NHS Greater Glasgow and Clyde	**Paper No. 22/101**
Meeting:	**NHSGGC Board Meeting**
Meeting Date:	**20 December 2022**
Title:	**Risk Management Strategy**
Sponsoring Director/Manager	**Colin Neil, Director of Finance**
Report Author:	**Andrew Gibson, Chief Risk Officer**

1. Purpose

The purpose of the attached paper is to seek Board approval on the updates to the Risk Management Strategy.

While the Audit and Risk Committee is responsible for *"Oversight and monitoring of the effectiveness of arrangements for the governance of the Board's systems for the management of risk"* the enclosed document represents an update to a key Board-wide strategy, therefore Board approval is required.

2. Executive Summary

The paper can be summarised as follows:

The current Risk Management Strategy was approved by the Audit & Risk Committee in September 2021. The updated Risk Management Strategy has been produced to build on the recent improvements made to the risk management arrangements following the appointment of the new Chief Risk Officer. This Strategy forms one element of an integrated risk management framework, which also includes the Board Risk Appetite Statement and an updated Risk Register Policy and Guidance for Managers document.

Each section of the Strategy has been updated to reflect best practice. The main changes include:

- Clearer definitions of risk, risk management
- Improved links to the Board Risk Appetite Statement
- An updated section on Risk Architecture, which clarifies the risk management structure and risk register hierarchy
- Updated and clarified Roles and Responsibilities section
- Updated section on Assurance

- An updated section on the risk management process, modelled on the international standard ISO:31000
- An updated section on communication

3. Recommendations

The NHS Board is asked to consider and approve the updated Risk Management Strategy.

4. Response Required

This paper is presented for **approval.**

5. Impact Assessment

The impact of this paper on NHS Greater Glasgow and Clyde's corporate aims, approach to equality and diversity and environmental impact are assessed as follows:

- Better Health Positive
- Better Care Positive
- Better Value Positive
- Better Workplace Positive
- Equality & Diversity Positive
- Environment Positive

6. Engagement & Communications

The issues addressed in this paper were subject to the following engagement and communications activity:

- Reviewed and endorsed by Risk Management Steering Group meeting on 16/11/2022.
- Reviewed and endorsed by CMT on 01/12/2022
- Reviewed and endorsed by Audit and Risk Committee on 13/12/2022

7. Governance Route

This paper has been previously considered by the following groups as part of its development:

As above

8. Date Prepared & Issued

13th December 2022

NHS Greater Glasgow and Clyde
Risk Management Strategy

Lead Manager:	**Chief Risk Officer**
Responsible Director:	**Director of Finance**
Approved by:	**NHS Board**
3Updated:	**TBC**
Date for Review:	**December 2025**
Replaces previous Version:	**Risk Management Strategy V1.0** **Approved by Audit & Risk Committee 14th September 2021**

Contents

1. Introduction

At NHS Greater Glasgow and Clyde (NHSGGC) our purpose is to: *"protect and improve population health and wellbeing while providing a safe, accessible, affordable, integrated, person centred and high quality health service."*

In fulfilling this purpose, NHSGGC has established a robust and effective framework for the management of risk. The framework is proactive in identifying and understanding risk, builds upon existing good practice and is integral to strategic and service planning, decision making, performance reporting and health care service delivery.

The Risk Management Strategy sets out the principles and approach to risk management to be followed throughout NHSGGC. The strategy draws on best practice from the International Standard for Risk Management ISO:310000; HM Government's Risk Appetite Guidance Notes; and the Blueprint for Good Governance in NHS Scotland. Its objective is to achieve a consistent and effective application of risk management and enable it to be embedded into all core processes, forming part of the management and corporate governance activity of the organisation. Risk Management, when deployed effectively, should add value by supporting day-to-day service delivery as opposed to being seen as a separate, self-contained process. The Risk Management Strategy supports that approach.

The Risk Management Strategy should be read in conjunction with the **Risk Register Policy and Guidance for Managers** and the **NHSGGC Board Risk Appetite Statement**. All risk management guidance and supporting documentation can be accessed via Staffnet: Click the link.

2. Scope

The objective of the Risk Management Strategy is to promote an integrated and consistent approach across all parts of the organisation to managing risk.

The strategy applies to all Board staff, contractors and other third parties, including honorary contract holders, working in all areas of the Board. Risk management is the responsibility of all staff and managers at all levels are expected to take an active lead to ensure that risk management is a fundamental part of their operational area.

The Board encourages an open culture that requires all Board employees, contractors and third parties working within the Board to operate within the systems and structures outlined in this strategy.

