



**Dudley**  
Clinical Commissioning Group

# RISK MANAGEMENT FRAMEWORK

**UNIQUE REF NUMBER:** GB/AC/001/V2.1  
**DOCUMENT STATUS:** Approved by Audit & Governance Committee – 18 October 2018  
**DATE ISSUED:** November 2018  
**DATE TO BE REVIEWED:** November 2021



## AMENDMENT HISTORY

VERSION	DATE	AMENDMENT HISTORY
GB/AC/001/D1	19 April 2013	Version prepared by Paul Capener, Interim Governance Support
GB/AC/001/V1	2 May 2013	Approved by Dudley CCG Board
GB/AC/001/V1.1	December 2013	Addition of branding, minor formatting changes and unique reference number prior to publication
GB/AC/001/V2	November 2016	Reviewed by Governance Support Manager
GB/AC/001/V2.1	October 2018	Updated to reflect current monitoring processes and also who the owners and leads are

## REVIEWERS

NAME	DATE	TITLE/RESPONSIBILITY	VERSION
P Capener	April 2013	Interim Governance Support	D1
E Smith	November 2016	Governance Support Manager	V2
S Johnson	November 2016	Deputy CFO & Governance Lead	V2
P Capener	November 2016	Governance Support	V2
E Smith	October 2018	Governance Support Manager	V2.1

## APPROVALS

This document has been approved by:

NAME	DATE	VERSION
Dudley CCG Board	2 May 2013	V1
Audit & Governance Committee	1 Dec 2016	V2
Dudley CCG Board	12 Jan 2017	V2
Audit & Governance Committee	18 October 2018	V2.1
Dudley CCG Board	TBC	V2.1

NB: The version of this policy used on the intranet must be a PDF copy of the approved version.

## DOCUMENT STATUS

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of the document are not controlled.

## RELATED DOCUMENTS

These documents will provide additional information:

REFERENCE NUMBER	DOCUMENT TITLE	VERSION

**CONTENTS**

**1.0** INTRODUCTION 4

**2.0** RISK STRATEGY AND VISION 5

**3.0** RISK MANAGEMENT POLICY 8

**APPENDIX 1 GLOSSARY OF RISK TERMINOLOGY**

**APPENDIX 2 RISK ASSESSMENT SCORING METHODOLOGY**

**APPENDIX 3 BAF & RISK REGISTER FORMAT**

**APPENDIX 4 GOVERNANCE STRUCTURE**

## RISK MANAGEMENT FRAMEWORK – 2016/2017

### 1.0 INTRODUCTION

- 1.1 Successful organisations manage risks to the delivery of their core business objectives explicitly and effectively.
- 1.2 Risk to the Group's business can take various forms, e.g. financial risk, risk to the services commissioned, risks to patients, the public or specific stakeholders, risks from missed opportunities or from policy failures, and risks to our reputation. Accordingly, we need a clear understanding of how such risks should be managed. Doing this properly is central to planning to succeed and avoiding failure; to meeting our key objectives and targets; to creating confidence in a watchful public; to take opportunities; and to meeting the demands of good corporate governance. It will also make us better able to learn the value of appropriate risk-taking and benefit from innovation.
- 1.3 The purpose of this Risk Management (RM) Framework is to set out the way in which the Group identifies, monitors and manages its strategic, operational, financial and compliance risks.
- 1.4 The RM Framework has two elements:

#### **2.0 Risk Strategy & Vision**

This sets out why risk management is important for the Group

#### **3.0 Risk Management Policy**

This details the Risk Management system of the Group

## **2.0 RISK STRATEGY & VISION**

### **2.1 INTRODUCTION**

2.1.1 The purpose of this strategy is to set out why Risk Management (RM) is important, in what context it should be seen and why it needs to be an intrinsic part of the way in which the Group operates.

2.1.2 All organisations face uncertainty. Uncertainty presents both risk and opportunity. Effective Risk Management increases the probability of success and reduces both the probability of failure and the uncertainty of achieving the Group's overall objectives. It provides a rigorous and robust framework for the Group to focus on what it needs to measure, monitor and manage if it is to deliver its core objectives. In summary, the successful implementation of a robust Risk Management process is vital to achieving the Group's objectives.

