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.

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.

Changes in this version

This framework and process has undergone significant changes, hence no shading.

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 B.

- **General:**
- All Staff
- Supervisors & Line Managers
- Senior Management Teams (SMT) & Oversight Bodies (includes CEO, Executive Directors, Non-Executive Directors and Oversight Bodies)
- **Individuals:**
- Chief Executive Officer (CEO)
- All Executive Directors (Portfolio Owner)
- Director of Strategy
- All Non-Executive Directors
- 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)
- **Other Roles:**
- Risk Owners
- Control Owners
- Action Owners
- Business Partner Risk Leads
- Authors & Owners of Risk Documents

Process Description

Statement of Intent

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.

To further enhance NHSBT's commitment to safety and quality, information obtained via the risk management process supports continuous improvement and contributes towards wider organisation learning.

This on-going commitment to safety and quality across NHSBT is supported by NHSBT's risk management programme. All persons employed by NHSBT, irrespective of role, grade or permanency have a responsibility to contribute towards the risk management process.

This manual incorporates NHSBT's Risk Management Framework and provides information covering the principle components of NHSBT's Risk Management Process:

a. **Risk Management Framework** (**Green** section, page 5) describes the structure and governance of risk, NHSBT's risk appetite and over-arching components including communication and improvement.

b. **Guidance for specific staff groups** (**Purple** section, page 10) are one-page references that all staff can refer to, signposting them to expectations regarding their role and responsibilities and areas of the manual (including other supporting guidance packages) they should familiarise themselves with.

c. **Risk Management Process** (**Yellow** section, page 15) includes the risk assessment process, risk treatment and the processes for the recording, reporting, monitoring and reviewing of risks in Pentana.

d. **Further guidance in Appendices** (page 33) includes terms and definitions, roles and responsibilities, guidance on impact and likelihood scoring, and a risk assessment template (**FRM6604**).

Betsy Bassis

NHSBT Chief Executive Officer

CONTENT

Introduction & How to use this manual

What is Risk Management? Risk Management refers to a coordinated set of activities and methods that is used to direct an organisation and to control the many risks that can affect its ability to achieve objectives.

Why is it important to NHSBT? Effective and consistent risk management within NHSBT is an essential requirement supporting the culture of safety and quality. NHSBT recognises that the activities undertaken within the organisation, by their very nature, involve a degree of risk. To ensure the continued delivery of high-quality products and services, the identification, assessment and management of risk is paramount.

Compliance with the Framework and Processes described within this manual supports NHSBT with its ongoing commitment to safety, openness, learning, governance and continuous improvement. It supports compliance with NHSBT's legal/statutory requirements, those of external regulators and other relevant bodies. In addition, there are sound moral, financial and good practice reasons for identifying and managing risks. Failure to manage risks effectively can lead to harm, loss and/or damage, such as: clinical harm, personal injury, damage to NHSBT's reputation, financial loss, complaints, incidents, litigation or unwanted publicity.

Who is responsible for risk management within NHSBT? It is the responsibility of every member of staff within NHSBT (including those operating on behalf of NHSBT) to contribute towards risk management and its processes. Specific roles and responsibilities are delegated to groups or posts as detailed within **Appendix B**. Further guidance is provided in the **Purple** section of this manual (page 10).

How is risk managed within NHSBT? This manual describes NHSBT's integrated approach to the overall management of risk irrespective of the primary cause of the risk, for example, clinical, financial or quality. All directorates and departments within NHSBT must comply with, and apply the framework, processes and guidance to their own functional or operational risk management processes. This ensures risks are assessed and managed consistently and can be understood by any staff within NHSBT. To ensure best practice, this manual is based on *BSI ISO 31000:2018 Risk Management – Guidelines*. The online risk management tool, *Pentana*, is used to record, manage and report risks, aiding visibility and transparency of risks through all directorates, functions and departments of NHSBT.

When are risks assessed/managed? Once a risk has been identified, it should be assessed as soon as practicably possible at the appropriate forum *e.g.* SMT or equivalent. All High scoring risks (residual score of 15 or more) must be reviewed within 6 months as a minimum, and all other risks must be reviewed within 12 months (including associated actions and controls). Risks should be re-assessed when the situation changes, *e.g.* following a new event/incident, increase or decrease in complaints, change in actions/controls, change in suppliers, change in staffing numbers, *etc.*