2.1. What is a Risk?

A risk can be defined as 'the effect of uncertainty on objectives' (*ISO31000 Risk Management Standard).* It is any uncertain event which can have an impact on an organisation's ability to achieve its objectives – either reducing the likelihood of achievement or stopping it altogether. Not every perceived problem is a risk. In this context we can understand to risk to be "uncertainty that matters."

Another important distinction to make is that between a risk and an issue or an incident – or in other words, an uncertainty and a certainty. A risk is an event that may or may not happen. An issue or incident is something that is currently happening or has already happened. Issues or incidents should not be recorded and treated as risks.

2.2. What is Risk Management?

Risk Management is a systematic way of dealing with that uncertainty which involves the identification, assessment, evaluation and management of risk. Risk management activities are designed to reduce uncertainty in support of delivering corporate objectives. An effective, structured and consistent system of risk management will draw together all types of risks and enable a co-ordinated, interrelated view of the NHSGGC risk profile.

2.3. Why do we need Risk Management?

An effective system of risk management will deliver a range of benefits:

- Enhances strategic planning and prioritisation of resources
- Ensures that decision making is informed and risk-based in order to mitigate threats to the achievement of corporate objectives
- Provides assurance to internal and external governance groups that risks are being effectively controlled
- Helps to ensure compliance with legislation, regulations and other mandatory obligations
- Raises awareness of the need for everyone to adopt consistent risk management behaviours and actions in our everyday business
- Empowers all staff to make sound judgements and decisions concerning the management of risk and risk taking

- Anticipates and responds to changing political, environmental, social, technology and legislative requirements and / or opportunities
- Prevents injury and / or harm, damage and losses
- Supports organisational resilience

An effective system of risk management will be achieved by:

- Clearly defining roles, responsibilities and governance arrangements for individuals and teams within NHSGGC
- Incorporating risk management in NHS Board, Standing Committee and CMT reports to support decision making
- Demonstrating and reinforcing the importance of effective risk management principles in our everyday activities
- Maintaining risk registers at all levels that are linked to the organisation's corporate objectives
- Seeking assurance that controls relied on to mitigate risks are effective

3. Risk Statement

Effective risk management is a fundamental cornerstone of good corporate governance and internal control, and is an essential component in the delivery of the Board's corporate objectives.

The Board is committed to having a risk management and safety culture that underpins and supports the achievement of corporate objectives. The Board intends to demonstrate an ongoing commitment to improving the management of risk throughout the organisation.

The NHSGGC Risk Management Strategy:

- Represents a major element of our healthcare governance arrangements
- Affirms our commitment to improve our capability and capacity to manage risk across all areas of clinical, staff and corporate governance
- Formalises risk management roles and responsibilities
- Supports us to drive continuous improvement and have a positive impact on the quality of care, our staff wellbeing and our overall efficiency and effectiveness
- Sets how the public and key stakeholders can be assured that our risks are managed effectively

Where this is done well, this ensures the safety of our patients, visitors, and staff, and that as an organisation the Board and management is not surprised by risks that could, and should, have been foreseen.

Risks are not necessarily to be avoided, but, where relevant, can be embraced and explored in order to improve services, and take opportunities in relation to the risk. Above all, the response to risk must be informed, proportionate and aligned to organisational risk appetite.

Senior management will lead change by being an example for behaviour and culture; ensuring risks are identified, assessed and managed. Line managers will encourage staff to identify risks to ensure there are no unwelcome surprises. Staff will not be blamed or seen as being unduly negative for identifying risks. All Staff should have an awareness and understanding of the risks that affect patients, visitors, and staff and are encouraged to identify risks.

Staff will be competent at managing risk. In order to facilitate this, staff will have access to comprehensive risk guidance and advice; those who are identified as requiring more specialist training to enable them to fulfil their responsibilities will have this provided internally.

There will be active and frequent communication between staff, stakeholders and partners.

4. Risk Appetite Statement

Risk Appetite is the amount and type of risk that NHSGGC is willing to seek or accept in the pursuit of its objectives. The Board is responsible for setting and monitoring its risk appetite when pursuing its corporate objectives.

The Risk Appetite Statement will be published as a separate document and it will define the Board's appetite for each type of risk in relation to the achievement of corporate objectives. Risks throughout the organisation will be managed within the Board's approved risk appetite and, where this is exceeded, additional action will be taken to reduce the risk(s).

