**. Monitoring forum: Directorate - monthly where risk domain is within directorate. Risk Management Group: Monthly Overseeing committee: CEC - Monthly. GB – bimonthly where proximity is within the quarter.
🟨	🟩	**Ensure risks are monitored for changes within the risk that could affect risk score.** Monitoring forum: Director's weekly meeting: quarterly reviews inside proximity and with no downturn in exposure, KPIs, control and assurance. Risk Management Group in month if proximity is within 4 weeks and/or downturn in exposure, KPIs, control and assurance.
🟩	🟥	**Ensure activities to reduce controlled risk are prioritised and are on track and proximity, exposure, KPIs, control & assurance is verified with CEO.** Immediate Chief Executive Officer awareness. Monitoring Forum: Director's weekly meeting. Directorate - monthly where risk domain is within directorate. Risk Management Group: Monthly. Overseeing committee: CEC - Monthly. GB - bimonthly.
🟩	🟧	**Ensure activities to reduce controlled risk are on track and inside proximity and with no increase in exposure, effectiveness or assurance**. Monitoring forum: Director's weekly meeting where proximity is within the next 2 weeks. Risk Management Group: Monthly. Directorate - monthly where risk domain is within directorate. Overseeing committee: CEC - Monthly. GB - bimonthly for controlled current risk score greater or equal to the significant risk tolerance.
🟩	🟨	**Ensure activities to reduce controlled risk are on track and inside proximity and with no increase in exposure, effectiveness or assurance**. Monitoring forum: Directorate - monthly where risk domain is within directorate. Risk Management Group: Monthly Overseeing committee: CEC - Monthly. GB – bimonthly where proximity in report period.
🟩	🟩	**Ensure risks are monitored for changes within the risk that could affect risk score.** Monitoring forum: Director's weekly meeting: quarterly reviews inside proximity and with no downturn in exposure, KPIs, control and assurance. Risk Management Group in month if proximity is within 4 weeks and/or downturn in exposure, KPIs, control and assurance.

APPROVED for Silver Phase

A41.6 Strategic risks: The table below shows the monitoring activities that should be undertaken to manage strategic risks.

UC	CC	**Monitoring activities – strategic risks** (UC = Uncontrolled risk RAG, CC = Current Controlled risk RAG)
🟥	🟥	**Ensure activities to reduce controlled risk are prioritised and are on track and proximity, exposure, KPIs, control & assurance is verified with CEO.** Immediate Chief Executive Officer awareness. Monitoring forum: Director’s weekly meeting. Risk Management Group: Monthly. Overseeing committee: CEC - Monthly. GB - bimonthly.
🟥	🟧	**Ensure activities to reduce controlled risk are on track and affect from proximity, exposure KPIs, control & assurance.** Monitoring forum: Director’s weekly meeting where proximity is within the next 2 weeks. Risk Management Group: Monthly Overseeing committee: CEC - Monthly. GB bimonthly for controlled current risk score greater or equal to the significant risk tolerance.
🟥	🟨	**Ensure activities to reduce controlled risk are on track and affect from proximity, exposure KPIs, control & assurance.** Monitoring Forum: Risk Management Group: Monthly Overseeing committee: CEC - Monthly. GB – bimonthly where proximity is within the quarter.
🟥	🟩	**Ensure controls are effective as high reliance on controls to mitigate risk.** Monitoring Forum: Director’s weekly meeting where proximity is within the next 2 weeks. Risk Management Group: Monthly.
🟧	🟥	**Ensure activities to reduce controlled risk are prioritised and are on track and proximity, exposure, KPIs, control & assurance is verified with CEO.** Immediate Chief Executive Officer awareness. Monitoring forum: Director’s weekly meeting. Risk Management Group: Monthly. Overseeing committee: CEC - Monthly. GB - bimonthly.
🟧	🟧	**Ensure activities to reduce controlled risk are on track and inside proximity and with no increase in exposure, effectiveness or assurance**. Monitoring forum: Risk Management Group: Monthly. Overseeing committee: CEC - Monthly GB bimonthly for controlled current risk score greater or equal to the significant risk tolerance.
🟧	🟨	**Ensure activities to reduce controlled risk are on track and inside proximity and with no increase in exposure, effectiveness or assurance**. Monitoring Forum: Risk Management Group: Monthly Overseeing committee: CEC - Monthly. GB – bimonthly where proximity is within the quarter.
🟧	🟩	**Ensure risks are monitored for changes within the risk that could affect risk score.** Monitoring Forum: Director’s weekly meeting: quarterly reviews inside proximity and with no downturn in exposure, KPIs, control and assurance. Risk Management Group in month if proximity is within 4 weeks and/or downturn in exposure, KPIs, control and assurance.
🟨	🟥	**Ensure activities to reduce controlled risk are prioritised and are on track and proximity, exposure, KPIs, control & assurance is verified with CEO.** Immediate Chief Executive Officer awareness. Monitoring forum: Director’s weekly meeting. Risk Management Group: Monthly. Overseeing committee: CEC - Monthly. GB - bimonthly.

