NHS
Wiltshire
Clinical Commissioning Group

Clinical Commissioning Group Governing Body
Paper Summary Sheet
Date of Meeting: 23 September 2014

For: PUBLIC session ☒ PRIVATE Session ☐

For: Decision ☒ Discussion ☐ Noting ☐

Agenda Item and title:	**GOV/14/09/09 Review of Risk Management Strategy**
Author:	Susannah Long, Governance & Risk Manager
Lead Director/GP from CCG:	David Noyes, Director of Planning, Performance and Corporate Services
Executive summary:	Sound risk management in the CCG and its partner organisations is essential for meeting objectives and identifying and managing future opportunities. The Risk Management Strategy aims to deliver a pragmatic and effective multidisciplinary approach to risk management, which is underpinned by a clear accountability structure. The Risk Management Strategy is a rolling three year document for the period 2012 to 2015. The strategy is reviewed on an annual basis by the Governance and Risk Manager to ensure that it correctly drives the risk management agenda and documents CCG risk management arrangements.
Evidence in support of arguments:	The Risk Management Strategy provides a comprehensive document defining the risk management ethos and arrangements within the CCG.
Who has been involved/contributed:	The Governance & Risk Manager has reviewed the strategy taking into account comments from Internal Audit.
Cross Reference to Strategic Objectives:	The strategy contributes to all strategic objectives which are listed within the document.
Engagement and Involvement:	This is an internal document and has not received further engagement or involvement at this time.
Communications Issues:	The Risk Management Strategy will be made available on the internet.

Financial Implications:	There are no direct financial implications.
Review arrangements:	The Risk Management Strategy has been updated on an annual basis.
Risk Management:	The strategy details risk management arrangements.
National Policy/ Legislation:	It is NHS standard practice to have a Governing Body approved Risk Management Strategy in place.
Equality & Diversity:	The report has no negative E&D impact.
Other External Assessment:	This strategy will contribute to external assessments.
What specific action do you wish the Governing Body to take?	To approve the updated Risk Management Strategy.

RISK MANAGEMENT STRATEGY 2012 to 2015

Please be aware that this printed version of the Strategy may NOT be the latest version. Staff are reminded that they should always refer to the Intranet for the latest version.

Purpose of Agreement	The organisation is committed to the implementation of a strategy that develops and maintains an open and proactive culture associated with all aspects of risk management.
Document type	Strategy
Reference Number	
Version	2.1 - Post 2013/14 Review for 14/15
Name of Approving Committee/Groups	NHS Wiltshire CCG Governing Body
Operational Date	September 2014
Document Review Date	September 2015
Document Sponsor (Name & Job)	David Noyes, Director of Planning, Performance and Corporate Services
Document Manager:	Susannah Long, Governance and Risk Manager
Document developed in consultation with	Central Southern Commissioning Support Unit
Intranet Location	
Website Location	
Keywords (for website/intranet uploading)	Risk Management, Risk Assessment

Amendments Summary:

Amend No.	Page(s)	Subject	Action Date
1	6 10 18	Update to Strategic Objectives Role of Director of Planning, Performance & Corporate Services Update use of Risk Register	Sep'13
2	6 10 10 & 11 11 & 12 18 18 & 19	Update to Strategic Objectives Removal of NHSLA assessments Further detail on roles and responsibilities Removal of support provided by CSCSU Introducing use of 'Top 10' for reporting to the Governing Body Removal of role of CSCSU in reporting	Sep'14
3			
4			
5			
6			
7			

Review log:

Version number	Review date	Lead name	Approval process	Notes
1	Sep'13	S.Long	Gov Body	
2	Sep'14	S.Long	Gov Body	

Contents

Table of Contents

Risk Management Strategy

This document aims to provide an overarching strategy for the management of internal and external risk by the CCG. It provides the framework for the continued development of risk management processes throughout the organisation and describes levels of accountability, processes and frameworks.

The Risk Management Strategy aims to deliver a pragmatic and effective multidisciplinary approach to risk management, which is underpinned by a clear accountability structure.

This Risk Management Statement and the effectiveness of the risk strategy will be subject to on-going review and, where necessary, amendment.

This strategy must be read in conjunction with the CCG Constitution.

1. INTRODUCTION

The organisation has a statutory responsibility to patients, staff and the public to ensure that it has effective processes, policies and people in place to deliver its objectives and to control any risks that it may face in achieving these objectives.

The Governing Body recognises that sound risk management in the CCG and its partner organisations is essential for meeting objectives and identifying and managing future opportunities, by ensuring risk management forms a fundamental element of its business rather than a separate programme. The Governing Body is committed to ensuring that risk management is embedded throughout the organisation and is part of every day practice.

The purpose of this strategy is to set out the overall aims, objectives and rationale for risk management within the organisation and when working in conjunction with stakeholders in recognition of the changing NHS environment.

2. RISK MANAGEMENT OVERVIEW

Risk refers to uncertainty, the possibility of incurring misfortune or loss or missing opportunities. This is measured in terms of the likelihood of something happening and the impact of the possible consequences. In the CCG a risk may be looked upon as anything which has the potential to damage or threaten the achievement of the strategic objectives or the reputation of the CCG.

For the purposes of this strategy:

- **Clinical risk** is any issue that may have an impact on the provision of high quality, safe and effective clinical care for patients;
- **Organisational risk** is any issue that may have an impact on organisational objectives, business continuity or the organisation's reputation;
- **Financial risk** is any issue that may have an impact on financial objectives or arrangements.

The task of the organisation is to effectively identify, analyse and respond to these risks so as to maximise the likelihood of the organisation achieving its vision and in doing so ensure the best use of resources.