The Risk Appetite will be reviewed and updated through the full Board annually. This annual update will incorporate a review of risk appetite levels for each risk type to ensure these remain current and accurate. It will also consider any additional or new risk types to be incorporated into the statement and thresholds for risk escalation.

The Risk Appetite Statement will be communicated to relevant staff involved in the management of risk and should be read in conjunction with this Risk Management Strategy.

5. Risk Architecture

The arrangements for communication, governance, reporting, and roles and responsibilities forms the organisation's overarching risk architecture. Defining a consistent approach to how and where risk information is communicated is essential to developing a positive risk culture and to ensuring risk management is appropriately deployed to support NHSGGC.

5.1. Risk Management Structure

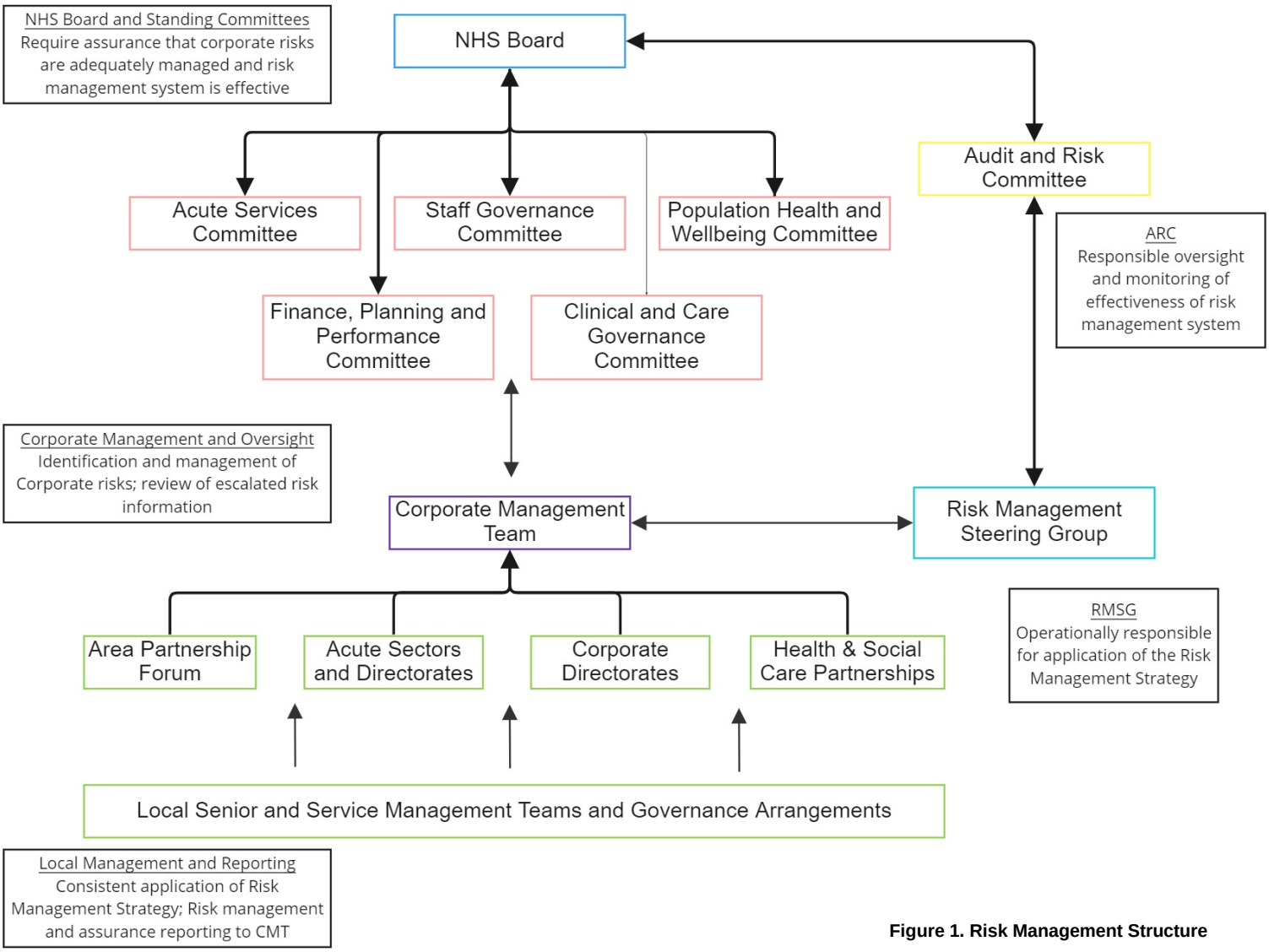

Figure 1. Risk Management Structure

5.2. Risk Register Hierarchy

Risks, once identified, are captured on risk registers. Each Directorate will hold a set of risk registers for its area with risks escalated through each level depending on their significance. Overall there are five levels of risk register available for use. This can be tailored to meet the requirements of individual Directorates or Services. For more information on developing risk registers, refer to the **Risk Register Policy and Guidance for Managers.**

