NHS
Blood and Transplant

Board Meeting in Public

Tuesday, 02 December 2025

Title of Paper	Risk Management Framework	**Agenda No.**	4.2.1
Nature of Paper	☒ Official	☐ Official Sensitive	
Author(s)	Andrew Weal, Head of Compliance, Risk & Assurance		
Lead Executive	Helen Gillan, Director of Quality & Governance		
Non-Executive Director Sponsor	Ian Murphy		
Presenter(s) at Meeting	Helen Gillan		
Presented for	☐ Approval ☐ Assurance	☒ Information ☐ Update	
Is there a plan to communicate this to the organisation?	☒ Yes	☐ No	☐ Yet to be determined

Executive Summary

NHSBT's approach to risk management has matured since the previous risk framework was implemented. To support and continue the journey of positive risk maturity, the existing risk management framework has been updated. This update:

- ensures better alignment with the HM Treasury Orange Book and the associated suite of documents,
- it provides greater clarity of shall criteria, supporting consistency
- it removes areas previously open to interpretation

The attached framework is a full re-write of the previous manual.

Previously Considered by

Risk Management Committee October 2025
Audit, Risk and Governance Committee November 2025

Recommendation

The Board is asked to review and consider the information contained within the Risk Managemnent Framework

Risk(s) identified (Link to Board Assurance Framework Risks)

The Risk Management Framework aligns to all risks across NHSBT

Strategic Objective(s) this paper relates to:

☐ Collaborate with partners ☐ Invest in people and culture ☐ Drive innovation
☐ Modernise our operations ☐ Grow and diversify our donor base

Appendices:	

Risk Management Framework

Policy

NHS Blood and Transplant (hereafter referred to as NHSBT) is committed to ensuring the continuous delivery of safe, high-quality services and products. This commitment includes ensuring the on-going safety of donors, patients, service users, staff, and the public. The full policy statement can be found in BLP5.

Objective

This document outlines NHS Blood and Transplants risk management process, including associated roles and responsibilities. This document supports the consistent and effective management of risk across NHS Blood and Transplant

New Document – Replaces previous MPD1336

Roles

Responsibility for compliance with this document exists at all levels throughout NHSBT. Specific responsibilities are delegated to groups or posts as detailed within Appendix 2.
General:

- All Staff
- Supervisors & Line Managers
- Senior Management Teams (SMT) & Oversight Bodies (Includes CEO, Executive Directors, Non-Executive Directors and Oversight Bodies)
- Business Partner Risk Leads
- Clinical Safety Officer
- Administrative Role in NHSBT's Risk Management System
- Authors & Owners of Risk Document

Individuals:

- Chief Executive Officer (CEO)
- All Executive Directors (Portfolio Owner)
- Director of Strategy
- All Non-Executive Directors
- SMT (Senior Management Team) Chair (or chair of equivalent risk review group)
- Risk Managers
- Risk Leads
- All Heads of Centres

Oversight Bodies:

- NHSBT Board
- Executive Team
- Audit, Risk & Governance Committee (ARGC)
- Risk Management Committee (RMC)
- Risk Leads Forum
- Senior Management Teams (SMT)
- Centre Partnership Committees (CPC)
- Corporate Risk Team

Other Roles:
- Risk Owners
- Action Owners

Table of Contents

1.0 Purpose and scope

This framework outlines NHS Blood and Transplant's (NHSBT) integrated approach to risk management, to be adopted across the organisation. It is based on the principles and guidance set out in HM Treasury's Orange Book – Management of Risk: Principles and Concepts.

This document is intended for use by all individuals involved in the design, operation, and delivery of risk management activities within NHSBT. The principles set out in this framework apply to all staff, regardless of grade or employment status. This includes permanent and temporary employees, agency staff, contractors, and others working on behalf of the organisation.

In line with the Orange Book, the term 'shall', as used throughout this framework, denotes a mandatory requirement.

2.0 Introduction

In line with NHS Blood and Transplant's (NHSBT) commitment to the continuous delivery of safe, high-quality, and cost-effective products and services, NHSBT adopts a proactive and systematic approach to risk management.

This includes the early identification, assessment, and management of risks that may affect staff, donors and/or patient safety, service delivery quality, legal requirements' regulatory compliance or long-term sustainability.

Risks are managed within a structured governance framework to ensure they are appropriately escalated, monitored, and addressed at the right level. Where necessary, proportionate and timely actions are taken to mitigate risks, inform decision-making, and support continuous improvement.

NHSBT adopts the principles set out in HM Treasury's Orange Book: Management of Risk – Principles and Concepts, which provides the foundation for effective risk management across government and public sector bodies. These principles support an integrated, evidence-based approach to risk that aligns with recognised best practice and regulatory expectations.

3.0 Governance and Leadership

The Chief Executive (Accounting Officer), supported by the Assistant Director Risk and Resilience (Chief Risk Officer), has overarching responsibility for the organisation's approach to risk management, and is accountable for ensuring the effective design and systematic implementation of risk-related policies, procedures, and practices. This includes the processes for identifying, assessing, treating, monitoring, and reporting risks.

Day-to-day responsibility for the development, implementation, and ongoing monitoring of the risk management framework is delegated to the Head of Compliance, Risk and Assurance, supported by the Corporate Risk and Assurance Team.

4.0 Risk Management - Overarching Requirements

Risk management is an essential component of governance and leadership and is fundamental to how NHSBT is directed, managed, and controlled at all levels. This principle is embedded across the organisation through the following commitments:

- Continuously enhancing governance arrangements to ensure they remain effective, transparent, and responsive to emerging risks.
- Embedding and promoting a strong risk management culture, where staff at all levels understand their role in identifying and managing risk.
- Ensuring the Board regularly and frequently reviews and considers the nature and extent of NHSBT’s principal risks, as part of its oversight responsibilities.

