NHS
Yorkshire
Ambulance Service
NHS Trust

Risk Management and Assurance Strategic Framework

Document Author

Associate Director: Performance, Assurance and Risk

Date Approved: March 2020

Document Reference	ST- Risk Management and Assurance Strategic Framework
Version	6.1
Responsible Committee	Trust Board
Responsible Director (title)	Executive Director of Quality, Governance and Performance Assurance
Document Author (title)	Associate Director of Performance, Assurance and Risk
Approved By	Trust Board
Date Approved	March 2020
Review Date	March 2023
Equality Impact Assessed	Not Applicable
Protective Marking	Unrestricted

Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
3.0	Sept 2012	Kevin Wynn, Associate Director Risk & Safety	**A**	Full review
3.1	Feb 2013	Kevin Wynn, Associate Director Risk & Safety	D	
3.2	Aug 2013	Mark Hall, Associate Director Risk & Safety	D	Update to reflect changes in Structure and practice
4.0	Nov 2013	Mark Hall, Associate Director Risk & Safety	**A**	Approved by Board 26 November 2013
4.1	Jul 2015	Becky Monaghan Associate Director Risk and Safety	D	Update to reflect changes in Structure and practice
5.0	May 2016	Maxine Travis	D	Include risk appetite statement (Approved Trust Board May 2016)
5.1	Mar 2018	Risk Team	D	Application of corporate visual identity
5.2	July 2018	Maxine Travis	D	Update titles of groups and roles, 3.8 amend Internal Audit assurance levels
5.3	June 2019	Kate Taylor – Head of Risk	**A**	TMG approved extension until September 2019.
5.4	July 2019	Kate Taylor – Head of Risk	**A**	Board approved risk appetite statement revised.
6.0	March 2020	David O'Brien Associate Director: Performance, Assurance and Risk	**A**	Full review and refresh as part of the document review cycle timeframe
6.1	Nov 2020	David O'Brien Associate Director:	**A**	Appendix 2 updated to reflect new BAF strategic risks approved by Trust Board

Status Key: **A** = **Approved** D = Draft

Associated Documentation:

- Risk Management Policy
- Information Governance Policy
- Business Continuity Management Policy and Guidance
- Governance Handbook
- Incident and Serious Incident Management Policy
- Investigations and Learning Policy
- Health and Safety Policy
- Statutory and Mandatory Training Policy

CONTENTS

1.0 INTRODUCTION

1.1 Risk is inherent in all activities and at all levels of the Trust. Risk management is everybody's business.

1.2 Risk management is a statutory and regulatory requirement for the Trust. It is also an indispensable core component of good practice in all aspects of strategy, planning and operational management.

Managing Risks

1.3 At an operational level good risk management is essential for the delivery of safe, efficient and high quality services. Dynamic risk assessment links to resilience and business continuity activities to help sustain frontline operations and support functions. At a strategic level good risk management underpins the Trust's planning and development activities, both as an organisation in its own right and in collaboration with others as a wider system partner.

1.4 Failure to identify and manage risks in a timely and effective manner could result in:

- Harm to patients, staff, volunteers, or others
- Failure to deliver the Trust's strategies, policies, plans and operational priorities
- Failure to achieve required levels of organisational resilience and business continuity
- Loss or damage to the Trust's reputation or influence at national, regional or community level
- Loss or damage to the Trust's property, assets, systems and data
- Financial and commercial losses
- Adverse publicity, complaints, and litigation

Taking Opportunities

1.5 Managing risk is not just about avoiding adverse future events. Risk management good practice also includes considered, well-controlled risk-taking in pursuit of opportunities to develop, improve and add value to the services and functions of the Trust.

1.6 Failure to identify and manage opportunities in a timely and effective manner could result in a reduced ability to:

- Deliver improvements in quality and the safety of patients, staff and volunteers
- Optimise the operational impact of the Trust's strategies, policies and plans
- Realise the benefits expected from change projects, transformation programmes, and digital solutions
- Achieve targets for cost improvement, efficiency and income
- Realise future opportunities for Trust development
- Protect and enhance the Trust's reputation as an influential and innovative system partner and valued community partner

1.7 Through its risk management and assurance arrangements, including proactive risk assessment, resilience and business continuity processes, the Trust supports an open, dynamic and balanced approach to managing risk and taking opportunities.

2.0 PURPOSE AND SCOPE

Purpose

2.1 The purpose of this Risk Management and Assurance Strategic Framework is to set out the overarching principles and processes that enable the Trust to manage risk well and uphold high standards of risk governance and assurance. It describes how the Trust's risk management activities dovetail with other governance and assurance arrangements to form a coherent system of internal control.

2.2 This framework supports the Trust to deliver its objectives by ensuring that:

- Risks to objectives are identified and managed in a timely and effective manner
- Opportunities for strategic development and service improvement are embraced and delivered safely
- The prevailing risk management and assurance culture is open and constructive
- Risk management and assurance activity, including risk assessment and business continuity, adds value to the life and work of the Trust

Scope

2.3 This framework:

- Supersedes the previous 'Risk Management and Assurance Strategy' and any equivalent predecessor documents
- Is formally known as the 'Risk Management and Assurance Strategic Framework', and is also referred to in this document as 'the framework' or 'this framework'
- Is owned by and applies to the Yorkshire Ambulance Service NHS Trust, referred to throughout this document as 'the Trust'
- Applies to all directly employed staff, agency staff, contractors and volunteers engaged in work or other activities on behalf of the Trust
- Sets out the systems, processes and responsibilities developed and maintained by the Trust to support effective risk management practice, reinforced by sound and proportionate governance and assurance arrangements
- Aligns with and supports delivery of the Trust's purpose, vision, values, ambitions and key priorities as set out in the *One Team, Best Care* Strategy 2018-23 and the associated suite of enabling strategies
- Complements and links to other related Trust policies, procedures, and guidance (such as the Business Continuity Policy)

- Takes account of external considerations and requirements, including those associated with commissioners, regulators, partners, and other relevant stakeholders. This includes the expectations set out in the Well Led Framework for NHS Trusts

- Takes account of risk management and assurance good practice as developed and promoted by relevant professional bodies, such as the Institute of Risk Management, the Chartered Institute of Internal Auditors, and the International Standards Organisation (ISO:31000) and by government bodies such as HM Treasury and the Cabinet Office

3.0 PRINCIPLES

3.1 This Risk Management and Assurance Strategic Framework is informed by a set of design principles. These are presented in 3.2 below.

Risk Management and Assurance Strategic Framework: Design Principles

3.2 The Trust:

- Recognises that risk is inherent in all activities and at all levels of the organisation

- Believes that risk management is everybody's business, and applies its risk management and assurance arrangements to all directly employed staff, agency staff, contractors and volunteers engaged in work or other activities on behalf of the Trust

- Seeks to control risks in a proportionate and cost-effective manner such that exposures are reduced to an acceptable level (in accordance with agreed risk appetite) or are eliminated as far as is reasonably practicable

- Acknowledges that some risks can never be eliminated entirely

- Seeks to mitigate and control its identified risk exposures either by treating, terminating, tolerating or transferring risks

- Recognises that risk management good practice facilitates the taking of opportunities to innovate and improve

- Encourages considered and controlled risk taking within authorised limits in order to develop and transform its services and functions

- Applies its risk management and assurance framework to all categories of risk, including (but not limited to): strategic, operational, clinical, technology (including healthcare technology), financial, fraud, commercial, programme/project, security, business continuity, information, regulatory, environmental and reputational risks

- Will adopt and adapt instances of good practice found in established risk management and assurance methodologies, but where appropriate will develop bespoke risk management arrangements tailored to its own local needs

- Will ensure that its risk management and assurance arrangements support transparency, accountability and the wider public interest regarding the activities of the organisation

4.0 OBJECTIVES

Risk Management Objectives

4.1 The Trust seeks to adopt good practice in the identification, evaluation and cost effective control of risks to ensure that they are reduced to an acceptable level or are eliminated as far as is reasonably practicable. In addition, the Trust seeks to maximise appropriately controlled opportunities to deliver its strategic objectives and operational priorities, and to continuously improve its service provision and support functions.