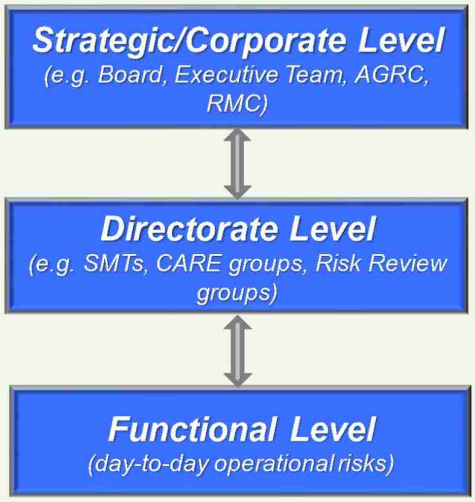
How to use this manual: This manual is set out in several sections to enable staff to reference specific areas:

- **Green** = The Risk Management Framework (page 5)
- **Purple** = Guidance for specific staff groups (page 10)
- **Yellow** = The Risk Management Process (page 15)
- **Appendices** = Further guidance (page 34)

Staff groups with roles and responsibilities within this manual will be contacted to complete relevant training packages. Should any staff feel they require training or guidance, contact the Risk Management Team by emailing pentanariskmanagement@nhsbt.nhs.uk

Structure and Governance

NHSBT's risk management structure adopts a three-tier model, where descriptions for each risk level are detailed in **Diagram 1**.



	Strategic risk themes include those risks that threaten to disrupt the assumptions at the core of NHSBT's strategy or operational activity. **Corporate risk themes** include the risks against compliance with statutory, regulatory and legal requirements to which NHSBT has to adhere.
	Directorate-level risk themes include those risks that impact on the delivery of the objectives of each business-unit within NHSBT. Governance committees and groups are responsible for reviewing the status of these risks which are set by the 'worst-child' score of the Functional Risks below.
	Functional risks are risks which could influence the safe and effective delivery of the day-to-day functional and operational tasks undertaken across NHSBT for the timely provision of products and services.

Diagram 1: *NHSBT's Three-tier Risk Management Structure*

This structure is reflected in the risk management tool, *Pentana*. It allows risks to be 'connected' to each other up-and-down the tiers as well as across the relevant governance groups/committees, and operational/supporting functions.

This means should any risk be (or become) the highest scoring risk (known as 'worst-child'), it will flow upwards or communicated downwards to the relevant level as well as to the relevant supporting functions such as Digital, Data and Technology Services (DDTS), Quality, Finance, People, *etc.,* thus allowing visibility in real-time.

Risk Appetite

Risk Appetite (or risk criteria) is the level of risk that an organisation can (or will) accept. It is used to evaluate the significance or importance of the organisation's risks. They are used to determine whether a specific level of risk is acceptable or tolerable. In practice, risk appetite guides NHSBT to determine the commitment to undertake or continue an activity and informs decisions regarding treatment of the risk(s).

NHSBT's risk appetite has been agreed at Board level (**Diagram 2,** *NHSBT's Risk Appetite Framework*) where the approach is generally to remove or minimise all risks that impact on safety, quality of services and products, statutory requirements, licensing conditions, regulatory compliance and other areas.

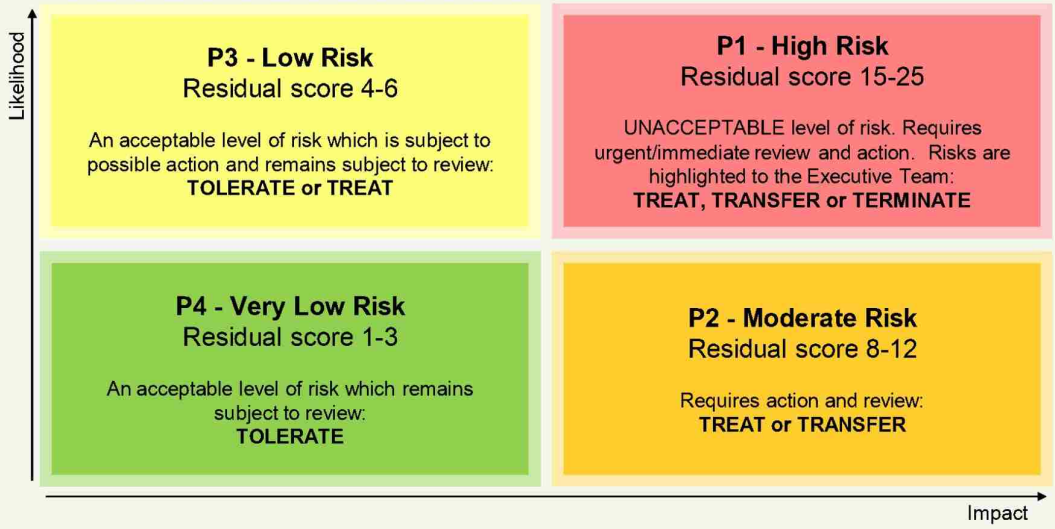


Diagram 2: *NHSBT's Risk Appetite Framework*

Residual risk scores (with NHSBT's controls) are classified into four levels: **P1-P4**:

- **P1 Red Risks** are 'High' and are unacceptable to NHSBT, thus must be treated, transferred or terminated (*i.e.* further actions/justification must be put in place);
- **P2 Amber Risks** are also generally not acceptable and should be treated or transferred. In cases where a P1 or P2 risk cannot be mitigated any further (*i.e.* the Target score is at Red or Amber level), then the Target score must be discussed and approved at the SMT level (or equivalent risk review group). **Should the SMT or risk review group be unable to reduce or influence the scoring, this risk must be escalated to the Risk Management Committee (RMC);**

- P3 and P4 risks can generally be tolerated, or, if deemed appropriate, a P3 risk can be reduced further to a P4 level by treating it with further actions.
- The decision to treat, transfer or terminate must be recorded within Pentana, especially if they differ from the guidance set in **Diagram 2**.

How to use Diagram 2 (NHSBT's Risk Appetite Framework) to determine the significance and treatment of a Risk

Below summarises the *general* guidance on how to use Risk Appetite during a risk assessment. (For full risk assessments, refer to the **Yellow** section, page 15).

1. After the initial identification and analysis of a risk (*i.e.* determining its causes, consequences, inherent score and residual score), make note of the Residual Score (the score after considering NHSBT's controls already in place).
2. Compare the Residual Score to the guidance in **Diagram 2**, *i.e.* the options that must be taken for that particular residual score (tolerate, treat, transfer or terminate).
3. The chosen option must be agreed and entered into Pentana. As a general rule, all **P2 Moderate and P1 High risks** must be treated. Should the option of transferring or terminating the risk be chosen, this must be discussed and agreed by the relevant SMT (or risk review group). This also applies to 'archiving' risks in Pentana.
4. **Target Scores and Dates** must be set in Pentana even if the risk is to be tolerated:
   - If the risk is to be **tolerated**, this means the risk level is acceptable and it is low. The Target Score can be set as equal to the Residual Score. No further action is needed, thus enter the Target Date as the same date the Residual Score was agreed, and set the risk's Scheduled Review Date at 12 months;
   - If the risk is to be **treated, transferred or terminated**, this means the current risk level is not acceptable and actions need to be put into place to further mitigate the risk. The Target Score should be agreed (for example a score of 6 or less) along with the actions and dates for completion. At least one action must be entered into Pentana and the Target Date can then be set at one month from the completion of the last action. The risk's Scheduled Review Date must be set no longer than 6 months for P1 High risks, and no longer than 12 months for P2-P4 risks.

Note 1: For each risk, should the appetite and/or treatment(s) be different to the guidance stated in this manual, the Risk Owner must raise this to the appropriate Senior Management Team (SMT) (or equivalent risk review group) and provide sufficient justification within Pentana. The same applies should the action(s) or Target Score not be achieved.

Note 2: All **P1 High (Red) risks** (residual score of 15 or more) will be highlighted to the Executive Team through assurance reports from the Risk Management Team.

Communication & Training

Communication and Discussion

The purpose of Communication and Discussion is to assist relevant stakeholders (*i.e.* other business units or supporting departments which may be impacted by a given risk) in understanding risk, the basis on which decisions are made and the reasons why particular actions are required.

Close coordination between Communication and Discussion should facilitate factual, timely, relevant, accurate and understandable exchange of information in order to effectively manage the risk and support organisational learning. Communication of risk information should be cascaded to the relevant areas of the business to enable effective organisational learning.

Note 1: Communication and Discussion with stakeholders should take place within and **throughout all steps** of the risk management process.

Note 2: **Timeliness and reactiveness** – Should the risk appear to pose an imminent and significant threat to any aspect or area of NHSBT, or outside of NHSBT's risk appetite levels, it should be raised and escalated to the appropriate SMT (or equivalent risk review group) as soon as possible, not to be delayed until the next business-as-usual discussion group/meeting.

Note 3: **Internal resilience** – Risk Leads will ensure resilience within their directorate, function or department with regards to appointing deputies to manage risks, actions or controls in the absence of currently appointed persons.

Training and Awareness

The management and design of Training and Awareness programmes to support NHSBT's Risk Management Programme are the responsibility of the Risk Management Team. These packages will be managed, designed, implemented, rolled-out and updated as deemed appropriate by the Risk Management Team.

Any persons who need support to clarify any doubts or questions regarding risk management or the use of Pentana should contact the Risk Management Team by emailing: pentanariskmanagement@nhsbt.nhs.uk. 'Bite-size' guidance packages are available *via* NHSBT's intranet through *Support Functions*, *Risk Management*.

Improvement

Improvement (Organisational Learning)

Learning identified from thematic and trend reviews will be raised and discussed at the Risk Management Committee with onward cascade through to the directorate and functional operational groups (for example training and education teams and staff forums).