APPROVED for Silver

🟨	🟧	**Ensure activities to reduce controlled risk are on track and inside proximity and with no increase in exposure, effectiveness or assurance**. Monitoring forum: Risk Management Group: Monthly. Overseeing committee: CEC - Monthly GB bimonthly for controlled current risk score greater or equal to the significant risk tolerance.
🟨	🟨	**Ensure activities to reduce controlled risk are on track and inside proximity and with no increase in exposure, effectiveness or assurance**. Monitoring Forum: Risk Management Group: Monthly Overseeing committee: CEC - Monthly. GB – bimonthly where proximity is within the quarter.
🟨	🟩	**Ensure risks are monitored for changes within the risk that could affect risk score.** Monitoring Forum: Director's weekly meeting: quarterly reviews inside proximity and with no downturn in exposure, KPIs, control and assurance. Risk Management Group in month if proximity is within 4 weeks and/or downturn in exposure, KPIs, control and assurance.
🟩	🟥	**Ensure activities to reduce controlled risk are prioritised and are on track and proximity, exposure, KPIs, control & assurance is verified with CEO.** Immediate Chief Executive Officer awareness. Monitoring forum: Director's weekly meeting. Risk Management Group: Monthly. Overseeing committee: CEC - Monthly. GB - bimonthly.
🟩	🟧	**Ensure activities to reduce controlled risk are on track and inside proximity and with no increase in exposure, effectiveness or assurance**. Monitoring forum: Risk Management Group: Monthly. Overseeing committee: CEC - Monthly GB bimonthly for controlled current risk score greater or equal to the significant risk tolerance.
🟩	🟨	**Ensure activities to reduce controlled risk are on track and inside proximity and with no increase in exposure, effectiveness or assurance**. Monitoring Forum: Risk Management Group: Monthly Overseeing committee: CEC - Monthly. GB – bimonthly where proximity is within the quarter.
🟩	🟩	**Ensure risks are monitored for changes within the risk that could affect risk score.** Monitoring Forum: Director's weekly meeting: quarterly reviews inside proximity and with no downturn in exposure, KPIs, control and assurance. Risk Management Group in month if proximity is within 4 weeks and/or downturn in exposure, KPIs, control and assurance.

APPROVED for Silver Phase

APPENDIX 5: RISK APPETITE MATRIX, DEVELOPMENT AND REVIEW

A51.1 Establishing a risk appetite will enable the CCG to increase its rewards by optimising risk taking and accepting calculated risks within parameters approved by the Clinical Executive Committee and the Governing Body.

A51.2 The CCG needs to establish their risk appetite and the reasons for it in order to prevent subjective decision making which may lead to over exposure or over cautious outcomes.

A51.3 Risk appetite needs to be measurable to avoid narrative descriptions of risk appetite being misinterpreted subjecting the CCG to potential peril.

A51.4 The risk appetite review should be performed as part of the continuous improvement of the CCG's risk management strategy and to ensure that the appetite does not become antiquated and is fit for purpose for the CCG both strategically and operationally. The review must also reflect any changes in the environment and conditions affecting the statutory duties or the strategic objectives of the CCG.

A51.5 The risk appetite review will provide a revised risk appetite which will be published and appropriately communicated to stakeholders.

A51.6 The risk appetite review must include:

- Consideration for strategic and operational level appetite (throughout the organisation and the health and care system) for risk in order for objectives to be met and for it to be fit for purpose for the CCG.

- Consideration for the CCG's *risk capability* to protect the organisation and the health and care system until capability is sufficient for the level of risk.

- Its effectiveness in supporting correct decision making in relation to the exposure from the consequences of an event or situation and in relation to reward.

- Confirmation from decision makers that the risk appetite clearly and effectively defines the degree in which they operate in risk exposure.

- Confirmation from executives that the aggregate and/or interlinked risk position is clear in relation to the risk appetite.