4.2 The objectives of risk management across the Trust are to:

- Minimise the potential for harm to patients, staff, volunteers and visitors, reducing this to levels that are as low as is reasonably practicable
- Protect everything of value to the Trust (such as high quality patient care, staff and patient safety, reputation and influence, physical and intellectual assets, current and future income streams, information systems and data)
- Enable the Trust to anticipate, respond to, and remain resilient in changing strategic and operational circumstances
- Maximise opportunities for Trust development, innovation, and improvement of services and functions in a safe, considered and controlled manner
- Ensure that the Trust achieves and sustains compliance with statutory, policy, regulatory and legal frameworks and other similar requirements
- Inform the Trust's strategies, policies and operational decisions by identifying risks and their likely impact, and by developing actions and controls to manage these risks
- Ensure that risk management and assurance activity is embedded into standard management practice across the Trust and is not regarded as separate or niche
- Ensure that risk management and assurance activity is seen as a live and dynamic process that is embedded in the work of governance bodies and managerial groups at all levels of the Trust
- Provide a standard set of policies, procedures and processes to support consistent risk management practice across all functions and at all levels of the Trust

4.3 To achieve these objectives the Trust will:

- Consider risk when:

  - developing, approving and implementing strategies, plans and policies
  - developing and approving business cases or other investment proposals (for instance, as part of the organisation's internal 'Gate Review' process)
  - scenario planning for exceptional circumstances such as major incidents or escalation in status relating to its Resource Allocation Escalation Plan
  - planning and delivering transformation programmes and change projects
  - implementing cost improvement or other efficiency programmes
  - implementing service improvements and digital innovations
  - entering into contractual relationships or other partnership arrangements
  - taking other strategic and operational decisions
  - preparing and presenting reports and proposals for governance bodies

- Clearly define risk management roles, responsibilities and reporting lines within the organisation, including appropriate linkages with the organisation's internal Accountability Framework (as it is developed, implemented and embedded)

- Apply appropriate and proportionate risk management principles and practice in all activities of the Trust

- Reinforce the importance of effective risk management as part of the everyday work of all staff and volunteers employed or engaged by the Trust

- Ensure that the importance of effective risk management and assurance is reflected in the role and responsibilities of internal governance bodies and captured as appropriate in the approved terms of reference for each of these bodies

- Maintain timely, accurate and comprehensive intelligence about all identified risks on a single management information system (Datix) and use this to produce corporate and local risk registers and other forms of risk analysis and reporting

- Ensure that appropriate actions and controls are in place to mitigate risks and that these are well understood by those expected to apply them

- Ensure that gaps in controls are identified and rectified in a timely and appropriate manner

- Provide training and engagement activities to strengthen risk management capacity and capability within the workforce and to generate and sustain a good level of general awareness and understanding of risk management across the Trust

- Maintain appropriate linkages between risk management and other relevant governance, assurance and internal control frameworks, policies and processes (such as business continuity, information governance, physical and cyber security).

- Work with its internal audit provider to plan and deliver an annual programme of risk-based reviews and related assurance processes, and implement improvement actions and learning opportunities arising from these in a timely and appropriate manner

- Monitor, review and seek continuous improvement in risk management and assurance arrangements across the organisation

5.0 STRATEGIC CONTEXT

Trust Objectives

5.1 The foundation of an organisation's risk management and assurance framework is its set of strategic and operational objectives: risks are identified, evaluated and managed in the context of the effect of uncertainty on objectives. This Risk Management and Assurance Strategic Framework is organised around the need to identify, evaluate and manage risks and opportunities associated with delivery of the Trust's objectives.

5.2 The Trust's objectives are set out in its five-year strategy, *One Team, Best Care 2018-23*. This strategy presents four overarching ambitions for the Trust:

- Patients and communities experience fully joined-up care, responsive to their needs
- Our people feel empowered, valued and engaged to perform at their best
- We achieve excellence in everything we do
- We use resources wisely to invest in and sustain services

5.3 Eight priorities support the achievement of these overarching ambitions:

- Deliver the best possible response for each patient, first time
- Attract, develop and retain a highly skilled, engaged and diverse workforce
- Equip our people with the best tools, technology and environment to support excellent outcomes
- Embed an ethos of continuous improvement and innovation that has the voice of patients, communities and our people at its heart
- Be a respected and influential system partner, nationally, regionally and at place
- Create a safe and high performing organisation based on openness, ownership and accountability.
- Generate resources to support patient care and the delivery of our long-term plans, by being as efficient as we can be and maximising opportunities for new funding
- Develop public and community engagement to promote YAS as a community partner; supporting education, employment and community safety.

5.4 The overall landscape relating to Trust objectives includes its purpose, vision, values, ambitions and key priorities as set out in *One Team, Best Care* along with an associated suite of enabling strategies. Appendix 1 summarises all of these in the form of a strategy on a page.

5.5 The Trust's annual business plan, operational plans, and other service and programme plans support delivery of these strategic objectives.

Strategic Risks

5.6 Strategic level risks to the delivery of the Trust's stated objectives are identified, evaluated and overseen by the Trust Board. These strategic risks, along with associated controls and mitigation actions, are captured and monitored via the Board Assurance Framework (see 6.28 – 6.34).

5.7 The Trust Board reviews and updates the set of strategic risks captured in the Board Assurance Framework each year as part of the annual planning process. Appendix 2 sets out the strategic risks identified by the Board for the current year.

Risk Appetite

5.8 Risk appetite is generally understood to be the agreed level of risk that the Trust is prepared to accept or be exposed to in pursuit of its strategic objectives. Appendix 3 includes some authoritative definitions of risk appetite.

5.9 Risk appetite guides the organisation regarding permitted levels of risk exposure, encourages consistency of approach to controlled risk-taking, and ensures that finite resources are not used to reduce risk exposures that are already being managed at an acceptable level.

5.10 The Trust Board owns and approves risk appetite relating to the organisation's strategic objectives. The Trust Board publishes an annual statement of its risk appetite. Appendix 3 sets out the risk appetite statement approved by the Trust Board for the current year.

5.11 Precise measurement of risk appetite is not always possible and instead it is often expressed as a broad statement of intent to be applied generally across the organisation. This is the approach adopted by the Trust Board. By stating its general intentions regarding risk appetite the Trust Board endorses an appropriate balance between innovation and caution. This enables the Trust to show that it has broad appetite for some types of risk and a general aversion to others, depending on the context of the risk and the associated balance of threats versus benefits.

5.12 The Trust Board reviews and updates its risk appetite statement each year as part of the annual planning process. To inform its annual review and update of risk appetite the Trust will refer to the risk appetite matrix developed for NHS bodies by the Good Governance Institute. Appendix 4 presents this matrix.

6.0 RISK MANAGEMENT AND ASSURANCE ARRANGEMENTS

6.1 Key components of the Trust's risk management and assurance arrangements include:

- Policies and procedures
- Roles and responsibilities
- Systems and tools
- Reporting and escalation
- Governance and risk assurance

Policies and Procedures

Risk Management Policy

6.2 The Trust's Risk Management Policy supports the application of this Risk Management and Assurance Strategic Framework. The Risk Management Policy sets out the processes and procedures to follow in order to identify, evaluate and manage risks in the Trust. The policy applies to all directly employed staff, agency staff, contractors and volunteers engaged in work or other activities on behalf of the Trust.