Within health care some exposure to risks or risk taking will be necessary, fundamental and tolerated. However, this must be under a clear risk management methodology that enables:

- the facilitation of identification, recording and management of risk at all levels within the CCG;
- consistent risk measurement so that risk priorities can be identified through a combination of impact and likelihood;
- an understanding of the type of risk and level of risk exposure that can be tolerated by the CCG in going about its activities and defines the risk appetite of the CCG;
- mitigation and control that is proportionate to the level of risk;

- appropriate mechanisms to ensure that risks can be escalated to a level of management that can effectively respond to them;
- the on-going monitoring of the effectiveness of mitigation and control; and
- the provision of assurance to responsible committees.

The Risk Management Framework should be suitably robust and transparent to support the on-going business of the organisation whilst being proportionate and reasonable to facilitate innovation in the commissioning of high quality health care.

The establishment of effective risk management is recognised as being fundamental to ensuring good governance and is reported as part of the Annual Governance Statement (AGS) in the Annual Report of the CCG and is included in the Financial Statements. The AGS is a public report that confirms the on-going effectiveness of the internal control in the management of all type of business risk, both clinical and non-clinical.

3. STRATEGIC OBJECTIVES

The CCG has agreed its vision and values and from these has identified strategic objectives. An effective risk management framework is an essential part of corporate governance to support delivery of these strategic objectives. Risks will be identified to outputs to clearly programme appropriate risk mitigation. It should not be forgotten that the same principles of risk management can be equally effectively used to identify opportunities. It is therefore a highly effective tool for guiding resource allocation and service mix within the commissioning framework. Hence a strategic approach to risk will support delivery of the following strategic objectives:

- To drive towards a clinically led model which delivers integrated high quality patient services within the community based upon neighbourhood teams to provide 'wrap around' care at or close to home.
- Commission appropriate services to meet~~ing~~ the needs of the local population and national priorities, delivered in the right place (ideally in a primary care setting but acute where necessary) and accessible at the right times identifying and addressing health inequalities.

- Engage effectively with the local population to enable patients and practices to ~~have greater~~ influence the~~on~~ services that we commission.

- Achieve a sustainable health economy optimising appropriate use of resources for the delivery of efficient and effective healthcare.

- Develop an effective and responsive clinically led commissioning organisation, working collaboratively with partner organisations ~~to develop seamless care pathways~~.

- Enhance quality and safety of services by ensuring effective mechanisms are in place to set quality standards, assess performance, address concerns and drive continuous improvement.

- Encourage and support the Wiltshire population in managing and improving their health and wellbeing, wherever possible increasing the ability of people to manage their own care and to make their own choices.

4. RISK MANAGEMENT OBJECTIVES

The following objectives have been identified which form the basis of the risk management strategy. These objectives will be achieved through various mechanisms that are outlined in the strategy and associated programmes of work and documents:

- Promote awareness of risk management and embed the approach in all functions and management throughout the organisation;
- Ensure the CCG has and maintains the required level of risk management support to successfully manage its risks;
- Seek to identify, record, measure, control, report and monitor any risk that will undermine the achievement of objectives, both strategically and operationally, through appropriate analysis and assessment criteria;
- Protect the services, patients, staff, reputation and finances of the organisation through application of sound risk management;
- Provide the Governing Body with assurance that risk is being effectively managed through the establishment of appropriate risk management escalation mechanisms for the purposes of decision making, coupled with proportionate monitoring and compliance with agreed processes;
- Utilise risk management proactively as a tool for business planning, resource allocation and service improvement as part of the Project Management Office (PMO) arrangements.

Ultimately it is the role of Governing Body to ensure that risk is identified and appropriately mitigated on a day to day basis. The Chief Officer is accountable for Risk Management. The Governing Body delegates the management of risk to the Audit & Assurance Committee which will provide assurance to the Governing Body on the effectiveness of the risk management framework.

The objectives will be achieved through:

- Leadership and commitment from the top, supporting a culture of risk awareness and personal, professional and corporate responsibility and accountability;
- Providing a clear system and framework within which risks and adverse events may be identified, reported, analysed, managed and monitored;
- Sharing good practice, effective risk management actions and audit recommendations which reduce exposure to risk;
- Providing appropriate training to ensure staff have the correct knowledge and skills;
- Complying with legislation, regulations and standards;

- Reducing the impact of adverse events and learning from adverse events, complaints and claims;

- Working in collaboration with healthcare providers and Wiltshire Council to sustain the provision of high quality and effective healthcare that demonstrates value for money and sound risk management.

5. RISK MANAGEMENT FRAMEWORK

The following elements make up the Risk Management Strategy:

- Approach
- Roles and Responsibilities
- Processes
- Risk Identification
- Risk Assessment and Measurement
- Risk Appetite
- Reporting and Monitoring

5.1 RISK MANAGEMENT APPROACH

The organisation's approach to risk management will encompass the breadth of the organisation by considering financial, organisational, reputational and project risks, both clinical and non clinical and for all parts of the organisation involved. Please see the CCG Constitution for the organisation's committee structure. This will be achieved through:

- having an appropriate risk management framework delegating authority, seeking competent advice and seeking assurance
- Having a clear risk culture, philosophy and resources for risk management
- Integration of risk management into all strategic and operational activities and discussing risk appetite
- Identification and analysis, active management, monitoring and reporting of risk across organisation
- Ensuring appropriate and timely escalation of risks
- Excellent communication encouraging the sharing of experiences and learning in a fair blame/non-punitive culture
- Consistent compliance with relevant standards, targets and best practice
- Business continuity plans and recovery plans established and regularly tested.