Evaluation

NHSBT measures the performance of the risk management framework against pre-determined Key Performance Indicators, including:

- Risk Appetite, Action Status, Due Date, Risk Movement.

NHSBT measures the effectiveness of the risk management framework using outputs including:

- Performance, Claims, Incidents, Complaints.

Guidance for All Staff

All members of staff (including those acting on behalf of NHSBT *e.g.* temporary staff, agency, and contractors) are responsible for maintaining risk awareness, identifying and escalating risks as appropriate to their Supervisor or Line Manager. In addition, they will ensure that they familiarise themselves and comply with NHSBT's policies and procedures and attend mandatory and other relevant training courses.

Whilst it is of benefit for all members of staff to be aware of the overall risk management programme within NHSBT, there are two main elements of the process that staff must be aware of:

Risk Identification and **Escalation**

It is the responsibility of all members of staff to identify and escalate any hazards or risks in accordance with the process summarised in **Diagram 3** below.

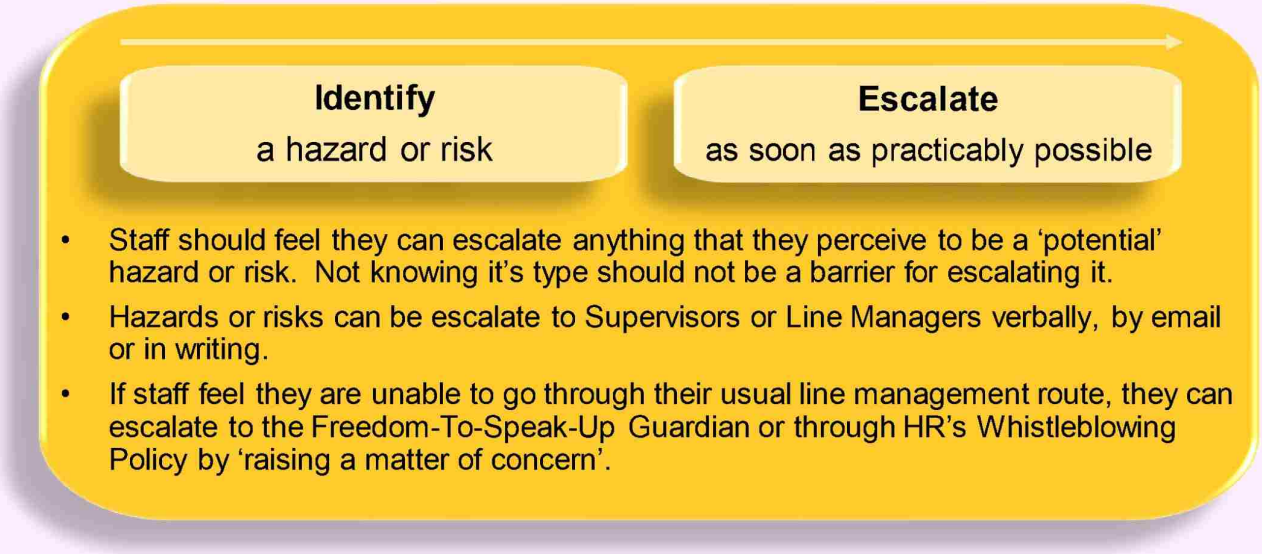


Diagram 3: *Initial Identification and Escalation of Risks*

Further Escalation is summarised in **Diagram 4,** below, and the **Yellow** section of this manual (page 15) details guidance on performing formal risk assessments.

Guidance for Supervisors / Line Managers
(including Risk Leads)

Once a hazard or risk had been initially identified and escalated, from any source, Supervisors, Line Managers and Risk Lead can refer to the guidance in **Diagram 4**, describing the further escalation and communication of the hazard or risk.

Supervisors / Line Managers (including Risk Leads):
Further Escalation (bottom-up) and Communication (top-down) of a hazard or risk

Further Escalation (bottom-up)

- All directorates/functions/departments should understand and document their internal process for recording, escalating and communicating hazards/risks up and down their line management chain. The process should be consistent with **MPD1336** and include a risk assessment template (*e.g.* **FRM6604**).
- Upon notification of a hazard/risk (from any source), Supervisors and Line Managers (including Risk Leads) are responsible for deciding on the necessary course of action and whether it is appropriate to arrange for a formal risk assessment to be undertaken.
- Should it be decided that the hazard/risk needs a formal risk assessment, and the risk has been found to impact on the delivery of a function/service/objective, it MUST be made available for review and challenge by the Senior Management Team (SMT) Meeting (or equivalent risk review group).