This approach aligns with the principles set out in HM Treasury’s Orange Book and supports a consistent, organisation-wide understanding of risk, enabling informed decision-making, resilience, and continuous improvement in service delivery.

5.0 Risk Reporting

As part of its governance commitments, the organisation produces a range of risk reports tailored to the specific requirements of its oversight committees. Reports will be taken using data derived directly from the risk management system with the expectation that these are maintained by risk owners and responsible managers and committees. These reports include:

5.1 Operational Risk Visibility via Directorate Dashboards

Operational risks are accessible through the Directorate Dashboard, which enables Risk Review Groups and SMTs to tailor the visible content to suit the agenda and focus of each meeting.

5.2 Deep Dive Risk Reports to RMC and relevant Board Committees

The ARGC or committees with delegated responsibility review risks in a Deep Dive on a rotational basis. Each Deep Dive explores a principal risk and its contributory risks, with controls, assurances and actions.

5.3 Risk Performance Reports for the Risk Management Committee (RMC)

These reports provide an overview of the organisation's performance against agreed risk Key Performance Indicators (KPIs), supporting the RMC in assessing overall risk effectiveness.

5.4 Quarterly and Annual Reports to the RMC

Structured to meet the requirements outlined in the RMC Terms of Reference, these reports provide comprehensive updates on risk activity, key developments, and performance trends.

5.5 Annual Risk Report for the Audit, Risk and Governance Committee (ARGC)

This report outlines the organisation's overall risk profile and management performance over the past 12 months. It also includes the Corporate Risk Team's objectives for continuous improvement against the risk management framework.

5.6 Board Assurance Framework (BAF)

The BAF provides the Board with detailed information on the status, management, and movement of each principal risk. It also explains how contributory risks impact these principal risks and the overall risk landscape.

6.0 External Stakeholders

The Corporate Risk and Assurance Team is responsible for producing risk reports required by the Department of Health and Social Care (DHSC), ensuring the content aligns with DHSC's specific reporting requirements.

In addition, the Corporate Risk and Assurance Team retains responsibility for providing reports—or contributing relevant information to reports—as required by other external stakeholders.

7.0 Recording Risk in the Risk Management System

NHSBT's risk management system serves as a central tool for supporting assessment, and documentation of risks across the organisation. The system enables the capture of comprehensive information for each risk.

The primary output of the risk management system is the Corporate Risk Register. This register provides visibility and transparency over the key risks that could potentially impact the achievement of NHSBT's strategic objectives. By maintaining a robust Corporate Risk Register, NHSBT ensures that risks are visible, monitored systematically and managed proactively.

8.0 Three- Line Model

NHSBT's adopts the 'Three Lines' model to inform risk management activities. This approach is fully aligned with the assurance mapping framework. This alignment supports clarity in the allocation of responsibilities and facilitates a comprehensive view of assurance activities and coverage.

9.0 Risk Appetite

Risk appetite is defined as:

the level of risk it is willing to accept in pursuit of its strategic and operational objectives

The Board sets and reviews the organisation's risk appetite on an annual basis. The process underpinning this assessment is detailed in BLP5: Risk Policy, which outlines how risk appetite is determined, communicated, and applied across the organisation.

Risk appetite provides a structured framework that supports informed decision-making by:

- Defining target and acceptable risk positions
- Clarifying the behaviours and levels of control associated with different levels of risk

By setting clear risk appetite thresholds, NHSBT ensures that risks are taken deliberately and responsibly, balancing opportunity and control to support sustainable performance and effective governance.

Risk appetite is aligned to the primary risk impact areas, each having an appetite statement, which includes the required behaviours.

The risk appetite levels set by the Board are:

Risk Limit – A level of risk that NHSBT is unable to accept or tolerate. Risks assessed at this level shall be escalated to the Risk Management Committee and reported to the Board through the Board Assurance Framework (BAF) and the monthly Board Performance and Risk report.

Judgement Zone – A level of risk that is generally considered unacceptable and shall have actions in place to manage and reduce it. These risks shall be subject to frequent SMT review.

In certain circumstances, the responsible Senior Management Team (SMT) may agree to tolerate a risk within the Judgement Zone for a defined period (not exceeding six months), if they result in a recognised benefit, provided that adequate controls are in place and a clear plan exists to reduce the risk to an acceptable level.

Tolerable Level – In situations where it is neither practical nor affordable to fully manage risks to the optimal level, the responsible Senior Management Team (SMT) may determine that the risk is at a tolerable level and agree to accept it.

Risks assessed as tolerable shall be subject to dynamic reviews based on the environment and level of uncertainty, however these reviews shall be undertaken on an annual basis as a minimum, should there be no change. These risks require effective controls and ongoing action monitoring.

If the risk profile changes and the score increases, moving the risk into the Judgement Zone or higher, the behaviours and management approach must immediately align with the requirements of the new risk appetite.

Optimal Level – This represents the desired level of risk within which NHSBT aims to operate. Risks at this level are considered acceptable and well-managed but still require ongoing monitoring and regular review to ensure they remain within the defined risk appetite. Risks recorded at this appetite level, shall be supported by performance indicators and other measures, demonstrating that relevant systems are in control.

Consideration shall be given to risk(s) recorded at this level to determine whether the uncertainty driving the risk has been sufficiently addressed and whether the risk can be archived, with a view to reactivating it should the situation change.

Low Risk – The risk has been assessed and determined to pose minimal or negligible threat to the achievement of NHSBT's objectives.