### **2.2 GROUP RISK PROFILE**

2.2.1 The key risks facing the Group relate to:

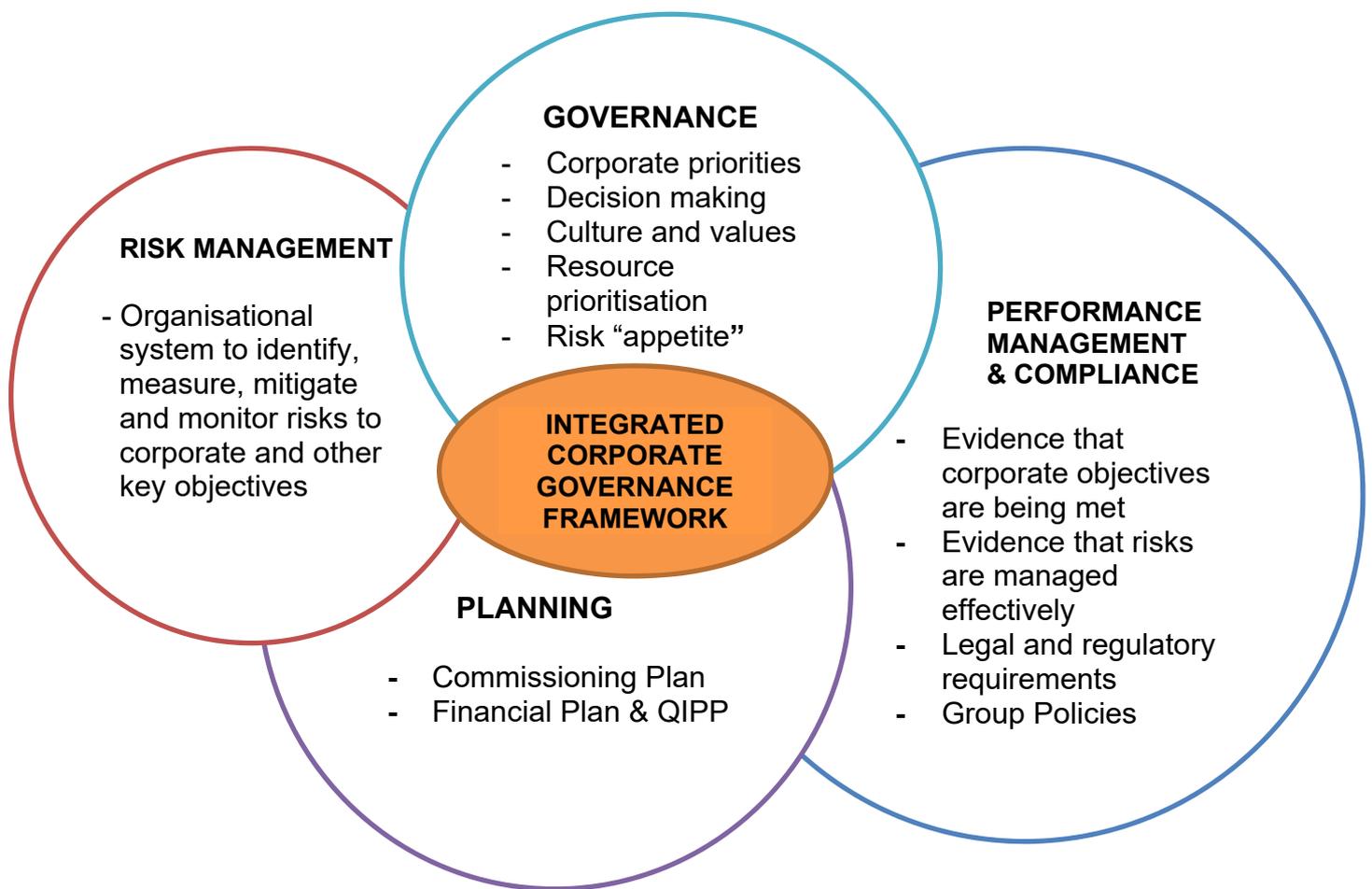
- Commissioning safe, high quality services for patients
- Remaining financially viable
- Working effectively with others to deliver patient-centred health services
- Operating in accordance with the statutory and regulatory framework
- Developing and maintaining an effective and well motivated workforce

### **2.3 AN INTEGRATED APPROACH**

2.3.1 In contextual terms, Risk Management is one element of an integrated approach to corporate governance for every organisation. Both Performance Management and Risk Management are ultimately concerned with the achievement of the organisation's strategic objectives. They are critical elements of the Group's corporate governance framework along with leadership. How significant risks are managed can have a major impact on performance and the way in which an organisation's objectives are achieved.

2.3.2 Risk Management is one tool to improve performance. It must be part of a coherent system of management within the organisation with the other following key elements:

- Business planning
- Financial planning and management
- Performance management and monitoring
- Appraisal and personal development of staff



## 2.4 RISK MANAGEMENT FRAMEWORK STATEMENT

2.4.1 The Group recognises the important contribution that effective and explicit RM can make to the achievement of objectives at strategic, operational, financial and compliance level.

2.4.2 Risk Management does not exist to stifle innovation or risk taking itself but to demonstrate that the organisation clearly identifies risks to its objectives, measures these, has monitoring systems in place and manages risk in a proportionate way. Risk Management is an essential and important activity because it:

- is an intrinsic part of good management, not an add-on activity
- focuses on what is important in achieving the organisation’s objectives
- promotes better decision making, planning and prioritisation by a comprehensive and structured understanding of Group activity and the volatility of our business
- assists project management by aiding in the identification of opportunities and threats to a given project
- promotes greater and clearer accountability within the Group
- promotes stakeholder confidence in the organisation

2.4.3 Our Risk Management activities are therefore designed to:

- relate to what the Group states it wants to achieve
- support effective delivery of services and partnerships
- be targeted at critical risks
- be proportionate to those risks
- not seek to stifle innovation or promote the avoidance of all risk
- track and report critical risks in a transparent manner
- be integrated into everyday management of the Group
- act in concert with planning, resource allocation and performance management activities

- meet regulatory requirements.

2.4.4 The critical success factors for effective Risk Management include:

- clearly identified responsibilities for senior management and governing body members
- an agreed and effective Risk Management Framework
- the existence of an organisational culture which supports well thought-through risk taking and innovation
- management of risk embedded in day-to-day management processes and consistently applied
- management of risk is linked to the achievement of strategic and operational objectives
- Risks are actively monitored and regularly reviewed on a constructive 'no blame' basis

## **2.5 RISK – THE REGULATORY REQUIREMENTS**

2.5.1 As well as the practical benefits to be gained by Risk Management, the Group is also required to meet a variety of regulatory requirements in respect of risk management.

### **NHS England**

2.5.2 NHS England requires CCGs to operate a framework that effectively identifies and manages risk.

### **The Annual Governance Statement (AGS)**

2.5.3 All NHS bodies are required to produce an AGS that summarises the main systems and processes in place for risk management and internal control and discloses any material control weaknesses in any financial year. This is a statutory requirement and must be signed off by the Chief Accountable Officer.