Communication (top-down)

- The Supervisor or Line Manager (or Risk Lead) must provide timely feedback to the reporting member of staff with a simple explanation how the hazard/risk/concern will be managed (*e.g.* whether 'no further action required' or 'a formal risk assessment will be undertaken').
- Should the SMT (or risk review group) agree the risk, its score, treatment, and entry into Pentana (risk register/ management online system), this information should be cascaded as above, as well as to the appropriate staff-groups and business areas that need to be aware of the particular risk.

Diagram 4: *Further Escalation and Communication of a Hazard or Risk*

Risk Leads can refer to further guidance within the page below.

Guidance for Risk Leads

A full description of the Role & Responsibility of a Risk Lead can be found in **Appendix B**. In the main, the nominated Risk Lead of a directorate, function or department will be a 'champion' for risk management within their directorate at SMT's (or equivalent risk review group) and coordinate the risk management process at the appropriate governance oversight group/committee in accordance with the guidance in this manual.

For risks that impact on their directorate, function or department, the Risk Lead is the communication link between the responsible Director, Risk Owners, staff who raise risks to them and any supporting areas of business that may be assisting with mitigations to reduce those risks.

It is thus paramount that Risk Leads familiarise themselves with this manual (MPD1336) in detail, attend training sessions offered to them, and be aware of further guidance available through **NHSBT's Risk Management intranet page**.

Guidance for Business Partner Risk Leads

A full description of the Role & Responsibility of a Business Partner Risk Lead can be found in **Appendix B**. In the main, Business Partner Risk Leads are subject matter experts from NHSBT's Support Services such as: Health & Safety, Quality, Business Continuity, People, Clinical, DDTS, Estates & Facilities, Finance, Communications and Risk.

They have a key role in supporting their associated areas of business with regards to (i) understanding the related risks, (ii) challenging the details of the risk and the controls/actions to ensure they are appropriately recorded and managed, (iii) escalating the risk to their own SMT (or equivalent risk review group) for consideration, and (iv) communicating any risks their own SMT has identified across to the relevant Risk Leads.

Business Partner Risk Leads should familiarise themselves with this manual (MPD1336), attend training sessions offered to them, and be aware of further guidance available through **NHSBT's Risk Management intranet page**.

Guidance for Owners of Risks/Actions/Controls

With reference to Pentana, the online risk management tool used by NHSBT, the Roles and Responsibilities of 'Owners' of risks, actions and controls within Pentana can be found in **Appendix B**.

In the main, a Risk Owner is an individual who has been given the autonomy and responsibility for the addition and overall management of NHSBT's response to a particular risk recorded within Pentana. When adding a new risk, the Risk Owner is responsible for adding Controls and Actions as appropriate. Should the tasks need to be delegated, the Risk Owner is responsible for nominating the Action Owner(s) where appropriate.

As per **Diagram 5**, there should be close communication between the Risk Owner, Action Owner, Control Owner and their Risk Lead when a risk is first assessed and when it needs to be re-assessed (see **Yellow** section on '*Monitoring & Review*', page 30).

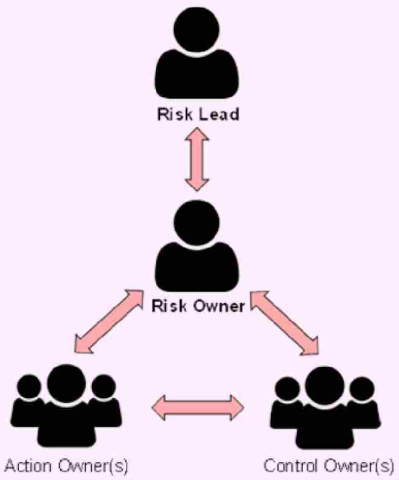


Diagram 5: *Communication between Risk/Action/Control Owners and their Risk Lead*

Throughout the process of updating risks (and their actions and controls), it is likely that the Risk Owner, Action Owner and Control Owner will liaise with each other to ensure any changes are reflected in Pentana as accurately as possible and in a timely manner.

Once an action is completed and implemented, it is the responsibility of the Action Owner to communicate this with the Risk Owner

It is paramount that Owners of Risks/Actions/Controls familiarise themselves with this manual (MPD1336) in detail, attend the appropriate risk training sessions offered to them, and be aware of further guidance available through **NHSBT's Risk Management intranet page** (such as the 'Bite-size' guidance packages for using Pentana).

Guidance for Authors/Owners of Risk Documents

Authors and Owners of any risk-related documentation produced for use within NHSBT have a responsibility to liaise with the Risk Management Team during risk-related documentation development. This is to ensure risk management processes (and associated training) across the organisation (*e.g.* Health, Safety & Wellbeing, Quality, *etc.*) remain consistent.