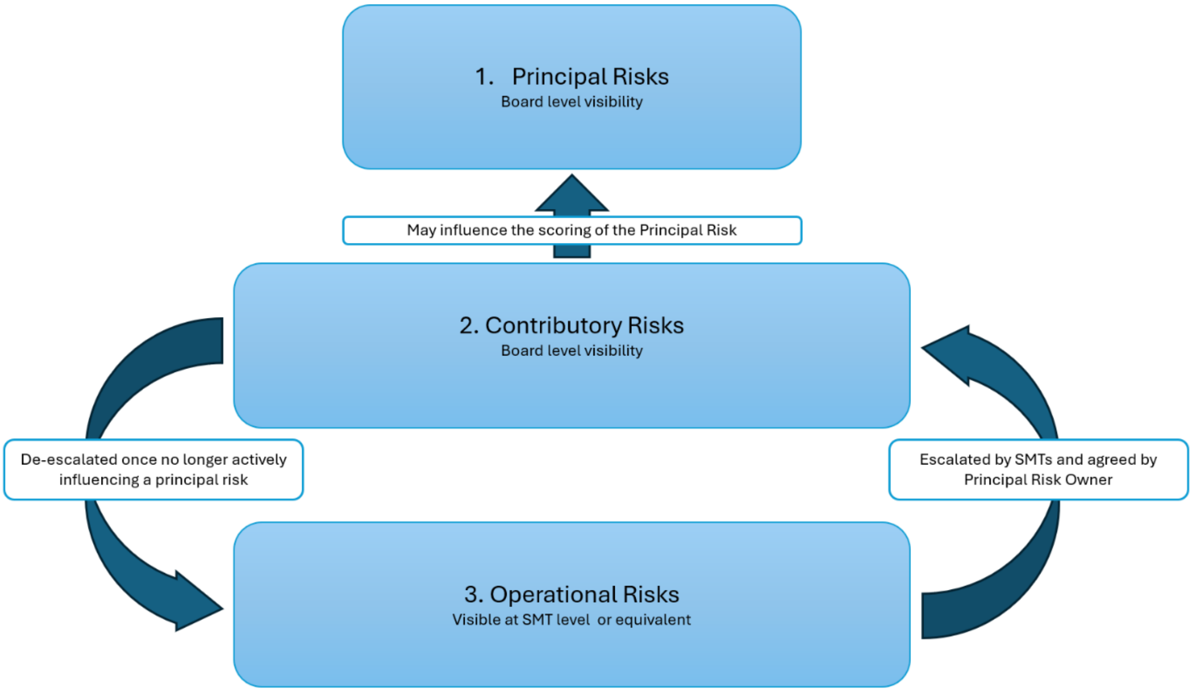
While it remains the responsibility of the Senior Management Team (SMT) to decide how to approach these risks, it is generally unnecessary for such risks to absorb significant resources or finances to reduce them further. Consideration shall be given to risk(s) recorded at this level to determine whether the uncertainty driving the risk has been sufficiently addressed and whether the risk can be archived, with a view to reactivating it should the situation change.

10.0 Risk Structure and Oversight

NHSBT's risk management approach is structured around three layers of risk, each supported by dedicated monitoring and oversight mechanisms to ensure effective governance, accountability, and escalation across the organisation.

It is important to note that the risk management processes outlined in section 12, apply uniformly to all risks, regardless of their position within the three-tiered risk structure. This ensures a consistent and comprehensive approach to risk identification, assessment, treatment, monitoring, and reporting throughout NHSBT.

10.1 Diagram 1 Risk Levels and Flow


1. Principal Risks
Board level visibility
May influence the scoring of the Principal Risk
2. Contributory Risks
Board level visibility
De-escalated once no longer actively influencing a principal risk
Escalated by SMTs and agreed by Principal Risk Owner
3. Operational Risks
Visible at SMT level or equivalent

The risk structure is described further below:

10.2 Principal Risk

A principal risk is defined as:

a risk that could significantly and adversely impact NHSBT's ability to fulfil its obligations under the Establishment and Constitution Order 2005

The Board is responsible for determining the nature and extent of the principal risks to which the organisation is exposed. While oversight and management of principal risks are delegated to the relevant Executive Directors (who will be designated Risk Owners), the Board retains overall accountability.

Principal risks are monitored through the Board Assurance Framework (BAF), which provides a structured mechanism for tracking the status of principal risks, assessing the effectiveness of controls and mitigation actions and ensuring alignment with strategic priorities.

The Board conducts a full review of principal risks annually, with interim updates provided as necessary to ensure that emerging risks and significant changes are appropriately considered and addressed.

Principal risks are stand-alone risks; however, their risk scoring and risk appetite will be influenced by the contributory risks related to them.

10.3 Ownership and Articulation of Principal Risks

Each principal risk is owned by the responsible Executive Director, who is accountable for both its articulation and its oversight. If amendments to the risk articulation are required, the Director is responsible for approving the revised wording. Any changes are subsequently presented to the Risk Management Committee (RMC) and the relevant Board committee for notification and oversight.

10.4 Governance Oversight of Principal Risks

Each Principal Risk shall be assessed monthly. The assessment will be conducted by the Director assigned, as the owner of the respective risk. Following each assessment, the responsible Director shall provide a narrative update (or approve a narrative provided to them). This narrative shall:

- Clarify the status of the risk; and
- Outline actions being taken to reduce risk scores that remain outside of the organisation’s defined tolerance levels.
- In instances where there is no change to the risk status, the Director shall provide an overview of ongoing actions and initiatives related to the management of the risk.

All narrative updates from Directors shall be made visible within the Board Assurance Framework (BAF).

The RMC and the ARGC are the key oversight committees actively monitoring principal risks, with responsibility for clinical risks delegated to the Clinical Governance Committee and for staffing risks delegated to the People Committee. ARGC shall be updated on any risk that is reviewed by these committees. The Board reviews each principal risk—its articulation and associated risk appetite—on an annual basis, ensuring alignment with NHSBT’s strategic direction.

10.5 Contributory Risks

A contributory risk is defined as

a risk that actively influences a principal risk to which it is related.

These risks are strategic in nature and provide insight into the underlying causes, drivers, or aggravating factors that influence a principal risk. Contributory risks are aligned to the primary impact area where the impact would be most significantly felt.

Contributory risks shall be owned and managed by the business area in which the risk primarily resides, with responsibility for regular and ongoing oversight held by the Senior Management Team.