2.5.4 The accompanying Risk Management Policy sets out the detail of the Group's Risk Management Framework. It details how risks are identified, quantified, how options to deal with them are identified, how decisions on risk management are taken, implemented and evaluated. The governing body, managers and staff are responsible for ensuring that the Risk Management Framework is implemented. A glossary of risk management terms is included as Appendix 1.

## **3.0 RISK MANAGEMENT POLICY**

### **3.1 INTRODUCTION**

3.1.1 The purpose of the Risk Management Policy is to set out the Risk Management Framework used by the Group to support the achievement of its strategic, operational, financial and compliance based objectives.

3.1.2 This policy covers in detail the following:

- Definition of risk
- Leadership and accountability arrangements
- Our RM approach
- Risk measurement
- Risk appetite
- Monitoring arrangements
- Decision making
- Risk registers

- Risk training
- Annual Governance Statement

## 3.2 DEFINITION OF RISK

3.2.1 Before attempting to write a Risk it is important to understand the difference between a risk and an issue. There are many definitions of risk. The one used for the purposes of this policy is that risk is defined as ***the possibility that an event will occur and adversely affect the achievement of objectives.***

3.2.2 The fundamental difference between a risk and an issue is that an issue has already occurred – it is affecting your objective at the present time. However, a risk only has the potential to affect your objective but has not yet occurred, hence why we assess the likelihood of a risk occurring. In this respect you can say that a risk could become an issue if it materialises.

3.2.3 One of the basic requirements in identifying risk is to describe each one in such a way that it is meaningful to stakeholders who aren't necessarily involved in the management of the risk or who lack subject matter expertise. To that end, it is common practice to describe risks using 'cause and effect' or 'if, then' sentence structures.

3.2.4 The resources available for managing risk are finite and so our aim is to achieve an optimum response to risk, prioritised in accordance with our evaluation of the risks. We use the term 'risk appetite' to refer to the amount of risk which we are prepared to accept, tolerate, or be exposed to at any point in time.

3.2.5 Risk Management is the process by which we:

- Identify risks in relation to the achievement of our objectives;
- Assess their relative likelihood and impact;
- Respond to the risks identified, taking into account our assessment and risk appetite;
- Review and report on risks - to ensure the risk profile is up to date, to gain assurance that responses are effective, and identify when further action is necessary;

3.2.6 The goals of Risk Management are to:

- take a proactive approach, anticipating and influencing events before they happen;
- facilitate better informed decision making;
- improve contingency planning.

## 3.3 LEADERSHIP AND ACCOUNTABILITY ARRANGEMENTS

3.3.1 An integral part of an effective risk management framework is having explicit accountabilities for risk. Every member of staff employed by, working on behalf of or engaged in the activities of Dudley CCG has a collective and an individual responsibility for the management of risk within their own remit. With this in mind, every individual should make an effort to familiarise themselves with the Risk Management Framework

3.3.2 The leadership and accountability arrangements for Risk Management in the Group are as follows:

### **The Governing Body**

3.3.3 The governing body has responsibility for establishing the overall strategic direction of the Group. It provides oversight of risk management by:

- creating the environment for risk management to operate effectively;

- being periodically apprised of the corporate risk profile and examining whether management is responding appropriately; and
- considering the formal annual review of the effectiveness of the system of internal control (the AGS).

3.3.4 Further information about the duties and delegated responsibilities for each group can be found in our Constitution.

#### **Audit & Governance Committee**

3.3.5 The Audit & Governance Committee considers and advises the governing body on the strategic processes and policies for risk, control and governance and the system of internal control, including the content of the AGS prior to endorsement by the governing body. This Committee will provide input to risk management by:

- monitoring the development and continuous improvement of the risk management process and the Board Assurance Framework (BAF);
- reviewing the level of risk accepted;
- being regularly apprised of the corporate risk profile and examining whether management is responding appropriately. This will involve at least annual presentations by other Committee chairs and their respective Chief Officer/Director of on the management and assurance of risk that falls to that Committee's responsibility; and
- advising on the formal annual review of the effectiveness of the system of internal control and the content of the AGS.

3.3.6 The Audit & Governance Committee will be provided with:

- A report summarising any significant changes to the Group's BAF and Risk Register for each meeting, with associated action plans
- The Group's Risk Management Strategy and Policy and proposals for continuous improvement of the risk management process and culture as appropriate.

#### **Other Committees**

3.3.7 Other governing body Committees will consider and advise the governing body (and periodically the Audit & Governance Committee) on the management of risks specific to their area of responsibility (e.g. the Quality & Safety Committee will consider and advise on risks related to quality and safety)

3.3.8 Each Committee will be provided with:

- A report summarising any significant changes to the Group's BAF and Risk Register, in relation to the risks assigned to that Committee for each meeting, with associated action plans.

#### **Chief Accountable Officer**

3.3.9 The Chief Accountable Officer is responsible for ensuring that a system of risk management is maintained. This includes:

- setting and communicating the Risk Management strategy;
- providing leadership and direction over the risk management process;
- regularly reviewing the risk profile;
- conducting an annual review of the effectiveness of the system of internal control in support of the AGS.