- The ability for senior managers and executives to identify changes to conditions which may affect the risk appetite.

- The amount of risk to be taken on (number and quantum for reward).

- Improvement opportunity from evidence that the CCG has implemented risk appetite effectively.

APPROVED for Silver Phase

- The criteria which subject a risk to escalation and catalysts which will trigger escalation.

- Consideration of the CCG's risk management maturity in its ability to have sufficient risk capability.

- Consideration of the CCG's risk capacity in its ability to carry risk.

A51.7 The risk appetite review should update the risk appetite statement (where used by the CCG) and the Risk Appetite matrix in the context of and in order to achieve the CCG's strategic objectives.

A51.8 The Risk Appetite Matrix provides an objective tool to be used within the risk assessment process to identify whether the risk is acceptable to the organisation within the risk domain.

A51.9 The Risk Appetite Matrix enables a risk to be assigned to a risk appetite category within a domain which facilitates reporting on the amount (volume) and type (domain) of risks the organisation is currently exposed to.

A51.10 The Risk Appetite Matrix acts as a trigger for escalation and/or further actions to be undertaken.

APPROVED for Silver Phase

A51.11 Choose the domain for the identified risk from the Risk Appetite Matrix table below along the left hand side of the table. Then work along the columns in the same row to the risk rating score of the risk. If there is a tick for the chosen column and row, then this is the appetite that the CCG wishes to achieve i.e. our target risk rating score should be within this appetite.

Domain	RISK APPETITE CATEGORY				
	NO	LOW	GUARDED	CAUTIOUS	DESIRABLE
	RISK GRADING				
	EXTREME (25)	EXTREME (15-20)	HIGH (8-12)	MODERATE (4-6)	LOW (1-3)
(A) Impact on the safety of patient, staff or public (physical / psychological harm).	x	x	x	x	✓
(B) Quality / complaints / audit.	x	x	x	✓	✓
(C) Human resources / organisational development / staffing / competence.	x	x	x	✓	✓
(D) Statutory duty / inspections.	x	x	x	✓	✓
(E) Adverse publicity / reputation.	x	x	x	✓	✓
(F) Business objectives/projects.	x	x	✓	✓	✓
(G) Finance including claims.	x	x	✓	✓	✓
(H) Service / business interruption or Environmental impact.	x	x	x	✓	✓

Note: the above table has been shared with the Governing Body 7.11.19: The above represents an example of how risk appetite can be applied.

APPROVED for Silver Release

APPENDIX 6: DEFINITIONS

A61.1 Risk: is a potential situation or event which creates exposure to either positive or negative impact.

A61.2 Risk Management: is the proactive identification, assessment and controls of the situations or events that subject the organisation to *risk*. It uses *risk treatment option* of *Treat* to control the consequences (*likelihood* and *severity*) of threatening events.

A61.3 Governance: is the framework by which the CCG oversees, regulates and seeks assurance from its corporate affairs (Corporate Governance), clinical practice (Clinical Governance) and its information management (Information Governance).

A61.4 Risk Score: is the outcome of the likelihood and severity calculation. Calculate the risk score by multiplying the *severity* by the *likelihood*: S (severity) x L (likelihood) = R (risk score) as defined in Appendix 3.

A61.5 Likelihood: is qualitative description of probability or frequency of a *risk*.

A61.6 Severity: is the scale of consequence from a *risk*.

A61.7 Risk Grading: is a grouping of *risk score* as defined in Appendix 3.

A61.8 Risk RAG Rating: is the red, amber or green colour rating from the *risk score* as defined in Appendix 3.

A61.9 Controlled Risk RAG Rating: is the remaining *risk RAG rating* which is calculated to reflect the performance of the *risk controls*.

A61.10 Clinical Risk: is a *risk* that a patient suffers harm from an error caused by a treatment (physical, emotional or pharmaceutical).

A61.11 Hazard: is a source (object, situation or behavior) of potential harm with a potential to cause loss (e.g. injury, ill health, harm, damage).

A61.12 Mitigation: is the lessening of *likelihood* or *severity.*

A61.13 Risk Capacity: the resources (financial, human, and tangible) that is able to be deployed for *risk*. The amount of *risk* that the CCG "must" take in order to reach an aim; calculated in £ (*likelihood* * financial impact) to identify what the financial consequence would be should any of the *risks* (*risk exposure*) within the aim be realised.