Contributory risks are dynamic and shall not remain permanently fixed to a principal risk. Their relevance and influence must be reviewed regularly.

When a contributory risk is no longer actively influencing a principal risk—for example, when it has been effectively mitigated, or is confirmed as a low risk, and no longer warrants Board or Executive level visibility—it shall be managed as follows:

- Archived, if the risk has been fully addressed and no longer requires active management; or
- Transferred to an Operational Risk Register, where it will be managed by the relevant business area as part of ongoing operational oversight.

This approach ensures that risk ownership and focus remain current, targeted, and proportionate to the level of threat posed.

10.6 Visibility and Monitoring of Contributory Risks

Contributory risks are included within the Board Assurance Framework (BAF) to provide visibility to the Board and Executive Team of risks that require full organisational awareness and oversight.

However, a key principle of contributory risk management is that these risks must not become permanently fixed to a principal risk. Their inclusion in the BAF shall be based on ongoing relevance and significance. A contributory risk that no longer warrants Board or Executive-level visibility, discussion, or senior decision-making shall be unrelated to a principal risk allowing focus to be maintained on risks actively influencing the principal risk.

10.7 Oversight and Review Mechanisms

Contributory risks are reported regularly to the Risk Management Committee (RMC). They are also reviewed as part of the Audit, Risk and Governance Committee (ARGC) Principal Risk Deep Dives.

Monthly principal risk reviews, completed by the Director responsible for the principal risk include a review of each related contributory risk. The owner (or appropriate deputy) of an associated contributory risk shall attend the review meeting and provide sufficient updates and forecast of the status of the contributory risk.

It is the responsibility for the Director owning the principal risk to:

- Hold contributory risk owners to account for attendance at review meetings
- Challenge the status and relevance of each contributory risk
- Determine whether a contributory risk continues to actively influence the principal risk
- Recommend removal of the contributory risk when appropriate. The Risk and Assurance Manager will facilitate communication and dissociation of the contributory risk.

10.8 Ownership and escalation of Contributory Risks

The Chair of the Senior Management Team (SMT) for each business area holds ownership and overall responsibility for the contributory risks within their remit. This responsibility can be delegated, by the SMT Chair to an Assistant Director, or appropriate Head of Function.

If the SMT determines that an operational risk has escalated to a point where it is actively impacting on the delivery of objectives or influencing a principal risk, the SMT shall consider its escalation to contributory risk status.

In such cases:

- The Risk and Assurance Manager shall facilitate communication with the relevant Principal Risk Owner who shall consider the operational risk for approval as a contributory risk.
- In the event the Principal Risk owner does not approve the risk, this shall be escalated to the RMC for discussion.

The SMT shall:

- Review their contributory risks at each SMT meeting, and
- Gain assurance that these risks are being appropriately managed and mitigated.

10.9 Governance Oversight of Contributory Risks

Contributory risks are subject to governance oversight through the following mechanisms:

- The Risk Management Committee (RMC) and the Audit, Risk and Governance Committee (ARGC) shall receive regular reports and updates on contributory risks.
- The Board shall have visibility of contributory risks via the Board Assurance Framework (BAF), ensuring awareness of risks that require organisational-level attention without unnecessarily escalating operational matters.

This structured process ensures that contributory risks are managed at the appropriate level, escalated when necessary, and removed when no longer relevant, preserving the integrity and focus of the overall risk management framework.

10.10 Operational Risks

Operational risks are defined as:

those that have the potential to disrupt the achievement of business area objectives or day-to-day activities.

These risks may arise from inadequate or failed internal processes, people, systems, or infrastructure, or from external events.

Responsibility for identifying, managing, and mitigating operational risks lies with the relevant business areas or the appropriate supporting group service areas.

All risks identified across NHSBT, irrespective or the source, shall follow the principles contained within this framework. This includes health, safety and wellbeing, projects and programmes, incidents and complaint management.

10.11 Visibility and Monitoring of Operational Risks

Operational risks are visible through the Directorate Dashboard, which enables Risk Review Groups and SMTs to tailor the content to suit the agenda and focus of each meeting.

Operational risks that fall within the Judgement Zone for a period greater than six months or exceed established Risk Limits are reported by the Corporate Risk Team to the Risk Management Committee (RMC) for awareness and, where necessary, decision-making.

Operational risks are also the subject of discussion and review at the Risk Leads Forum.

10.12 Ownership of Operational Risks

All operational risks shall be owned and managed by a named individual. Oversight and monitoring of operational risks will generally reside with the business area most directly impacted. Where an operational risk affects multiple business areas, ownership typically rests with the area experiencing the greatest potential impact. However, ownership can be agreed upon collaboratively between the relevant stakeholders, based on the nature and scope of the risk.

Duplicate risks shall not be recorded in the risk management system. Where duplicates are identified, the Risk Manager shall work with the relevant business areas to remove them and ensure appropriate stakeholder involvement in managing the remaining risk.

11.0 Centre Based Risks

A centre-based risk is defined as

A risk that impacts on the safety and suitability of NHSBT's estate

There are occasions where greater visibility of a risk's impact area is required. An example of this is centre-based risks. It is essential that NHSBT maintains visibility and understanding of all risks affecting a specific location or centre, with clear identification of where each risk applies and who holds ownership.

Responsibility for managing corporate level risks, such as fire, flooding, or Legionella—rests with the appropriate Group Service, for example, Estates and Facilities.

Risks that are the responsibility of functional areas located within a centre shall be relevant and specific to their operations. For example, a risk to a functional area may be defined as the inability to continue service provision due to an unsuitable environment. In such cases, the primary risk is the disruption to service delivery, regardless of the underlying cause. These risks shall be recorded within the Operational Risk Register, however, shall be assigned the relevant category on the risk management system, allowing them to be separately reported.