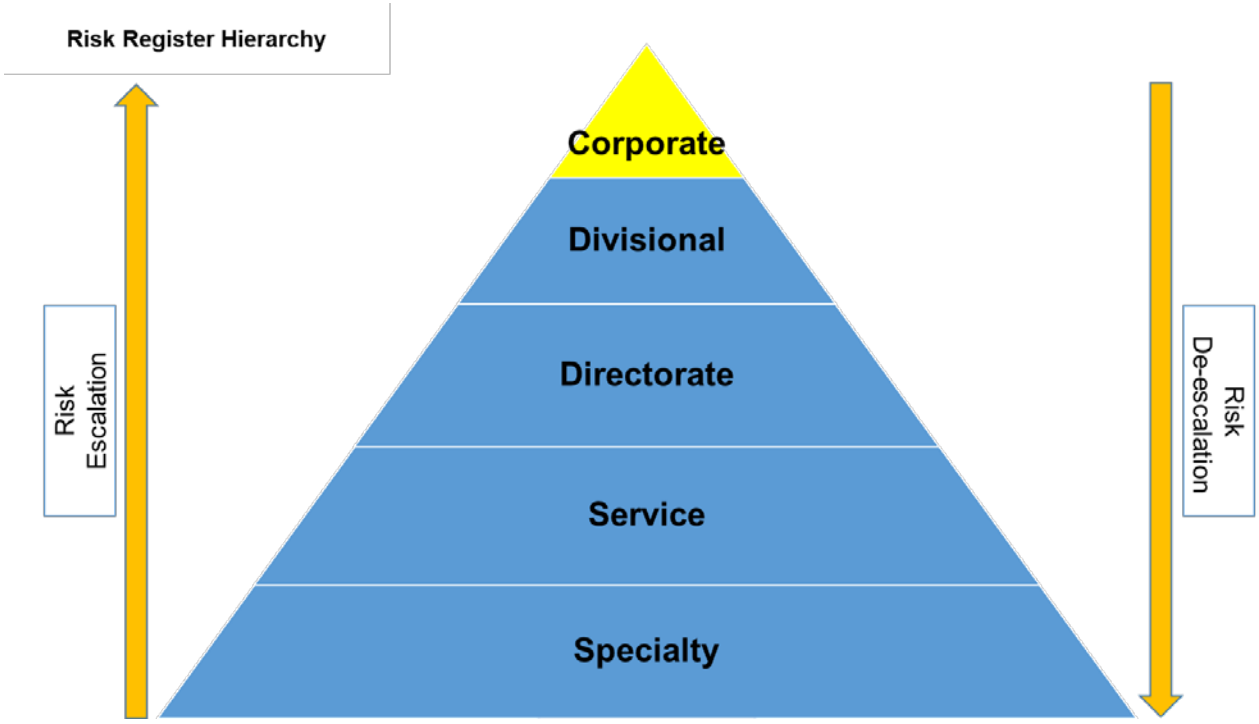

Figure 2. Risk Register Hierarchy

Corporate Risk Register

The Corporate Risk Register contains high level risks that could impact the long term corporate objectives of NHSGGC. It also contains the most significant operational risks escalated through the underlying risk register levels – these may be cross-cutting risks that present a short-medium term but significant threat to the organisation or multiple Directorates.

Divisional Risk Registers

A Divisional Risk Register contains the most significant operational risks highlighted by Directorates as exceptions. Risks are escalated via the Directorate Risk Registers. The requirement for a Divisional Risk Register will depend on the size, complexity and number of Directorates within an operational area. Where a Divisional Risk Register is not required, risks are escalated from directly Directorate to Corporate level.

Directorate Risk Registers

Each Directorate holds a risk register that contains the most significant operational risks escalated from its component Services. Risks are escalated to Directorate level from Service Risk Registers.

Service Risk Registers

Each Service holds a risk register that contains the most significant operational risks escalated from its component Specialties. Risks are escalated to Service level from Specialty Risk Registers.

Specialty Risk Registers

Each Specialty holds a risk register for its area. These form the bottom level of risk registers and risks that can be fully managed at a local level. The requirement for a Specialty Risk Register will depend the size, complexity and number of Specialities within an operational area. Where a Specialty Risk Register is not required, Service Risk Registers will form the bottom level of risk registers.

