Southern Health and Social Care Trust

Quality Care - for you, with you

Interim Risk Management Strategy 2019 -2022

Risk Management Strategy	
Author	Trudy Reid Interim Assistant Director of Clinical and Social Care Governance
Date of Issue	September 2019
Date of Approval by Governance Committee	5th September 2019
Date of Review	September 2022

Contents

Foreword

The Southern Health & Social Care Trust (the Trust) seeks to deliver high quality care in all aspects of its services to patients/service users, staff, visitors, and the local communities. Risks occur daily in most activities undertaken within the Trust. Failure to manage these risks can result in injury or loss to patients/service users, staff or visitors, claims against the Trust and resources lost from patient care. It is therefore vital to implement a strategy to effectively manage risks, which will result in better quality of care.

The strategy is based on best practice, statutory requirements, national guidance and complies with the following:

- BSI ISO 31000:2018 – Risk Management Guidelines
- HM Treasury's 'Management of Risk – Principles and Concepts (the 'Orange Book')
- Assurance Frameworks –HM Treasury-December 2012
- DoH guidance document - An Assurance Framework : a Practical Guide for Boards of DHSSPS Arm's Length Bodies 2009
- Institute of Risk Management
- Audit and Risk Assurance Committee Handbook (NI) 2018
- Good Governance Institute –Risk Appetite Matrix
- This document complies with a number of Departmental circulars including
    - Circular HSS (PPM) 4/2005 – Risk Management
    - Circular HSS (PPM) 5/2003 (updated 2016/17) - Governance in the HPSS – Risk Management

This strategy will assist the Trust understand what might prevent achievement of Trust objectives (the risk). It also assists in responding to our risks. This means trying to reduce the chance of each risk happening, or reducing the consequences if it does occur. It is not about totally eliminating risk, as this is not possible within a health and social care environment. Therefore we must then decide which risks are urgent and more likely to occur, and the importance of their consequences.

The Trust and HSCB works in a constantly changing environment, with circumstances evolving both within and outside the Trust. This strategy reflects current best practice across the National Health Service (NHS) and Health & Social Care (HSC) and the guidance's in Departmental circulars and related areas such as risk management, controls assurance and clinical and social care governance.

The Trust is fully committed to the effective management of risks in all areas. This strategy provides the tools to make our risk management systems robust and systematic. Please use it to help you understand and appreciate why your job is so important in the management of risk.

This document should be read in conjunction with other Trust Risk management documents which include:

- Health & Safety Risk Assessment Guidance

- Control of Substances Hazardous to Health: Guidance Note on Risk Assessment
- Display Screen Equipment (DSE) Guidance
- LOLER & Manual Handling Policy
- Guidance on the Risk Assessment process for New and/or Expectant Mothers at Work
- Guidance for Risk Assessment of Young Persons at Work
- Guidance on Shared Work Premises
- Incident Management Strategy
- Health and Safety Policy and Whistleblowing Policy also highlight the responsibility on each employee to report any relevant issues
- Trust Business Continuity Management Plans

Section 1 – Context

Optimising and improving Patient and Service User quality and safety are core aims of the Southern Trust. Sound Clinical and Social Care Governance and Risk Management and Assurance processes are essential in realising these aims. The Clinical and Social Care Governance Strategy and its measures are dealt with in a separate publication. These strategies are to be read in conjunction with the Southern Trust Patient and Service User Strategy.

Risk Management Policy Statement

It is the policy of the Trust that a proactive approach to risk management is taken in order to:

- Bring about the desired continual improvements in the care/services the Trust provides;
- Ensure the Trust does its reasonable best to ensure the safety of staff and clients and the security of Trust premises for those that visit, live or work in them;
- Improve the way the Trust conducts its business;
- Enhance the services, reputation and efficient management of resources of the Trust
- Comply with the statutory and public duties placed upon the Trust.
- To ensure that there is a consistent approach to the assessment and recording of risk across the organisation

Trust Vision and Key Objectives

The Risk Management Strategy has been developed in line with the Trust vision and key objectives.

Vision and Purpose

The Trust's vision is to deliver safe, high quality care, that is co-produced and co-designed in partnership with service users and staff who deliver our serves

Our vision and values guide all that we do and will do in the future. Alongside this we want to be very clear about what we want to achieve. The Trust's priorities are set out in our six key objectives:

The Corporate Objectives are:-

Aims and Objectives

The aims and objectives of the Risk Management Strategy underpin the vision and corporate objectives of the Trust and are outlined below.

The aim of the Trust Risk Management Strategy is to:

- Cultivate and foster an 'open and fair' culture in order to encourage openness, honesty, reporting and facilitate learning for all staff
- Ensure a systematic approach to the identification, assessment and analysis of risk, and the allocation of resources to eliminate, reduce and control risk.
- Mitigate risks and/or manage those risks which are deemed as acceptable.

The objectives of the Risk Management Strategy which underpin the above aims are to:

- Manage risks to the quality of services provided and the safety of service users, clients, visitors, staff and contractors
- Manage risks associated with the corporate functions of Human Resources, Finance and Informatics
- Manage risks associated with service continuity
- Manage risks associated with the reputation, community expectation and equity of services of the Trust
- Minimise damage and financial losses that arise from avoidable, unplanned events

Section 2 - Definitions of Risk and Risk Management

This section of the Strategy provides a definition of risk and risk management. It also establishes the Trust's risk management strategy statement and associated objectives.

Definition of Risk

Risk is the chance, great or small, that damage or an adverse outcome of some kind will occur as a result of a particular hazard. It is the threat that an event or some action will adversely affect the Southern Trust's ability to successfully execute its strategies and achieve its objectives. Risk also includes failing to exploit opportunities and maintain organisational resilience.

Based on the ISO 31000: 2018 the following definition of risk is used regionally:-

Risk is the "effect of uncertainty on objectives".

Risk is also often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

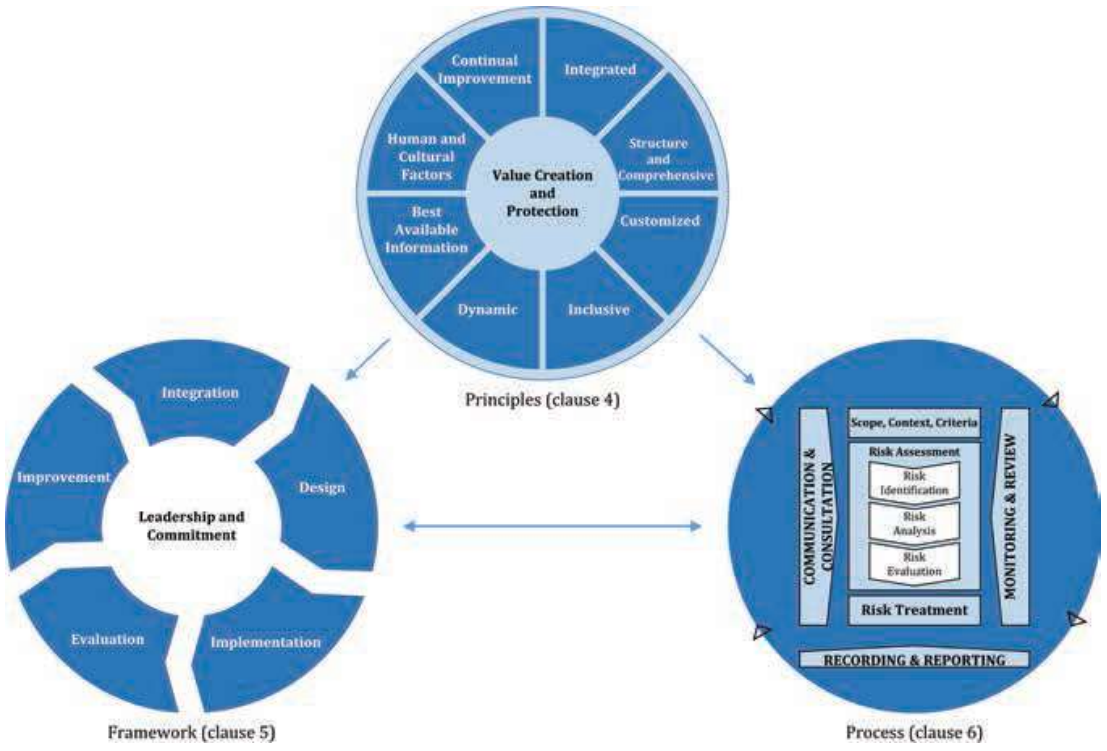
Section 3 - Principles of Risk Management

Managing Risk (Aligned with ISO 31000)

Managing risk is part of good governance and is fundamental to how an organisation is managed at all levels. Managing risk is part of all activities associated with an organisation and includes interaction with stakeholders; consideration of the external and internal context of the organisation, including behaviour and cultural factors.