6.3 The Risk Management Policy sets out the Trust's requirements regarding risk management practice. This includes, amongst other things, the Trust's expectations about how to:

- Identify a risk and articulate it using the Trust's standard format for describing a risk: "IF… THEN…. RESULTING IN…"
- Evaluate the likelihood, consequence and overall exposure relating to a risk, using the approved risk evaluation matrix (see 6.13 and Appendix 11)
- Record risk intelligence on the Trust's risk information management system (Datix)
- Identify controls and gaps in controls relating to a risk
- Identify an appropriate risk owner
- Develop actions to address gaps in controls and to mitigate a risk
- Monitor, review and report on a risk
- Escalate, de-escalate and transfer a risk
- Close a risk

6.4 The Risk Management Policy and supporting guidance is available to all staff via the Trust's intranet platform.

Risk Assessment Processes

6.5 The Risk Assessment Procedure aims to protect the interests of staff, patients, the public, and other stakeholders by embedding risk assessment in the day-to-day working practices of all employees. It sets out a suite of risk assessment processes for identifying potential sources of harm and putting in place measures to control these. In so doing it enables the Trust to fulfil its duty of care towards staff and others, and supports compliance with health and safety legislation and related regulations.

6.6 Risk assessments must be 'suitable and sufficient' and records must be kept to demonstrate that:

- A proper check has been made
- All affected groups and individuals have been identified
- All obvious and significant hazards have been identified and addressed
- The proposed controls are reasonable and proportionate
- The controls are effective in ensuring that the remaining level of risk is low

6.7 The Risk Assessment Procedure and a repository of completed risk assessments are available to all staff via the Trust's intranet platform.

6.8 The Risk Management Policy and the Risk Assessment Procedure operates alongside other relevant Trust policies and procedures. These include, but are not limited to, the following:

- Information Governance Policy
- Business Continuity Management Policy and Guidance
- Governance Handbook
- Incident and Serious Incident Management Policy
- Investigations and Learning Policy
- Health and Safety Policy
- Statutory and Mandatory Training Policy
- Inspections for Improvement Process

Roles and Responsibilities

6.9 This Risk Management and Assurance Strategic Framework applies to all directly employed staff, agency staff, contractors and volunteers engaged in work or other activities on behalf of the Trust.

6.10 This framework also identifies certain designated roles with specific responsibilities relating to risk management and assurance in the Trust. These roles are:

- Trust Chairman and Non-Executive Directors

- Chief Executive Officer, as the Trust's Chief Accounting Officer
- Executive Director of Quality, Governance and Performance Assurance
- Executive Directors
- Associate Director for Performance, Assurance and Risk
- Risk Management Team
- Risk Leads (for individual services and functions)
- Managers and Specialist Roles

Appendix 5 presents more information about these roles and their specific responsibilities relating to risk management and assurance.

Systems and Tools

Risk Management Information System

6.11 The Trust maintains an organisation-wide information management system to support a standard approach to risk management practice. The system in use across the Trust is the enterprise risk management module of the Datix Cloud IQ suite of applications. The Datix system is used by the Trust to record and maintain information about risks, controls and mitigations, and to generate risk registers.

6.12 The Trust's Risk Management Policy requires all identified risks to be recorded and managed via the Datix system. No identified risks should be recorded or managed in local systems or spreadsheets external to Datix. This applies to all categories of risk, including programme and project risks as well as operational business risks. This requirement supports consistent practice in recording and managing risks relating to all activities and at all levels of the Trust. It also gives the organisation a fully informed view of its current and projected risk exposures and of the controls and actions in place to mitigate these.

Risk Registers

6.13 Risk registers support day-to-day risk management and facilitate the monitoring and reporting of risk information, including changes to risk exposures and the delivery of mitigation actions.

6.14 Risk registers are maintained on and generated by the Trust's risk management information system (Datix). This includes the Corporate Risk Register as well as risk registers produced for other tiers of activity such as directorates, teams, programmes and projects.

6.15 The Trust's Risk Management Policy does not endorse the development and use of local risk registers external to Datix. All risk registers should be generated using the risk information recorded in Datix.

Risk Evaluation Matrix

6.16 The Trust provides an approved methodology and supporting matrix to guide the evaluation of identified risks. Each risk is evaluated by calculating the likelihood and consequence of it materialising and then ascribing to it an overall risk rating of 'low', 'moderate' or 'high'. The rating ascribed to a given risk determines the approach required to manage that risk. Appendix 11 sets out the Trust's risk evaluation matrix and risk scoring criteria.

Quality Impact Assessment Tool

6.17 The Trust provides an approved methodology and supporting tool to guide the assessment of quality impact risks. The risks to quality are assessed in respect of the potential impact on the following domains:

- Clinical quality
- Patient safety
- Patient and carer experience
- Operational performance
- Equality
- The wider health and social care system
- The Trust's reputation

Reporting and Escalation

Corporate Risk Report (CRR)

6.18 The Corporate Risk Report is one of the Trust's key management and assurance reports. It is routinely considered by internal governance bodies, including:

- Trust Board
- Quality Committee
- Finance and Investment Committee
- Audit Committee
- Trust Management Group

6.19 The Corporate Risk Report presents information about high level business risks identified and moderated by the Risk Assurance Group or via other appropriate channels. Typically these risks have either escalated up from local business areas and / or Directorate level, or are associated with gaps in control identified in the Board Assurance Framework.

6.20 In the interests of transparency, accountability and the wider public interest, and unless exceptional circumstances apply, the Corporate Risk Report is discussed by the Trust Board during the public session of its formal meetings.

Project and Programme Risks

6.21 Risks relating to the delivery of transformation programmes and other change projects are captured and reported via highlights reports and risk registers. These risks are reported to the relevant programme board or project steering group as appropriate. Significant risks relating to the Trust's major transformation programmes are reported to the Trust Executive Group and the Trust Management Group.

6.22 The Trust's Risk Management Policy requires that all project and programme risks are recorded on the risk management information system (Datix).

Integrated Reporting

6.23 The Trust supports an integrated model of reporting in which information about operational performance, programme delivery and risk is joined-up, triangulated, and mutually reinforcing. Performance reporting in the Trust revolves around the Integrated Performance Report (IPR) which contains a range of metrics relating to performance, workforce, finance and quality. Monitoring of these metrics enables the Trust to identify areas of emerging risk and to focus development activity on mitigating those risks.

6.24 Information about performance and risk relating to the delivery of transformation programmes is reported in the Strategic Transformation Dashboard. The focus of many change and transformation initiatives in the Trust is to develop new models, processes and approaches in response to identified risks to current and future performance.

Governance and Risk Assurance

Governance Bodies

6.25 Appendix 6 sets out the main bodies that constitute the Trust's internal governance arrangements. Details of the role and operations of these bodies are set out in the Trust's Governance Handbook.

6.26 All management groups and governance bodies have a role to play regarding management of risks within their specific remits. Some of these bodies have particular roles and responsibilities in respect of the Trust's risk management and assurance arrangements. These include:

- Trust Board
- Quality Committee
- Finance and Investment Committee
- Audit Committee
- Risk Assurance Group
- Trust Management Group

6.27 Appendix 7 describes the roles of these bodies, plus some other supporting bodies, in respect of the Trust's risk management and assurance activities. Further detail is found

in the Terms of Reference for each of these bodies. The diagram at Appendix 8 presents a high-level representation of the risk and assurance information flows between these bodies.

Annual Governance Statement

6.28 The Trust produces an Annual Governance Statement as part of the year-end process to prepare and approve its Annual Report and Accounts. These documents are published on the Trust's website.

6.29 The Department of Health and Social Care requires the Trust to produce the Annual Governance Statement for external assurance purposes. However, the Trust does not produce its Annual Governance Statement solely to comply with external assurance or regulatory requirements. The Trust views its Annual Governance Statement positively as an important channel of accountability and transparency that supports the wider public interest in the activities of the organisation.

6.30 The Annual Governance Statement sets out the Trust's main risk management, governance and internal control arrangements, provides analysis of key risks and issues identified and managed by the Trust during the year, and explains any significant control issues faced by the Trust and the actions taken to resolve these.

