Walsall Clinical Commissioning Group

Risk Management Framework

Risk Management Framework

The Walsall Clinical Commissioning Group Audit and Governance Committee approved this framework on:

Date: Sept 2018

Document reference information

Version:	Version 3
Status	Ratified
Director responsible	Prof Simon Brake Chief Officer
Title of author:	Head of Corporate Governance
Ratified by:	Walsall Clinical Commissioning Group Audit and Governance
Date ratified:	17 Sept 2018
Date Policy is Effective From	12 Feb 2014
Review date:	The author is responsible for the review at least 3 months prior to expiry date
Expiry date:	March 2021
Date of Equality and Diversity Impact Assessment	August 2012
Target audience: See section 2 for further clarification	All WCCG staff Any persons employed as third party contractors Bank staff Agency staff Work experience students
Monitoring arrangements	The strategy will be monitored by the regular updates of the risk register system by the Governing Body Committees Regular reports will be received by the Audit Committee on the monitoring and effectiveness of the Risk Management Strategy and Risk Management Plan and the corporate risk register and assurance framework
Linked documents	AS/NZ 4360:2004 Risk Management Standard WCCG Constitution The Orange Book – Management of Risk – Principles and concepts HM Treasury 2004
Dissemination and implementation	Cascaded to GPs via email. Information agenda item for team meetings. Available on Intranet site. Awareness sessions for staff. Development session for Governing Body
Location of archived versions	The Integrated Governance Function holds the master copy of all previous versions.

Please note that the Intranet version of this document is the only version that is maintained. Any printed versions should therefore be viewed as 'uncontrolled' and may not be the most up-to-date.

CONTRIBUTION LIST

Key individuals involved in developing the document

Designation
Chief Officer
Head of Corporate Governance
Lay member for Audit and Governance
Chief Finance Officer
Head of Performance

V 2.5 Circulated to the following for consultation

Name/Committee/Group/	Designation
Senior Officers	
Lay members	
PMO	
internal audit	

Comments received from V2.5 consultation

Name/Committee/Group	Comments
PMO	the framework is in line with PMO risk management suggested minor wording changed

Version Control Summary
Significant or Substantive Changes from Previous Version

Version	Date	Comments on Changes	Author
V1	April 2012	This version is based on the previous NHS Walsall Risk strategy and Risk Management Plan. It has been revised to reflect the CCG requirements as a commissioning organisation. Accountability has been revised to reflect the CCG and its Governing Body. It is acknowledged that after the shadow period the strategy will require further review to incorporate the requirements of the future organisation.	Risk and Assurance Manager
V1.1	April 2012	Incorporate the comments from consultation	Risk and Assurance Manager
V 1.2	Aug 2012	Reviewed the risk register process to align with Governing Body Committees. Strengthen links to financial risk management processes and PMO	Risk and Assurance Manager

		approach.	
V1.3	Sept 2012	New front cover	Risk and Assurance Manager
V1.4	April 2013	Reflect new organisational structure and responsibilities Incorporate the Orange Book HMT model Committee/PMO based risk identification Introduce risk appetite and assurance levels Revised risk register template Revised descriptors for risk consequences Assurance framework	Risk and Assurance Manager
V2	Feb 2015	Ratified SQP	Risk and Assurance Manager
V2.5	Aug 18	Revised to align BAF register format for committee risk register use Include a reporting and monitoring table	Head of Corporate Governance
V3	Sept 2018	Ratified by Audit and Governance Committee	

Contents

1 Introduction

Risk is the chance of something happening that will have an impact on objectives. It is measured by a combination of the consequence of an event and its likelihood. Risk may have a positive or negative impact.

Risk management, along with business continuity and emergency planning are part of a system wide business resilience framework that seeks to ensure that the CCG has the ability to effectively prepare for, respond to and successfully recover from an event that might compromise the delivery of its corporate objectives.

This framework sets out the CCGs approach to the management of risk and the supporting infrastructure which enables informed management decisions in the identification, assessment, treatment and monitoring of the risk environment.

The annual governance statement will summarise the main systems and processes in place for risk management and internal control and disclose any material weaknesses in any financial year. The annual governance statement is a statutory requirement which is signed off by the Accountable Officer and included in the annual report.