Authors and Owners of risk-related documentation should familiarise themselves with this manual (MPD1336) and will be offered appropriate risk training sessions. They should be aware of further guidance available through **NHSBT's Risk Management intranet page**.

Below are a few examples of important areas of this manual to align with:

- **Governance** - check that any reference to where and how risks are discussed/approved are consistent with the new governance structure and Terms of Reference of the relevant groups/committees.
- **Roles & Responsibilities** - check that these are consist with the roles within any risk-related document/training. Roles in MPD1336 have been agreed at Board level.
- **Terms & Definitions** – ensure any risk-related document/training is using the same terms and definitions, or at least not significantly differing from those in this manual (MPD1336). Terms & definitions in MPD1336 have been agreed at Board level.
- **Risk Appetite** – ensure that any reference to appetite levels are consistent with NHSBT's Appetite Framework.
- **Articulation of a Risk** – all risks must be articulated as per agreed format. It is therefore essential that the format below is in any risk-related document/training:

> "***There is a risk that***……. ***caused by***…… ***resulting in***……"

- **Risk Assessment Process** – ensure that the processes described in any risk-related documentation/training is consistent with the risk management process set out in MPD1336 which aligns with *ISO31000:2018 Risk Management Guidelines*.
- **Risk Matrix & Scoring Guidance** – the 5x5 risk matrix and scoring guidance (for impact and likelihood) in MPD1336 *must* be used in any risk-related document/training. Ensure the wording and descriptions are aligned as these are exactly the same descriptions used in *Pentana*, NHSBT's online risk management system.
- **Inherent, Residual & Target Risk Scores** – if not already included, ensure the inclusion of guidance relating to inherent, residual and target risk scores. All risks that are entered into Pentana require all three scores.

The Risk Management Process - Introduction

The risk management process should be an integral part of management and decision-making and integrated into NHSBT's structure, operations and processes. The dynamic and variable nature of human behaviour and culture should be considered through the risk management process. Although the risk management process is often presented as sequential, in practice it is iterative.

This **Yellow** section describes NHSBT's over-arching risk management process (**Diagram 6**) irrespective of the primary cause of the risk (*e.g.* clinical, financial, quality, *etc.*) or the directorate or department that is managing the risk(s).

All directorates and departments within NHSBT *must* comply with, and apply, the processes in this manual to their own functional or operational risk management processes. This ensures risks are assessed and managed consistently and can be understood by any staff within NHSBT. **FRM6604** gives an example of a **risk assessment template**.

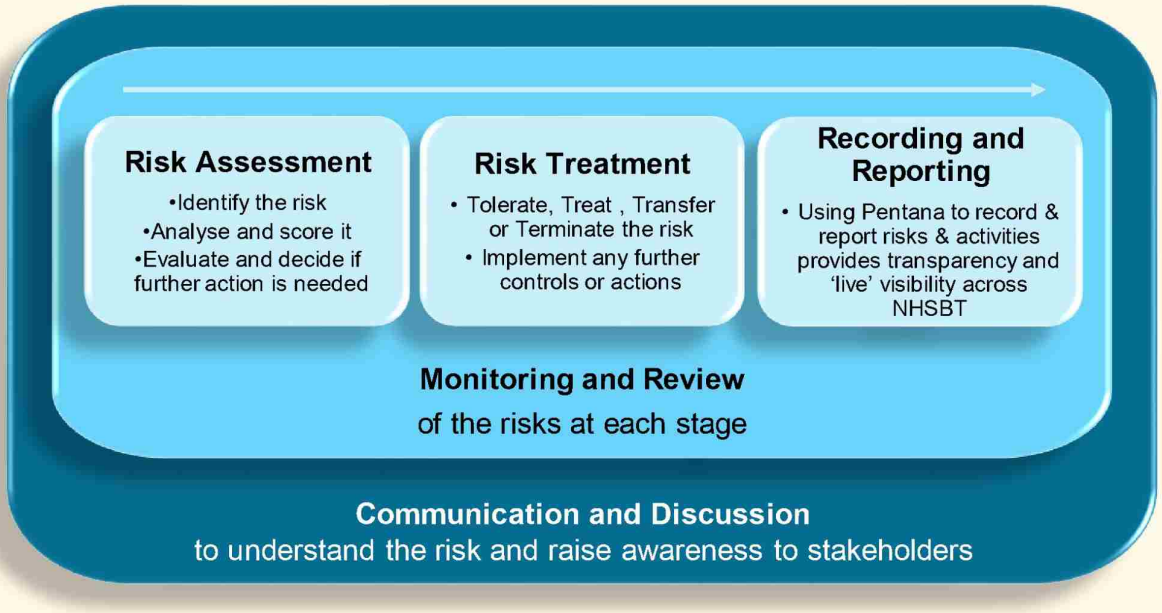


Diagram 6: *NHSBT's Risk Management Process*

Note: Detailed guidance on populating and managing risk registers (within **Pentana**) are available *via* the intranet page under *Support Functions*, *'Risk Management'*, *'Bite-size Guidance'*.