6.31 The Annual Governance Statement includes the Head of Internal Audit's formal 'opinion' regarding the overall effectiveness and level of assurance provided by the Trust's risk management, governance, and internal control arrangements. The Trust will tolerate an overall assurance rating of no lower than 'good' and aims to achieve the highest available rating of 'substantial.'

Board Assurance Framework (BAF)

6.32 The Board Assurance Framework is owned by the Trust Board. It represents ownership by the Trust Board of the key areas of risk to the achievement of the Trust's strategic objectives.

6.33 The Board Assurance Framework sets out the main strategic risks to the organisation's objectives and the associated controls and mitigation actions. It presents an assessment of the strength of internal controls in place to reduce the likelihood and impact of key risks materialising, and it identifies the main sources of internal and external assurance regarding the effectiveness of those internal controls.

6.34 The Board Assurance Framework:

- Sets out the key risks identified to the achievement of the Trust's strategic objectives
- Presents current and projected levels of exposure associated with those key risks
- Presents in-year updates regarding levels of exposure associated with the key risks

- Identifies the controls in place to mitigate those risks
- Identifies any significant gaps in the controls required to mitigate those risks
- Sets out agreed actions to resolve any significant gaps in controls
- Presents in-year updates on progress to resolve gaps in controls
- Sets out sources of assurance regarding the effectiveness of controls
- Provides a structure and evidence-base for the information about risk, assurance and control presented in the Annual Governance Statement

6.35 Progress in implementing the actions set out in the Board Assurance Framework is formally assessed and reported on a quarterly basis following review sessions with Executive Directors and other senior leaders. Evidence is triangulated with other sources of corporate intelligence such as the Corporate Risk Register, the Integrated Performance Report, and the Strategic Transformation Dashboard.

6.36 Progress updates regarding Board Assurance Framework actions are reported to:

- Trust Board
- Quality Committee
- Finance and Investment Committee
- Audit Committee
- Trust Management Group

6.37 The Trust Board reviews and updates the set of strategic risks captured in the Board Assurance Framework each year as part of the annual planning process. Appendix 2 sets out the strategic risks identified by the Board for the current year.

6.38 The Board Assurance Framework and associated processes are subject to periodic review by the Trust's internal audit provider. The most recent review, carried out in 2019, reported a substantial level of assurance that the Board Assurance Framework is rigorous and makes an effective contribution to the governance of the Trust.

Risk Assurance: Three Lines of Defence

6.39 The Trust's approach to risk assurance is based on the widely-adopted Three Lines of Defence model as endorsed by professional bodies such as the Chartered Institute of Internal Auditors, the Chartered Governance Institute, and the Institute of Risk Management. Appendix 9 presents a high-level diagram to show how the Three Lines of Defence model operates in the Trust.

6.40 The Three Lines of Defence model provides a useful way to understand how the Trust's risk management and assurance functions operate and interact. The model shows the boundaries between different roles and responsibilities in the management and assurance of risks. This helps the Trust to avoid duplications and gaps in its risk management, governance and control arrangements. By setting out roles and

responsibilities relating to risk management and assurance the model links to the Trust's Accountability Framework.

6.41 The first line of defence contains operational functions that directly own and manage risks. The Trust's first line of defence constitutes teams and managers in operational or service delivery functions and in support functions. Typically these are operational managers and staff who manage risks as part of their day-to-day work. Managers and staff in the first line are responsible for the correct and consistent application of Trust policies and procedures regarding risk management practice.

6.42 The second line of defence contains 'corporate' or 'central' functions that oversee, assure or specialise in risk management or related control and compliance activities. For instance, the Trust's second line of defence includes the corporate Risk Management Team and the Risk Assurance Group. The second line of defence provides the frameworks, policies, procedures, guidelines, tools, techniques and other forms of support to enable first line operational managers and staff to manage risk well. The second line also carries out quality assurance, monitoring and reporting activities relating to risk management.

6.43 The third line of defence contains functions that provide independent and objective assurance regarding the integrity and effectiveness of risk management and related controls in the Trust. Internal audit is the key function in the Trust's third line of defence. Reporting to the Trust Board via the Audit Committee, internal audit provides risk-based evaluation of the effectiveness of risk management, governance and internal control in the organisation. The third line of defence has interfaces with other external providers of independent and objective assurance, including external audit, regulators (such as the Care Quality Commission) and commissioners (such as NHS England).

Board Assurance

6.44 The Trust Board seeks and receives assurance that risk management arrangements are appropriate and operating effectively. Sources of such assurance include the following:

- Board Assurance Framework
- Corporate Risk Report
- Corporate Risk Register
- Progress reports regarding delivery of the Trust's strategic and operational objectives
- Progress reports regarding delivery of the Trust's transformation programmes and other change projects
- Performance reports outlining achievement against key performance, safety and quality indicators
- Assurance reports from Board sub-committees and the Audit Committee
- Assurance reports from the Trust Management Group
- Compliance with national standards, policies and regulatory frameworks

- Assurance from internal and external audit reports

Independent Assurance

6.45 The Trust routinely receives independent and objective assurance from external sources regarding the effectiveness of its risk management, governance and control arrangements. Sources of independent assurance include:

- Registration with, and inspection by, the Care Quality Commission (and other regulators / inspectorates as appropriate)
- Annual programme of internal audit risk-based reviews (see 6.42 to 6.44 below), and particularly its annual risk-based review of risk management and assurance
- Lead commissioner performance monitoring, and annual governance and assurance arrangements
- Department of Health and Social Care
- NHS England / NHS Improvement
- External Audit

Internal Audit

6.46 The Trust Board approves an annual programme of risk-based internal audit reviews to provide independent assurance on matters of risk, compliance and internal control. This internal audit activity is a key component of the third line of defence in the Trust's risk management and assurance framework.

6.47 Reports from risk-based internal audit reviews provide assurance based on the effectiveness of the controls tested and the degree of compliance found. One of four levels of assurance can be reported following an internal audit review: 'substantial assurance', 'good assurance', 'reasonable assurance' and 'limited assurance.' Appendix 10 presents the definitions of these levels of assurance. The Trust aims to achieve mostly 'good' and 'substantial' levels of assurance from internal audit reviews.

6.48 Risk-based internal audit reviews produce recommendations that require management to agree actions to address any identified weaknesses in controls or compliance. Such recommendations are categorised as either 'high priority', 'medium priority' or 'low priority'. Appendix 10 presents definitions of these categories.

6.49 As part of its third-line assurance activity the Trust's internal audit provider carries out independent and objective monitoring of the implementation of management actions arising from risk-based reviews. The internal audit provider reports on the implementation of such actions to the Trust's Audit Committee.

6.50 As part of its second-line assurance activity the Trust's Risk Management Team provides internal monitoring of the implementation of actions arising from risk-based internal audit reviews. The Risk Management Team adopts a risk-based approach, focussing on those actions arising from reviews rated as providing either 'reasonable assurance' or 'limited

assurance.’ The Risk Management Team reports on the implementation of audit actions to the Trust Management Group and to the Trust’s Audit Committee.

6.51 As well as its annual programme of risk-based reviews, the Trust’s internal audit provider delivers assurance activity relating to specialist areas of risk, compliance and controls. These include technology risk and fraud risk. In addition, the internal audit provider carries out advisory reviews on specified topics at the request of the Trust management.

7.0 TRAINING EXPECTATIONS FOR STAFF

7.1 All members of Trust staff receive an introductory overview of risk management practice as part of the mandatory corporate induction programme.

7.2 The Trust may identify and mandate specific additional risk management training requirements for any staff groups in accordance with the responsibilities of the role and the needs of the service.

7.3 Board members and other senior leaders will receive specialist risk management development opportunities throughout their service with the Trust where this is relevant to their role.

7.4 The Trust’s Risk Management team will plan and deliver an annual programme of training and other development activities to raise awareness and understanding of risk management and to strengthen the capacity and capability for risk management within the Trust workforce.