ISO 31000: 2018 has three components for managing risk. These relate to (i) the identification of core **principles of risk management** with the intention that these will be addressed by (ii) the development of a **risk management framework.** In turn, the framework assists in managing risk through the (iii) **risk management processes** as outlined in the ISO 31000 standard. These are illustrated in diagrammatic format at Figure 1 below.

Figure 1 – Principles, Framework and Processes for Risk Management[1]



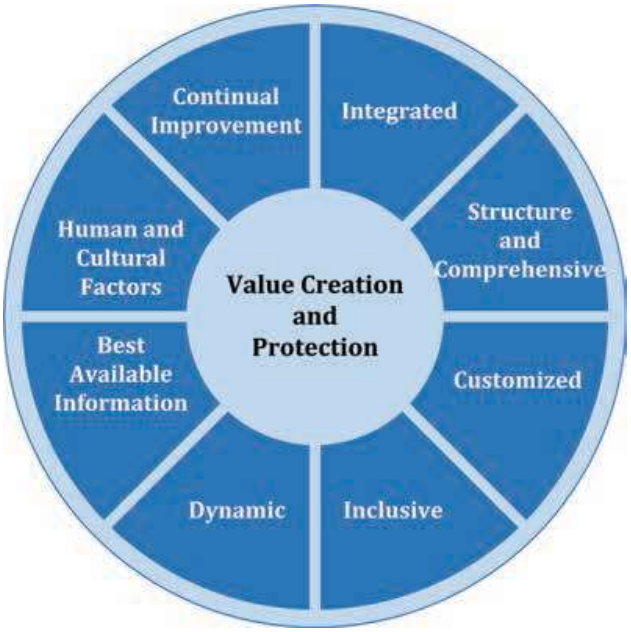
Principles of Risk Management

To be fully effective any risk management process must satisfy a minimum set of principles or characteristics. ISO 31000 includes a section (Clause 4) on these principles and these are shown in diagrammatic format in Figure 2 below. The

[1] Source – BSI ISO 31000:2018 – Risk Management Guidelines

principles are the foundation for managing risk and should be considered when establishing the organisation's risk management framework and processes and will help the organisation manage the effects of uncertainty on its objectives.

Figure 2 - Principles of Risk Management[2]



The principles are further explained in a short narrative format below:-

Component	Description
Integrated	Risk management should be integrated within all organisational activities.
Structured and comprehensive	A structured and comprehensive approach to risk management contributes to assurances in the Governance Statement.
Customised	The risk management framework and process should be customised and proportionate to the organisation's external and internal context related to its objectives.
Inclusive	Appropriate and timely involvement of stakeholders needs to be considered. This will better inform the organisation's risk management system.
Dynamic	Risks can emerge, change or disappear as an organisation's external and internal context changes. The risk management system needs to respond to these changes in a timely manner.
Best available information	Information should be timely, clear and available to relevant stakeholders.
Human and cultural factors	Human and cultural factors significantly influence all aspects of risk management.
Continual improvement	Risk management is continually improved through learning and experience and will feed into the organisation's quality improvement framework/systems.

[2] Source – BSI ISO 31000:2018 – Risk Management Guidelines

Section 4 - Risk Management Framework

Figure 3 below illustrates the elements of the second component - Risk Management Framework that is proposed to be adopted. Whilst each item is self-explanatory a short narrative about each is listed below.

Figure 3 – Components of a Risk Management Framework[3]

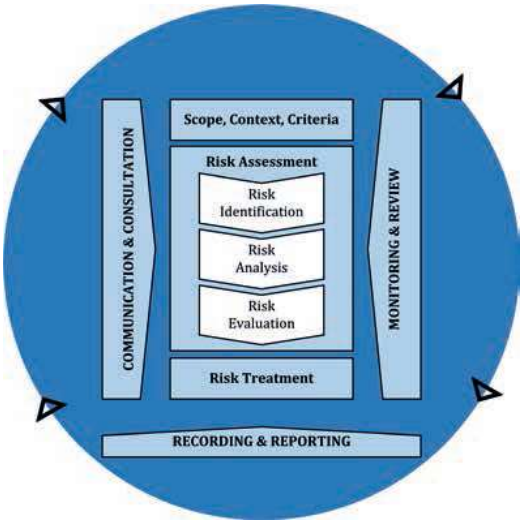
Component	Description
Leadership and Commitment	Management needs to ensure that risk management is integrated into all organisational activities and demonstrate leadership and commitment by implementing all components of the framework. This in turn will help align risk management with its objectives, strategy and culture.
Integration	Integrating risk management relies on an understanding of organisational structures and context. Risk is managed in every part of the organisation's structure. Everyone in an organisation has responsibility for managing risk.
Design	The organisation should examine and understand its external and internal context when designing its risk management framework.
Implementation	Successful implementation of the framework requires the awareness of all staff within the organisation.
Evaluation	The organisation should periodically measure its risk management framework against its purpose, implementation plans, risk management key performance indicators and expected behaviour. This will ensure it remains fit for purpose.
Improvement	The organisation should continually review, monitor and update its risk management framework to ensure it is fit for purpose.

[3] Source – BSI ISO 31000:2018 – Risk Management Guidelines

Section 5 - Risk Management Process

The third component – Risk Management Process is outlined in diagrammatic format in Figure 4 below with short descriptors of each item.

Figure 4 – Risk Management Process[4]



Communication and consultation

Communication and consultation with appropriate external and internal stakeholders should take place within and throughout all steps of the risk management process.

Scope, context and criteria

Scope, context and criteria involve defining the scope of the process, and understanding the external and internal context.

Risk Assessment

Component	Description
Risk identification	Risk identification should be a formal, structured process that considers sources of risk, areas of impact, and potential events and their causes and consequences.

[4] Source – BSI ISO 31000:2018 – Risk Management Guidelines

Risk Analysis	Risks should be analysed by considering the consequences/severity of the risk and the likelihood/frequency that those consequences may occur. The risk criteria contained within the regionally agreed Risk Rating Matrix and Impact Assessment Table will provide a guide for analysis.
Risk Evaluation	Risk evaluation involves making a decision about the level of risk and the priority for attention through the application of the criteria developed when the context was established. This stage of the risk assessment process determines whether the risks are acceptable or unacceptable. Acceptable risks are those as outlined in the organisation's Risk Management Strategy i.e. its risk appetite.

Risk Treatment

The purpose of risk treatment is to select and implement options for addressing risk. Risk treatment involves an iterative process of:

- Formulating and selecting risk treatment options;
- Planning and implementing risk treatment;
- Assessing the effectiveness of that treatment;
- Deciding whether the remaining risk is acceptable;
- If not acceptable, take further treatment/action.

Monitoring and Review

Monitoring and review should take place in all stages of the process. Monitoring and review includes planning, gathering and analysing information, recording results and providing feedback. The results of monitoring and review should be incorporated throughout the organisation's performance management, measurement and reporting activities.