12.0 Risk Management Process

Main Principle - Risk management processes shall be structured to include:

1. Risk identification and assessment to determine and prioritise how the risks can be controlled and managed
2. The design and implementation of risk treatment options that support achievement of intended outcomes and manage risks to an acceptable level
3. The design and operation of integrated, insightful and informative risk monitoring

4. The availability of timely, accurate and interactive risk reporting to enhance the quality of decision-making and to support management and oversight bodies in meeting their responsibilities.

12.1 Risk Management Guidance and Support

The Risk and Assurance team shall provide, to all business areas across NHSBT, ongoing guidance and support across all the four stages listed above.

12.2 Risk Identification and Assessment

The Orange Book: Management of Risk – Principles and Concepts, defines risk as "the effect of uncertainty on objectives." While each potential risk may carry some importance, it is essential to assess and measure risks to understand their significance.

A core element of effective risk identification and assessment is determining which uncertainties truly matter—specifically, those uncertainties that could significantly impact the achievement of objectives.

Risk identification is the first step in the risk management process. It involves a systematic approach to identifying, documenting, and categorising potential risks that may hinder a business area or NHS Blood and Transplant (NHSBT) from fulfilling its responsibilities and achieving its goals.

It is important to note that risk identification and scoring should not be carried out in isolation. Gathering input from a range of stakeholders ensures a more accurate and well-rounded assessment of risk levels. Risk and Assurance Managers are available to provide support, advice, and guidance throughout this process. Bite-size guidance videos covering risk identification and assessment are available on the Risk Management Intranet page.

12.3 Risk Articulation

Risks shall be articulated in a manner that ensures the nature of the risk is clear, easily understood, and recognised by all relevant stakeholders. Adopting this format helps ensure that the actual risk to the achievement of objectives is clearly identified and effectively communicated.

Risks recorded in the risk management system shall follow NHSBT's agreed format: "There is a risk that [event] caused by [cause], resulting in [impact]."

- The Risk – The actual uncertain event or condition that could impact the achievement of objectives.
- The Cause – The underlying condition or factor that gives rise to the risk.
- The Result – The potential impact or negative outcome if the risk materialises.

12.4 Risk Analysis

Risk analysis is a dynamic process carried out regularly throughout the lifecycle of a risk.

Once a risk has been identified, analysis involves a detailed examination of its nature, causes, and potential impact. The primary purpose of this stage is to develop a clear understanding of the risk's characteristics, enabling informed decision-making and effective prioritisation.

Risk analysis shall be repeated at regular intervals or whenever changes occur in the risk profile or operating environment. Risk analysis shall be used in conjunction with NHSBT's Risk Appetite. Ongoing analysis ensures that the risk remains accurately described and scored, and that the mitigating controls remain effective and continue to operate as intended.

Risk analysis shall be conducted using NHSBT's standardised approach, which includes, at a minimum, the following four elements. This model ensures a consistent and systematic method for assessing risks across the organisation:

- Primary Risk Impact Area – The domain where the consequences of a risk materialising would primarily be felt. This is used to determine the risk appetite level.
- Likelihood – The probability of the risk materialising, expressed through likelihood scoring.
- Consequence (Impact) – The potential consequences if the risk occurs, reflected through consequence scoring.
- Control Identification and Effectiveness – The identification of controls which when in place mitigate the risk, and an assessment of the effectiveness of the controls.

12.5 Risk Scoring

NHSBT scores its risks at three different stages of the risk life cycle:

Inherent risk - This refers to the level of risk that exists naturally due to the characteristics of an activity, product, system, or situation — before any internal controls, safeguards, or mitigation strategies are applied. It represents the raw or untreated risk, providing a baseline for evaluating how effective existing or proposed controls are.

Residual risk - is the level of risk that remains after existing risk mitigation efforts have been applied — including the implementation of controls, processes, or other safeguards designed to reduce or eliminate the original (inherent) risk.

Target risk - represents the anticipated level of risk after all planned mitigation actions have been fully implemented. The target date is typically set shortly after the final mitigation action is completed. This brief interval allows the Risk and Action Owners to assess whether the actions taken have successfully achieved their intended goals and addressed any identified gaps or weaknesses.

Risk scoring at all levels, wherever possible, shall be based on the best available information, to ensure consistency, objectivity, and accuracy in assessing risk levels. NHSBT provides risk scoring guidance tables to support the consistent assessment of risks. However, these tables shall be used in conjunction with relevant evidence and contextual information.

12.6 Risk Evaluation

Risk evaluation involves comparing the results of the risk analysis with the organisation's risk appetite - level of risk that NHSBT is willing to accept. This stage enables informed decision-making regarding the appropriate course of action and, where necessary, the identification of additional control measures.

Possible risk response options include:

- Tolerate the Risk – Retaining the risk based on an informed decision, where the residual risk level is considered acceptable within NHSBT's risk appetite.

- Treat the Risk – Taking action to remove the risk or reduce its likelihood and/or impact. This may involve implementing additional controls, mitigation strategies, or contingency planning.

- Transfer the Risk – Reallocating the risk to a third party, where appropriate, through mechanisms such as insurance, outsourcing, or the use of external experts.

- Terminate the Risk – Eliminating the risk by deciding not to start or continue with the activity that gives rise to it, where feasible.

The outcome of the risk evaluation process must be documented, communicated, and validated at appropriate levels within the organisation. All risks shall be subject to regular review and revision to reflect changes in their nature, likelihood, and impact, in recognition of the dynamic environment in which NHSBT operates.

13.0 Control Planning

An internal control is a mechanism or process designed to proactively modify, manage, or reduce inherent risk to a tolerable or desirable level. Once controls are applied to a risk, the remaining level of exposure is referred to as the residual risk.

13.1 Types of Internal Controls

Internal controls influence risk at various stages and shall be considered as part of the risk assessment and treatment process. NHSBT recognises the following categories of control:

1. Preventive Controls - Proactive measures designed to prevent undesirable events from occurring. Examples: Access controls, segregation of duties, mandatory training.