8.0 REFERENCES

Cabinet Office, *Management of Risk in Government*, 2017

Care Quality Commission, *Well-Led Framework – Management of Risk and Performance*, 2018

Chartered Institute of Internal Auditors, *Governance of Risk: Three Lines of Defence*, 2019

Global Institute of Internal Auditors, *The Three Lines of Defence in Effective Risk Management and Control*, 2013

Good Governance Institute, *Risk Appetite for NHS Organisations*, 2019

HM Treasury, *Management of Risk: Principles and Concepts* ('The Orange Book'), 2019

Institute of Risk Management, *Risk Management Standard*, 2002

International Organisation for Standardisation, *ISO 31000 Standard: Risk Management Principles and Guidance*, 2018

Office of Government Commerce, *Management of Risk*, 2010

APPENDICES

APPENDIX 1: *One Team, Best Care* Trust Strategy 2018-23

APPENDIX 2: Trust Board Assurance Framework - Strategic Risks (2020/21)

Strategic Ambition	Strategic Risk
1. Patients and communities experience fully joined-up care responsive to their needs	1a) Ability to deliver and sustain the required performance standards and service developments in 999/A&E operations
	1b) Ability to deliver the required performance standards and service developments in Integrated and Urgent Care
	1c) Ability to deliver the required performance standards and service developments in the Patient Transport Service
	1d) Ability to influence and respond to system-wide developments in urgent and emergency care
2. Our people feel empowered, valued and engaged to perform at their best	2a) Ability to ensure provision of sufficient clinical workforce
	2b) Ability to support the physical and mental health and well-being of staff
	2c) Ability to embed strategies to meet statutory and regulatory requirements and the Trust's own ambitions relating to diversity and inclusion
	2d) Ability to embed strategies for excellence in leadership, management and organisational culture
3. We achieve excellence in everything we do	3a) Capacity and capability to deliver and manage planned transformational changes
	3b) Ability to respond well to specific wider external challenges
4. We use resources wisely to invest in and sustain services	4a) Ability to robustly manage Trust finances to deliver the required financial performance
	4b) Ability to deliver our requirements and ambitions regarding key enabling infrastructure (digital technology, estates)

APPENDIX 3: Trust Board Risk Appetite Statement

The Trust's risk appetite for 2020/21 is described as follows:

Introduction

Risk is inherent in all Trust activities.

Effective risk management is a cornerstone of the Trust's *One Team, Best Care* strategic priority to *create a safe and high performing organisation based on openness, ownership and accountability*.

The Trust believes that risk management is everybody's business.

Quality and Safety

The Trust has a low appetite for risk relating to the safety and quality of patient care.

The Trust has a low appetite for risk relating to the safety of staff, volunteers and others engaged in activity on behalf of the organisation.

The Trust recognises that risk exposures relating to patient care and staff safety are not always complementary and can create a dynamic and complex operating environment in which to identify and control risk appropriately. The Trust recognises its responsibility to provide its managers and staff with appropriate guidance and training to support assessment and management of risks in this complex environment.

Compliance and Security

The Trust has a low appetite for risk relating to statutory compliance, regulatory requirements and the delivery of national standards and targets, including statutory financial compliance.

The Trust has a low appetite for risk relating to the security and integrity of its technology infrastructure, information systems and other digital solutions. This includes cyber security and matters of risk and compliance relating to data protection, information governance and the management of person identifiable information.

Development and Innovation

The Trust has an open appetite for investment risk relating to new business developments consistent with the organisation's strategic priorities.

The Trust has an open appetite to risk relating to viable service improvements and opportunities to pursue new and innovative ways of working, either internally or in collaboration with external partners.

The Trust recognises that, with due consideration for safety and compliance issues, an open appetite for controlled risk-taking relating to business development, service improvement and innovation creates opportunities which may bring positive gains to the quality and efficiency of its services, the wider organisation, and the health and care system generally.

Authoritative definitions of risk appetite include:

- *"The level of risk that is acceptable to the board or management"* (Institute of Internal Auditors)
- *"The amount of risk that an organisation is prepared to accept, tolerate or be exposed to"* (HM Treasury)
- "*The amount of risk that an organisation is willing to seek or accept in the pursuit of its long-term objectives*" (Institute of Risk Management)

APPENDIX 4: Good Governance Institute Risk Appetite Matrix

Good Governance Institute

RISK APPETITE FOR NHS ORGANISATIONS
A MATRIX TO SUPPORT BETTER RISK SENSITIVITY IN DECISION TAKING

TO USE THE MATRIX: IDENTIFY WITH A CIRCLE THE LEVEL YOU BELIEVE YOUR ORGANISATION HAS REACHED AND THEN DRAW AN ARROW TO THE RIGHT TO THE LEVEL YOU INTEND TO REACH IN THE NEXT 12 MONTHS. 0 - 6

Risk levels / Key elements	0 **Avoid** Avoidance of risk and uncertainty is a Key Organisational objective	1 **Minimal (ALARP)** (as little as reasonably possible) Preference for ultra-safe delivery options that have a low degree of inherent risk and only for limited reward potential	2 **Cautious** Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward.	3 **Open** Willing to consider all potential delivery options and choose while also providing an acceptable level of reward (and VfM)	4 **Seek** Eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk).	5 **Mature** Confident in setting high levels of risk appetite because controls, forward scanning and responsiveness systems are robust
Financial/VFM	Avoidance of financial loss is a key objective. We are only willing to accept the low cost option as VfM is the primary concern.	Only prepared to accept the possibility of very limited financial loss if essential. VfM is the primary concern.	Prepared to accept possibility of some limited financial loss. VfM still the primary concern but willing to consider other benefits or constraints. Resources generally restricted to existing commitments.	Prepared to invest for return and minimise the possibility of financial loss by managing the risks to a tolerable level. Value and benefits considered (not just cheapest price). Resources allocated in order to capitalise on opportunities.	Investing for the best possible return and accept the possibility of financial loss (with controls may in place). Resources allocated without firm guarantee of return – 'investment capital' type approach.	Consistently focussed on the best possible return for stakeholders. Resources allocated in 'social capital' with confidence that process is a return in itself.
Compliance/ regulatory	Play safe, avoid anything which could be challenged, even unsuccessfully.	Want to be very sure we would win any challenge. Similar situations elsewhere have not breached compliances.	Limited tolerance for sticking our neck out. Want to be reasonably sure we would win any challenge.	Challenge would be problematic but we are likely to win it and the gain will outweigh the adverse consequences.	Chances of losing any challenge are real and consequences would be significant. A win would be a great coup.	Consistently pushing back on regulatory burden. Front foot approach informs better regulation.
Innovation/ Quality/Outcomes	Defensive approach to objectives – aim to maintain or protect, rather than to create or innovate. Priority for tight management controls and oversight with limited devolved decision taking authority. General avoidance of systems/ technology developments.	Innovations always avoided unless essential or commonplace elsewhere. Decision making authority held by senior management. Only essential systems / technology developments to protect current operations.	Tendency to stick to the status quo, innovations in practice avoided unless really necessary. Decision making authority generally held by senior management. Systems / technology developments limited to improvements to protection of current operations.	Innovation supported, with demonstration of commensurate improvements in management control. Systems / technology developments used routinely to enable operational delivery Responsibility for non-critical decisions may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. New technologies viewed as a key enabler of operational delivery. High levels of devolved authority – management by trust rather than tight control.	Innovation the priority – consistently 'breaking the mould' and challenging current working practices. Investment in new technologies as catalyst for operational delivery. Devolved authority – management by trust rather than tight control is standard practice.
Reputation	No tolerance for any decisions that could lead to scrutiny of, or indeed attention to, the organisation. External interest in the organisation viewed with concern.	Tolerance for risk taking limited to those events where there is no chance of any significant repercussion for the organisation. Senior management distance themselves from chance of exposure to attention.	Tolerance for risk taking limited to those events where there is little chance of any significant repercussion for the organisation should there be a failure. Mitigations in place for any undue interest.	Appetite to take decisions with potential to expose the organisation to additional scrutiny/interest. Prospective management of organisation's reputation.	Willingness to take decisions that are likely to bring scrutiny of the organisation but where potential benefits outweigh the risks. New ideas seen as potentially enhancing reputation of organisation.	Track record and investment in communications has built confidence by public, press and politicians that organisation will take the difficult decisions for the right reasons with benefits outweighing the risks.
APPETITE	**NONE**	**LOW**	**MODERATE**	**HIGH**	**SIGNIFICANT**	

APPENDIX 5: Roles and Responsibilities in Risk Management and Assurance

Chairman and Non-Executive Directors

The Chairman and Non-Executive Directors are responsible for ensuring that systems for governance, risk management and internal control are effective and maintained across all functions and at all levels of the Trust. They set the Trust's objectives, identify risks relating to these, set the Trust's risk appetite, and own the Board Assurance Framework. They constructively challenge and contribute to the development of risk management systems. One of the Non-Executive Directors is appointed as the Chair of the Audit Committee which has oversight of for risk management, assurance and internal controls.