#### **The Chief Operating & Finance Officer (COFO)**

3.3.10 The COFO co-ordinates the risk management process and works with the Audit Committee and Clinical Executive in establishing effective RM processes, but is not responsible for the

management of risks. He/she is responsible for developing and implementing the process and maintaining the BAF and Risk Register and reporting mechanisms. The COFO will:

- Refresh and update the Group's RM Framework as necessary
- Act as the key link to the Audit & Governance Committee
- Ensure corporate and other key risks are reported to each meeting of the Audit & Governance Committee, highlighting any significant changes
- Co-ordinate the production of the AGS

#### **Chief Officers and Directors of**

3.3.11 All Chief Officers and Directors Of are responsible for:

- Ensuring the Risk Management Framework is implemented consistently within their own areas of responsibility
- Taking an active and visible role in the management of risks within the Group
- Ensuring that risks in relation to their areas of responsibility are suitably captured and kept up to date within the BAF and Risk Register, and that is regularly reviewed by their respective management teams
- Demonstrating how significant risks are being managed
- Providing assurance for the AGS
- Incorporating risk into decision making process

#### **Other Managers**

3.3.12 Everyone with a line or project management role is responsible for assessing and communicating risks within their sphere of responsibility, including assessing when a risk should be considered for escalation to the BAF and Risk Register. Hence responsibilities include:

- Ensuring that the Risk Management Framework is implemented in their area of responsibility
- Contributing to the identification and management of risks
- Include risk in decision making

#### **Risk Owners and Leads**

3.3.13 Risk owners are responsible for ensuring that each risk assigned to her/him, is managed and monitored over time. There are a number of dedicated leads for specific risk areas and are outlined in the table below:

<b>Area</b>	<b>Owner</b>	<b>Lead</b>
<b>Governance Risk</b>	Chief Operating and Finance Officer	Governance Manager
<b>HR &amp; OD</b>	Director of HR & OD	HR & OD Lead
<b>Equality, Diversity and Human Rights (EDHR)</b>	Director of HR & OD	HR & OD Lead
<b>Health and Safety Risk</b>	Chief Nurse	Head of Quality & Safety
<b>Information Governance Risk</b>	Senior Information Risk Officer (SIRO)	Governance Manager
<b>Quality Risk</b>	Chief Nurse	Head of Quality & Safety
<b>Financial &amp; Performance Risk</b>	Chief Operating & Finance Officer	Head of Financial Management (Corporate and Commissioning)

<b>Commissioning Risk</b>	Director of Commissioning	Deputy Director of Commissioning
<b>Primary Care Risk</b>	Chief Nurse	Primary Care Contracts Manager

### **All GP Members and Group Employed Staff**

3.3.15 Whilst this policy document sets out defined processes for managing risk, successful risk management can only be accomplished on a day to day basis by staff at all levels through their working practices. Risk management is part of every GP member and group employed staff's responsibilities and everyone has a role in carrying out appropriate risk management, through awareness of the risk profile, supporting risk identification and assessment, and designing and implementing risk responses.

3.3.16 The responsibilities of individual members of staff are therefore to:

- Be familiar with the Risk Management Policy
- Take general steps in their every day working to reduce risk
- Inform their GP Locality Chair in the case of GPs and line manager / supervisor in the case of employed staff, of issues in their work activities that they consider are material risks
- Immediately report any incidents or near misses or any other incident they feel is relevant to their line manager / supervisor

### **Internal Audit**

3.3.17 The Internal Audit team plays a key role in evaluating the effectiveness of, and recommending improvements to, the Risk Management process. This is based on the systematic review and evaluation of the policies, procedures and operations in place to:

- establish, and monitor the achievement of, the Group's objectives;
- identify, assess and manage the risks to achieving these objectives;
- advise on, formulate, and evaluate policy;
- ensure the economical, effective and efficient use of resources;
- ensure compliance with established policies (including behavioural and ethical expectations), procedures, laws and regulations;
- safeguard the Group's assets and interests from losses of all kinds, including fraud, irregularity or corruption; and
- ensure the integrity and reliability of information, accounts and data, including
- internal and external reporting and accountability processes.

3.3.18 In addition, Internal Audit should add value through:

- supporting and facilitating the identification of risks and the development of processes and procedures to assess and effectively respond to risks;
- the identification and recommendation of potential process improvements;
- the provision of advice to manage risks in developing systems, processes, projects, and procedures; and
- encouraging best practice.

### **Responsibilities of Management Teams**

3.3.19 The collective responsibilities of the Chief Officers and Directors Of are to:

- Ensure consistent implementation of the Risk Management Framework across the Group
- Assess that suitable actions are taken to mitigate different levels of risk, including those raised by Internal Audit or other external sources of assurance
- Ensure that controls are prioritised and that risk responses are proportionate

- Include risk in the decision making process

3.3.20 The responsibilities of the **Executive Team** are to:

- Share learning, intelligence, experience and good practice across the organisation
- Analyse and prioritise risks requiring corporate action
- Advise the Audit & Governance Committee on significant risk issues and their mitigation
- Co-ordinate the quarterly risk report to the Audit & Governance Committee
- Prepare the AGS
- Championing risk within the Group
- Oversee business continuity within the Group.