A61.14 Risk Exposure: the level of outcome from a risk. Calculation of financial impact or *risk score*/RAG rating/*risk grade/likelihood/severity*.

A61.15 Risk Tolerance: The level at which risk is considered *acceptable* or unacceptable as the boundary for *risk exposure*. Tolerance levels must not

APPROVED for Silver Phase

impact upon the CCG's ability to fulfil its strategic aims and objectives, service provision or *risk capacity.*

A61.16 Acceptable Risk: is a *risk* which the CCG consents to bear and is approved as an outcome of risk assessment as a combination of the *risk exposure* within the *risk tolerance* and *risk appetite*.

A61.17 Risk assessment: is a process comprising of risk identification, risk analysis, and risk evaluation.

A61.18 Risk analysis: is a process that is used to understand the nature, sources, and causes of the risks that you have identified and to estimate the level of risk. It is also used to study impacts and consequences and to examine the controls that exist.

A61.19 Risk evaluation: is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or tolerable.

A61.20 Risk identification: is a process that is used to find, recognise, and describe the risks that could affect the achievement of organisation's objectives.

A61.21 The Statement of Internal Control: is a public accountability document that describes the effectiveness of internal controls in the CCG and is personally signed by the Chief Executive of the CCG.

A61.22 Risk Register: is a register of risk data which has been defined as a standard for the CCG. CCG risk registers are held on the CCG's risk system.

A61.23 A significant risk: is a risk with a risk score within a defined range, set by the Governing Body. It reflects the potential quantum of threat to the organisation from risks with a score within this range which is deemed sizable enough to warrant particular action or focus which is outlined in the organisation's risk management strategy.

A61.24 Risk Domain: A classification of the subject area which pertains to the *risk* used in the calculation of the correct *severity* level to the initial, current or target risk RAG rating.

A61.25 Risk Accumulation: the *risk* that arises when a large number of individual *risks* are correlated (geographically or otherwise) such that a single event will affect many or all of these risks simultaneously.

A61.26 Risk Aggregation: is the collection of *risks* gathered together to form a total quantity e.g. a number of risks in order to produce a total *risk exposure* for all or a part of an organisation/department/category/strategic objective.

A61.27 Assurance flow: is the flow of information which serves to support or confirm assurance within the CCG.

APPROVED for Silver Phase

A61.28 Organisational Risk: is a *risk* (excluding those that fall within the Clinical Risk definition), that could cause injury or ill-health of people, damage or loss to property, equipment, materials, environment or a combination of those factors.

A61.29 Risk Capability: is the knowledge and leadership competencies of individuals or a collective group responsible for managing *risk*. It is a function of *risk capacity* and *risk management maturity* which combined enable the CCG to manage *risk*.

A61.30 Risk Controls: is any measure or action that modifies or regulates *risk* to minimise the *likelihood* of the *risk* occurring, and/or minimise the consequences should the identified *risk* occur. The four types of risk control are preventative *(mitigation)*, detective, collaborative and corrective *(contingency)*.

A61.31 Risk Appetite: is the amount and type of *risk* which the organisation considers justifiable should the *risk* realise in order to obtain the benefits (or rewards) in order to meet its strategic objectives.

A61.32 Risk Universe: is the full portfolio of *risk* which could impact positively or negatively on the ability to achieve the CCG's strategic objectives.

A61.33 Risk Management Maturity: is the level of acumen within defined dimensions which executives use to determine preparedness to embark on risk.

A61.34 Consequence: is the outcome of an event and has an effect on objectives.
A single event can generate a range of consequences which can have both positive and negative effects on objectives. Initial consequences can also escalate through cascading and cumulative effects.

A61.35 Risk treatment: is a process that modifies risk. It involves selecting and implementing one or more treatment options.

A61.36 Risk treatment option: is a choice which when implemented becomes a control or it modifies existing controls. Options are:

- Terminate: a risk that can be changed or removed without it materially affecting the organisation.
- Treat: controlling the risk to reduce the *likelihood* or *severity* and or contingency if the risk is realised.
- Transfer: transferring the exposure (part or whole) of the risk from one party to another; insuring against the risk realising or outsourcing work/functions; the use of insurance, or the payment to third parties who are prepared to take the risk on behalf of the organisation..
- Tolerate: no action is taken to reduce a risk because it is not cost-effective or the risks of impact are low and considered acceptable to the organisation.

APPROVED for Silver Phase

A61.37 Risk Plan: is a plan which is aimed at ‘treating’ the risk, specifying how the risk treatment option will be implemented.