2 Scope

This strategy applies to all employees of Walsall CCG and staff employed on their behalf and to all areas where employees and third party contractors deliver services.

3 Aims

Walsall CCG has adopted a pro-active approach with a programme of effective risk management that aims to

1. ensure that risks to the achievement of the corporate objectives are understood, communicated and effectively managed
2. commission high quality services,
3. protect and support staff and our reputation
4. ensure value for money whilst maintaining financial balance
5. demonstrate that the CCG is committed to manging risk appropriately

4 Roles and Responsibilities

The **Governing Body** is responsible for ensuring effective systems and processes for internal control, financial control, organisational control, corporate governance and risk management are in place. It has overall responsibility for setting the risk appetite and reviewing and testing the effectiveness of internal controls through the Assurance Framework.

The **Audit and Governance Committee** will monitor the development and continuous improvement of the risk management process and the Assurance Framework, review the level of risk accepted, appraise the risk register and examine whether management is responding appropriately and advise on the formal annual review of the effectiveness of the system of internal control and the content of the annual governance statement.

The **Operational Leads and Chairs** of committees are responsible for identifying and managing risks that are discussed in committee and recording them on the risk committee register. The Chair must ensure that the risk register is reviewed each time the committee meets. This includes amending, closing, adding new risks, gaining assurance that the actions are completed and effective and that any residual risks that fall outside of the risk appetite are appropriately escalated. The management of all red risks is reported to the governing body through the committee assurance report.

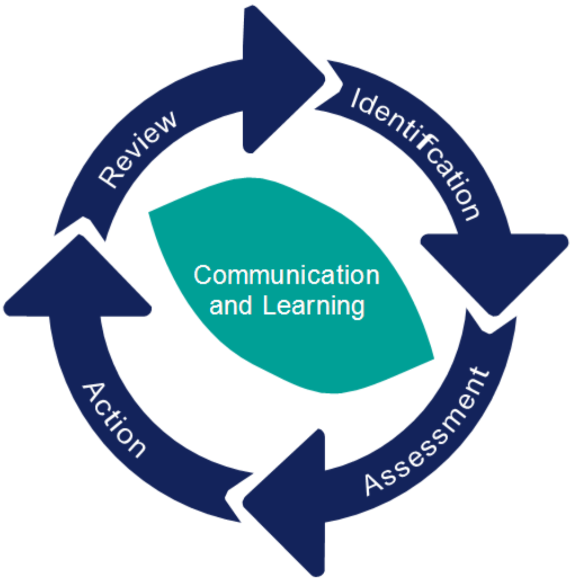
It is the responsibility of all **Senior Officers and Managers** to understand and implement the Risk Management Strategy. They are responsible for ensuring that:

1. Appropriate and effective risk management processes are in place within their designated area(s)
2. All staff are made aware of the risks within their work environment and of their personal responsibilities
3. Identified risks from the managers area of responsibility which are not managed within the relevant risk appetite are escalated to the appropriate forum to ensure that the risk is controlled within an acceptable range. Any risks that require urgent management prior to the next committee meeting should be escalated to the relevant Director for consideration and management.
4. All staff attend mandatory training and risk assessment training/awareness relevant to their roles in order for them contribute to working in a safe environment

All staff must participate in the implementation risk management and have a duty to comply with the risk framework and all Walsall CCG policies, regulations and instructions.

5 Risk Management Process

Walsall CCG has based its fundamental approach to risk management from a combination of the frameworks set out in the Orange Book and the AS/NZ 4360:2004 Risk Management Standard.



Risk management is the process of identifying risk referred to as inherent risk. Assessing the inherent risks and agreeing the most appropriate measures to control the risk to an acceptable level, referred to as residual risk.

Once this has been implemented the residual risk must be reviewed to ensure that the actions taken have had the desired effect in controlling or mitigating the risk.

5.1 Step 1 - Identify the risks

When identifying risks it is important not to describe issues which have already occurred. A risk is the possibility that something will happen that may impact positively or negatively on the achievement of objectives.

Walsall CCG adopts a committee led approach to the identification of risk. Each corporate objective is monitored by a GB committee with a lead director who ensures that progress is made against the delivery of the objective and management of the risks identified against the objective.

The operational lead and chair of the committee/group ensure that any reports presented to the committee or discussions held in committee that identify a risk are recorded on the appropriate committee risk register. This is a continual process and the risk registers will be reviewed by the committee at each meeting.