How To Perform A Risk Assessment

Risk Assessment

Risk Assessment is a process used to evaluate the risk and establish if the current controls are adequate or further action is required to manage the risk. It is the overall process of **risk identification, risk analysis and risk evaluation**.

Risk Identification

The purpose of risk identification is to find, recognise and describe risks that might help or prevent NHSBT from achieving its objectives. Relevant, appropriate and up-to-date information is important in identifying risks. A variety of resources can be used such as historical data, theoretical analysis, informed opinions, expert advice and stakeholder input.

Any member of staff wishing to raise anything they perceive as a potential risk should feel confident in raising it and must not let uncertainty regarding categorisation act as a barrier to reporting.

The principle of risk identification should apply whether or not their sources are under NHSBT's control. Consideration should be given that there may be more than one type of outcome, which may result in a variety of tangible or intangible consequences.

The responsibility of risk or hazard categorisation is with supervisors, managers and Risk Leads and can be agreed once further details have been established.

A full list of Terms & Definitions can be found in **Appendix A**, however, the definitions below are important to keep in mind for risk identification:

- **Risks** are things/events that might happen, which could result in harm/loss/damage or an opportunity. In NHSBT, this harm, loss or damage could potentially impact adversely on NHSBT's *objectives* including harm to staff/donors/patients/visitors and the delivery of safe, high quality products or services.
- A **Hazard** is something that has the potential to cause harm.
- An **Incident** is something that has happened which was not expected or planned.
- An **Event** is an occurrence or change of a particular set of circumstances. In NHSBT we may refer to this as an incident.

- A **Risk Source** (or source) is an element which alone or in combination has the potential to give rise to risk. It is where the risk originates and has the intrinsic potential to give rise to risk.
- A **Cause** is the reason why something could go wrong. The existence of the cause does not mean the event will happen.
- The **Impact (or consequence)** is the outcome of an event affecting objectives. A single event can generate a range of impacts which can have both positive and negative effects on objectives.
- The **Likelihood** is the chance of something happening. It can be thought of as the possibility, probability or frequency of something happening.

A range of techniques (such as PESTLE analysis) can be used for identifying uncertainties that may affect one or more objective. The following factors, and the relationship between these factors, should be considered:

- whatever can stop the delivery functional objectives;
- tangible and intangible sources of risk;
- causes and events;
- threats and opportunities;
- vulnerabilities and capabilities;
- changes in the external and internal context;
- indicators of emerging risk;
- the nature and value of assets and resources;
- consequences and their impact on objectives;
- limitations of knowledge and reliability on information;
- time-related factors;
- biases, assumptions and beliefs of those involved.

Risk Analysis

Risk analysis is the process of understanding the nature of the risk, its characteristics (events, sources, impact, likelihood, *etc.*) and the level of risk, providing an input into risk evaluation and treatment decisions.

Risk analysis can be undertaken with varying degrees of detail and complexity, depending on the purpose of the analysis, the availability and reliability of information, and the resources available. Analysis techniques can be qualitative, quantitative, or a combination of these, depending on the circumstances and intended use.

The risk analysis may be influenced by opinions, biases, perceptions of risk and judgements. Additional influences are the quality of information used, the assumptions and exclusions made, any limitations of the techniques and how they are executed. <u>These influences should be considered, documented and communicated to decision makers.</u>

Risk analysis provides an input to risk evaluation, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods.

Risks must be assessed using the approved *NHSBT Risk Assessment Matrix*, **Diagram 7** below, taking into account:

- the **Inherent** risk score (without NHSBT's controls in place);
- the **Residual** risk score (with NHSBT's current and live controls in place):
  - the potential **impacts (or consequences)** of the risk should it be realised, and the nature and magnitude of impacts/consequences;
  - the **likelihood** of event/risk occurring, as well as the likelihood of the impact/consequences occurring;
- the **Target** risk score (as defined by NHSBT's Risk Appetite, see **Green** section, page 5);
- other factors to consider include: complexity and connectivity; time-related factors (*e.g.* projects over a certain period) and volatility; the effectiveness of existing controls;
- The Risk Score is calculated by Impact (I) x Likelihood (L).

Diagram 7 shows both numerical scoring and colour bandings which are assigned to Risk Ratings (P1-P4) which reflect High-Low Priority ratings (see **Appendix C** for more guidance on Impact and Likelihood scoring).