Recording and Reporting

The risk management process and its outcomes should be documented and reported through appropriate mechanisms

Risk Registers

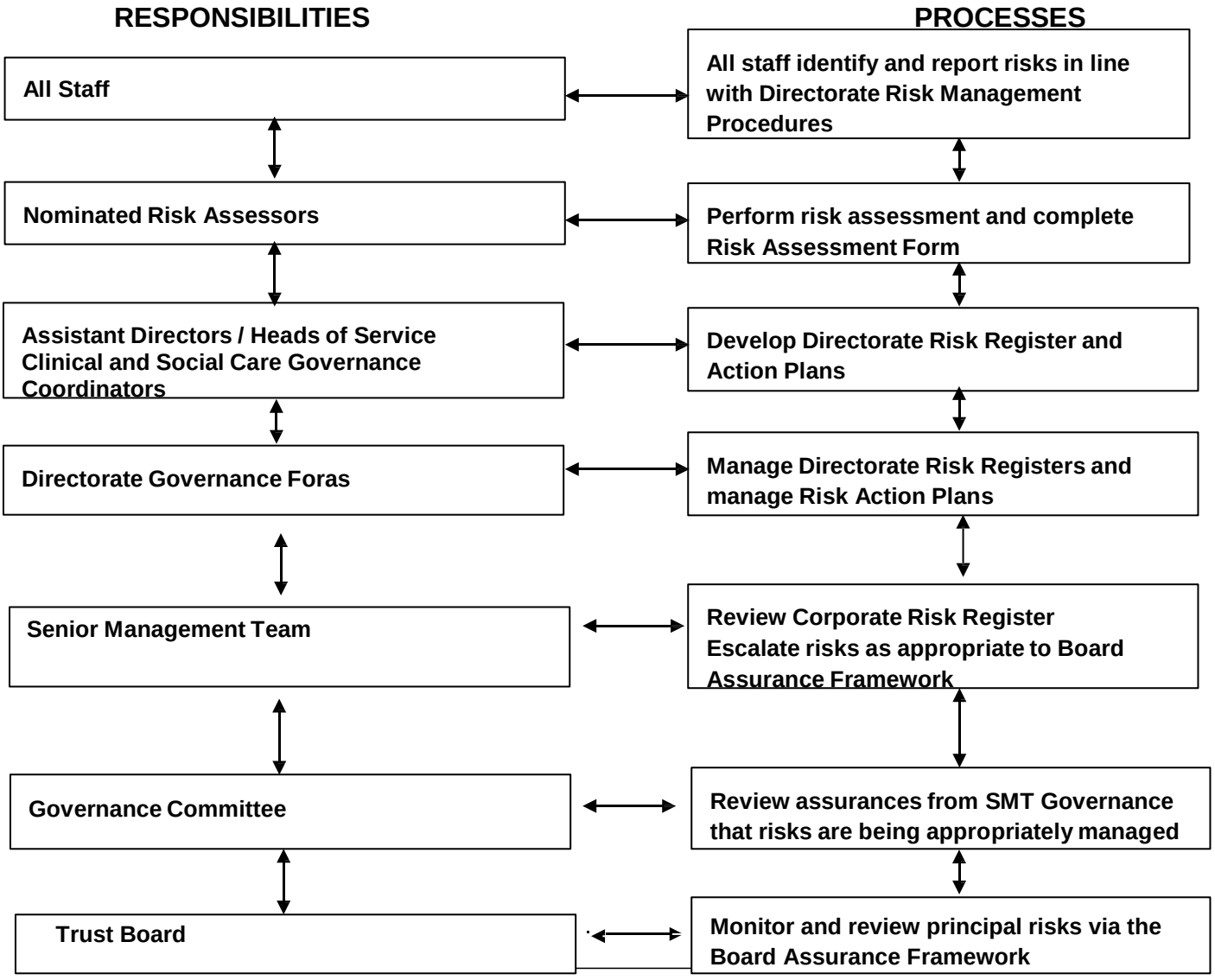
In order to develop and be aware of its risk profile and to identify the key areas for investment in risk reduction/management, the Trust has developed a framework for risk registers. This comprises both Corporate and Directorate risks. The Risk Registers will enable the Trust to identify the totality of its risk and quantify those that are deemed as acceptable or present significant risks that may affect the objectives of the Trust.

A Risk Register is a log of significant risks (clinical, non-clinical, financial etc.) that threaten the Trust's success in achieving its aims and objectives. It is populated through the various risk assessments undertaken within the organisation, together with external reviews and reports. This enables risk to be quantified and ranked to inform the Trust Board and aid decision-making and resource allocation processes.

Section 6 - Governance Arrangements in place to manage risk in the Trust

The specific governance arrangements relating to the Risk Management Strategy are described in the sub-sections which follow. A summary of the responsibilities and processes associated with risk management in the Trust is illustrated in Figure 5.

Figure 5 - Governance Arrangements in place to manage risk in the Trust



Trust Board

Within the context of this Strategy the Trust Board has a specific role in reviewing principal risks and significant gaps in control and assurance via the Board Assurance Framework, and ensuring that where gaps have been identified, corrective actions are taken.

The Trust Board is responsible for ensuring that the organisation consistently follows the principles of good governance applicable to HSC organisations. This includes reviewing the effectiveness of internal controls - financial, organisational, clinical and social care governance and risk management. In the context of this Strategy the Trust Board will:

- Demonstrate its commitment to risk management through the endorsement of the Risk Management Strategy
- Ensure, through the Chief Executive, that the responsibilities and structure for risk management outlined in this document are fully introduced
- Oversee risk assurance processes
- Consider strategic and corporate level risks, including agreeing the related risk control measures and monitoring implementation of same
- Ensure that the Trust has robust and effective arrangements in place for clinical and social care governance and risk management
- Ensure that high standards of corporate governance and personal behaviour are maintained in the conduct of the business of the whole organisation

Governance Committee

The remit of the Governance Committee is to ensure that:

- There are effectively and regularly reviewed structures in place to support the effective implementation and development of integrated governance across the Trust
- Risk management is a planned and systematic approach to identifying, evaluating and responding to risks and providing assurance that responses are effective
- Principal risks and significant gaps in controls and assurances are considered by the Trust Board
- Timely reports are made to the Trust Board, including recommendations and remedial action taken or proposed, if there is an internal failing in systems or services
- There is sufficient independent and objective assurance as to the robustness of key processes across all areas of governance.

Both the Governance and Audit Committees separately review the adequacy of all governance and risk management and control related disclosure statements (the Governance Statement).

Within the context of this Strategy the Governance Committee will receive assurances from the Trust Senior Management Team (SMT) that risks are being effectively managed.

Senior Management Team (SMT)

It is the remit of the Senior Management Team to:

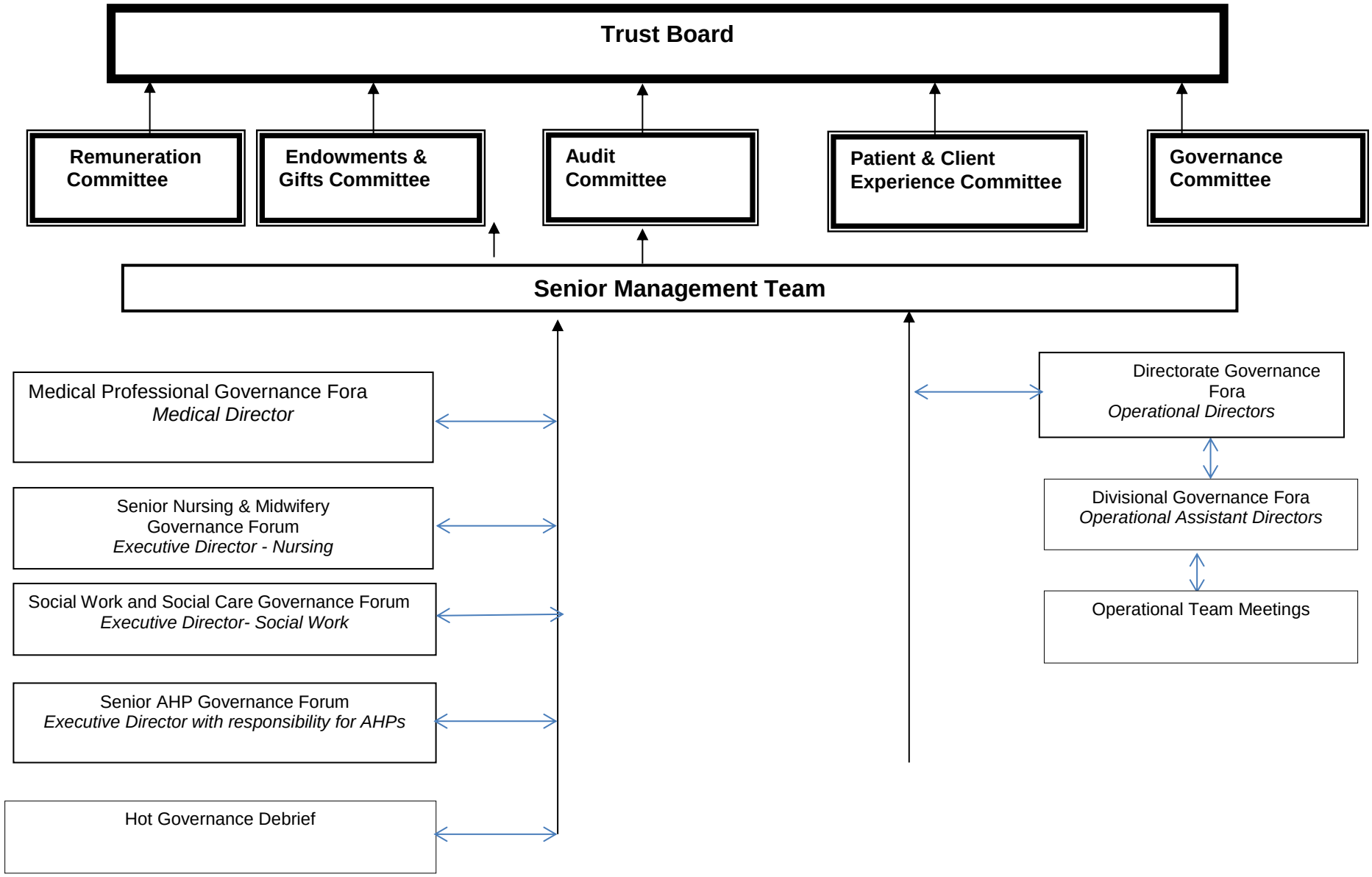
- Ensure that the Trust has an effective Corporate Risk Register
- Review the Corporate Risk Register and ensure and that risks are escalated to the Board Assurance Framework as appropriate
- Receive completed investigation reports of serious adverse events
- Receive completed reports of findings of Root Cause and Systems Analysis
- Implement and keep under review the Integrated Governance Framework
- Receive assurance of the
    - adequacy of systems for quality assurance,
    - managing risk / risk management strategies/ interventions
    - control of the environment
- Receive assurance regarding the implementation of activities associated with action plans for the
    - Controls Assurance programme,
    - HPSS Quality Standards
    - RQIA Recommendations etc.
- Accept and review reports and strategy documents pertaining to risk management and governance for endorsement by the Governance Committee
- Assess the adequacy of the Governance Sub Committees to provide accountability and assurance that governance arrangements are effective