5.1.1 Risk categories

Risk categories are used to describe the types of risk that the CCG will need to consider. They are useful to assist in identifying risks

Quality	Finance	Workforce
Health & Safety	Complaints	Environment
Reputation	Compliance	Project
Engagement	Business interruption	

5.1.2 Joint risks

Joint risks with partner organisations will be identified, reported and managed through the governance arrangements between organisations. This will be mainly through the joint committee structures, for example Walsall Joint Commissioning Committee and Safeguarding Boards. Where possible the organisation which is most likely to be able to affect change should be the organisation that takes ownership of the risk. It may be the case that the joint risk may require each organisation to take action to mitigate the risk and these actions may differ for each organisation.

In any event it is important to ensure that accurate records are kept detailing the management and accountabilities of shared risks. Each organisation is responsible for ensuring that joint risks are communicated to their organisations appropriate committee in a timely manner.

5.1.3 Describing a risk

When a risk is identified it is important to be able to describe the risk in clear terms so that is it is meaningful to others especially stakeholders.

When describing a risk it is helpful to use the 3 Cs

Table 1 Three Cs for Describing Risks

Consequence	Describe the potential **consequence** if the risk were to materialise.
Causal	Describe the **causal** factors that could make the risk materialise
Context	Include the **context** of the risk e.g. define the risk target (staff, patients) and the nature of the risk (safety, financial, reputation)

An example of a risk would be:

There is a financial risk to the CCG staff that they may not receive their wages on time if the change over to a new payroll system is not successful.

5.1.4 Key Risk Questions

Once the risk has been identified and described a series of key questions need to be answered. This is a logical process once a risk is identified and one that may happen simultaneously whilst identifying the risk.

Key Questions are:

1. What can go wrong?
2. When, where, why, how are the risks likely to occur?
3. Who might be involved?
4. What are the consequences?
5. What is the potential in terms of time, money, reputation and harm to others?
6. What resources are currently available?

5.2 Step 2 - Assess the risks

It is important to have an objective method for assessing risks so that the minor acceptable risks can be separated from the risks that need to be managed.

5.2.1 Determine the Likelihood

To determine the likelihood of a risk, descriptors are described in both frequency and probability in a five point scale. This is a subjective approach based on the managers experience and knowledge of the risk, but within described parameters it is effective. The probability descriptor is more appropriate when there is a time limited issue.

Table 2 Likelihood Descriptors

What is the likelihood of the consequence occurring?					
	1	**2**	**3**	**4**	**5**
Descriptor	Rare	Unlikely	Possible	Likely	Almost Certain
Frequency	Not expected to occur for years	Expected to occur at least annually	Expected to occur at least monthly	Expected to occur at least weekly	Expected to occur at least daily
Probability	< 2.5%	2.5 - < 10%	10 – 49%	50 – 80%	> 80%
	Will only occur in exceptional circumstances	Unlikely to occur	Reasonable chance of occurring	Likely to occur	More likely to occur than not

5.2.2 Determine the Consequences

The consequence scale is broken down into several descriptors that fit into the context of the organisation in a five point scale. Managers should use their judgement and experience and the descriptors for consequences as a guide to determine the level of consequence for the risk that they are assessing.

Table 3 Consequences Descriptors

Descriptors for identified risk categories					
	1	**2**	**3**	**4**	**5**
Descriptor	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Quality Audits	No significant effect on quality	Noticeable effect on quality of care provided	Significant effect on quality	Quality is significantly impaired, potential for long term impact	Quality is significantly impaired, potential for permanent impact
Project management	Insignificant cost increase / schedule slippage. Barely noticeable reduction in scope or quality	< 5% over budget / schedule slippage. Minor reduction in quality / scope	< 25% over budget / schedule slippage. Reduction in scope or quality requiring client approval	<50 % over budget / schedule slippage. Doesn't meet secondary objectives	>50 % over budget / schedule slippage. Doesn't meet key objectives
Engagement			Moderate engagement or not an appropriate CCG response to engagement	Minimal engagement or not covering all stakeholders	No engagement for decommissioning of major services