5.2 ROLES & RESPONSIBILITIES

This section of the strategy identifies the roles and responsibilities of key individuals and committees, highlighting accountability levels. A detailed account of individual and committee responsibilities is provided in the CCG Risk Management Policy and Procedure, job descriptions and committee terms of reference.

Committees

5.2.1 The Governing Body

The Governing Body will be responsible for:

- Having overall accountability for the management of governance, risk and assurance, determining the strategic approach to risk and setting the risk appetite for the organisation;
- Ensuring and approving the structure and framework for risk management;
- Consideration of whether the organisation has implemented an effective system of internal control, including appropriate risk management arrangements, with reference to available assurance;
- Regularly receiving the Board Assurance Framework (BAF) and the High Level Risk Register which contain the most significant risks that can impact on the achievement of the strategic objectives;
- Monitoring management of significant risks and seeking assurance that management decisions balance performance within appropriate limits defined by the Group committees.

The Governing Body delegates operational responsibility for the delivery of risk management to the Audit & Assurance Committee.

5.2.2 Audit & Assurance Committee

The Audit & Assurance Committee will be responsible for:

- Providing assurance to the Governing Body on the effectiveness and adequacy of the processes for managing principle risks and risk management framework
- Challenging the way in which risk is managed, particularly where there is uncertainty or concerns over the effectiveness of existing arrangements. This could include requesting attendance at meetings for the purpose of providing relevant information for assurance purposes
- Ensuring that arrangements for risk management are regularly included in the cycle of independent audits.
- Being accountable for providing the Governing Body with overall assurances that the management of risk is effective;

- Overseeing and monitoring governance and performance, including corporate, information, clinical and non-clinical governance and risk management and quality (clinical governance and quality is the responsibility of the Quality and Clinical Governance Committee). It will report regularly to the Governing Body on these areas;

- Overseeing the operation of the risk management framework to ensure that the organisation is appropriately managing risks, including operating safely and legally and exploiting potential opportunities, providing assurance of its effectiveness to Governing Body;

- Programming work related to external and internal assessments of the organisation's risk management arrangements~~, including any assessment by the NHS Litigation Authority~~;

- Receiving and reviewing the High Level Risk Register and Board Assurance Framework at each meeting;

- Challenging the progress made by responsible Directors in the mitigation of identified risks;

- Approving, on behalf of the organisation, those policies that fall within the remit of the committee's terms of reference;

5.2.3 Quality & Clinical Governance Committee (QCG)

The QCG will be responsible for:

- Identifying clinical and quality facets of risk, through their work and the work streams of its subordinate groups. The Governance & Risk Manager will be a core member of this committee to ensure a consistent approach to the identification and management of clinical risk.

Individuals

5.2.4 Chief Officer

The Chief Officer is ultimately accountable for all risks relating to the operations of the organisation and will lead on determination of the strategic approach to risk, establishing and maintaining the structure for risk management. The Chief Officer will ensure that leadership and expertise in the field of risk management is available to the organisation.

5.2.5 Chief Financial Officer

The Chief Financial Officer is accountable for internal financial control and sound financial governance through the development of sound systems and process and through the identification and management of financial risks.

5.2.6 Director of Quality and Patient Safety

The Director of Quality and Patient Safety is responsible for the identification and management of clinical and quality related risks within the CCG and those identified risks within provider organisations that may impact on the quality and safety of patients' care commissioned by the CCG.

5.2.7 Director of Planning, Performance and Corporate Services

The Director of Planning, Performance and Corporate Services is responsible~~accountable~~ for the governance framework within the CCG.

5.2.8 Locality Group Directors

Locality Group Directors are responsible for the identification and management of risks during the commissioning process and for the duration of the contract periods with providers. These risks are likely to have components of financial risk, clinical risk and organisational risk.

5.2.9 Governance & Risk Manager

The Governance & Risk Manager is responsible for ensuring that the Board Assurance Framework (BAF) is developed, reviewed and reported to the Audit & Assurance Committee and Governing Body as appropriate. The BAF must adequately reflect the analysis of assurances around significant risks to the organisation's strategic objectives.

The Governance & Risk Manager will retain an overview of the risk register and assist Directors with their management of directorate risk registers~~this document~~.

The Governance & Risk Manager will ensure that business continuity and disaster recovery plans are established and are regularly tested.

5.2.10 Risk Management Support

The CCG retains responsibility for management of risk within the organisation. Risk management support will be provided by the Central Southern Commissioning Support Unit (CSU).

Risk Management Support will be made available to:

- ~~Receive and analyse~~ Provide the DATIX system on which to record adverse event (incidents / near misses) reports, including Information Governance breaches, for analysis to identify issues and opportunities for learning~~, communicating these to the Governance & Risk Manager~~;
- Receive and disseminate alerts, monitor actions and undertake central reporting;
- Ensuring compliance with Health and Safety legislative requirements in regard to risk assessments, appropriate control measures, raising outstanding concerns, staff training, ensuring safe working procedures / practices are in place and continued monitoring and revision of these. These responsibilities extend to cover anyone affected by the organisation's operations including sub-contractors, members of the public and visitors;

- ~~Monitor Provider risk management information in relation to adverse events, external visits, national reports and alerts to inform the commissioning process;~~
- ~~Benchmark organisational information, encouraging learning from best practice;~~
- ~~Work closely within the organisation to promote continuous improvement and consistency with risk management approaches and processes;~~
- ~~Report and manage Serious Incidents Requiring Investigation (SIRI) including the support of investigations, in liaison with the CCG Quality Team;~~
- ~~Raise concerns regarding the risk management framework of the organisation, generated through the information received, and act as critical friend;~~
- ~~Contribute, where applicable, to the Board Assurance Framework and risk register;~~
- Provide specialist advice in support of risk management;
- The CCG will monitor the CSU performance through its internal audit arrangements and regular contract meetings.