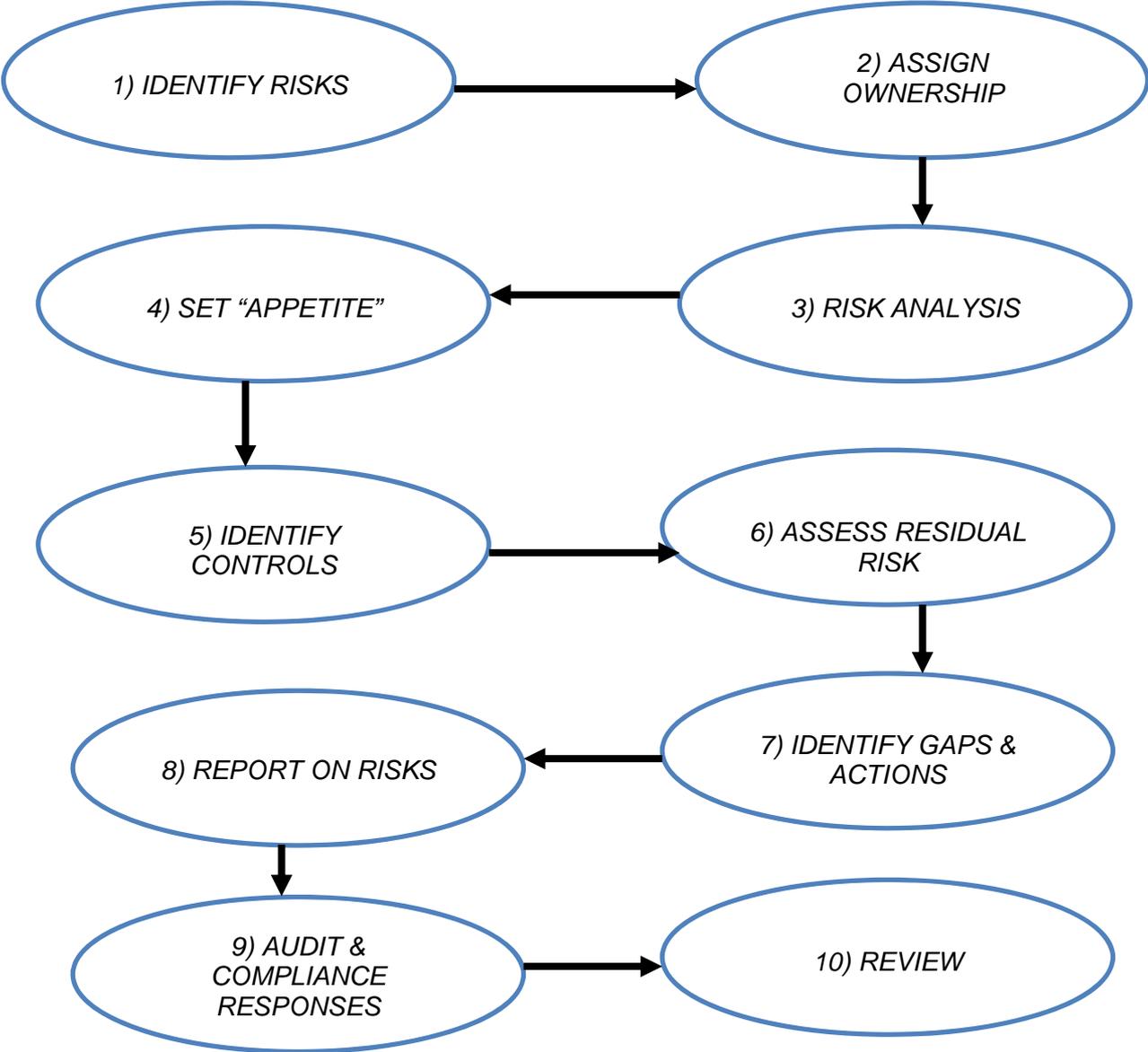
### 3.4 OUR RISK MANGEMENT APPROACH

3.4.1 The eight components of our Risk Management Framework are described below.

- **Internal environment** – The internal environment encompasses the tone of the Group, and sets the basis for how risk is viewed and addressed by the Group’s people, including risk management philosophy and appetite, integrity and ethical values, and the environment in which they operate.
- **Objective setting** – Objectives must exist before our managers can identify potential events affecting their achievement. Risk Management ensures that we have in place a process to set objectives and that the chosen objectives support and align the Group’s mission and are consistent with its risk appetite.
- **Event identification** – Internal and external events that could potentially affect achievement of the Group’s objectives must be identified, distinguishing between risks and opportunities.
- **Risk assessment** – Risks will be analysed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and residual basis.
- **Risk response** – Our managers select risk responses (avoiding, accepting, reducing or sharing risk) developing a set of actions to align risks with the Group’s risk tolerances and risk appetite
- **Control activities** – We will ensure that policies and procedures are established and implemented to help ensure the risk responses are effectively carried out by our managers
- **Information and communication** – Relevant information is identified, captured and communicated in a form and timeframe that enables our people to carry out their responsibilities.
- **Monitoring** – The RM process is monitored and modifications made as necessary. Monitoring is accomplished through governing body, Committee and management activities, separate evaluations and risk based auditing.

3.4.2 The Risk Management cycle requires that there is clarity about what our corporate objectives are, and that an appropriate environment is in place to facilitate the effectiveness of Risk Management. It is important to establish that everybody involved has a common understanding of what needs to be achieved, before risks are managed. Our ten step approach to managing risk is set out overleaf. This will be adopted throughout the Group.

**Risk Management Cycle**



<b>MANAGING RISK</b>	
<b>STEP</b>	<b>ACTIVITY</b>
<p><b>1) EVENT IDENTIFICATION – IDENTIFYING RISKS</b></p> <p>Identify what are the critical risks to achieving objectives.</p>	<p>We will use workshops; interviews; incident reporting and other systems to identify risks</p> <p>All risks captured on the Group’s BAF and Risk Register should be categorised according to our Strategic Objectives. The BAF and Risk Register must be produced in the approved Group format.</p>
<p><b>2) EVENT IDENTIFICATION - OWNERSHIP</b></p> <p>Establish who is responsible for managing the risk</p>	<p>All risks will be assigned an owner.</p> <p>The owner means the person who must understand, monitor and control the risk but does not have to be the one that directly takes all actions to mitigate a particular risk. It is important that the owner is involved in determining a risk score. Risk owners must have sufficient authority to take on responsibility for their risks</p>
<p><b>3) RISK ASSESSMENT - RISK ANALYSIS</b></p> <p>Measure the risks identified to determine a risk score</p>	<p>We will score the risks identified using the risk assessment set out in the risk measurement section.</p> <p>This stage will rank risks in order of relative importance.</p>
<p><b>4) RISK ASSESSMENT – SET “APPETITE”</b></p> <p>The level of risk we are prepared to accept to achieve our objective</p>	<p>Our aim is not to remove all risk and it is necessary to recognise that some level of risk will always exist. Risk appetite is the amount of risk that the Group is prepared to accept, tolerate, or be exposed to at any point in time.</p> <p>Our risk appetite can be expressed as a boundary, above which we will not tolerate the level of risk and further actions must be taken. The risk appetite is monitored by the inherent and residual risk assessment figures.</p> <p>Our risk appetite is not necessarily static. The governing body may vary the amount of risk which it is prepared to take depending on the circumstances.</p>