The SMT is constituted from the following membership:

- Chief Executive (Chair)
- Executive Medical Director
- Interim Executive Director of Nursing , Midwifery and AHPs
- Executive Director of Social Work / Director of Children
- Director of Human Resources and Organisational Development
- Executive Director of Finance, Procurement and Estate
- Director of Performance and Reform
- Director of Mental Health & Disability
- Director of Acute Services
- Director of Older People & Primary Care
- Director of Children & Young People/Executive Director of Social Work

Other senior staff members will be required to attend meetings as the SMT considers necessary.

High Level Governance Structure



Operational Directorate Governance Foras

Operational Directorate Governance Foras are responsible for reviewing and managing Directorate Risk Registers. Directorates will be supported in this function by the Clinical and Social Care Governance (CSCG) Co-coordinators and Governance Officers aligned to each of the directorates. Directorate Governance Foras meet monthly and are reflective of all speciality interests/service areas across Directorates/Divisions.

Membership of Directorate Governance Foras should be drawn from (though not limited to) Associate Medical Directors, Clinical Directors, Assistant Directors, Heads of Service and the Clinical and Social Care Governance (CSCG) Coordinators and Governance Officers aligned to the Directorates of Acute, Children & Young People, Older People & Primary Care and Mental Health & Disability, as appropriate.

Within the context of this strategy, the Directorate Governance Foras manage the processes associated with developing, assessing and evaluating risk and developing Risk Registers within the Directorates as outlined in Section 3 of this Risk Management Strategy.

The Directorate Governance Foras through the appropriate Director present those risks which cannot be managed at Directorate level and/or may require consideration in respect of addition to the Corporate Risk Register to the Senior Management Team.

The processes associated with developing, assessing and evaluating risk and developing Risk Registers is documented in Section 4 of this Risk Management Strategy.

Section 7 - Roles and Responsibilities

Chief Executive

The Chief Executive is the Accounting Officer of the Trust and has overall responsibility for the effective and efficient management of the Trust and for the quality of health and social care provided. This responsibility encompasses the financial arrangements within the Trust and for the statutory duty of quality, as well as the governance, risk management and controls assurance arrangements. Whilst this overall responsibility is maintained, responsibilities for some aspects of governance have been delegated to executive directors as outlined below

Medical Director

The Medical Director is the Executive Director with delegated responsibility for risk management and clinical and social care governance.

This role encompasses:

- The effective co-ordination of clinical and social care risk and governance – specifically this relates to the functional areas of patient/service user safety, patient/service user liaison, litigation, effectiveness and evaluation, risk management and multi-disciplinary research.
- The provision of risk management support to Trust Directors via the clinical and social care governance structures of the medical directorate.
- Clinical and social care governance support for clinicians, nursing staff, social workers and allied health professionals.
- Regional/national initiatives related to clinical and social care governance are addressed and brought to the attention of appropriate staff.
- Regular clinical and social care governance reports/information are brought to the Governance committee (in line with the Governance reporting framework) and the Trust Board.

The Executive Medical Director is supported by the **Assistant Director for Clinical and Social Care Governance and the Medical Directorate** who are responsible for the development of systems and processes for clinical and social care governance and risk management. This includes the development of the strategic approach to patient client safety initiatives, patient service user liaison (this includes management of complaints and users' views), litigation, effectiveness and evaluation (this includes standards, guidelines and audit) and risk management.

Executive Directors of Nursing & AHP and Social Work

The Executive Directors of Nursing & AHP and Social Work with accountability for professional governance are responsible for ensuring effective risk management and

governance arrangements are in place across the Trust in respect of their professional group. The Directors will be supported by professional governance leads in ensuring that professional standards of care and practice are maintained

Directors

Whilst the Chief Executive has overall responsibility for Risk Management, Trust Directors are required to ensure that the Risk Management processes outlined in this Strategy are applied and working effectively in their own relevant areas. With the support of Assistant Director of Clinical and Social Care Governance and the Clinical and Social Care Governance Coordinators' aligned to Directorates, Trust Directors are required to:

- Ensure local Risk Management procedures are established for their area of responsibility based on the Trust-wide strategy including Risk Assessment, adverse incident reporting and Risk Registers
- Ensure that risk identification, reduction and management is a standing agenda item at team meetings
- Ensure there is a system for monitoring the application of risk management within the Directorates and that risks are actioned in accordance with the risk grading action guidance
- Provide reports that contribute to the Trust-wide monitoring and auditing of risk
- Ensure staff attend relevant mandatory and local training programmes and training in risk management
- Ensure there is a system in place to facilitate feedback to staff on risk management issues and the outcome of adverse incident reporting
- Ensure the specific responsibilities of managers and staff in relation to risk management and controls assurance are identified within the job descriptions of posts and that objectives are reflected in the individual performance review/staff appraisal process

Managers

Managers at all levels in the Trust must encourage, support and facilitate staff in the application of good risk management practice and ensure staff are provided with the education and training to allow them to do so.

Managers must be fully conversant with the Trust's approach to risk management and where applicable Controls Assurance and the Quality Standards for Health and Social Care. Managers will be supported in this role by the Clinical and Social Care Governance Co-ordinators and Governance Officers aligned to their directorates.

All Staff

All staff of the Trust are responsible for providing each patient/service user with the highest possible quality of care/services and for taking all appropriate action to promote patient and staff safety by minimising risk where possible.

Issues of concern should be highlighted through existing professional and or line management lines of accountability and expect timely feedback on what has been done to address their concerns. Where individual staff continue to have specific concerns of risks which may impact on the delivery of safe and effective care, they have a duty to highlight them through the Trust's Whistle Blowing Policy and to expect timely feedback on what has happened as a result.