5.2.11 Directors and Senior Managers

Directors and Senior managers will provide leadership for the risk management agenda and ensure that responsibilities to identify, record, analyse, control and communicate risk issues (via processes such as Risk Assessment, Adverse Event Reporting and Risk Registers) are undertaken.

Directors and Senior Managers will:

- Ensure that staff receive training in line with the Training Needs Analysis and mandatory updates are completed~~attended~~;
- Undertake a workstation assessment with each direct report on at least a three yearly basis or earlier should there be relevant changes;
- Ensure that all employees who require Health Surveillance according to risk assessments are identified; ensuring that where Health surveillance is required no individual carries out specific duties covered by the surveillance until they have attended the Occupational Health Service;
- Making adequate provision to ensure that fire and other emergencies are appropriately dealt with and business continuity arrangements are in place;
- Ensure compliance with all Information Governance requirements through the Connecting for Health IG Toolkit, staff training, subsequent plans and associated policies.

5.2.12 Staff

All staff have a responsibility to understand, accept and implement the mechanisms in this Strategy. Staff have a responsibility for actively identifying and addressing risk and for undertaking their roles with full appreciation for the risks and the potential consequences of their actions.

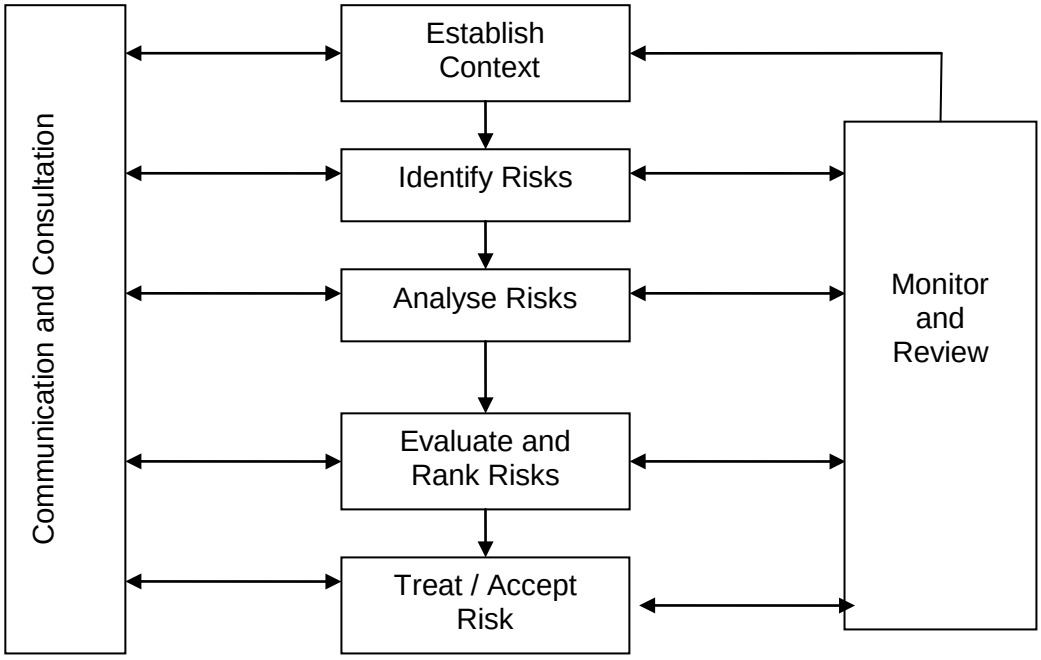
All staff have a responsibility in relation to health and safety risks, to take action to protect themselves and others. Organisational policies and the Training Needs Analysis (TNA) detail the required training that is provided in each risk area. Staff must take responsibility to ensure that they attend training as required.

All staff are responsible for:

- Ensuring that identified risks and adverse events are dealt with swiftly and effectively, and reported via DATIX to ensure further action/learning may be taken as necessary. This may be via the risk register;
- Adherence to their professional codes and the NHS Code of Conduct;
- Complying with all approved policies and Standard Operating Procedures;
- Reporting inefficient, unnecessary or unworkable risk controls;
- Neither intentionally, nor recklessly interfering with nor misusing any equipment provided for the protection of safety and health;
- Being aware of relevant emergency procedures e.g. first aid~~resuscitation~~, evacuation and fire precaution procedures, relevant to their location and role;
- Co-operating with management on adverse event investigations;
- Providing assistance as reasonably requested in times of crisis.

5.3 RISK MANAGEMENT PROCESS

Risk Management is the responsibility of everyone in the organisation. The risk management process is a continual cycle, taking a systematic approach to all risks, as illustrated below:



5.4 RISK IDENTIFICATION

Risk management is an integral part of the culture of the organisation with leadership from the Governing Body and a structure that permits staff to identify and report risk at all levels.

Risk identification establishes the organisation's exposure to risk and uncertainty. There is no one correct way to identify risks and, in practice, the use of multiple methods by different staff groups, is more successful. The risk identification processes used by the organisation will include, but is not limited to:

- Risk assessment process
- Adverse Event Report (AER), including trends and data analysis
- Serious Incidents Requiring Investigation (SIRI)
- Claims and complaints data
- Business decision making and project management~~planning~~
- Strategy and policy development analysis
- External/Internal audits findings.

5.4.1 Risk Assessment Process

The organisation has a structured risk assessment process. The Governance & Risk Manager will provide support to this process.

Directors and Senior Managers are responsible for managing action planning against identified risks and for escalating risks with additional resource implications or implications for other parts of the organisation. Identified risks must be recorded, analysed and monitored using the Risk Register. The Governance & Risk Manager ~~CSU receives and~~ centrally records risk assessments to identify commonalities for organisational risk treatment.