5.3. Roles and Responsibilities

The following arrangements will ensure that, from a governance perspective, there is a clear focus on corporate and operational risk management processes across all areas of NHSGGC.

NHS Board and formal Committees:

- The NHS Board is corporately responsible for NHSGGC's risk management strategy along with ensuring that significant and corporate risks are adequately addressed either through controls or response plans. It delegates this responsibility to the Audit and Risk Committee.
- To support the Board, a number of formal committees have been established and are responsible for different risks and different elements of the risk management system across NHSGGC (outlined in figure 1).

Risk Management Roles & Responsibilities

NHS Board

- Provides Oversight and scrutiny of NHSGGC's risk management arrangements to seek assurance on their effectiveness
- Approves risk appetite within NHSGGC

Chief Executive

- Has overall accountability for the risk management system across NHSGGC
- Provides leadership and endorsement of the Risk Management Strategy and application of its principles

Risk Management Roles & Responsibilities

Corporate Management Team

- Management of the NHSGGC Corporate Risk Register
- Considers risk appetite within NHSGGC (for Board approval)
- Ensures risk management processes are supported to enable adequate assurance related to corporate and operational risks
- Has accountability for implementation of risk management arrangements in their area(s) of responsibility in accordance with the Risk Management Strategy and supporting guidance
- The Finance Director is the lead executive responsible for corporate risk management arrangements and the Risk Management Strategy via the Chief Risk Officer
- The Medical Director is the lead executive responsible for Clinical Risk Management arrangements and the Clinical Governance Policy through established schemes of delegation

Audit and Risk Committee

- Provides oversight and monitoring of the effectiveness of arrangements for the governance of the Board's systems for the management of risk
- Evaluates and approves strategies and frameworks in respect of risk management on behalf of the NHS Board
- Reviews NHSGGC's risk culture and maturity and directs action in pursuit of continuous improvement in this area.

Standing Assurance Committees

- Provide oversight and scrutiny and ultimately approve updates and provide direction in respect of corporate risks aligned to each committee
- Provide oversight and scrutiny to ensure that an appropriate approach is in place to deal with risk management across the system working within the NHSGGC Risk Management Strategy

Risk Management Steering Group

- Provides advice on the development and maintenance of the supporting processes in place to ensure risks to corporate objectives are effectively managed
- Has responsibility for updating the Risk Management Strategy and Risk Appetite Statement within their respective review timescales
- Reviews the Risk Management Annual Objectives and Performance Report, monitoring progress against delivery
- Is accountable to the Audit and Risk Committee, with the RMSG Chair being accountable to the Chief Executive, for the implementation of the Risk Management Strategy and supporting processes

Chief Risk Officer

- Has responsibility for implementation of the Risk Management Strategy, Risk Appetite Statement and supporting processes
- Provides advice and guidance to Risk Owners to ensure risks are properly identified, understood and managed across all levels of NHSGGC

Risk Management Roles & Responsibilities

- Reports on the NHSGGC risk profile to various levels of governance, including CMT and ARC and other standing committees
- Periodically reviews and updates the Risk Management Strategy and Risk Appetite Statement
- Drives an improving risk culture through risk education and awareness to embed risk management into day-to-day management
- Provides managerial and professional leadership for risk management across NHSGGC's activities

Risk Owner

- Has accountability for ensuring the effective management of individual risks in accordance with the Risk Management Strategy and supporting guidance

Risk Lead

- Has responsibility for managing a risk on a day-to-day basis, assessing the risk score, updating the management plan, reviewing the risk and updating the risk management system (DATIX), on behalf of the Risk Owner

Risk Champion

- Has responsibility within an individual Specialty, Service or Directorate area for co-ordinating risk management activity, administering risk registers and maintaining lines of communication with the Chief Risk Officer

5.4. Assurance

As a result of the devolved accountability for all operational matters within NHSGGC, the Board, through the Audit and Risk Committee requires assurance that local systems are capable of identifying their objectives and managing the risk to their achievement.