All members of staff should:

- Demonstrate and awareness of risk/patient safety and its consequences at all times
- Consider the risks to patient/staff safety involved in what they do and minimise those risks where possible to an agreed acceptable level
- Practice in accordance with their professional Codes of Conduct
- Comply with the Risk Management Strategy and associated procedures for example The Incident Management Procedure
- Notify line managers of any hazard or risk identified in their area of work which cannot be managed and requires attention
- Participate in the Trusts Risk Management training and education programmes
- Accept personal and collective responsibility for maintaining a safe working environment

Clinical and Social Care Governance Co-ordinators'

The Key role of the CSCG Co-ordinator is to, on behalf of the Director, ensure that there are processes in place to support the implementation of this strategy and they must challenge and support the Directorate in the regular review of:

- Directorate/department Risk Registers
- Support the Assistant Directors and Heads of Service Directorate in preparation of actions plans to manage and minimise risk
- To monitor the progress of action plans and escalate barriers to progress to the appropriate directorate and Governance Fora
- Support and assist the Directorates in reviewing adverse incident trends
- Co-ordinate investigations into serious adverse incidents, medium to extreme incidents
- Support and monitor the Directorates in implementing recommendations arising from investigations on behalf of the Director
- Ensure that there are systems and processes in place to provide feedback to staff reporting risks and adverse incidents
- Report through the Assistant Director for Clinical and Social Care Governance to the Medical Director and Senior Management Team using weekly Governance Debrief using an agreed proforma.

Board Assurance Manager

On the delegated authority of the Chair (the Chief Executive) of SMT, the Board Assurance Manager is responsible for maintaining the Corporate Risk Register and Board Assurance Framework and supporting the Governance Committee and Trust Board in ensuring the provision of regular risk reporting and monitoring information and assurances.

Internal Audit

The internal audit function is responsible for providing independent advice and assurance to the Trust Board that risk management systems are in place, fit for purpose and meeting Trust objectives of improving Patient Quality Care and Safety.

Patients, Service Users and the Public

The Trust welcomes the value of risk reporting from patients and or members of the public, and assumes a positive approach to the complaints or comments from which potential risks are identified. The Trust is an open and learning organisation and will ensure that learning from the investigation of complaints, compliments and comments is shared to improve patient/service user quality care and safety.

External Providers, Contractors and Agency Staff

It is essential that External Providers, Contractors and agency staff are advised of their responsibilities to work safely within the Trust and acknowledge that the management of risk is an individual as well as a collective responsibility.

They should be informed of the reporting mechanisms in the local area they are working in for reporting any hazards, risks and incidents whether they impact upon the contractor, agency staff, patient, client, staff or visitor. All Service Level Agreements and Contracts will include a section on Risk Management.

Section 8 – SHSCT Trust Risk Management Procedure

The Trust's Risk Management Model is based on the ISO 31000 Standard as adopted by all regional HSC Trusts.

Establish the Scope, Context and Criteria

The following risk impact assessment criteria have been derived from the risk management objectives and will be used for the assessment of risks as part of the impact grading in the Trust's Risk Grading Matrix:

- Risks to people (impact physical/psychological on the Health/Safety/Welfare of any person affected: e.g. Patient/Service User, Staff, Visitor, Contractor)
- Risks to quality and professional standards/guidelines (Meeting quality/professional standards/statutory functions/responsibilities and Audit Inspections)
- Risks to reputation (Adverse publicity, enquiries from public representatives/media Legal/Statutory requirements)
- Risks to Finance, Information and Assets (Protect assets of the organisation and avoid loss)
- Risks to resources (Service and business interruption, problems with service provision, including staffing (number and competence), premises and equipment)
- Risks to the environment (air, land, water, waste management)

Risk Identification/Safety Management

There are several aspects to risk identification, all of which need to be present in an effective risk management system. Risks should be assessed anytime when there is the potential for unexplored and unidentified issues diverting the organizational resources from its objectives and goals. The risk management process should be applied to business planning at all levels and risk management issues should be communicated to key stakeholders where necessary.

Adverse incident reporting, legal claims, complaints, and user views, internal and external e.g. RQIA audit reports provide robust data but by definition are retrospective. Internal and external assessment are less quantifiable than adverse incident information but are critical in identifying key risks which have the potential to impact on the Trust.

The key elements for risk identification are detailed below:-

External Scrutiny and Inspection	Occurrences	Internal Assessments
Prospective	**Retrospective**	**Prospective**
Internal Audit Reports External Audit Reports Accreditation Bodies Report RQIA reports Reports from Professional Bodies Health and Safety Executive Reports/Visits Environmental Health Reports Independent Reviews Coroner's Reports Contract management meeting reports from external providers Contract management meeting reports from external contractors All internal C&SCG data e.g. safety thermometer, waiting time report etc. NCEPOD enquiries/reports	Adverse Incident Reporting User Views Complaints Locally resolved expressions of dissatisfaction Legal Claims Patient and Client Satisfaction Measures Employee Satisfaction Measures Measures of psychological safety Sickness and Absence Records Staff Turnover Levels of Agency Utilisation Medical Device and Equipment Alerts Introduction of new Standards and Guidelines Outcome of Audit	Controls Assurance – Self Assessments Performance reporting Specialist Committees e.g. Infection Control Health & Safety etc. Risk Assessments (including H&S; business/project planning e.g. new activities, services; referrals) Management of relationship risk – i.e., service partners/key suppliers taking into account the behaviour and risk priorities of those partners Networking – use of media reports and information from other Trusts Other self-assessment tools - Health and Social Care Quality Standards Audit Commission.

Directorates are required to develop appropriate systems and mechanisms to support the identification of risk. Some potential mechanisms are:

- Data review – review of adverse incidents, complaints, lessons learned from investigations, user views, claims data, and patient safety data.
- Workplace Risk Assessment – review of current risk assessments to identify trends and recurrent risks across the organisation e.g. staff shortages, psychological safety, engagement
- External Review(s) – examine review reports to identify risks identified by the external review team e.g. coroners investigations, RQIA, Internal Audit, Standards & Guidelines, College & Professional Body Reports, National and Confidential Enquiries.
- Contract management meeting reports from external providers & contractors

Using the above identification methods risks should be identified and recorded in Risk Registers.

A risk assessment form (Appendix 1) should be applied to this risk assessment process.

Risk Analysis and Evaluation

For each risk identified an assessment will be made of the **likelihood** of the risk occurring and the consequence or **impact** if this were to happen. The assessment will be made taking into account the effectiveness of controls that are already in place to mitigate the risk.

Once identified, risks will be analysed and actioned following the steps below:

i) Step 1 - Determining Risk Likelihood

In assessing **likelihood** it is important to consider the nature of the risk being assessed. On the one hand, risk may be scored in relation to **probability of future occurrence**. However, in using **likelihood scores** reactively, for example, when reviewing adverse incidents a more appropriate perspective might be 'How likely is this to occur again? / How frequently has this occurred?'

Figure 4 should be used to assign a descriptor for this perceived risk. This should be determined by **either** frequency or **likelihood.**

Risk Likelihood Scoring Table			
Likelihood Scoring Descriptors	**Score**	**Frequency (How often might it/does it happen?)**	**Time framed Descriptions of Frequency**
Almost certain	**5**	**Will undoubtedly happen/recur on a frequent basis**	**Expected to occur at least daily**
Likely	**4**	**Will probably happen/recur, but it is not a persisting issue/circumstances**	**Expected to occur at least weekly**
Possible	**3**	**Might happen or recur occasionally**	**Expected to occur at least monthly**
Unlikely	**2**	**Do not expect it to happen/recur but it may do so**	**Expected to occur at least annually**
Rare	**1**	**This will probably never happen/recur**	**Not expected to occur for years**

ii) Step 2 – Determining the Risk Impact/Consequence

The risk impact/consequence table at Figure 5 (known as the 5x5 matrix) provides guidance on applying the impact criteria. In determining the risk impact/consequence the following question should be asked:

If harm occurred, what are the likely consequences to the Trust achieving its objectives?

All risks should be assessed **across each** of the 5 consequence / impact categories. The highest value attained against any one of the categories will be the impact / consequence grade will be used to indicate the level of risk.