Complaint / litigation	Informal complaint or query locally resolved	Formal complaint locally resolved	Upheld complaint Claim < £10 000.	Multiple upheld complaints / ombudsman Claim > £10 000.	multiple ombudsman reviews Multiple claims or single major claim
Business Interruption	Loss / interruption > 1 hour	Loss / interruption > 1 day	Loss / interruption > 1 week	Loss / interruption > 1 month	Permanent loss of service or facility
Workforce	Short term low staffing level/competence temporarily reduces service quality < 1week	On-going low staffing level/competence reduces service quality >1 week	Unsafe staffing level or competence >1 month Late delivery of key objective/service due to lack of staff Low staff morale Poor staff compliance for mandatory training	Unsafe staffing level or competence >3 month uncertain delivery of key objectives/service due to lack of staff loss of key staff No staff completing mandatory training	Ongoing or critical unsafe staffing level or competence > 6 month non delivery of key objectives/service due to lack of staff No staff completing training on an ongoing basis
Finance	£100K – £1M	>1% of budget > £5M	>5% of budget > £20M	> 20% of budget > £30M	> 40% of budget > £40M
Regulatory Compliance	Minor recommendations. Minor non-compliance with standards	Recommendations given. Non-compliance with minor standards Breach of statutory legislation	Reduced rating. Challenging recommendations. Non-compliance with core standards Challenging external recommendations/improvement notice	Enforcement Action. Critical report. Multiple challenging recommendations. Major non-compliance Low performance rating Critical report Improvement notices	Prosecution. Zero Rating. Severely critical report Complete systems change required.
Reputation Adverse publicity	Rumours potential for public concern	Local Media coverage short term reduction in public confidence Minor effect on staff morale	Local Media coverage long term reduction in public confidence MP Concern Significant effect on staff morale	National Media coverage < 3 Days Multiple MP Concerns	National Media coverage > 3 Days Questions in the House Service well below public expectations
Health and safety	Minor <1 day shortfall in safety system or insignificant impact on health	Temporary <1 week shortfall in safety system or minor impact on health	Sustained < 1 month Failure of safety system or moderate impact on health	Significant failure of safety system or major impact on health	Failure of multiple critical components of safety system or critical impact on health
Environmental Impact	Minor non-compliance with standards Minimal increase in environmental impact	Non-compliance with non-core standards Small increase in environmental impact	Non-compliance with core standards Significant increase in environmental impact	Enforcement Action. Critical report. Major non-compliance with core standards Unacceptable increase in environmental impact	Prosecution Severely critical report Severe impact on environment

5.2.3 Determine risk rating

To determine the rate of risk a simple equation is used:

Likelihood X Consequence = Risk rating.

The scores for likelihood and consequence are put into the risk matrix and that indicates the risk rating.

The risks ratings are used on the risk register and are an indication of how a risk is reduced when controls are put into place. The risk rating is used to indicate the organisational risk appetite for the specified risk categories.

Risk ratings are categorised into four levels:

Table 4 Levels of Risk Rating

Risk rating	*Low 1-3*	*Moderate 4-6*	*High 8 -12*	*Extreme 15 – 25*
	Green	Yellow	Amber	Red

Table 5 Risk Matrix

Matrix	**Consequence**				
Likelihood	**1**	**2**	**3**	**4**	**5**
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

5.2.4 Risk Appetite

It is acknowledged that it is not reasonable or practical to remove all risk and there will be a point where the organisation is willing to accept some element of risk to a level that is justifiable and tolerable – this is known as risk appetite.

The risk appetite that the CCG is willing to accept is not static and may vary depending on a number of external and internal factors. The governing body will regularly review the risk appetite to give the organisation a steer on what is tolerable and when risks need to be actively treated.

When considering the risk appetite the cost (financial, reputational or otherwise) of constraining the risk must be compared with the cost of exposure should the risk become a reality and then an acceptable balance can be agreed.

All risks with a residual rating of 8 or above are required to be managed closely with a plan to mitigate the risk. The CCG will only tolerate residual levels of risk (i.e. take no further action) that are classified as 8 or above where the action to mitigate further is recorded as either not cost effective or reasonably practicable.

Any risk that is above 15 or above will be reported to the Governing Body as part of the assurance framework.

The Governing Body have the freedom to vary the risk appetite at any one time depending on external factors and circumstances, but should review the risk appetite at least annually.