To assist the Board meet its governance requirements in respect of the management of risk:

- The Chief Risk Officer, supported by senior management teams, will provide regular reporting on the Corporate Risk Register to the CMT
- the RMSG will provide assurance to the NHSGGC Audit and Risk Committee on risk management arrangements
- the Chief Executive and the Senior Management Teams will evaluate assurances for the most significant and widespread risks contained within the NHSGGC corporate risk register
- risks will be reviewed and approved by the relevant Standing Committee to ensure adequate oversight, with decisions recorded in the minutes of the meeting reviewing
- The Corporate Risk Register is reviewed by the Audit and Risk Committee quarterly
- Twice a year the Corporate Risk Register is reviewed by the full Board
- Once a year the Risk Appetite Statement is reviewed by the full Board

This process (summarised in figure 3) will ensure that risk management is firmly embedded as a Board responsibility and that assurances can be provided at all levels on the overall effectiveness of the risk management processes across NHSGGC.

To provide confidence to patients, staff and the public that this is the case, NHSGGC will include an assessment of the effectiveness of the risk management arrangements within the Governance Statement in its published annual financial accounts.

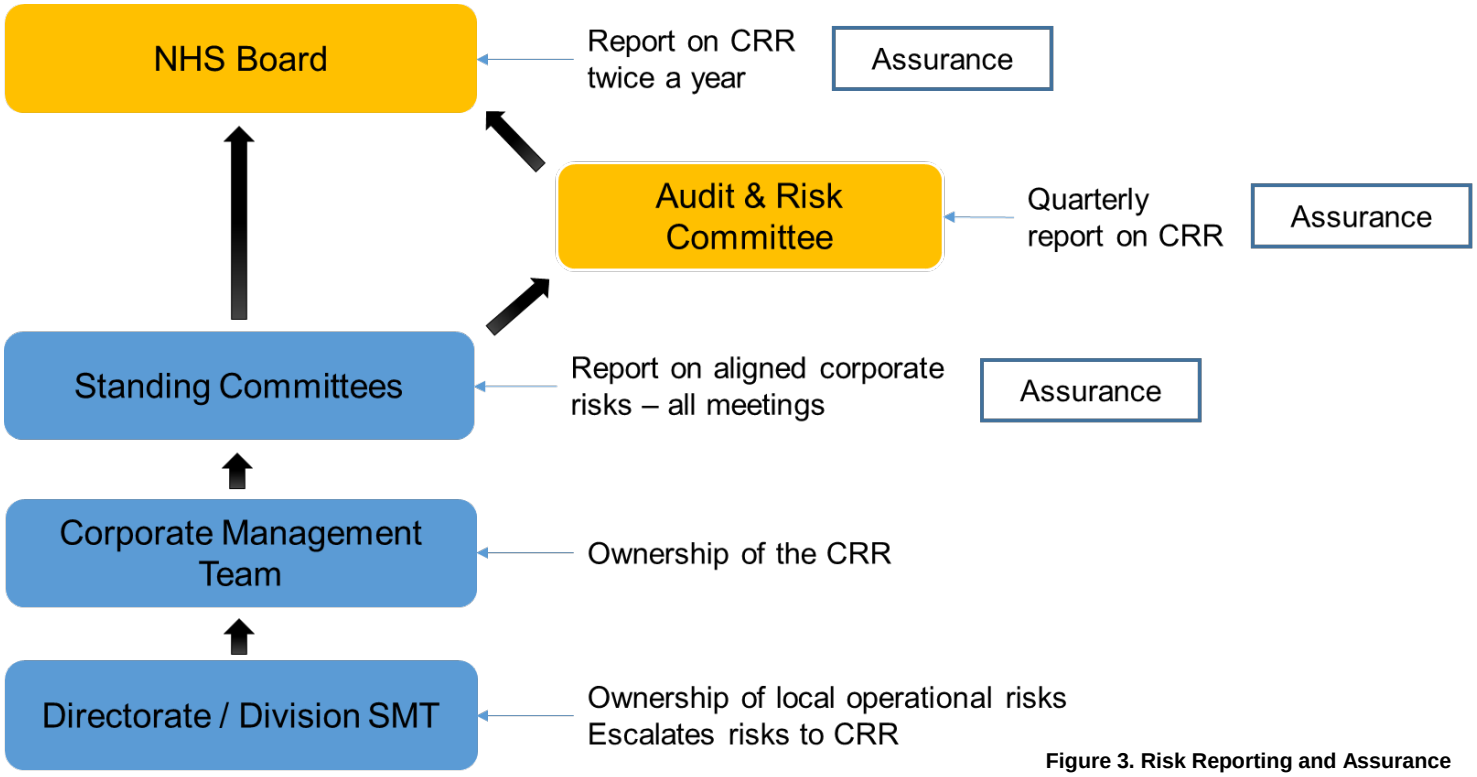

Figure 3. Risk Reporting and Assurance

6. Risk Management Process

NHSGGC is committed to establishing, maintaining and embedding a robust and effective framework for the management of risk that supports delivery of our risk management strategy across the organisation. The framework is based on the use of a dynamic process, based on the international standard ISO 31000. For detailed guidance on the risk management process refer to the **Risk Register Policy and Guidance for Managers.**