Chief Executive, as the Trust's Chief Accounting Officer

The Chief Executive has overall responsibility for ensuring that an effective system of risk management and assurance is in place and that the Trust meets its statutory and regulatory requirements in respect of good corporate governance. The Chief Executive is accountable to the Board for maintaining a sound system of internal control and is responsible for the Annual Governance Statement that sets out the Trust's risk management and assurance arrangements and demonstrates how these support the achievement of the organisation's objectives.

Executive Director of Quality, Governance and Performance Assurance

The Executive Director Quality, Governance and Performance Assurance has overall lead responsibility the direction, development, management and implementation of the Trust's strategic framework for risk management and assurance. This Executive Director is the Trust's designated Senior Information Risk Officer (SIRO).

Executive Directors

All Executive Directors have responsibility for ensuring that the Trust's Risk Management Policy is implemented within their directorates and that risk management is embedded within their governance arrangements. The Executive Medical Director has designated responsibilities relating to clinical risk

Associate Director of Performance, Assurance and Risk

The Associate Director of Performance, Assurance and Risk is responsible for developing, supporting and embedding effective risk management and assurance processes within the Trust, and for risk reporting to various governance bodies. This Associate Director chairs meetings of the Risk and Assurance Group

Risk Management Team

The Risk Management Team, led by the Head of Risk, is responsible for operational implementation of the Risk Management Policy and related systems and procedures. The team provides risk management support, guidance and training and owns the production and reporting of the corporate risk register.

Managers and Specialist Roles

All managers within the Trust are responsible for identifying and managing risk within the remit of their roles and responsibilities. They are expected to comply with the designated risks management policies, systems and associated procedures, and ensure all efforts are made to encourage their teams to escalate potential risks they become aware of. In addition, there are managers with specific interest and responsibility for oversight of risk management within specialist areas of work. These include, but are not limited to, the following:

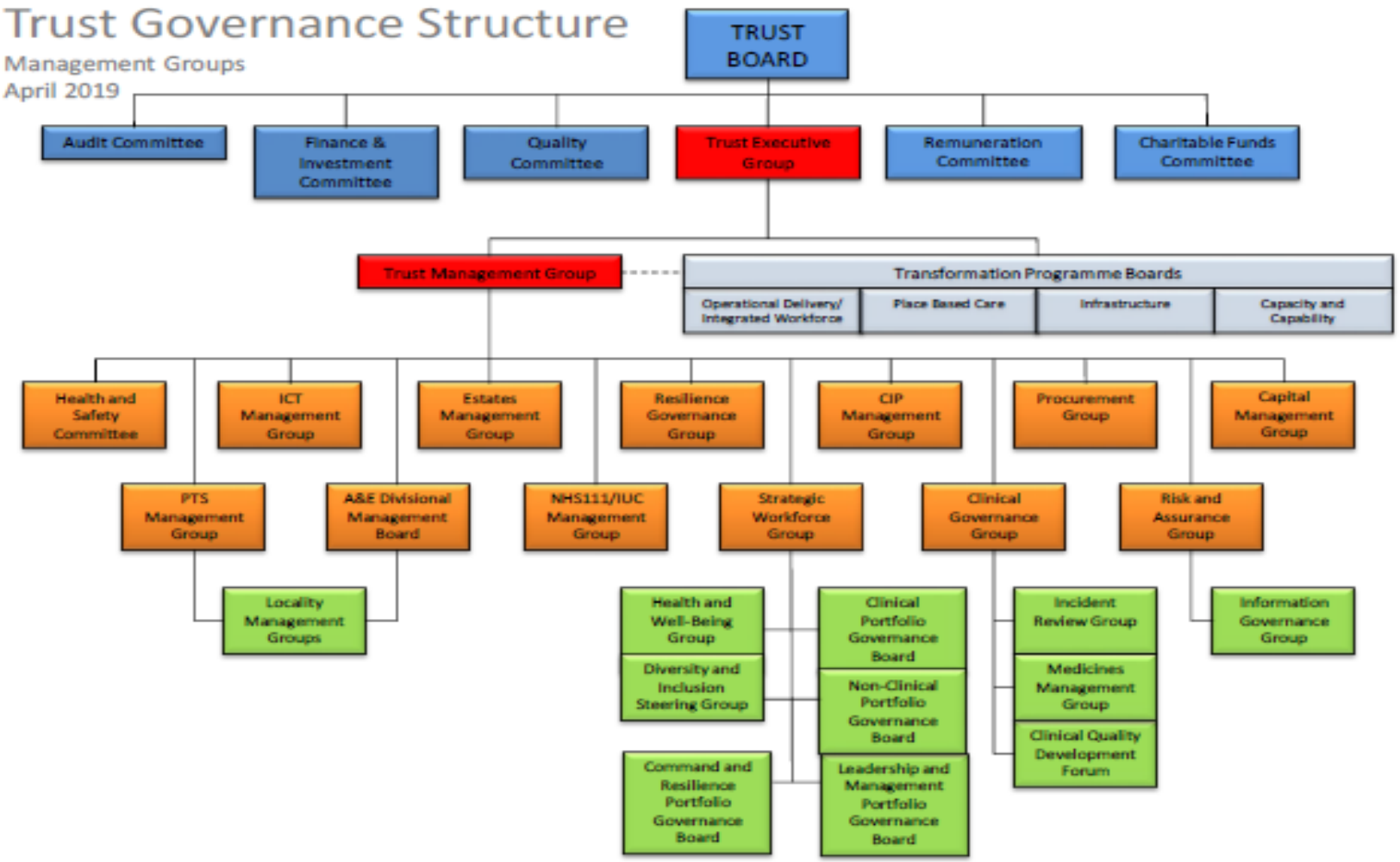
- Health and Safety Manager
- Local Security Management Specialists (LSMS)
- Information Governance Manager
- Caldicott Guardian
- Head of Safeguarding
- Head of Safety

Risk Leads

Risk Leads will operate with their designated directorates/committees/groups to manage the identification, management, escalation and review of risk. Risk Leads will:

- Ensure risk registers and risk treatment plans are produced in their respective directorates/committees and groups and filed correctly in a timely manner, and that they are considered appropriate to mitigate risks.
- Attend relevant directorates/committees and group forums to discuss and present new/revised risks (particularly any risks rated 12 or more for consideration and/or addition to the directorate level risk register or for further escalation).
- Conduct regular updates and maintenance of their respective directorates/committees and group risk registers.
- Ensure that risks are acted upon immediately and reviewed/agreed at regular intervals.
- Monitor and review progress against directorates/committees and group risk registers and risk treatment plans, in the respective areas.
- Ensure completion of risk register assessment forms, where appropriate e.g. to identify and transfer risks.
- Ensure action is taken as soon as possible, at the lowest possible level to eliminate, transfer or reduce risk.
- Ensure any risks scoring 12 or above, or other risks that have significant consequence to Trust objectives, are acted upon immediately (escalate extreme risks to the attention of the Risk and Assurance Group).
- Monitor and progress identified actions from the Corporate Risk Register, appropriate to their respective directorates/committees and groups,
- Attend the Risk and Assurance Group monthly to present new and revised risks in the form of a report (particularly any risks scored as ‘12’ or more and/or with a consequence score of 5 alone, for consideration to the Corporate Risk Register).
- Ensure the risk escalation and reporting procedure is adhered to within their respective directorates/committees and groups.