2. Directive Controls - Controls that provide guidance, instructions, or expectations to promote desired behaviours or outcomes. While they guide behaviour, they do not prevent undesirable actions on their own. Examples: Codes of conduct, standard operating procedures (SOPs), safety signage.

3. Detective Controls - Measures designed to identify and alert to errors, irregularities, or adverse events after they have occurred. Examples: Audits, inventory reconciliations, financial statement reviews, alarms, smoke detectors.

4. Corrective (Reactive) Controls - Controls that take effect after an issue has been detected, aiming to correct, contain, or prevent recurrence. Examples: Incident investigations, business continuity plans, corrective action plans, post-incident reviews.

13.2 Application and Monitoring of Internal Controls

All internal controls shall be:

- Proportionate to the level and nature of the risk
- Monitored and reviewed regularly for effectiveness

This structured approach ensures that controls not only exist but are actively influencing and reducing risk in a measurable and transparent way.

13.3 Principal Risk Controls

Assurance mapping shall serve as the primary method for identifying and documenting controls associated with each Principal Risk. These controls will provide the Board with a clear understanding of both the nature and effectiveness of the corporate controls in place to mitigate each Principal Risk.

14.0 Risk Validation and Entry into the Risk Management System:

Once the risk assessment is complete, including clear articulation and scoring, the risk must be validated and formally accepted by the relevant Senior Management Team (SMT) or the Risk Review Group.

Only after this validation process can the risk be added to the Risk Management System.

Important: Under no circumstances should draft or incomplete risks be entered into the Risk Management System, as they will automatically appear in risk dashboards, potentially leading to confusion or misinterpretation.

This ensures that only verified and approved risks are visible and used to inform decision-making at all levels of the organisation.

14.1 Developing and Documenting Risk Treatment Actions

To effectively address identified gaps or weaknesses in controls, an assessment must be conducted to determine the most appropriate and efficient corrective actions. This assessment shall include engagement and collaboration with key stakeholders to ensure that proposed actions are realistic, cost-effective, and capable of delivering the required outcomes.

14.2 Risk Monitoring

Risk management shall be a dynamic and ongoing process, ensuring Risk Owners maintain continual awareness of their risk profiles and are able to respond effectively to any changes. Risk details and associated scores must be regularly reviewed and updated to reflect the current level of risk accurately. Risks shall be reviewed and managed in line with the risk appetite.

15.0 Continuous Improvement

The Corporate Risk and Assurance Team is responsible for the ongoing monitoring and continuous improvement of all components of the risk management framework — including policy, guidance, tools, and education — to ensure it continues to meet the evolving needs of the organisation.

The team is also responsible for regularly benchmarking the organisation’s risk maturity against the Orange Book Risk Maturity Model, and for ensuring that a realistic and actionable improvement plan is in place to drive continuous development of the framework.

16.0 Integration

Risk management shall be an integral part of all organisational activities to support decision-making in achieving objectives.

The assessment and management of opportunity and risk shall be an embedded part of, and not separate from:

- setting strategy and plans
- evaluating options and delivering programmes, projects or policy initiatives
- prioritising resources
- supporting efficient and effective operations
- managing performance
- delivering improved outcomes

The Chief Executive as the Accounting Officer, supported by senior management, shall ensure that risks are transparent and considered as an integral part of appraising options, evaluating alternatives and making informed decisions.

17.0 Collaboration

Risk management shall be a collaborative process, informed by the best available information and expertise.

The Chief Risk Officer, supported by the Risk Management Committee and the Audit and Risk Assurance Committee, shall ensure that all elements of an effective risk management framework are in place. This framework shall address all types and sources of risk.

All business areas across NHSBT shall carry out their risk management responsibilities systematically, drawing upon the knowledge and perspectives of experts and stakeholders. The Corporate Risk and Assurance team is available to provide support and guidance as required.

Each business area within NHSBT shall play an integral role in identifying, assessing, and managing risks that may arise and threaten the successful achievement of objectives.

The Corporate Risk and Assurance team shall provide expert judgement and advice to the Accounting Officer to:

- Develop and implement realistic strategies, planning and programmes
- Support effective risk-based decision-making.
- Ensure risks are identified, evaluated, and addressed appropriately.
- Promote consistency in risk management practices across the organisation.
- Facilitate assurance and reporting mechanisms that provide clear visibility of key risks and mitigations.
- Determine the nature and extent of the risks that the NHSBT is willing to take to achieve its objectives
- Design and operate internal controls in line with good practice

Appendix 1: Risk Ownership

To support the effective management of risk, ownership and responsibility shall be managed via the following structure:

Senior Level Ownership and Oversight

The Portfolio Owner and the Responsible Operating Unit are accountable for the senior-level oversight of risks and the associated risk registers.

- **Portfolio Owner**
- **Role:** The individual with responsibility for the business area to which the risk applies. For principal risks this will be an Executive Director, contributory risks will be owned by a Director or Assistant Director and operational risks by an Assistant Director or Head of Function.
- **Accountability:** Owns the risk at an appropriate level ensuring alignment with relevant objectives.

- **Responsible Operating Unit (OU)**
- **Role:** The committee with oversight responsibility. This may be a Board level committee or an SMT.
- **Accountability:** Ensures that the risk is being effectively managed and mitigated in accordance with organisational risk appetite and policy.

Risk Management Activities

Risk management activities are carried out by named individuals with clearly defined responsibilities. It should be noted that the Risk Owner and the person the risk is Managed by can be the same individual. In such cases, that person retains full responsibility for fulfilling the duties associated with both roles.

- **Managed by**
- **Role:** Oversees and facilitates the risk management process.
- **Responsibilities:**
    - Allocate the risk to an appropriate Risk Owner.
    - Ensure the risk is effectively managed and monitored.
    - Maintain timely updates in the risk management system.
    - Keep the Portfolio Owner informed of all relevant developments.
    - Ensure that Judgement Zone and Risk Limit risks are continuously presented to the appropriate Senior Management Team(s) (SMTs).
- **Risk Owner (Risk Lead & Managers)**
- **Role:** Day-to-day manager of the risk.