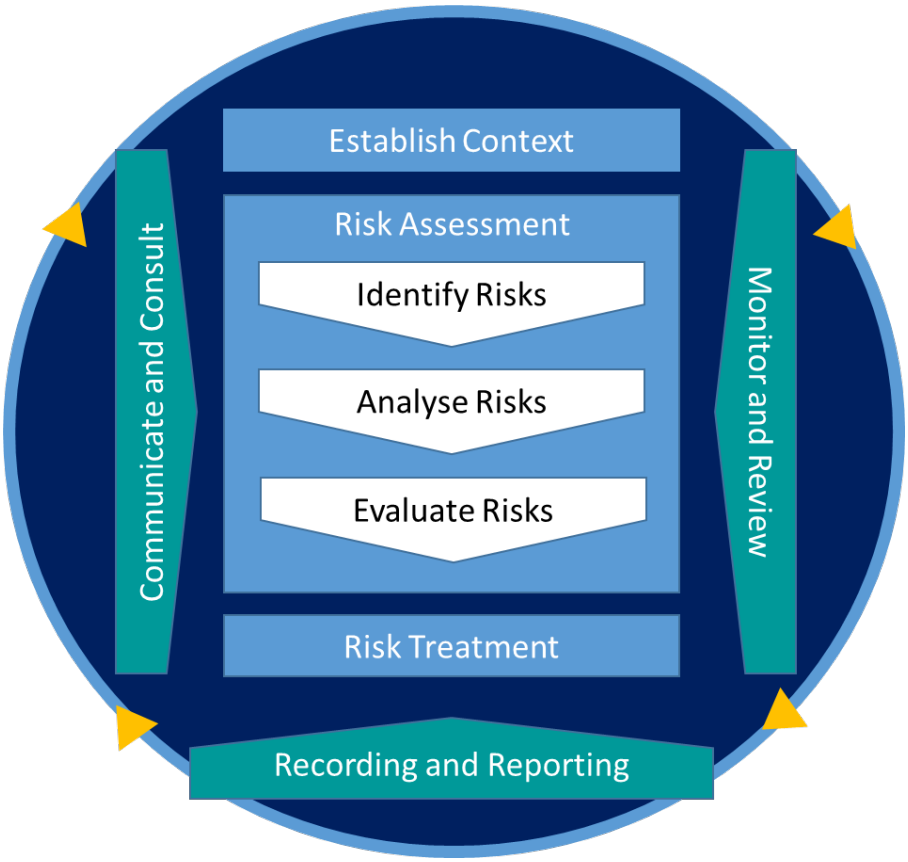

Figure 4. Risk Management Process

6.1. Establish Context

Risks should be set against what we are trying to achieve as an organisation – our corporate objectives. In this stage of the risk management process it is important to ensure there is a common understanding of what those objectives mean at a team, service and organisational level.

6.2. Identify Risks

Find, recognise and identify the uncertain events, or risks, that might prevent us from achieving our corporate objectives.

6.3. Analyse Risks

Once a risk has been identified it must be described in a certain way to understand the nature of the risk. This involves articulating underlying risk causes, the risk event itself and resultant risk impacts.

6.4. Evaluate Risks

The evaluation of a risk, through scoring the likelihood of occurrence and organisational impact enables us to gain an understanding of the level of exposure and in turn prioritise our risk response.

6.5. Risk Treatment

The purpose of this step in the process is to select and implement the appropriate management response to a risk. There are four management responses we can apply to manage a risk, known as the four T's:

- **Treat** – this involves action to implement risk controls in order to mitigate the likelihood and/or impact of a risk
- **Terminate** – this is the decision to stop the activity associated with the risk, thereby avoiding the risk altogether
- **Transfer** – this involves transferring the consequences of the risk, either partially or entirely, to a third party. The most common form of risk transfer is insurance.
- **Tolerate** – this is the decision to accept the risk, and any potential consequences, at its current level without further intervention.

6.6. Monitor and Review

This step involves the ongoing review of the effectiveness of the risk management process, the adequacy of risk controls and treatment methods. It also involves monitoring the operating environment for any changes and whether new risks have emerged.

6.7. Recording and Reporting

This step involves continuous reporting on the management of risk through appropriate governance levels, as detailed in Section 5 of this strategy.