HSC Regional Impact Table – with effect from April 2013 (updated June 2016 & August 2018)

DOMAIN	IMPACT (CONSEQUENCE) LEVELS [can be used for both actual and potential]				
	INSIGNIFICANT (1)	**MINOR (2)**	**MODERATE (3)**	**MAJOR (4)**	**CATASTROPHIC (5)**
PEOPLE *(Impact on the Health/Safety/Welfare of any person affected: e.g. Patient/Service User, Staff, Visitor, Contractor)*	• Near miss, no injury or harm.	• Short-term injury/minor harm requiring first aid/medical treatment. • Any patient safety incident that required extra observation or minor treatment e.g. first aid • Non-permanent harm lasting less than one month • Admission to hospital for observation or extended stay (1-4 days duration) • Emotional distress (recovery expected within days or weeks).	• Semi-permanent harm/disability (physical/emotional injuries/trauma) (Recovery expected within one year). • Admission/readmission to hospital or extended length of hospital stay/care provision (5-14 days). • Any patient safety incident that resulted in a moderate increase in treatment e.g. surgery required	• Long-term permanent harm/disability (physical/emotional injuries/trauma). • Increase in length of hospital stay/care provision by >14 days.	• Permanent harm/disability (physical/ emotional trauma) to more than one person. • Incident leading to death.
QUALITY & PROFESSIONAL STANDARDS/ GUIDELINES *(Meeting quality/ professional standards/ statutory functions/ responsibilities and Audit Inspections)*	• Minor non-compliance with internal standards, professional standards, policy or protocol. • Audit / Inspection – small number of recommendations which focus on minor quality improvements issues.	• Single failure to meet internal professional standard or follow protocol. • Audit/Inspection – recommendations can be addressed by low level management action.	• Repeated failure to meet internal professional standards or follow protocols. • Audit / Inspection – challenging recommendations that can be addressed by action plan.	• Repeated failure to meet regional/ national standards. • Repeated failure to meet professional standards or failure to meet statutory functions/ responsibilities. • Audit / Inspection – Critical Report.	• Gross failure to meet external/national standards. • Gross failure to meet professional standards or statutory functions/ responsibilities. • Audit / Inspection – Severely Critical Report.
REPUTATION *(Adverse publicity, enquiries from public representatives/media Legal/Statutory Requirements)*	• Local public/political concern. • Local press < 1day coverage. • Informal contact / Potential intervention by Enforcing Authority (e.g. HSENI/NIFRS).	• Local public/political concern. • Extended local press < 7 day coverage with minor effect on public confidence. • Advisory letter from enforcing authority/increased inspection by regulatory authority.	• Regional public/political concern. • Regional/National press < 3 days coverage. Significant effect on public confidence. • Improvement notice/failure to comply notice.	• MLA concern (Questions in Assembly). • Regional / National Media interest >3 days < 7days. Public confidence in the organisation undermined. • Criminal Prosecution. • Prohibition Notice. • Executive Officer dismissed. • External Investigation or Independent Review (e.g. Ombudsman). • Major Public Enquiry.	• Full Public Enquiry/Critical PAC Hearing. • Regional and National adverse media publicity > 7 days. • Criminal prosecution – Corporate Manslaughter Act. • Executive Officer fined or imprisoned. • Judicial Review/Public Enquiry.
FINANCE, INFORMATION & ASSETS *(Protect assets of the organisation and avoid loss)*	• Commissioning costs (£) <1m. • Loss of assets due to damage to premises/property. • Loss – £1K to £10K. • Minor loss of non-personal information.	• Commissioning costs (£) 1m – 2m. • Loss of assets due to minor damage to premises/ property. • Loss – £10K to £100K. • Loss of information. • Impact to service immediately containable, medium financial loss	• Commissioning costs (£) 2m – 5m. • Loss of assets due to moderate damage to premises/ property. • Loss – £100K to £250K. • Loss of or unauthorised access to sensitive / business critical information • Impact on service contained with assistance, high financial loss	• Commissioning costs (£) 5m – 10m. • Loss of assets due to major damage to premises/property. • Loss – £250K to £2m. • Loss of or corruption of sensitive / business critical information. • Loss of ability to provide services, major financial loss	• Commissioning costs (£) > 10m. • Loss of assets due to severe organisation wide damage to property/premises. • Loss – > £2m. • Permanent loss of or corruption of sensitive/business critical information. • Collapse of service, huge financial loss
RESOURCES *(Service and Business interruption, problems with service provision, including staffing (number and competence), premises and equipment)*	• Loss/ interruption < 8 hour resulting in insignificant damage or loss/impact on service. • No impact on public health social care. • Insignificant unmet need. • Minimal disruption to routine activities of staff and organisation.	• Loss/interruption or access to systems denied 8 – 24 hours resulting in minor damage or loss/ impact on service. • Short term impact on public health social care. • Minor unmet need. • Minor impact on staff, service delivery and organisation, rapidly absorbed.	• Loss/ interruption 1-7 days resulting in moderate damage or loss/impact on service. • Moderate impact on public health and social care. • Moderate unmet need. • Moderate impact on staff, service delivery and organisation absorbed with significant level of intervention. • Access to systems denied and incident expected to last more than 1 day.	• Loss/ interruption 8-31 days resulting in major damage or loss/impact on service. • Major impact on public health and social care. • Major unmet need. • Major impact on staff, service delivery and organisation - absorbed with some formal intervention with other organisations.	• Loss/ interruption >31 days resulting in catastrophic damage or loss/impact on service. • Catastrophic impact on public health and social care. • Catastrophic unmet need. • Catastrophic impact on staff, service delivery and organisation - absorbed with significant formal intervention with other organisations.
ENVIRONMENTAL *(Air, Land, Water, Waste management)*	• Nuisance release.	• On site release contained by organisation.	• Moderate on site release contained by organisation. • Moderate off site release contained by organisation.	• Major release affecting minimal off-site area requiring external assistance (fire brigade, radiation, protection service etc.).	• Toxic release affecting off-site with detrimental effect requiring outside assistance.

iii) Step 3 – Determining the Risk Rating

Following the identification of the level of likelihood and impact/consequence of the identified risk, a risk rating will be calculated using the matrix in Figure 6. This rating will prioritise and inform the further management of the risk identified.

Figure 6

	Impact (Consequence) Levels				
Likelihood Scoring Descriptors	Insignificant(1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Almost Certain (5)	Medium	Medium	High	Extreme	Extreme
Likely (4)	Low	Medium	Medium	High	Extreme
Possible (3)	Low	Low	Medium	High	Extreme
Unlikely (2)	Low	Low	Medium	High	High
Rare (1)	Low	Low	Medium	High	High

An example of a risk rating using the risk matrix is:

Likelihood x Consequence (Potential Impact) = Risk Rating e.g. Possible x Moderate = Yellow (9)

iv) Step 4 - Risk Action Planning

As part of the process, those carrying out the risk assessment exercise should also develop proposals for management of the risks identified. This should be documented in the risk action plan. All options should be considered including accepting a higher level of risk if doing so increases the quality of life for a patient/client. It is unlikely that proposals to completely eliminate all risks impacting on the organisation will always be feasible. Proposals should strike a balance between improving the risk situation, the level of resource input required and a realistic timescale in which to bring the risk faced to an acceptable level.

All action plans should clearly set out the action required to manage the identified risk. The Trust recognises it is not always possible to eliminate or reduce risks to the lowest level of rating and that some risks will have to be accepted at a high level. The process for acceptance of these risks is outlined in the Risk Acceptance Framework, Section 5.

In developing risk action plans consideration should be given where: -

- There are no control measures at all;
- Current control measures are ineffective; or
- Additional control measures are required to the existing effective controls in place.

1. An individual with explicit responsibility must be identified for ensuring the action is taken.
2. The name of this person together with a target date for completion of the action must be recorded against the proposed action in the plan.
3. A planned date for the first review of the risk assessment, to assess progress initially, should be agreed and recorded in the action plan.
4. This date should be determined by the initial risk rating.

A **predicted** risk rating once all control measures are implemented should be determined.

If there are anticipated resource implications associated with the action plan, details and costs should be recorded.

The relevant Trust manager should sign off each action plan and ensure the risk is managed according to the process outlined in the Risk Acceptance Framework.

The management of the risk must then be reviewed on an ongoing basis to:

- Monitor whether the risk profile is changing; and
- Gain assurance that the risk action plan is effective and to identify when further action is necessary.

Details of subsequent reviews should be recorded in the action plan, including the date of the review, a summary of the current position and a re-assessment of the risk rating. The risk rating may change as actions are completed and this should be recorded.

Section 9: Risk Acceptance Framework

The Trust recognises that it is impossible, and not always desirable, to eliminate all risks especially in the delivery of care to patients/clients. A mark of good risk management is the innovative and imaginative use of resources in finding ways to avoid or reduce risks whenever possible.