APPENDIX 6: Trust Governance Structure



APPENDIX 7: Main Trust Governance Bodies in Risk Management and Assurance

Trust Board

The Trust Board owns the strategic framework for risk management and assurance, oversees the system of internal controls which enables risk to be assessed and managed, and sets the organisations' risk appetite. The Board sets the Trust's strategic aims and ensures that resources are in place to meet its objectives. It receives reports at each meeting on the most significant risks and associated mitigation actions as detailed in the Trust's Board Assurance Framework.

Audit Committee

The Audit Committee is a formal committee of the Trust Board. It provides overview and scrutiny of risk management and of the Trust's system of internal control more generally. The committee meets quarterly and has an annual work plan which has been refined to reflect the increased focus on quality governance.

Quality Committee

The Quality Committee is a formal committee of the Trust Board. It undertakes scrutiny of the Trust's clinical governance, quality and workforce plans, compliance with external quality regulations and standards, and key associated functions. The committee oversees risks to delivery of plans and functions related to this remit.

Finance and Investment Committee

The Finance and Investment Committee is a formal committee of the Trust Board. It undertakes scrutiny of the Trust's financial plans, revenue and capital budgets, investment decisions, contract management and procurement. The committee oversees risk to delivery of plans and functions related to this remit.

Trust Management Group

The Trust Management Group supports the operational management of the Trust and the delivery of objectives set by the Trust Board. It carries delegated responsibility from the Trust Executive Group and in this capacity is the formal route to support the Chief Executive Officer in effectively discharging his responsibilities as Accountable Officer. The Group oversees the management of corporate-level risks and controls across all functions and activities of the Trust.

Risk and Assurance Group

The Risk and Assurance Group is a formally constituted sub-committee of Trust Management Group. It reviews, moderates and assures corporate-level risks and associated controls and mitigations. The Group receives reports on all directorate risk registers and specific risk issues from its members, including representatives from all other associated risk management groups.

Other Groups involved in risk management include:

Strategic Health and Safety Committee
This strategic Committee is responsible for the review and monitoring provision of a healthy, safe and secure environment for all employees, contractors and members of the public who may be affected by the activities of the Trust. The Committee is responsible for instigating appropriate action to address risks identified from issues that may compromise the above.

Clinical Governance Group
The Clinical Governance Group provides a focus for clinical risk and quality issues. It receives reports by exception on clinical risk issues and is responsible for directing action to manage clinical risk.

Clinical Quality Development Forum (CQDF)
Clinical Quality Development Forum is a sub-group of the Clinical Governance Group. The CQDF reviews clinical risks on a monthly basis, reporting to Clinical Governance Group on an exceptions basis.

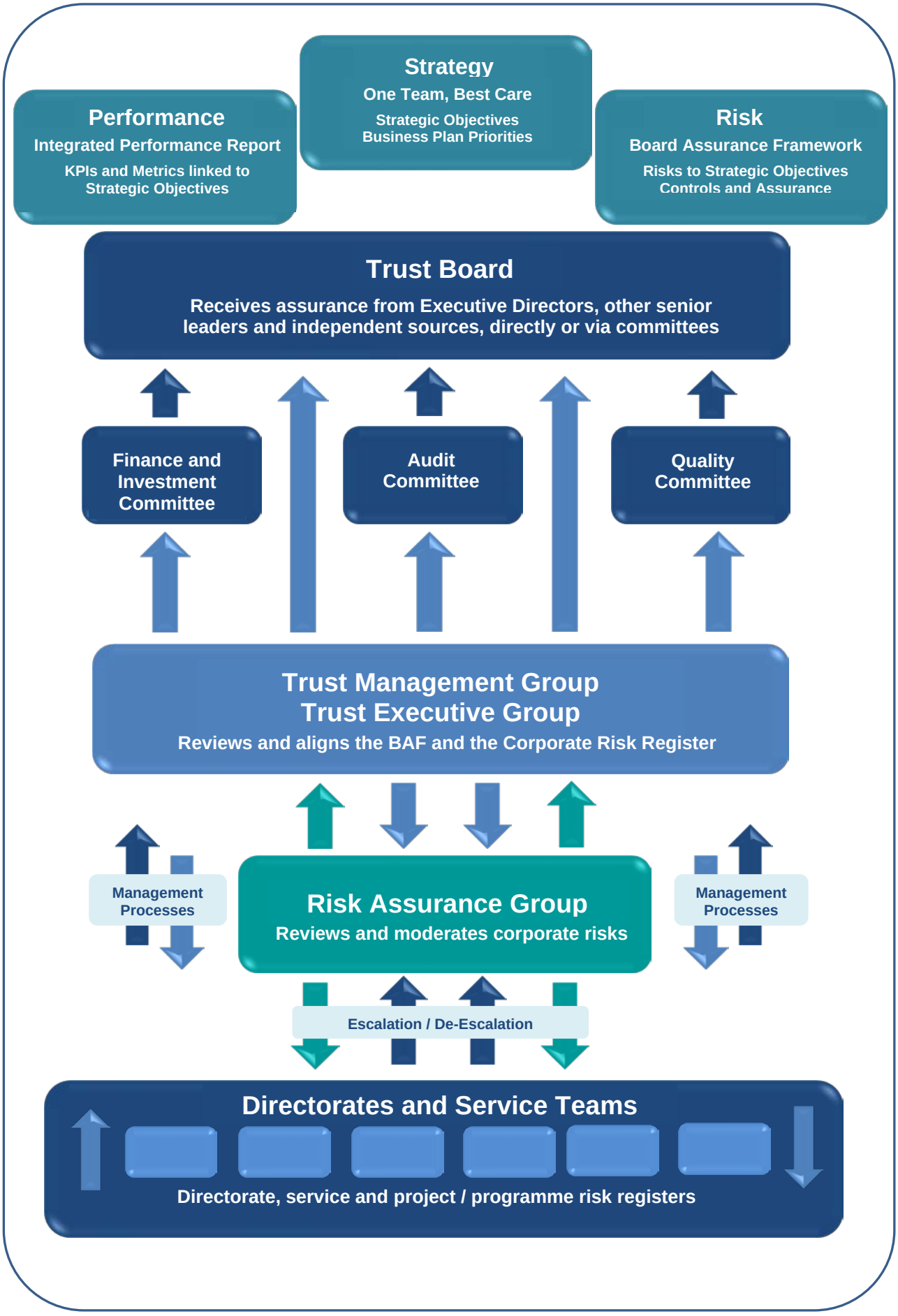
Medicines Management Group (MMG)
The Medicines Management Group reports directly into the Clinical Governance Group and is responsible for reviewing medicines-related incidents and serious incidents instigating appropriate action to address issues identified.