5.4.2 Adverse Event Report (AER) trends and data analysis

All staff are required to report incidents and near misses using the on-line Adverse Event Report (AER) form linked to the DATIX system. Line Managers and Service Managers use these reports to identify risks and take immediate and/or planned risk management action. Risks may also be included on the Risk Register. The ~~CSU carries out high level analysis to~~ Governance and Risk Manager identifies~~y~~ trends and risk issues~~, reporting to the Governance & Risk Manager~~.

5.4.3 Serious Incidents Requiring Investigation (SIRI)

Provider SIRI: The organisation receives reports regarding the most serious incidents that occur in Provider services. The reports investigate the incident to identify contributory factors and root causes where risk treatment will be instigated to prevent future occurrence and to identify and share learning points. The organisation has the responsibility to consider and close these incidents and monitor risk treatment as

appropriate. SIRI data and reports is an important source of information for the commissioning process. ~~Where appropriate,~~The Quality Team will report relevant information regarding Provider SIRI to~~will be considered at~~ the Quality and Clinical Governance Committee.

Other SIRI: SIRI may also occur outside Provider services for example in nursing homes, private providers or as part of commissioning services. The CCG will be involved with the investigation, reporting, learning from and monitoring of these SIRI where appropriate.

~~The Risk Management Support service~~The CCG Quality Team will manage the STEIS reporting system on behalf of the CCG.

5.4.4 Claims ~~and complaints~~

By analysing any trends from claims ~~and complaints~~ and by looking at the particulars of each, risks to the objectives of the organisation may be identified.

5.4.5 Complaints and concerns

By analysing the content and any trends from complaints and concerns made to the CCG, risks to the objectives of the organisation may be identified. Contracted NHS Provider organisations are also required to share complaints information with the commissioning CCG.

~~5.4.5~~5.4.6 Business decision making and project planning

Risk identification is an essential part of business planning to identify those risks that could impact on achievement of the organisation's strategic objectives and risks that would be present if objectives are not achieved. Risk identification will be used to seek business opportunities to exploit and as a fundamental supporting assessment~~part~~ of all proposed and ongoing projects.

~~5.4.6~~5.4.7 Strategy and policy development analysis

Developments in strategy and policy can and do have considerable impact on business activities, plans, organisational form and staff. Senior Managers will look to their own field and specialism to identify potential risks and opportunities to be added to the risk register and to inform the BAF.

~~5.4.7~~5.4.8 External/Internal audit findings

By commissioning internal and external audit, issues of control may come to light. Other external findings may also be available from sources such as NHS Protect or the Fire Officer.

5.5 RISK ASSESSMENT & MEASUREMENT

Once risks are identified further evaluation is required to establish the exposure of the organisation or service to risk and uncertainty. The result of risk analysis can be used to rate the significance of the risk and to prioritise risk treatment. The organisation will use the National Patient Safety Agency 5 by 5 likelihood and impact matrix to assign a risk score.

In all cases it is important to set the risk into context for evaluation. Unfortunately, some types of incident are more commonplace than others and may be linked to a particular service or client group. This does not mean that certain incidents should be tolerated but it could mean that risk treatment may take a different form.

It is also important to consider how the identified risk may impact on other tasks, functions or services. The risk itself may be of low significance but dependencies may raise the profile of the risk.

The organisation will adopt the following approach:

- Apply a scale of 1 to 5 to measure the impact and the likelihood to determine their score by multiplication and classify or prioritise the risk by this means. Please see the risk matrix below.

In order to assess the risk:

- Ask what the consequences would generally be if it occurs?
- Ask how likely is it to occur?
- Multiply the consequences by likelihood using the matrix to define the level of risk severity.

This process can and should be used for all types of risk, eg clinical, non-clinical, strategic, financial, operational, information governance etc. Matrices to aid with the assessment of risks within these specific areas can be found at appendix 1.

Risk Matrix (Likelihood x Impact)

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

5.6 RISK APPETITE

5.6.1 Risk appetite refers to the level of risk on the scale outlined above that the organisation is willing to tolerate or expose itself to when controlling risks as they arise or embarking on new projects. An organisation may accept different levels of risk appetite for different types of risk, or in relation to different projects. For example, it might be highly averse to reputational damage but willing to accept a level of financial loss.

The organisation's risk appetite ensures that risks are considered in terms of both opportunities and threats and are not confined to the financial consequences of a risk materialising. Risks also impact on the capability of the organisation, its performance and its reputation. Risk appetite is influenced by the objectives set by the organisation, individual programmes of work and the NHS landscape.

The Governing Body acknowledges that risk is a component of change and improvement and therefore does not expect or consider the absence of risk as a necessarily positive position. The organisation will, where necessary, tolerate overall levels of risk where action is not cost effective or reasonably practicable.

The organisation will not normally accept levels of risk rated extreme (red) which are scored between 15 and 25 using the risk scoring matrix. The organisation will ensure that plans are put into place to lower the level of risk whenever an extreme risk has been identified.

5.6.2 The organisation requires that all staff take responsibility for the treatment of identified risks. Identifying and reporting a risk does not end the responsibility of the individual staff member. A major part of risk treatment is control and the control to mitigate the risk may be easily put in place, for example by cleaning up a spillage.

The organisation expects that all reported and registered risks will be considered for risk treatment options. Risk treatment includes implementing controls, removing the risk completely, reducing the risk, transferring the uncertainty of the risk (for example by insurance) or making a decision to tolerate the risk in line with level of authority.

The organisation believes that the majority of risks will need to have controls implemented to reduce the likelihood or severity of the risk. The cost-benefit of the control needs to be considered to ensure that the risk reduction benefits outweigh the cost of the control and achieves the desired outcome.