A61.38 Contingency: is what would be needed as a control if the risk is realised.

A61.39 Proximity: is how close, in terms of time, to a risk occurring.

A61.40 Preventative Control: is a control which aims to reduce *likelihood* e.g. policies, procedures, guidelines, protocols, approvals, delivery plans, authorisations, police checks and training;

A61.41 Detective Control: is a control which aims to identify failures in the current control environment e.g., reviews of performance, reconciliations, audits, surveys and investigations.

A61.42 Corrective Control: is a control which aims to reduce the consequence and/or rectify a failure after it has been discovered e.g., crisis management plans, business continuity plans, insurance and disaster recovery plans.

A61.43 Collaborative Control: is a control which aims to share information across a joint forum so that actions or escalation can be agreed e.g. meetings/forums.

A61.44 Assurance: is a declaration or evidence that something is true. External assurance is supplied by independent sources and provides the organisation with evidence about how effective the controls are. Internal assurance provides the organisation with evidence for activity related to a control.

A61.45 Uncontrolled Risk RAG Rating: is the remaining risk RAG rating which is calculated to reflect no risk controls in place.

A61.46 Enterprise Risk Management first line of defence: is executed by the business function that performs the daily operational delivery of the organisation’s objectives. They manage risk in accordance to the organisation’s risk management policies and are be fully aware of the risk factors that should be considered in every decision and action. They execute effective internal control in their business functions, as well as the monitoring process and maintaining transparency in the internal control itself.

A61.47 Enterprise Risk Management second line of defence: is executed by risk management and compliance functions, responsible for risk management development, monitoring process and the implementation of the organisation’s overall risk management strategy. They ensure that all business functions comply with risk management policies and standard operating procedures, monitor, escalate and instruct actions in relation to risk management within the governance structure.

APPROVED for Silver Phase

A61.48 Enterprise Risk Management third line of defence: is executed by internal auditors the external auditors. The role of the internal auditor is more intense as they are independent to the CCG.

A61.49 Risk assurance framework reporting: is a subset of the GBAF and is produced in a standard format defined by the CCG.

A61.50 System Risk: A risk which exists in relation to an aim shared by a number of organisations who do not directly share the risk exposure.

A61.51 Partnership Risk: A risk which exists in relation to an aim shared by a number of organisations who share the risk exposure.

A61.52 Risk-issue plan: is an action plan that identifies actions, responsibilities and timelines that would be taken to address any risk-issue that occurs as a result of a risk realising.

A61.53 Risk-issue: is an issue which is created through a realised risk. As a result of risk management, risks may be prevents from realising, or the impact reduced. If the impact is reduced the net effect is wholly acceptable to the CCG.

A61.54 Target Risk RAG Rating: is the remaining *risk RAG rating* which is calculated to reflect the anticipated full effective performance of the *risk control,* against the level of *risk exposure* (future net risk position).

APPROVED for Silver Phase

APPENDIX 7: RISK ASSESSMENT

A71.1 A risk assessment is a function that ensures that the nature, causes, consequences and triggers of a risk are thoroughly analysed and understood. The analysis can include historical data, theoretical analysis, informed opinions, financial analysis, political, economic, social, technological, ecological and legal (PESTEL)/ Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis, expert advice and stakeholder input.

A71.2 It will ensure that the necessary due diligence has been performed so that the correct controls, assurance and risk RAG ratings are set in accordance to the RAG matrix as defined in Appendix 3 within the lifetime of the risk. The assessment should therefore be proportionate to the risk.

A71.3 By undertaking the measurement of the controls, evidence of their effectiveness can be demonstrated. In doing so, assurance that the risks with the most significant consequences should they materialise, are being effectively controlled. This level of assurance cannot be provided when control effectiveness is ‘guessed’ rather than assessed.

A71.4 The risk assessment process and template is defined within the Risk Management Risk Assessment Standard Operating Procedure.

A71.5 Risks may be subject to a reassessment post the initial risk assessment. Any reassessment of a risk should be approved by the Risk Owner.

A71.6 Risks that are reassessed will generate a new version of the risk assessment, which must be stored to reflect the updated version in the folder as specified in this policy.

A71.7 Risks would be reassessed if there is a change to the risk exposure, KPIs, controls, impacts or hazards.

APPROVED for Silver Phase

APPENDIX 8: RISK MANAGEMENT GROUP TERMS OF REFERENCE

Terms of Reference
Risk Management Cor

APPROVED for Silver Phase