5.3 Step 3 - Action the risks

Once the risk has been rated it allows for the appropriate risk action to be taken.

5.3.1 Internal control

The response initiated by the organisation to risk is called internal control. It can take one of the following four forms:

1. Tolerate – This is where the organisation accepts that there is little that they can do to control a risk i.e. terrorist attack and tolerate the risk. This is where contingency plans are put in place
2. Treat – this is where actions are identified which will constrain the risk to an acceptable level or to actively manage if the risk is positive.
3. Transfer – this is where the organisation may take out insurance and transfer the risk to a third party
4. Terminate – this is where the organisation stops carrying out the activity that gives rise to the risk thereby removing the risk altogether

The controls should be:

1. Based on active consideration of the options for controlling that risk to an acceptable level of residual exposure
2. Disseminated to all those who need to know about the controls
3. Regularly reviewed to consider whether they continue to be effective, best value for money as a response to the risk and documented by the relevant managers

5.3.2 Identify existing controls

Each identified risk must have the existing controls identified. There are many sources of control for key risks: business continuity plan, organisational culture and Scheme of Delegation are some broad organisational examples. Policies, protocols and guidelines however are one of the main sources of risk control.

5.3.3 Identify options

Control measures for identified risks will normally be identified during committee discussions. Mangers draw on previous events, experience and networking. It is also important to seek the opinion of internal risk advisors, specialist i.e. infection control nurse, Occupational Health and external risk advisors for example Police and Fire services, Health and Safety Executive, Local Authority and the Health Protection Agency.

5.3.4 Recording Risks

Once a risk is rated using the risk matrix it must be recorded onto the risk register. The CCG use the assurance framework format to record all identified risks. This supports the consistent reporting of risk from committee registers to Governing Body and ensures all risks are managed consistently.

5.3.5 Prepare and implement treatment plans

Identified leads must be accountable for implementing the identifying internal controls and seeing them through to completion and ensuring that the risk register is updated. This activity would be reported through the committee meetings and documented in the minutes and on the risk register.

5.4 Step 4 - Review

5.4.1 Monitor and review risk registers

The following monitoring arrangements will be applied according to the residual risk score.

Table 6 Monitoring Arrangements

Rating	Appetite	Monitored by	Frequency
15 - 25	Unacceptable risk requiring immediate action to reduce the risk	Governing Body Committee SMT	Six monthly Each meeting Quarterly
8 - 12	Unacceptable risk requiring active monitoring and review	Committee SMT	Each meeting Quarterly
4-6	Acceptable risk which can be tolerated Review for ongoing effectiveness of controls	Committee	Annual
1-3	Acceptable risk	Managers	Consider for closure

5.5 Assurance

Assurance is an evaluated opinion based on evidence gained from review of the organisations governance, risk management and internal control.

Effective assurance requires defined corporate objectives, effective internal controls and good quality data.

It is important for Walsall CCG to recognise the difference between assurance and reassurance which is not adequate for the purposes of risk management.

Table 7 Assurance or Reassurance

Assurance	*Reassurance*
Scope of assurance is defined to either whole systems or a specific investigation, backed by evidence of outcomes	Outcomes are based purely on implementation of processes, action plans or establishment of committees and not their effectiveness
Rigour: supporting evidence from either triangulation or collaboration from an alternative source	Inconsistent with previous or other reports
Staff are appropriately skilled to give assurance	Repeated single source with little evidence or collaboration
Independent: from external and or internal sources	Oral report with no back up
Relevant time period	Postponement/deferral

5.5.1 Levels of Assurance

By defining levels of assurance the organisation has a structured approach that pulls risk management and compliance together in a robust framework. There are three levels of assurance that can be sourced for the organisation.

Table 8 Levels of Assurance

Level of assurance	*Nature of assurance*	*Value added*
First level *Management*	This is direct from those responsible for delivering the specific objectives or operations within departments or functions. Controls are based on processes and systems. It provides assurance that performance is monitored, risks identified and objectives achieved.	This may lack objectivity but has value in the expertise and knowledge for the specified area.
Second level *Governing Body and its committees*	This work is associated with the oversight of management activity. It is based on corporate governance, the governing body committees which set policy, implement strategy and oversee the operations of the organisation. It is separate from those responsible for delivery but not totally separate from management. It includes compliance assessments, assurance reports from committees that have reviewed and challenged management level assurance and reviews carried out to determine that policy or arrangements are being met in line with expectations	It will provide more objective assurance than management level.

	for specific areas of risk across the organisation.	
Third level *Independent*	This is independent and the most objective type of assurance. It focuses on internal audit with an independent and objective opinion on the framework of governance, risk management and control. It places reliance on mechanisms in the first and second levels of assurance, directing its resources on the areas of highest risk or where there are gaps in other assurance arrangements. It also uses assurance from other independent sources for example external audit, regulators and peer reviews.	It is independent of the first and second levels of assurance and generally operates to professional and ethical standards.