Existing control mechanisms/activities and the level of confidence in these existing controls will be considered when identifying options for additional control measures. Potential dependencies between controls will also be considered.

The organisation has clear lines of delegation and authority.

Level	Authority / Ownership	Action
Low risk 1-3	Individuals and Team Managers	Managed through normal local control measures. Acceptable level of risk.
Moderate risk 4-6	Managers	Review control measures through formal risk assessment, record on the Risk Register
High risk 8-12	Senior Manager	Consider for risk treatment, identify mitigating actions, record on the Risk Register
Extreme risk 15-25	Director	Intolerable level of risk. **Immediate action** must be taken and the risk will be communicated via the High Level Risk Register to the Governing Body.

1-3: Low Risk

Individuals should manage low risks by maintaining routine procedures and taking proportionate action to implement any additional new control measures to reduce risk where possible. Individuals must escalate higher levels of risk

4-6: Moderate Risk

Managers must ensure that an action plan is identified to treat the risk. The risk must be entered on the risk register. Managers must escalate higher levels of risk.

8-12: High Risk

Senior Managers must prepare an action plan for high risks. There must be appropriate management, to oversee the action plan to reduce the risk. This may be an emerging risk which could rapidly escalate. Senior Managers must consider developing implications of the risk and report to the Audit & Assurance Committee if appropriate. The risk must be reported on the risk register.

15-25: Extreme Risk

Management action is required to ensure immediate risk treatment, in line with the context of the risk. Action plan must be overseen by a responsible lead, who will ensure that the risk is reported on the Corporate Risk Register. The risk will be monitored at the Governing Body where it falls within the 'Top 10' risks of the organisation.

The format and process of the organisational Risk Registers has been approved by the Governing Body and includes the following –

- Description of the risk
- Initial Risk score (likelihood and severity)
- Current controls
- Further mitigating actions required (with owners)
- Progress on actions
- Current risk score
- Status – open, accepted, closed
- Date of review

5.7 RISK REPORTING AND MONITORING

5.7.1 Risk Reporting

~~The Risk Management Support service will provide a quarterly report reflecting Adverse Event Report (AER) form and SIRI information.~~

The organisation will operate a risk register that will record all identified risks. Maintaining the Directorate risk register as a complete document is the responsibility of the relevant Director and Senior Managers, providing ownership and leadership for their teams. The Directorate Risk Register must comprehensively reflect the risks identified by the Directorate. Support for this process is available from the Governance & Risk Manager. A mechanism is in place to escalate risks to the attention of the Audit & Assurance Committee and the Governing Body. A risk register is not a static record but should be viewed as an action plan giving details of

current controls and auditable actions for risk treatment where appropriate. Defined actions should be specific, measurable, achievable, relevant and time-bound.

The ~~Risk Management Support service~~Quality Team will ~~log and~~ present a statistical report ~~relevant~~ of Serious Incidents Requiring Investigation (SIRI) ~~using~~ recorded on the STEIS system to the Quality and Clinical Governance Committee. ~~These incidents will be investigated and reported to the QCG.~~

~~Patient safety incidents relating to the CCG reported using the AER forms or SIRI Process will be regularly reported to the National Reporting and Learning System (NRLS) via web reporting by the Risk Management Support service.~~

5.7.2 Risk Monitoring

The organisation will review its risk performance at a strategic and corporate level and in relation to risk management action plans. This will be achieved through regular review of the Risk Register and Board Assurance Framework (BAF).

The organisation is required to maintain a comprehensive BAF. The BAF:

- is a high-level management assessment process and record of the primary risks to the delivery of strategic objectives assessing the strength of internal controls;
- identifies sources of assurance and evaluates them for suitability. By receiving and reviewing actual assurances and using findings, the adequacy of internal control can be tested, confirmed and/or modified.

The Board Assurance Framework is regularly reviewed at the Audit & Assurance Committee, and Governing Body and is fully updated annually in line with strategic objectives.

The organisation will maintain a comprehensive risk register. This is a principle tool that can be described as "*a log of all the risks that may threaten the success of the Trust in achieving its declared aims and objectives*". The Risk Register is a record that aims to illustrate the complete risk profile of the CCG by reflecting the extent to which the objectives of the organisation are threatened by the uncertainty that risk represents. The Risk Register is linked directly to the Board Assurance Framework to ensure that the organisation can demonstrate where evidence is available to give assurance that all significant risks to the business of the organisation are being appropriately managed.

The organisation-wide risk register is used to inform the Governing Body, the Audit & Assurance Committee and other relevant parties of the risks held by the organisation and is reviewed, as a minimum, every two months. Directors and Senior Managers are responsible for reviewing their risks on the risk register as part of their routine management and governance activities and providing accurate status reports on implementation of actions in line with deadlines.

An Annual Risk Management Report by Internal Audit will be presented to the Audit & Assurance Committee and ~~received by the Governing Body~~will inform the Annual Governance Statement of the CCG.

6. TRAINING

Training to ensure competency at all levels is recognised as one of the most cost effective controls for good risk management. The organisation is committed to a system of corporate induction for all new starters and those returning to work after a long absence. Risk Management related training is on-going for all staff. Systems are in place to ensure attendance for training and report training statistics to the appropriate committee.

The organisation recognises that senior managers will need governance and risk management training which is more suited to their role, level of accountability and authority. This training will be specified by the CCG ~~and facilitated/provided by the CSU~~ and will be formally recorded ~~with records supplied in an agreed format by the CSU to the CCG~~.