Fine and balanced judgments will be necessary regarding the health and welfare of individuals especially within a person centred approach to patient/client care. It is sometimes the case that a higher level of risk may be accepted to facilitate a new and innovative service, which increases the quality of life for patients/clients.

The risk management process should identify the hazard and apply appropriate risk assessment and management action plans. Regardless of the level of risk assessed, all risk assessments must be recorded in the risk register, monitored and reviewed when necessary, determined by the risk rating, to ensure desirable outcomes.

Despite thorough risk assessment and management action plans, things can still go wrong and it is therefore essential that there are controls in place to deal with this situation.

It is crucial that Business Continuity Plans/local emergency plans are in place for the management of situations in which control failure leads to material realisation of risk.

Definition of Risk Appetite and Tolerance

Definition of Risk Appetite
According to ISO 31000, a risk appetite definition is “the amount and type of risk that an organization is prepared to pursue, retain or take.”

Tolerance Is related to risk appetite. It is the level of variation the organisation is willing to accept around ***specific*** objectives. (Institute of Risk Management)

Risk Appetite General Statement

The Trust must take risks in order to achieve its aims and deliver beneficial outcomes to stakeholders. Risks will be taken in a considered and controlled manner. Exposure to risks will be kept to a level deemed acceptable by the Board

The risk appetite of the Trust is the decision on the appropriate exposure to risk it will accept in order to deliver its strategy over a given time frame. In practice, risk appetite should address several dimensions:

- The nature of the risks to be assumed;
- The amount of risk to be taken;
- The desired balance of risk versus reward;

The overarching areas of:

- Risk to patients / service users

- Organisational risk
- Reputational risk
- Opportunistic risk
- Financial risk

Risks throughout the organisation should be managed within the Trust's risk appetite, or where this is exceeded, action taken to reduce the risk."

Appetite Level	Described as
None	**Avoid** the avoidance of risk and uncertainty is a Key Organisational objective
Low	**Minimal** the preference for ultra-safe delivery options that have a low degree of inherent risk and only for limited reward potential
Moderate	**Cautious** the preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward
High	**Open** and be willing to consider all potential delivery options and choose while also providing an acceptable level or reward (and VfM)
Significant	**Seek** and to be eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk). Also described as **Mature** being confident in setting high levels of risk appetite because controls, forward scanning and responsiveness systems are robust.

The Trust recognises that its long term sustainability depends upon the delivery of its strategic objectives and its relationships with its patients, the public and strategic partners. As such, the Trust will not accept risks that materially impact on patient safety.
However, the Trust has a greater appetite to take considered risks in terms of their impact on organisational issues. The Trust's greatest appetite to pursue innovation and challenge current working practices in terms of taking opportunities where positive gains can be anticipated, within the constraints of the regulatory environment.

Risk Acceptance Framework Categorisations

The Risk Acceptance Framework for the Southern Trust applies a 'traffic light' system with regard to the categorisation of risks against the scale of very low, low, moderate and high. The categorisation of risk against these scales determines if a risk is acceptable or not, and the level and urgency of intervention required. The Risk Acceptance categorisation process should be applied as a guide. Individual managers are encouraged to consider the acceptance of risk on an individual case by case basis. This judgement should be used to inform the level and urgency of action required. The 'traffic light' system applied to the Risk Acceptance Framework is as follows:

Green Risks (Low)

Identified risks which fall in the green area are deemed as low (acceptable) risks and may require no immediate action, but must be monitored regularly to assess if and when action is required. These risks must be entered onto the local Risk Register.

Yellow Risks (Medium)

Identified risks which fall in the yellow area are deemed medium risk to the Trust but require action to reduce the risk. Responsibility for taking action would normally remain at a local level within the appropriate Directorates / Service Areas and be entered on the Team / Service Risk Register.

Where these risks cannot be managed locally they should be forwarded to the appropriate Directorate Governance Fora for consideration for further local action, resourcing or acceptance by the Directorate Governance Fora for the Directorate Risk Register.

These risks must be entered on the local risk register and where appropriate the Directorate Risk Register for information and monitoring purposes.

Amber Risks (High)

Identified risks which fall in the amber area are deemed high risk to the Trust and require prompt action to reduce the risk to an acceptable level. When risks cannot be reduced locally they should be submitted to the Directorate Governance Fora for consideration and recommended action, i.e. further local action, resourcing or acceptance.

Where these risks cannot be managed within the Directorate they should be referred to the Senior Management Team for consideration and/or addition to the Corporate Risk Register.

These risks must be entered on the local risk register and where appropriate the Directorate Risk Register.

Red Risks (Extreme)

Identified risks which fall in the red area are deemed extreme risk to the Trust and must be reported to the appropriate Director and Chief Executive. Immediate action is required to reduce the level of risks to an acceptable level. The appropriate Director will ensure the implementation of a time monitored action plan with regular reports to the Chief Executive and Governance Committee.

SMT will be the gate keepers of the Corporate Risk Register and will use the following criteria to inform their decision making in escalating risks to the Corporate Risk Register.

- The risk represents an issue that has the potential to hinder achievement of one or more of the corporate objectives
- The risk cannot be addressed at directorate level
- It requires further control measures to reduce or eliminate the risk
- It is likely to require considerable input of resources to resolve the risk (finance, people, time, etc)

These risks will be entered onto the Directorate, and if appropriate the Corporate Risk

Register(s) for monitoring by the SMT.

Where the identified risks have the potential to threaten the achievement of the Trust's corporate objectives, they will be escalated by the SMT to the Board Assurance Framework.

Any definition of risk must be pragmatic and time dependent as the passage of time will reduce the tolerance of risk once deemed acceptable. In an attempt to help prioritise all risks the following definitions should be applied as a guide to the management of risks by the Trust:

Definition of Acceptable Risk

As a guide the Trust considers green (low and medium) risks to be acceptable (as defined by the risk rating matrix, Figure 6).

This definition is to be used as a guide only and managers are encouraged to take action on green and yellow (low and very low) risks identified particularly when these risks can be easily eliminated or reduced.

Definition of Unacceptable Risk

The Trust considers all amber (high) and red (extreme) risks to be unacceptable (as defined by the risk rating matrix, Figure 6). Managers are expected to take immediate action on amber (high) and red (extreme) risks identified and document action taken.

Definition of Significant Risk

Those red (extreme) risks, which have been identified as potentially threatening the achievement of the Trust's objectives or represent significant gaps in controls / assurances, are escalated by the SMT Governance to the Board Assurance Framework.

In addition to these guidance notes, Directors, Directorates, Service Areas etc. should consider notifying the Governance Committee and Trust Board of frequently occurring lower graded risks via SMT.

The Corporate Risk Register will be reviewed monthly by the SMT. Trust Board review the Board Assurance Framework bi-annually in conjunction with a high level summary of the Corporate Risk Register.

The Corporate Risk Register is also shared with the Department of Health mid-year and year end as part of the accountability process.

Where the resolution of a risk includes funding implications that cannot be contained within the available budgets, a business case should be developed as part of the Trust's business planning process.

Risk Treatment / Action Planning

A risk action plan should be developed to document the management actions and controls to be adopted. The plans should involve:

- Formulating and selecting risk treatment options;
- Planning and implementing risk treatment;
- Assessing the effectiveness of that treatment;
- Deciding whether the remaining risk is acceptable;
- If not acceptable, take further treatment/action.

It is the responsibility of the Clinical and Social Care Governance Coordinators for the Directors of Acute, Children and Young People, Older People and Primary Care and Mental Health and Disability in conjunction with relevant Directors/Senior Managers/Heads of Service to develop and maintain risk action plans for Directorate/Departmental risk registers.

On the delegated authority of the Chair (the Chief Executive) of SMT Governance, the Board Secretary, is responsible for maintaining risk action plans for the Corporate Risk Register.

Risk action plans should be developed using the proforma (and maintained in a suitable electronic format) incorporating the following information:

- Risk ID Number
- The action to be taken and the risks such actions address.
- Identified individual(s) responsible for implementing the plan.
- Budgetary allocation (where appropriate)
- Timetable for implementation
- Details of mechanism and frequency or review of action plan

Risk Registers

Each Directorate maintains a risk register. Each Directorate has a forum in which these Risk Registers are monitored. Each Directorate Risk Register is owned by the Director for that Directorate. It is the responsibility of Clinical and Social Care Governance Coordinators for the Acute, Children and Young People, Older People and Primary Care and Mental Health and Disability Directorates to maintain Directorate level risk registers in conjunction with relevant Directors/Senior Managers/Heads of Service.