<b>MANAGING RISK</b>	
<b>STEP</b>	<b>ACTIVITY</b>
<b>5) RISK RESPONSE &amp; CONTROL ACTIVITIES - IDENTIFY RESPONSES / CONTROLS</b>  Identify what controls are used / will be used to mitigate the risk	Consider and agree which risk response(s) are most appropriate: <ul style="list-style-type: none"> <li>• Terminate: stop the activity that is producing the risk</li> <li>• Treat: put in place a mitigating process</li> <li>• Tolerate: accept the risk because its impact and likelihood are low and/or other control options are unacceptable (e.g. because of cost)</li> <li>• Transfer: move the risk to another organisation (e.g. through insurance or outsourcing).</li> <li>• Take the risk which relates to taking opportunities rather than doing nothing.</li> </ul> It is important to quantify in financial terms the actual or estimated costs of implementing the responses wherever possible. Risk responses need to be proportionate to the risks involved.
<b>6) RISK ASSESSMENT - ASSESS RESIDUAL RISK</b>	Score the risks again using the same risk assessment matrices. The 'residual risk' is the exposure arising from a specific risk after a risk mitigation procedure has been implemented to manage it and making the assumption that the control is working as expected.
<b>7) RISK RESPONSE &amp; CONTROL ACTIVITIES - IDENTIFY GAPS AND ACTIONS</b>	Where the residual risk has not reduced sufficiently to be within the Group's risk appetite then a further response is required. These actions should be recorded on the BAF and Risk Register as a 'Gap in Control'.
<b>8) INFORMATION &amp; COMMUNICATION - REPORTING</b>	Formally report on risks together with controls to mitigate risks and an assessment of their effectiveness. This can be done on a comprehensive basis (all risks), selective basis (only High risks), or categorical basis (strategic risks) depending on the requirements of the particular forum. The frequency of risk reporting to the different forum will be at agreed intervals.
<b>9) MONITORING - AUDIT CONTROLS &amp; RESPONSES/TEST COMPLIANCE</b>	Assurance will be obtained to confirm that the residual risk assessment, based upon the controls in place, is reasonable. Assurance may be sought from management, internal audit, external audit or other sources as and when appropriate. The sources and results of assurance will be recorded within the BAF and Risk Register
<b>10) MONITORING - REVIEW</b>	The Audit Committee will periodically review how effective the RM cycle and overall system of internal control has been overall.

## MANAGING RISK

STEP	ACTIVITY
	<p>Has the process added value? Has there been a positive outcome? What evidence exists to demonstrate this? How does this get communicated and to whom? Were the reporting processes appropriate and reports well received? What should be done differently next time?</p> <p>They will advise the governing body on RM improvements, and the content of the AGS, taking into account the views of Internal Audit (the Head of Internal Audit Opinion) and other independent advisers as appropriate</p>

**3.5 RISK MEASUREMENT**

3.5.1 It is essential that the same principles for measuring risks are used across all Group activities so that risks can be compared across functions in a consistent manner.

3.5.2 There are three important principles for assessing risks:

- ensure that there is a clear structure to the process so that both likelihood and impact are considered for each risk;
- record the assessment of risk in a way which facilitates monitoring and the identification of risk priorities;
- be clear about the difference between inherent and residual risk.

3.5.3 For each risk identified, an assessment should be made of the likelihood of it occurring and the relative impact on our work if it does. The more clearly risks are defined at the identification stage the more easily they can be assessed.

3.5.4 All risks should be scored in terms of their likelihood and potential impact using the following five point scale. The score for the likelihood and impact are multiplied to provide an overall risk assessment. More detail of how to assess likelihood and impact is contained in Appendix 2.

Likelihood		Impact	
5	Almost certain	5	Catastrophic
4	Likely	4	Major
3	Possible	3	Moderate
2	Unlikely	2	Minor
1	Rare	1	Insignificant

3.5.5 Each risk is assessed twice. Firstly the ‘inherent’ risk, which is the exposure arising from a specific risk in the absence of any actions management might take to alter either impact or likelihood. Secondly the ‘residual risk’ which is the exposure arising from a specific risk after action has been taken to alter the risk’s impact or likelihood.



**3.6 RISK APPETITE**

3.6.1 Our risk appetite can be expressed as a boundary, above which we will not accept the level of risk and further actions must be taken:

Impact	Multiplier					
Catastrophic	5	5	10	15	20	25
Major	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Minor	2	2	4	6	8	10
Insignificant	1	1	2	3	4	5
	Multiplier	1	2	3	4	5
Likelihood		Rare	Unlikely	Possible	Likely	Almost certain

Key	RISK APPETITE
20-25	Unacceptable level of risk exposure which requires immediate corrective action to be taken
10-16	Unacceptable level of risk exposure which requires constant active monitoring, and measures to be put in place to reduce exposure
5-9	Acceptable level of risk exposure subject to regular active monitoring measures
1-4	Acceptable level of risk exposure subject to regular passive monitoring measures

3.6.2 The risk appetite is monitored by the inherent and residual risk assessment figures. Generally we will wish to manage closely all residual risks scoring 10 or over and would not want to be exposed to residual risks scoring over 16.