7. COMMUNICATION & CONSULATION

In addition to the regular monitoring, annual review and reports to the Governing Body and its committees, key issues and actions arising from risk management, audit reports and related processes will be communicated to staff, patients, the public and other relevant stakeholder groups where necessary. If appropriate and/or required these key risk issues and actions will be communicated to external performance management/review bodies.

The Communications Manager will ~~circulate bulletins, using information supplied by CSU when necessary to~~ raise general staff awareness of particular risk issues by including briefings in the staff newsletter '14 days'.

This strategy will be made available to contracted bodies.

This strategy will be published on the organisation's website, intranet and staff will be made aware through training sessions and by ~~Weekly Brief~~'14 days'.

8. REVIEW

This Risk Management Strategy is a rolling three year document. The Strategy will be reviewed on at least an annual basis or earlier where there has been a significant change to the organisation or the organisation's objectives.

The strategy will be submitted to the Governing Body for ratification on an annual basis.

9. MONITORING COMPLIANCE

The Audit & Assurance Committee will be responsible for ongoing monitoring of this strategy, to ensure that the framework described is working effectively.

Independent assurance will be gained when required, by means of the Internal Auditors, to assess the operation of the risk management framework of the

organisation. Internal Audit support may also be requested to assess specific controls, areas or risks identified through these processes.

10. SUPPORTING DOCUMENTATION

The organisation intends to implement this strategy by means of the following key policies~~, which is not an inclusive list~~. Further advice and support may be requested from the ~~Risk Management Support service~~Governance & Risk Manager.

- Health & Safety Policy
- Adverse Event (Incident) Reporting Policy
- Significant Incidents Requiring Investigation (SIRI) Policy
- Security Management Policy
- Counter Fraud Policy
- Complaints Policy
- Learning & Development Policy – Training Needs Analysis
- Whistleblowing Policy
- Information Governance Policy
- Supporting staff involved in a Incident, Complaint or Claim Policy

11. REFERENCES AND LINKS TO OTHER DOCUMENTS

- The Risk Management Process, Federation of European Risk Management Associations (FERMA), 2005
- A Risk Management Standard, The Association of Insurance and Risk Managers, (AIRMIC), 2002
- International Organisation for Standardisation (ISO) / IEC Guide 73:2002 Risk Management
- Risk Management Model (HSG65), Successful Health & Safety Management, HSE Books, 1997
- Five Steps to Risk Assessment, HSE, 2006
- Corporate Manslaughter and Corporate Homicide Act, 2007
- A Risk Matrix for Risk Managers, NPSA, January 2008

- Department of Health (2003) Building the Assurance Framework: A Practical Guide for NHS Bodies London: Department of Health

- Consequence Grading Matrix (from A Risk Matrix for Risk Managers Jan 2008 – NPSA)

- ISO 31000 'Risk management – Principles and guidelines'

- 'A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000', Airmic, Alarm, IRM

- The Management of Health and Safety at Work Regulations 1999 and the Workplace (Health, Safety and Welfare) Regulations 1992 (As Amended 2002)

- Corporate Manslaughter and Corporate Homicide Act 2007

- The Data Protection Act 1998

- The Freedom of Information Act 2000

APPENDIX 1

Description of the application of the NPSA matrix

Score	Description	Broad descriptor	Time-framed descriptor	Probability descriptor
5	Certain	The event is expected to occur in all circumstances	Expected to occur at least daily	>50%
4	Likely	The even will occur in most circumstances	Expected to occur at least weekly	10-50%
3	Possible	The event should occur at some time	Expected to occur at least monthly	1-10%
2	Unlikely	The event could occur	Expected to occur at least annually	0.1-1%
1	Rare	May happen in exceptional circumstances	Not expected to occur for years	<0.1%

Impact on organisation

Choose the most relevant risk descriptor and use this to measure the impact of the risk.

Descriptor	Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Impact Heading: Safety **Injury (physical & psychological) to patient / visitor/ staff**	Minimal injury requiring no/minimal intervention or treatment	Minor injury or illness requiring minor intervention	Moderate injury requiring medical treatment and/ or counselling Agency reportable, e.g. Police (violent and aggressive acts) An event which impacts on a small number of patients	Major injuries / long term incapacity or disability (loss of limb) requiring medical treatment and/or counselling	Incident leading to death or major permanent incapacity An event which impacts on a large number of patients

Descriptor	Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Impact Heading: Service Delivery **Human Resources / Organisational development / Staffing & Competence**	Short tem low staffing level temporarily reduces service quality (<1 day). Short term low staff level (>1 day) where there is no disruption to patient care	Ongoing low staffing level reduces service quality Minor error due to ineffective training / implementation of training	Late delivery of key objective / service due to lack of staff. Unsafe staffing level or competence (>1 day). Low staff morale Poor staff attendance for mandatory / key training. Ongoing problems with staffing levels.	Uncertain delivery of key objective / service due to lack of staff Unsafe staffing level or competence (>5 days) Loss of key staff Very low staff morale No staff attending mandatory / key training	Non-delivery of key objective / 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.
Impact Heading: Service Delivery **Statutory duty / inspections**	No or minimal impact or breach of guidance / statutory duty Small number of recommendations which focus on minor quality improvement issues	Breach of statutory legislation Reduced performance rating if unresolved Recommendations made which can be addressed by low level of management action	Single breach in statutory duty Challenging recommendations that can be addressed with appropriate action plan / improvement notice	Enforcement action Multiple breaches in statutory duty Improvement notices Low performance rating Critical report	Multiple breaches in statutory duty Prosecution Complete systems change required Zero performance rating Severely critical report