- **Responsibilities:**
    - Conduct regular reviews of the risk.
    - Ensure the risk management system is updated after each review or as necessary.
    - Implement controls and actions to mitigate the risk.

Risk Administrator

Role: This role is typically held by someone working within the relevant business area and is responsible for updating the risk management system. It is recognised that this role may not exist in all areas of the organisation.

This is not a function performed by the Risk and Assurance Team; however, guidance can be provided where needed.

- **Responsibilities:**
    - Has system access and authority to input updates.
    - Records notes and updates provided by the Risk Owner or Risk Manager.
    - Supports system accuracy and completeness.

Risk Leads

Risk Leads act as risk champions, coordinating and overseeing risk management activities within their directorate, function, or department. They play a key role in promoting and developing a positive risk culture within their area, including at Senior Management Team (SMT) meetings, by encouraging open, informed, and honest discussions about risk.

Responsibilities include, but are not limited to:

- Coordinating risk management activities within the business area, ensuring compliance with and alignment to the Risk Management Framework.
- Representing the business area at the Risk Leads Forum.
- Presenting all business area risks recorded at Risk Limit or within the Judgement Zone to the appropriate Senior Management Team (SMT).
- Presenting risk details—including the proposal of new risks—at SMT meetings and other relevant governance or oversight meetings.
- Ensuring the Business Area Director is kept informed of relevant risk information that requires Director-level oversight or input and supporting the inclusion of risk as a standing agenda item at Directorate SMT meetings.

Risk and Assurance Managers

Risk and Assurance Managers are responsible for the development, implementation, and ongoing monitoring of NHSBT's Risk Management Framework. To fulfil these responsibilities, their role includes:

- **Promoting a Positive Risk and Assurance Culture** - visibly championing risk and assurance management across the organisation, ensuring NHSBT's commitment to managing risk is applied in a consistent, systematic, and transparent manner.
- **Supporting Business Areas** - acting as a key business partner for allocated areas by supporting the identification, assessment, and monitoring of risks, and building effective working relationships with Risk Leads.
- **Engaging in Senior Management Team (SMT) Meetings** - attending and contributing to SMT meetings within business areas to facilitate and support robust risk discussions.
- **Strategic Risk Engagement** - participating in cross-business risk discussions to support the alignment of risk management with the development and delivery of strategic objectives.
- **Risk Register Oversight** - assisting Risk Leads in maintaining and monitoring their Risk Registers and supporting the development and articulation of new risks.
- **Framework Development and Compliance** - contributing to the development, maintenance, and implementation of NHSBT's Risk Management Framework, ensuring alignment with the HM Treasury Orange Book and other regulatory requirements.
- **Guidance and Tools** - developing and maintaining supporting guidance materials, including bitesize guides, to assist in the consistent application of the framework.
- **Education and Support** - providing guidance, education, and ongoing support across NHSBT to ensure effective and consistent use of the risk management framework and supporting systems.

Appendix 2: Roles and Responsibilities

All Staff

All staff members, including those working on behalf of NHSBT (e.g., temporary, agency, and contracted staff), are responsible for maintaining risk awareness. They must identify and escalate any risks appropriately to their supervisor or line manager. Additionally, they are expected to familiarise themselves with and adhere to NHSBT policies and procedures, and to attend all mandatory and relevant training courses.

Supervisors and Line Managers

Upon notification of a risk (from any source), Supervisors and Line Managers (including Risk Leads) are responsible for determining the appropriate course of action, including whether a formal risk assessment should be initiated.

Supervisors or Line Managers must provide timely feedback to the staff member who reported the risk, clearly explaining how the concern will be managed (e.g. “no further action required” or “a formal risk assessment will be undertaken”).

All validated risks must be reviewed and approved at Senior Management Team (SMT) level or by the designated risk review group. It is therefore the responsibility of the Supervisor or Line Manager to escalate such risks through the appropriate management channels to the relevant Risk Lead and/or SMT group.

Chief Executive Officer (CEO) – Accounting Officer

The Chief Executive Officer (CEO), as the Accounting Officer, holds ultimate accountability for NHSBT’s overall risk management and assurance. The CEO shall delegate risk management tasks to others; however the CEO retains overall responsibility for ensuring these processes are effective.

CEO responsibilities include:

- The CEO is responsible for ensuring an effective risk management system is in place and for maintaining an adequate system of internal control.
- The CEO shall provide leadership in risk management, ensuring the approach to risk management is consistently applied across NHSBT.
- The CEO shall ensure that adequate staffing, finances, and other resources are available for managing risks that could negatively impact the delivery of NHSBT’s corporate responsibilities and strategic direction.

- The CEO is responsible for ensuring the Governance Statement within the Annual Report and Accounts accurately reflect NHSBT's risk management position.
- The CEO shall promote NHSBT's risk management priorities, integrating risk management, assurance and performance with the delivery of strategic objectives.

The Executive Director responsible for Risk (Director of Quality and Governance)

The Director of Quality and Governance is the Executive Director responsible for risk management and is delegated by the CEO to:

- leading risk management within NHSBT, and promoting a strong risk management culture
- chair the Risk Management Committee
- determine risk management performance indicators that align with NHSBT's other corporate performance indicators
- ensure risk management objectives align with NHSBT's corporate objectives and strategies
- ensure that the necessary resources are allocated to risk management
- ensure that the benefits of risk management are communicated to all stakeholders
- ensure that the framework for managing risk continues to remain effective
- ensure the allocation of appropriate resources for risk management, which can include, but is not limited to, people, skills and experience

Non-Executive Directors (NEDs)

Non-Executive Directors (NEDs) support the effectiveness of NHSBT's risk management framework by providing independent challenge to its risk management activities and behaviours.