It is helpful to use levels of assurance to establish the degree of assurance that is required for identified risks against corporate objectives. It is therefore possible to identify whether there are any gaps in the assurance and the level to which risks are adequately controlled.

Table 9 Levels of Assurance and Risk Appetite

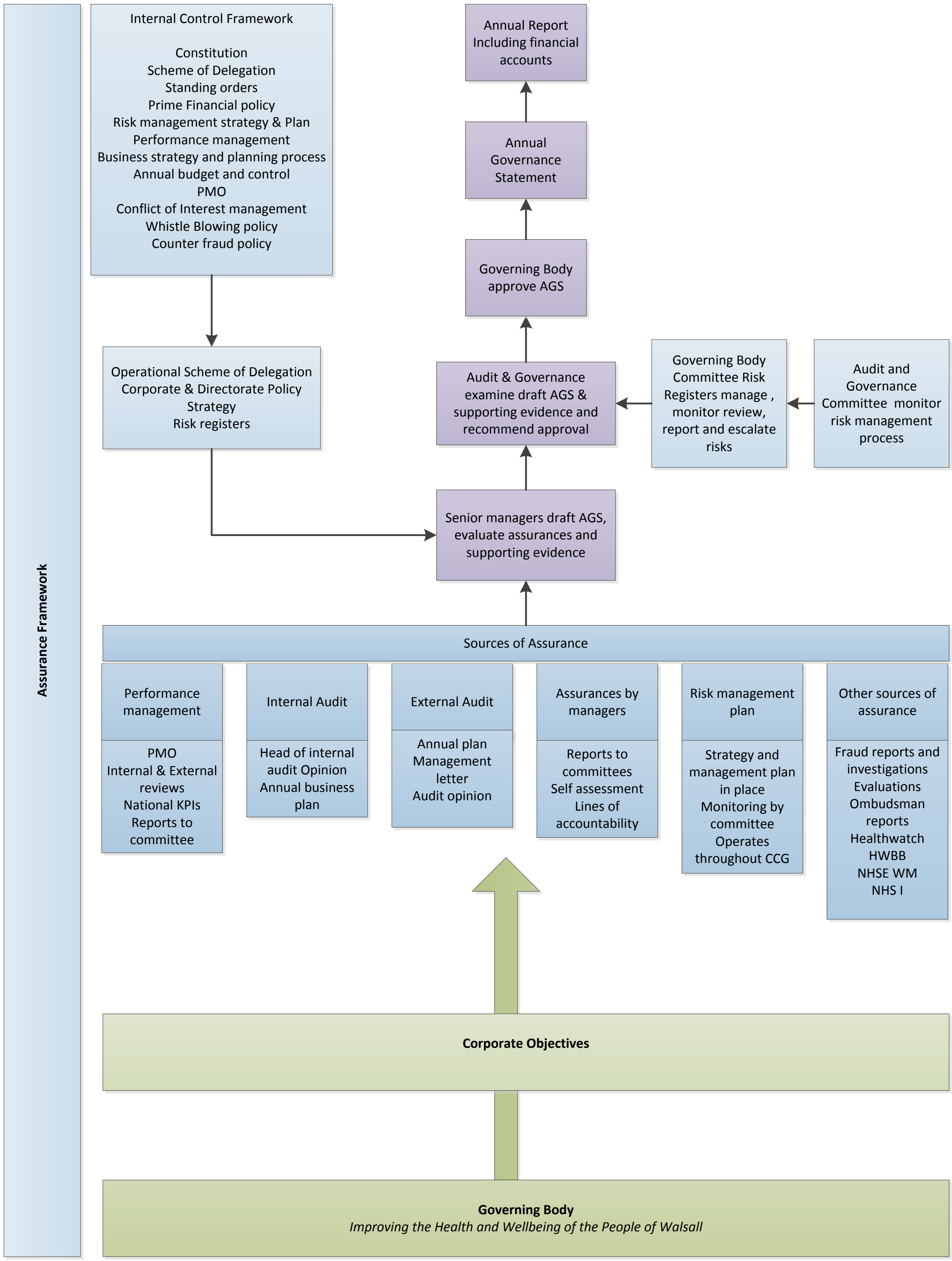
Risk Appetite	*Low*	*Moderate*	*High*	*Extreme*
	Not willing to accept any risk under any circumstances	Willing to accept some risk under some circumstances	Willing to accept risks that may result in identified impact	Accepts risks that are likely to results in identified impact
Level of assurance	Independent Assurance	Governing Body Assurance	Management and Governing Body Assurance	Management