Incident Review Group
The Incident Review Group is responsible for reviewing and instigating appropriate action to address issues identified in relation to incidents, potential serious incidents and near misses, along with identifying themes and trends from the following specialty areas;-

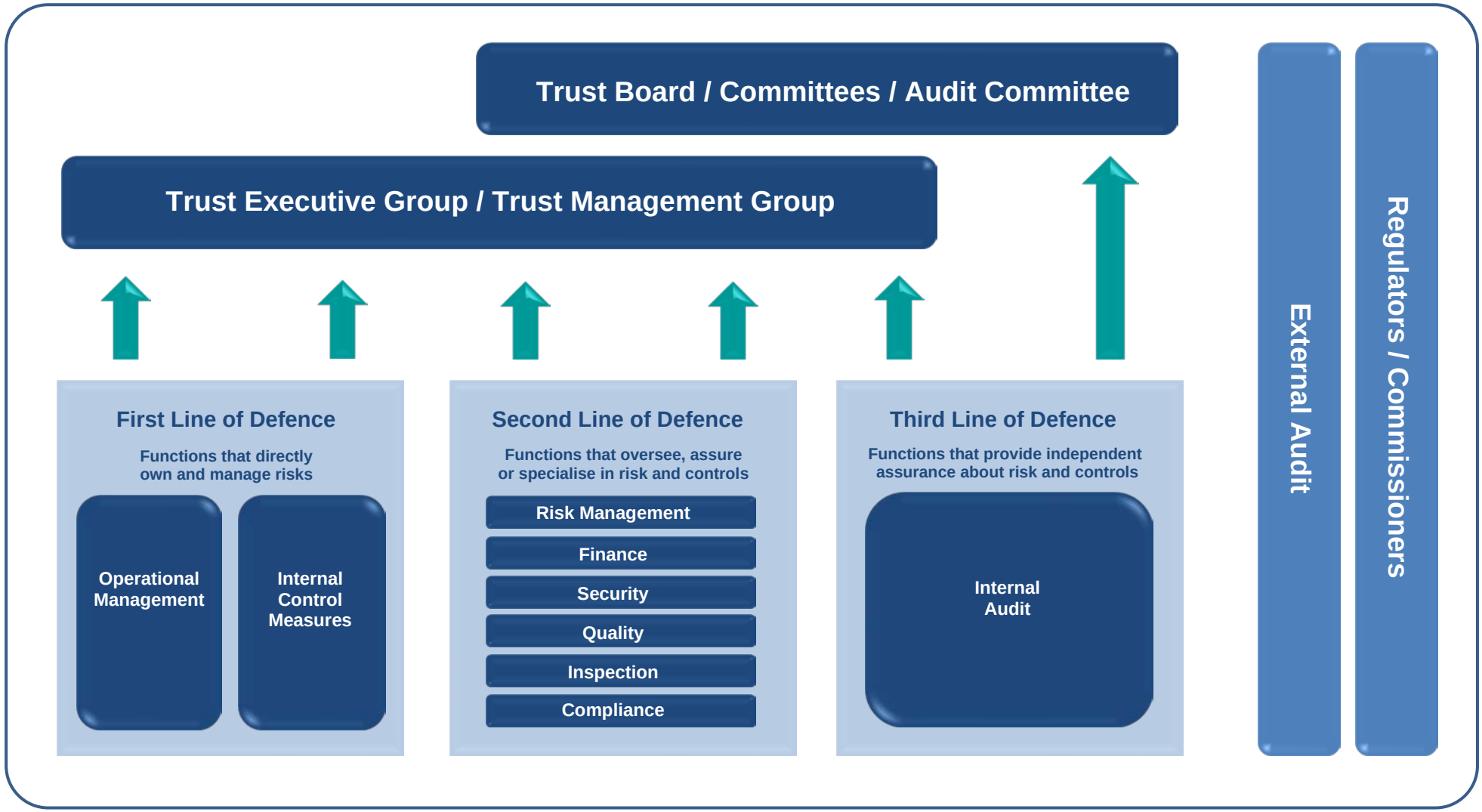
- Formal Complaints/Concerns
- Claims
- Coroner's inquest
- Clinical Case Reviews
- Human Resources processes

Information Governance Working Group
The Information Governance Working Group is responsible for advising upon and overseeing the management of all issues associated with information risk, confidentiality and information governance/security.

Appendix 8: Risk Management and Assurance Information Flows



APPENDX 9: Three Lines of Defence Risk Assurance Model



APPENDIX 10: Internal Audit Assurance Levels

Levels of assurance provided by internal audit reviews:

Substantial	Governance, risk management and control arrangements provide substantial assurance that the risks identified are managed effectively. Compliance with the control framework was found to be taking place.
Good	Governance, risk management and control arrangements provide a good level of assurance that the risks identified are managed effectively. A high level of compliance with the control framework was found to be taking place. Minor remedial action is required
Reasonable	Governance, risk management and control arrangements provide reasonable assurance that the risks identified are managed effectively. Compliance with the control framework was not found to be taking place in a consistent manner. Some moderate remedial action is required.
Limited	Governance, risk management and control arrangements provide limited assurance that the risks identified are managed effectively. Compliance with the control framework was not found to be taking place. Immediate and fundamental remedial action is required.

Prioritisation categories applied to internal audit recommendations and the associated management actions:

Low	Minor improvement to the system could be made to improve internal control in general and engender good practice, but are not vital to the overall system of internal control.
Medium	A significant weakness within the system that leaves some of the systems objectives at risk and / or some noncompliance with the control framework
High	A fundamental weakness in the system that puts the achievement of the systems objectives at risk and / or major and consistent non-compliance with the control framework requiring management action as a matter of urgency.

APPENDIX 11: Trust Risk Evaluation Matrix

Risk Evaluation Matrix: Consequence x Likelihood

Risk Score		Likelihood				
		Rare	Unlikely	Possible	Likely	Almost certain
Consequence		1	2	3	4	5
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
Negligible	1	1	2	3	4	5

More detailed guidance for calculating the consequence and likelihood scores is published as part of the Risk Management Policy and is available to staff via the Trust intranet.

The scores obtained from the risk matrix are used to assign ratings to risks as follows:

Key to Risk Ratings		
Risk Score	**Risk Rating**	**Risk Management Approach**
15-25	High	Managed at local team or departmental level and / or Directorate or Trust level or by a subject specific group depending on management control, treatment plan, or wider strategic implications for the Trust. Risk Leads consider escalation and review at Risk Assurance Group where consideration is given to escalating the risk into the Corporate Risk Report and / or the Board Assurance Framework
8-12	Moderate	Managed at local team or departmental level, unless escalated to Directorate or Trust level or to a subject specific group. Where there is a consequence score of 4 or 5 alone this may be considered for escalation to the Risk Assurance Group regardless of the likelihood score.
1-6	Low	Managed at a local team or departmental level. Local management to determine and develop risk treatment plans or to manage through routine procedures; and consider including on the risk register. This level of risk may be short-lived or aggregated into a higher risk.

APPENDIX 12: Well Led Framework – Risk Management Expectations

KLOE 5. Are there clear and effective processes for managing risks, issues and performance?

There is an effective and comprehensive process to identify, understand, monitor and address current and future risks.

Leaders across the organisation are able to describe the current and future quality, operational and financial risks that relate to their areas of work, and the plans to mitigate them.

Senior leaders can evidence that the organisation has effective, timely, horizon-scanning, scenario-planning and reporting processes so that it is sufficiently aware of changes in the internal and external environment (including risks from the wider local health and care economy) that may affect delivery of strategy and/or affect quality and financial sustainability.

Senior leaders can evidence that a board assurance framework and dynamic risk registers are in place and assessed by the board at least quarterly and demonstrate:

- attention to both internal and external risks, and their impact on planning
- a robust process for collating, evaluating, quantifying and reporting key risks
- a clear understanding of the board's risk appetite and tolerance, which is reviewed regularly (at least annually) and appropriately communicated to staff
- a commitment to learning lessons from inquiries (for example, safeguarding lessons from the 2015 Savile review), internal and external reviews of their own organisation, and of other organisations, and sharing this learning with staff, patients and the public.

Senior leaders can evidence that there is a clear risk management process understood by staff members, including the board, its subcommittees and subgroups, so that they identify, assess, understand, assign responsibility for and act on risks relevant to their area of responsibility. This includes internal escalation and external escalation if the risks affect other organisations.

Senior leaders can evidence that emergency preparedness/crisis management planning has been carried out and there is a robust business continuity plan.

Additional risk management expectations can be found threaded throughout other areas of the CQC Well-Led framework.