3.6.3 Our risk appetite is not necessarily static. The governing body may vary the amount of risk which it is prepared to take depending on the circumstances.

**3.7 MONITORING ARRANGEMENTS**

3.7.1 All risks will be monitored through Committees at each meeting. Risks allocated directly to the Governing Body will be monitored at each Governing Body Meeting as well as all risks that are 16 and over.

**3.8 DECISION MAKING (KEY DECISIONS, PROJECT DOCUMENTS, POLICY FRAMEWORK DOCUMENTS)**

3.8.1 There should be evidence to show that risks have been considered when making decisions. It is good practice to ensure that all reports to governing body, Committees and management meetings include an assessment of the risks related to the course of action being proposed. As such, all reports, Project Plans and Policy documents submitted to governing body and Committees must have a documented risk assessment that is summarised in the cover report.



### **3.9 BOARD ASSURANCE FRAMEWORK AND CORPORATE RISK REGISTER**

3.9.1 The purpose of the Board Assurance Framework (BAF) document is to maintain information on the principal risks to the Group and the sources of assurance and results of these, which are in place to confirm that risk mitigation is adequate and operating effectively. The Corporate Risk Register is used to record all the identified relevant risks of the Group.

3.9.2 The Group will maintain a BAF in accordance with NHS guidelines, which requires the Group to have a BAF in place that:

- covers all of the organisation's main objectives;
- identifies which objectives and targets the organisation is striving to achieve;
- identifies the risks to the achievements of objectives and targets;
- identifies and examines the systems of internal control in place to manage the risks;
- identifies and examines the review and assurance mechanisms which relate to the effectiveness of control; and
- records the actions taken by the Board to address the control and assurance gaps.

3.9.3 The Group has determined that it is more efficient and effective to maintain a combined BAF and Corporate Risk Register. As such, the combined BAF and Corporate Risk Register will be structured as set out in Appendix 3.

### **3.10 INCIDENT REPORTING**

3.10.1 Incident Reporting is a fundamental element of the identification of risk and a key component of NHS governance. All staff are actively encouraged to report incidents. The main aim is to record and analyse the overall profile of incidents and near misses and identify hotspots and prioritise action in order to learn from these events within a supportive culture. All incidents should be recorded on an incident form and entered onto the Group's database for analysis. The Group will report all patient safety incidents to the National Reporting and Learning System and staff must comply with policy on the reporting of Serious Incidents.

### **3.11 COMMUNICATION AND RISK TRAINING**

3.11.1 The Risk Management Framework will be available to all staff, service users, the public and other stakeholders on the Group's website. The Framework will also be communicated to all staff via management channels.

3.11.2 Effective implementation of the Strategy requires all staff to be aware of the Group's approach to risk management and clear about their roles and responsibilities within the process.

3.11.3 Training events will be provided for all managers to give them the necessary skills to carry out their own risk assessments and to produce and maintain the



Risk Register (including identification and implementation of risk controls). Governing body members will also be trained.

### **3.12 ANNUAL GOVERNANCE STATEMENT (AGS)**

3.12.1 All CCGs are required to produce an AGS that summarises the main systems and processes in place for risk management and internal control together with the findings of the annual review of effectiveness.

3.12.2 The scope of internal control spans all activities of the Group and is designed to ensure that the Group's policies and decisions are put into practice; the organisation's values are met; laws and regulations complied with; financial and other published information is accurate and reliable; and that human, financial and other resources are managed effectively and efficiently.

3.12.3 Chief Officers, Directors Of and their management teams are the main source of assurance about the organisation's system of internal control. They are also accountable for disclosure of significant internal control issues within their span of control.

3.12.4 There is no standard definition of what constitutes a significant internal control issue that should be disclosed in the AGS. The Chartered Institute of Public Finance and Accountancy (CIPFA) suggest the following criteria should be used in making these judgements:

- The issue seriously prejudiced or prevented achievement of a strategic objective
- The issue has resulted in a need to seek additional funds to allow it to be resolved, or has resulted in significant diversion of resources from another aspect of the business
- The external auditor regards it as having a material impact on the accounts
- The Audit & Governance Committee, or equivalent, advises it should be considered significant for this purpose
- The Head of Internal Audit reports on it as significant in the annual opinion on the internal control environment
- The issue, or its impact, has attracted significant public interest or has seriously damaged the reputation of the organisation

## APPENDIX 1 GLOSSARY OF RISK TERMINOLOGY

TERM	DESCRIPTION
ASSURANCE	An evaluated opinion, based on evidence gained from review, on the organisation's governance, Risk Management and internal control framework
EXPOSURE	The consequences (as a combination of impact and likelihood) which may be experienced by an organisation if a specific risk is realised
RISK RESPONSE or CONTROL	Any action taken to mitigate a risk
INTERNAL CONTROL	Systems in place to manage risk
RISK	The possibility that an event will occur and adversely affect the achievement of objectives.
RISK ASSESSMENT	The process of assessing the impact of a risk and the likelihood of its occurrence
RISK MANAGEMENT	The process of mitigating risks to ensure that they are reduced to an acceptable level
RISK MITIGATION	The action taken to reduce a risk through specific controls
RISK PROFILE	The documented and prioritised overall assessment of the range of specific risks faced by the organisation
INHERENT (GROSS) RISK	the exposure arising from a risk before any action has been taken to manage it
RISK RATING	this is derived from the scoring mechanism and is designed to allow the organisation to prioritise its Risk Management activities
RESIDUAL (NET) RISK	The exposure arising from a specific risk after action has been taken to manage it. Residual Risk should be lower than the inherent risk
ANNUAL GOVERNANCE STATEMENT	This is an annual Statement that summarises the main systems and processes in place for Risk Management and internal control together with the findings of the annual review of their effectiveness.