NED's responsibilities include:

- providing objective, independent challenge to the executive directors to ensure the effectiveness of the risk management system.
- ensure risk is assessed and managed within a framework of prudent and effective controls.
- monitor the reporting of risk and assurance, ensuring timely and relevant information is provided to the Board to keep them informed of key risks.
- Scrutinise and challenge NHSBT's overarching framework of governance, risk, and control, ensuring it effectively supports corporate responsibilities and strategic objectives.

- Promoting a positive risk and assurance culture across NHSBT, by supporting behaviours that reflect and reinforce NHSBT's desired approach to risk management and assurance.

Chief Risk Officer

The Chief Risk Officer shall:

- Develop and clearly communicate a vision to direct organisational risk management
- Develop and embed a strong risk management culture across NHSBT
- Provide strategic oversight of strategic risk across the organisation
- Build and develop strong stakeholder relationships with both internal and external stakeholders
- Communicate and engage with Executives and Non-Executives to develop risk capability and promote robust engagement with the risk management framework

SMT (Senior Management Team) Chair (or chair of equivalent risk review group)

The Chair is responsible for providing assurance to the RMC (Risk Management Committee) for all risks within the 'Judgement Zone' which they have agreed to tolerate for a given period up to, but no longer than a six-month period. This includes assurance that the controls in place have been reviewed and considered as effective. Where controls are not effective, assurance must be provided around actions in place to address this.

- The Chair is responsible in deciding and checking which risks affects the delivery of any NHSBT Strategic Priorities, and Business Unit Strategies, need escalating to the Board Assurance Framework (BAF).

Board and Board level Committees

The board is responsible for reviewing and reflecting the nature and extent of the principal risks that the organisation is exposed to and is willing to take to achieve its objectives - its risk appetite – and ensure that planning and decision-making reflects this assessment.

- The Board shall review and update the principal risks and appetite annually, or as required.
- The Board shall ensure that roles and responsibilities for risk management are clear, to support effective governance and decision-making at each level with appropriate escalation, aggregation, and delegation.
- The Board shall agree the frequency and scope of its discussions to review how management is responding to the principal risks and how this is integrated with

other matters, including planning and performance management processes. The board and Audit, Risk and Governance Committee (ARGC) should ensure that there are clear processes for bringing significant issues to its attention more rapidly when required, with agreed triggers for doing so as a part of risk reporting.

- The Board, supported by the Audit and Risk Assurance Committee, shall specify the nature, source, format and frequency of the information that it requires. It should ensure that the assumptions and models underlying this information are clear so that they can be understood and, if necessary, challenged.
- Factors to consider for reporting include, but are not limited to:
  - differing stakeholders and their specific information needs and requirements;
  - cost, frequency, and timeliness of reporting;
  - method of reporting; and relevance of information to organisational objectives and decision-making.

Executive Team

The Executive Team will keep the principal strategic risks and corporate responsibilities under regular review and will ensure that the organisation's culture and risk management framework are aligned.

Audit, Risk and Governance Committee (ARGC)

The ARGC is delegated by the Board to be the principal committee for the oversight of risk governance, ensuring that:

The risk management system is effective, providing the outputs that enable the Board to set strategy, allocate funding, determine priorities and respond to external issues.

The risk management system provides assurance for the Board, Internal Audit and the Annual Governance Statement on internal controls in place, to enable internal audit planning.

Deep Dives are conducted into all principal risks at least annually, and more frequently at the discretion of ARGC if the risk is at risk limit, actions are deemed inadequate, controls are weak or any aspect of the management of the risk is lacking.

There is challenge and review of the adequacy and effectiveness of control processes in responding to risks within the organisation’s governance, operations, compliance and information systems

Risk Management Committee (RMC)

The RMC is constituted as an executive committee of NHSBT. It has no executive powers, other than those specifically delegated to it through its Terms of Reference. The RMC is responsible for the oversight of NHSBT's risk management framework as described by risk management policies and procedures (where risk is defined and categories of risk are laid out) and demonstrated by operational practice.

• The RMC will thereby ensure the suitability, adequacy and effectiveness of NHSBT's risk management system.

• The RMC will assist and make recommendation to the NHSBT Board and Executive Team to fulfil their responsibilities regarding the risk appetite of NHSBT, its risk management and compliance framework, and the governance structure that supports it.

• The RMC is authorised by the NHSBT Executive Team to obtain external legal or other independent professional advice and to secure the attendance of outsiders with relevant experience and expertise if it considers this necessary.

• A full list of responsibilities can be found in the RMC's Terms of Reference.

Risk Leads Forum

The Risk Leads Forum is scheduled to be held two weeks before every Risk Management Committee meeting. The forum is chaired by the Risk and Assurance team, with membership consisting of Risk Leads and Heads of Function, with responsibility for risk. Responsibilities of the forum include:

- Oversee and provide assurance that implementation of NHSBT's risk management system is effective, by ensuring principal risks, their contributory risks as well as business area operational risks are being managed effectively, and risk mitigation is in place.
- Monitoring compliance with the policy and procedures associated with risk management governance, risk management procedures, and the risk control infrastructure, including risk management arrangements at Directorate level.
- Oversee the implementation of the NHSBT Assurance Framework, including monitoring the compliance status, and supporting action plans, of statutory, regulatory, Government Functions (including the Government Functional Standards) and Board level policies.
- Provide enterprise level input into principal risks and their contributory risks and monitoring their movement to enable contribution to principal risk 'deep dives' which are presented at the Risk Management Committee (RMC) and the Audit, Risk and Governance Committee (ARGC).

- Monitoring of high risk in the organisation and challenge risk detail, risk score, control and action plans as appropriate.
- Horizon scanning for emerging risk and monitoring of cross-directorate trends in risk.
- Make recommendations to the Risk Management Committee on priority risk areas based on above points.