Risks identified at a corporate level will be recorded on the Corporate Risk Register which is managed by the Senior Management Team. It is reviewed by SMT review on a monthly basis and reported to the Governance Committee who review it on a quarterly basis providing challenge and advice. Based on the knowledge of risks identified, Directors will determine the level of assurance that should be available to them with regard to those risks.

With regard to both Directorate/Departmental and Corporate Risk Registers risks will be

entered in accordance with the risk rating and action guidance. Risk registers should be developed using the proforma attached in Appendix 1.

- Risk ID Number
- Source
- Risk title and description (including location and local details)
- Potential for harm
- Summary of current control measures
- Initial risk rating
- Action plan
- Nominated person responsible for each action
- Review date
- Monitoring arrangements
- Lead individual

Board Assurance Framework

The Board Assurance Framework is the tool used by the Board to identify high level risks to the delivery of the Trust's corporate objectives and provide assurances for the control and management of those risks. The Board Assurance Framework works 'top down' from the Trust's corporate objectives determining proactively, the high level risks and what controls and assurance processes are in place. As part of the process, the Trust Board is committed to discussing and making the connections between the corporate objectives, the high level risks that could affect achievement of those objectives and the range and effectiveness of existing assurance reporting. The Trust Board own the Board Assurance Framework and review it on a six-monthly basis.

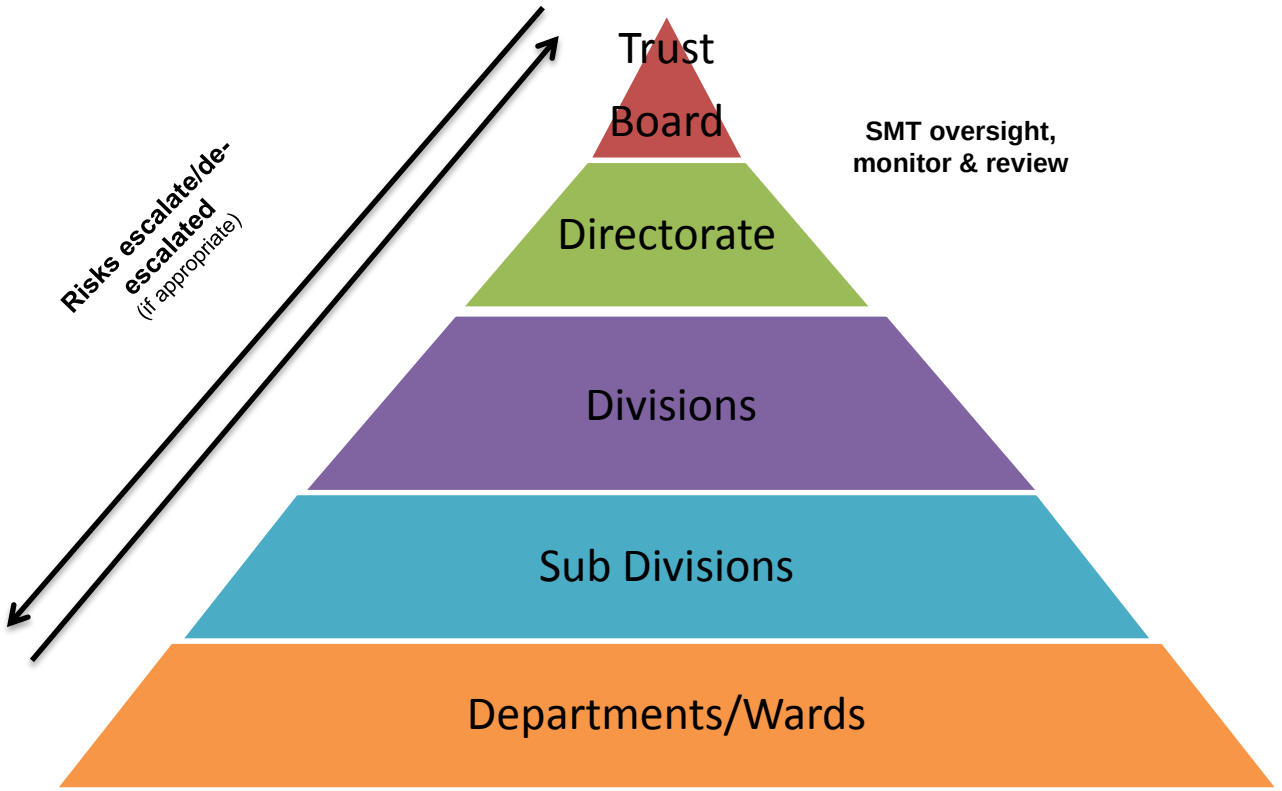
Risk Monitoring and Review

Monitoring and review should take place in all stages of the process. Monitoring and review includes planning, gathering and analysing information, recording results and providing feedback. The results of monitoring and review should be incorporated throughout the organisation's performance management, measurement and reporting activities.

Risk Escalation and De-Escalation

The grade of each risk not only determines who is responsible for managing the risk but also where it should be escalated to – Division, Directorate or Trust level. The timescale in which risks are escalated varies or assurance on the management of a risk varies according to the significance of the risk. This may be through routine monitoring systems or fast tracked. Senior Managers and Directors use judgement to determine the timescale for escalation, influenced by the impact the issue has on the delivery of safe, high quality care or organisational reputation.

It is the responsibility of the Chair of each group or committee to escalated risks, to ensure each escalated risk is reconsidered in the context of other risks already included in the Risk Register at that level. Each Risk Register should be reviewed to identify and understand themes in risks on the register, how this impacts on each other and the Trust and whether this identifies new risks or affects the grade of existing risks.
When actions to reduce a risk have been completed and the risk score is lowered to a level that no longer requires inclusion on a risk register, the risk can be de-escalated.



Assurance and Escalation Pyramid

Risk Owners

Each risk that is identified in a risk register will have a risk owner who will:-

- Ensure adequate and effective controls are implemented
- Review and update individual records regularly

Risk Recording and Reporting

The risk management process and its outcomes should be documented and reported through appropriate mechanisms

Risk Strategy Education and Training

The Trust is committed to the education and training of all staff which ensures the welfare and health and safety of patients, clients and the public.

Risk management training will be assessed and delivered by the Directorate Governance Teams based on organisational/staff needs. Directorates are required to maintain risk management training records, monitor attendance of staff at training, and report on risk management training to SMT Governance as required. Trust induction programmes will include standardised risk management training.

Appendix 1 – Trust Risk Assessment Form for Risk Register

SOUTHERN HEALTH & SOCIAL CARE TRUST		
RISK ASSESSMENT FORM		Risk ID No
Directorate:	Facility/Department/Team:	Date:
Where is this being carried out? (e.g. Trust premises/home of client/staff/ private nursing home etc)	Objective(s) i.e. Corporate, Legislative requirements etc.	
Risk Title: (Threat to achievement of objective) Description of Risk: (Describe the risk being assessed identifying who is at risk e.g. patient/staff/other care provider) **Outline the potential for harm:** (Consider injury to client, staff, litigation, etc.)		

Summary of current control measures: (Consider equipment, staffing, environment, policy/procedure, training, documentation, information - this list is not exhaustive).

Are these controls: (a) Effective or (b) Require Further Action *(if [b], complete Action Plan)*

Please list control measures considered but discounted and why (where appropriate):

Assessment of Risk	Likelihood e.g. Likely	Consequence/ Impact e.g. Moderate	Risk Rating L and C = RR e.g. Likely and Moderate = YELLOW

ACTION PLAN OF FURTHER CONTROL MEASURES REQUIRED (risk treatment):

Action/Treatment	Action Lead	Start Date	Target Date	Progress/Review Date
Date of first review (to be determined by risk rating)				

Predicted Risk Assessment once all control measures are implemented	Likelihood e.g. Likely	Consequence/ Impact e.g. Moderate	Risk Rating L and C =RR e.g. Likely and Moderate = YELLOW