6.8. Communicate and Consult

Communication of the risk management process is essential to assist relevant stakeholders to understand NHSGGC's risk profile and inform decision making as well as prioritisation of resources. Effective communication also supports assurance at each governance level throughout the organisation. The approach to communication is detailed in section 7 of this strategy.

7. Communication of Risk Management Strategy

Learning and Development

To implement this strategy, focused and effective learning and development support is essential to achieve:

- A workforce with the confidence, competency and capacity to manage risk and make appropriate risk based decisions
- An organisational focus to target underlying systems and process weaknesses

Training plans will continue to be developed and implemented to meet training needs and promote risk management learning and development across NHSGGC led by the Chief Risk Officer.

Provision of Support and Information

The availability of timely and accurate risk information is necessary for the implementation of this strategy.

Accordingly, NHSGGC will:

- Promote the development of systems to support the Risk Management Strategy
- Develop, through the Chief Risk officer, relevant supporting risk management policies and procedures and ensure they are up to date and easily accessible
- Develop a risk management training manual to educate managers on managing risk and the use of the Board's Risk Management system;
- Put in place effective systems of communication to ensure everyone in the organisation is informed about risk management; and
- promote continuous improvement and sharing of good practice.

The Corporate Risk Management Annual Performance Report annual risk management report to the Audit and Risk Committee will capture the necessary actions and detail progress against these.

Glossary of Terms

Assurance – Stakeholder confidence in our service gained from evidence showing that risk is well managed.

Corporate Risk Register – A Board level risk register, which covers strategic risks for NHSGGC across Operating; Legal; Financial/Commercial; Clinical; People/Workforce; Reputational; and Property risks.

Governance Statement – A statement by the accountable officer within the published Annual Report, required by HDL(2002)11, on the effectiveness of NHSGGC's systems of internal control, of which risk management is a key component.

Healthcare Governance – The system by which NHSGGC is directed and internally controlled to achieve objectives and meet the necessary standards of accountability, probity and openness in all three areas of clinical, corporate and staff governance.

Integration Joint Boards (IJBs) also known operationally as Health and Social Care Partnerships (HSCPs) – a partnership between the Health Board and a local authority to which they have delegated the responsibility and resources for adult health and social care.

Internal Control – Corporate governance arrangements designed to manage the risk of failing to meet NHSGGC corporate objectives.

Likelihood – a description of the probability that a risk may occur.

Impact – a description of the consequences should a risk occur.

Incident – An adverse event which causes or may have caused physical or psychological harm or loss.

Incident Recording – The system of reporting adverse events or near misses.

Issue – Something that has happened and is currently affecting the organisation in some way and needs to be actively dealt with and resolved.

Partnership - Way of working where staff at all levels, and their representatives, are involved in developing and putting into practice the decisions and policies which affect their working lives.

Risk – An uncertain event, or set of events, which, should it occur, will have an effect on the organisation's ability to achieve its corporate objectives.

Risk Appetite – the level of risk the organisation is willing to accept in pursuit of its objectives.

Risk Architecture – All of the risk management arrangements within an organisation – sets out lines of communication and reporting, delegation and roles / responsibilities.

Risk Assessment – The systematic process to identifying risks and evaluating their potential likelihood and impact.

Risk Champion – The person / role with responsibility in an individual Directorate for maintaining lines of communication with the Chief Risk Officer, administering the risk register process locally and co-ordinating risk management activities.

Risk Control – Measures put in place to effective manage a risk to within an acceptable level. Can be preventative or contingency and will reduce the likelihood or impact of the risk.

Risk Culture – The reflection of the overall attitude of every part of management of an organisation towards risk.

Risk Escalation – the process of a risk escalating to the Corporate Risk Register when the tolerable risk rating has been exceeded.

Risk Lead – The person / role responsible for managing a risk on a day-to-day basis, assessing the risk score and updating the management plan, reviewing the risk on a regular basis.

Risk Management – The integrated approach (culture, processes and structures) to the identification, assessment, control and monitoring of risk.

Risk Register – A tool used to capture, manage and monitor risks. Includes all information required about that particular risk and is intended to be used both as a management tool and a conduit for risk reporting.

Risk Management Strategy – Sets out the basis for the principles, processes and approaches to risk management to be followed in order to achieve consistent and effective application of risk management and allow it to be embedded into all core processes.

Risk Owner – The person / role with accountability for ensuring the effective management of a risk

Senior Management Teams – the Chief Executive, Directors and the Chief Officer, Acute Services; and the Chief Executive, Directors and IJB Chief Officers.