5.6 Assurance Framework

An assurance framework is a structured means of identifying and mapping the main sources of assurance in an organisation and coordinating them to best effect. It provides the Governing Body members with assurance that the risks to the corporate objectives are being positively managed. It is a key communication tool in the risk management plan which identifies the principal risks to the Governing Body and describes how these risks are being managed. It consists of a suite of documents and processes that together illustrate the organisations delivery against its corporate objectives.

The diagram below illustrates the formal structure of the assurance framework for Walsall CCG. The governance structure is detailed in figure 3.

Figure 1 Formal Structure of the Assurance Framework



6 **Definitions**

Risk suffers from an overabundance of jargon which can add to confusion and misunderstanding when communicating risk throughout the organisation. It is important to have consensus and universal understanding of the terminology and meaning of the language used within this risk strategy. These definitions have been taken from Risk Management, AS/NZS 4360:2004 p2-5, Assurance frameworks HMT 2012 and the Orange Book HMT 2004.

Annual Governance Statement	It is a key assurance document covering the organisations corporate governance risk management, and internal control arrangements. The statement should include an evaluation on how well the arrangements have operated in practice based on the on-going assessment processes.
Assurance	An evaluated opinion based on evidence gained from review on governance, risk management and internal control framework.
Assurance framework	A structured means of identifying and mapping the main sources of assurance in an organisation and co-ordinating them to best effect.
Exposure	The consequences as a combination of impact and likelihood which may be experienced by the organisation if a specific risk is realised.
Inherent risk	The exposure arising from a specific risk before any action has been taken to manage it.
Internal control	Any action originating within the organisation taken to manage risk. These actions may be taken to manage either the impact if the risk is realised or the frequency of the realisation of the risk.
Just Culture	An environment where staff are treated fairly and are able to report errors and talk about their problems without the fear of personal reprisal
Residual risk	The exposure arising from a specific risk after action has been taken to manage it and making the assumption that the action is effective
Risk	The chance of something happening that will have an impact on objectives. It is measured in terms of a combination of the consequence of an event and their likelihood. Risk may have a positive or negative impact
Risk appetite	The risk appetite is the level of risk that an organisation is prepared to accept before action is deemed necessary to reduce it.
Risk management	Is the culture, process and structures that are directed towards realising potential opportunities whilst managing adverse effects
Risk management system	Is the systematic application of management policies, procedures and practices to the tasks of communicating, establishing the context for identifying, analysing, evaluating, treating, monitoring and reviewing risk

Risk treatment	Is the process of selection and implementation of measures to modify risk
Risk assessment	Is the overall process of risk identification, risk analysis and risk evaluation.
Risk identification	Is the process of determining what, where, when, why and how something could have happen
Risk analysis	Is a systematic process to understand the nature of and to deduce the level of risk
Risk evaluation	Is the process of comparing the level of risk against risk criteria
Risk criteria	Are the terms of reference by which the significance of risk is assessed
Risk reduction	Is an action taken to lessen the likelihood, negative consequences or both associated with a risk
Risk control	Is an existing process, policy, device, practice or other action that acts to minimise negative or enhance positive opportunities
Event	Is the occurrence of a particular set of circumstances
Consequence	Is the outcome of impact of an event
Likelihood	Is used as a general description of probability or frequency
Probability	Is a measure of the chance of occurrence expressed as a number between 0 – 1
Frequency	Is a measure of the number of occurrences per unit of time