Descriptor	Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Impact Heading: Reputation **Adverse Publicity/ Reputation**	Rumours, no media coverage but potential for public concern Little effect on staff morale	Local media coverage – short-term reduction in public confidence. Elements of public expectation not being met. Minor effect on staff morale / public attitudes.	Local media coverage – long-term adverse publicity Significant effect on staff morale and public perception of the organisation	National media / adverse publicity, less than 3 days Service well below reasonable public expectation Public confidence in the organisation undermined Use of services affected	National / International media / adverse publicity, more than 3 days MSP/MP concern (Questions in Parliament) Court Enforcement Public Inquiry/ FAI Service well below reasonable public expectation Total loss of public confidence
Impact Heading: Service Delivery **Business objectives / projects**	Insignificant cost increase/ schedule slippage, reduction in scope or quality	<5% over project budget; minor reduction in scope, quality or schedule	5-10% over project budget; reduction in scope or quality of project; project objectives or schedule.	Non compliance with national 10-25% over project budget; significant project over-run; key objectives not met	Incident leading to >25% over project budget; Inability to meet project objectives; reputation of the organisation seriously damaged

Descriptor	Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Impact Heading: Financial **Financial (including damage / loss/ fraud) and Claims**	Negligible organisational / personal financial loss (less than £10K) Small loss risk of claim remote	Minor organisational / personal financial loss (£11k to £50K) Claim(s) less than £10,000	Significant organisational / personal financial loss (£51k to £100k) Claim(s) between £10,000 and £100,000	Major organisational / personal financial loss (£101k to £250k) Claim(s) between £100,000 and £1 million Purchasers failing to pay on time	Severe organisational / personal financial loss. (£251k plus) Failure to meet specification / slippage Loss of contract / payment by results Multiple claims or single major claim > £1 million
Impact Heading: Service Delivery **Services / Business Interruption Environmental impact**	Interruption in a service which does not impact on the delivery of pt care or the ability to continue to provide service Minimal or no impact on the environment	Short term disruption to service with minor impact on patient care Minor impact on the environment	Some disruption in service with unacceptable impact on patient care. Temporary loss of ability to provide service. Moderate impact on the environment	Sustained loss of service which has serious impact on delivery of patient care resulting in major contingency plans being invoked Major impact on the environment	Permanent loss of core service or facility Disruption of facility leading to significant 'knock-on' effect Catastrophic impact on the environment

Descriptor	Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Information Governance/ Records Management	Damage to an individual's reputation. Possible media interest, e.g. celebrity involved	Damage to a team's reputation. Some local media interest that may not go public	Damage to a services reputation/ Low key local media coverage.	Damage to an organisation's reputation/ Local media coverage.	Damage to NHS reputation/ National media coverage.
	Potentially serious breach. Less than 5 people affected or risk assessed as low, e.g. files were encrypted	Serious potential breach & risk assessed high e.g. unencrypted clinical records lost. Up to 20 people affected	Serious breach of confidentiality e.g. up to 100 people affected	Serious breach with either particular sensitivity e.g. sexual health details, or up to 1000 people affected	Serious breach with potential for ID theft or over 1000 people affected

Adapted from NPSA 'A risk matrix for risk managers' January 2008

NHS Wiltshire Clinical Commissioning Group

Equality Impact Analysis – the EIA form

Title of the paper or Scheme: **Risk Management Strategy**

For the record	
Name of person leading this EIA Susannah Long, Governance & Risk Manager	Date completed 16 September 2014
Names of people involved in consideration of impact Lynne Beta, Administration Assistant	
Name of director signing EIA David Noyes, Director of Planning, Performance and Corporate Services	Date signed 16 September 2014

What is the proposal? What outcomes/benefits are you hoping to achieve?
The Risk Management Strategy sets out the organisational arrangements for the effective management of risk. The Strategy clearly identifies roles and responsibilities and the objectives of good risk management.

Who's it for?
Use by the staff within the organisation and for information to partner organisations, stakeholders and auditors.

How will this proposal meet the equality duties?
By having a Risk Management Strategy, the CCG will have a framework by which it is open and transparent in regard to the risks to which it is exposed.

What are the barriers to meeting this potential?
The CCG operates within a finite financial resource. Although risks to work streams may be identified, it will not be possible to apply financial resources to address all risks which may lead to some element of inequitable treatment.

2 Who's using it Refer to equality groups
The Risk Management Strategy will support all equality groups.

What data/evidence do you have about who is or could be affected (e.g. equality monitoring, customer feedback, current service use, national/regional/local trends)?
The CCG carries out EIA for programmes and projects against which there are identified risks.

How can you involve your customers in developing the proposal?
The Risk Management Strategy sets the ethos for CCG risk management, the framework and identifies roles and responsibilities. The CCG would value feedback on the strategy which could be used to inform the 2015 review..

Who is missing? Do you need to fill any gaps in your data? (pause EIA if necessary)
No gaps.

3 Impact Refer to dimensions of equality and equality groups
Show consideration of: age, disability, sex, transgender, marriage/civil partnership, maternity/pregnancy, race, religion/belief, sexual orientation and if appropriate: financial economic status, homelessness, political view

Using the information in parts 1 & 2 does the proposal:

a) Create an adverse impact which may affect some groups or individuals. Is it clear what this is?

How can this be mitigated or justified?
There is no adverse impact.

What can be done to change this impact?
N/A

b) Create benefit for a particular group. Is it clear what this is? Can you maximise the benefits for other groups?
There is an equal benefit for all groups.

Does further consultation need to be done? How will assumptions made in this Analysis be tested?
No further consultation is needed at this time.

4 So what? Link to business planning process

What changes have you made in the course of this EIA?
None

What will you do now and what will be included in future planning?
The strategy will be published on the internet and be made available to the Auditors.

When will this be reviewed?
The EIA will be reviewed at each submission to the Governing Body for approval of the strategy.

How will success be measured?
N/A