## APPENDIX 2 RISK ASSESSMENT SCORING METHODOLOGY

The risk evaluation matrix is a simple approach to quantifying risk by defining qualitative measures of impact (severity) and likelihood (frequency or probability) using a simple 1-5 rating system. This allows the construction of a risk matrix, which can be used as the basis of identifying risk. The risk score is Impact x Likelihood=Risk Score

### Impact (Severity)

	Impact score (severity levels) and examples of descriptors				
Domains	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
<b>Impact on the safety of patients, staff or public (physical / psychological harm)</b>	Minimal injury requiring no/minimal intervention or treatment.  No time off work	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
<b>Quality / complaints / audit</b>	Peripheral element of treatment or service suboptimal  Informal complaint/inquiry	Overall treatment or service suboptimal  Formal complaint (stage 1)  Local resolution  Single failure to meet internal standards  Minor implications for patient safety if unresolved  Reduced performance rating if unresolved	Treatment or service has significantly reduced effectiveness  Formal complaint (stage 2) complaint  Local resolution (with potential to go to independent review)  Repeated failure to meet internal standards  Major patient safety implications if findings are not acted on	Non-compliance with national standards with significant risk to patients if unresolved  Multiple complaints/independent review  Low performance rating  Critical report	Totally unacceptable level or quality of treatment/service  Gross failure of patient safety if findings not acted on  Inquest/ombudsman inquiry  Gross failure to meet national standards
<b>Human resources / organisational development / staffing / competence</b>	Short-term low staffing level that temporarily reduces service quality (< 1 day)	Low staffing level that reduces the service quality	Late delivery of key objective/ service due to lack of staff  Unsafe staffing level or competence (>1 day)  Low staff morale  Poor staff attendance for mandatory/key training	Uncertain delivery of key objective/service due to lack of staff  Unsafe staffing level or competence (>5 days)  Loss of key staff  Very low 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 score (severity levels) and examples of descriptors				
Domains	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
<b>Statutory duty/ inspections</b>	No or minimal impact or breach of guidance/ statutory duty	Breach of statutory legislation  Reduced performance rating if unresolved	Single breach in statutory duty  Challenging external recommendations/ improvement notice	Enforcement action  Multiple breaches in statutory duty  Improvement notices  Low performance rating  Critical report	Multiple breaches in statutory duty and prosecution  Complete systems change required  Zero performance rating  Severely critical report
<b>Adverse publicity / reputation</b>	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
<b>Business objectives/ projects</b>	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
<b>Finance including claims</b>	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
<b>Service / business interruption Environmental impact</b>	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

### Likelihood (frequency or probability)

Likelihood score	1	2	3	4	5
<b>Descriptor</b>	<b>Rare</b>	<b>Unlikely</b>	<b>Possible</b>	<b>Likely</b>	<b>Almost certain</b>
<b>Frequency</b> How often might it / does it happen	This will probably never happen/recur	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it is not a persisting issue	Will undoubtedly happen/recur, possibly frequently
<b>Probability</b> Will it happen or not?	<0.1 per cent	0.1–1 per cent	1–10 per cent	10–50 per cent	>50 per cent

**Risk Score (Impact x Likelihood)**

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



# APPENDIX 3 BAF AND RISK REGISTER FORMAT

Dudley CCG Combined Board Assurance Framework and Corporate Risk Register 2015/16

02-Dec-16

Updates from Committees in November 2016

STRATEGIC AIMS	OBJECTIVES 2016/17
1. Reducing health inequalities	1A Primary care and Multi Speciality Community Provider (MCP) development
2. Delivering best possible outcomes	2A Ensure appropriate procurement of secondary care services
	2B Public engagement on model and procurement
	2C Develop the CCG: Fit for purpose for the future
	2D Performance management of the system and Value Proposition (VP) implementation
3. Improving quality and safety	3A Ensure on-going safety and performance of the system
4. System effectiveness	4A Procure the MCP
	4B Primary Care contract
	4C Actively participate in the Black Country Sustainability Transformation Plan (STP)

NOTE: TREND IN RESIDUAL RISK AGAINST PREVIOUS MONTH IS SHOWN ↕↔↖

ID	Original Date	Last Review (Committee Date)	Last Update (Risk Amended)	LINK TO CORPORATE OBJECTIVE	Risk Description	Accountable Committee	Accountability Sponsor & Owner	Management Lead	P	I	Initial Risk Score (Pi)	Key Controls What controls/systems are in place to assist in securing delivery of our objective. Such as strategies, policies and procedures	Gaps in Control Where are we failing to put controls/ systems in place. Where are we failing in making them effective. For example lack of training or no regular review of	Gaps in Assurance Where are we failing to gain evidence that our controls/ systems, on which we place reliance, are effective. Such as no assurance a strategy or policy is effective	(R) P	(R) I	Residual Risk Score (Pi)	Risk Trend Score following controls put in place	Internal Assurances Board Reports, Minutes of meetings	External Assurances Internal and External Audit Reports, CQC Reports	Actions To improve control, ensure delivery of principal objectives, gain assurance	Timescales Date action will be completed	COMMENTS	

## APPENDIX 4 GOVERNANCE STRUCTURE