NHSBT's Risk Assessment Matrix		Impact				
		Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	Almost Certain 5	**5**	**10**	**15**	**20**	**25**
	Likely 4	**4**	**8**	**12**	**16**	**20**
	Possible 3	**3**	**6**	**9**	**12**	**15**
	Unlikely 2	**2**	**4**	**6**	**8**	**10**
	Rare 1	**1**	**2**	**3**	**4**	**5**

Risk Rating	Risk Scores	Priority
P1	15 - 25	High
P2	8 - 12	Moderate
P3	4 - 6	Low
P4	1 - 3	Very Low

Diagram 7: *NHSBT's Risk Assessment Matrix*

Guidance on Impact & Likelihood Scoring

Guidance on Impact (or Consequence) Scoring

(Refer to **Appendix C** for more guidance on Impact and Likelihood scoring. **Note, this guidance gives *examples* of some risk scenarios and is not an exhaustive list**).

1. When undertaking a risk assessment, it is important to first define the risk(s) explicitly in terms of adverse impacts/consequences that might arise from the risk. In NHSBT, the impact is defined as the outcome of an event affecting objectives. There may be more than one impact/consequence of a single event, and it may be positive or negative.
2. Wherever possible, impact must be assessed against objective definitions across different areas. In NHSBT this is referred to as *Primary Impact Areas* (see the *Impact Table* in **Appendix C** for examples). The guidance in the table aims to provide consistency in risk scoring when used by staff across all directorates within NHSBT.
3. Despite defining impacts as objectively as possible, it is inevitable that the rationale and scoring of some risks will involve a degree of subjectivity. Thus, is it important to articulate the risk well, attend training sessions as appropriate, and follow the guidance provided by NHSBT within this manual (MPD1336).
4. Using the *Impact Table* in **Appendix C**:

   - The guidance gives examples of some risk scenarios and is not an exhaustive list, thus the importance of discussing and approving risks in the appropriate forum with the appropriate subject-matter-experts present (*e.g.* at SMT or equivalent risk review group).
   - Use the guidance in the table to determine the Impact Score of the risk (for inherent, residual and target scores).
   - Choose the most appropriate *Primary Impact Area* from the first column of the table, then work along the columns in the same row to assess the severity of the risk on the scale of 1-5 as defined at the top of the table.
   - A single risk area may have multiple potential consequences, and these may require separate assessment.
   - It is also important to consider from whose perspective the risk is being assessed (organisation, member of staff, patient) because this may affect the assessment of the risk itself, its consequences and the subsequent action taken.
   - For Residual Scores, the effectiveness of any current controls already in place must be taken into consideration and reflected in the impact score as appropriate.

Guidance on Likelihood Scoring

1. Once a specific area of risk has been assessed and its impact score agreed, the likelihood of that impact/consequence occurring can be identified by using the *Likelihood Table* in **Appendix C**. The likelihood of a risk occurring is assigned a number from 1-5: the higher the number the more likely it is the impact/consequence will occur.
2. **If the risk has occurred before in similar situations, and there is objective data (*e.g.* incidents, audit findings, research/reports, complaints, claims, *etc.*), use this information in the first instance to predict the risk occurring in the future.** The risk matrix is based over a period of 5 years, thus a look-back of any objective data over the same period would be appropriate.
3. If there is no objective data available, the likelihood can be based on expert experience or opinions, thus the importance of discussing and approving risks in the appropriate forum with the appropriate subject-matter-experts present (*e.g.* at SMT or equivalent risk review group) so that a consensus of the risk scoring can be achieved.
4. For Residual Scores, the effectiveness of any current controls in place must be taken into consideration. The likelihood score is a reflection of how likely it is that the adverse impact/consequence described will occur.
5. Using the *Likelihood Table* in **Appendix C**:

   - Likelihood can be scored by considering: (a) **Timeframes** (how many times will the adverse impact/consequence being assessed actually be realised?), or (b) **Probability** (what is the chance the adverse impact/consequence will occur in a given reference period?). For example, when assessing the risk of staff shortages in a department, the likelihood of it occurring could be assessed as expected to occur daily or even weekly depending on staffing levels. However, if staff shortages are unlikely it could be graded as expected to occur annually.

   - Sometimes, timeframes are not a useful way of scoring certain risks, especially those associated with the success of time-limited or one-off projects such as a new system that is being delivered as part of a three-year programme, or business objectives. For these kinds of risks, the likelihood score cannot be based on how often the impact/consequence will materialise.

   Instead, it must be based on the **Probability** that it will occur at all in a given time period. For example, a three-year project cannot be expected to fail 'once a month', and the likelihood score will need to be assessed on the probability of adverse impacts/consequences occurring within the project's timeframe. Another example, a project which is more likely to fail than succeed (that is, the chance of failing is greater than 90%) should be assigned a score of 5.

   - With regard to achieving a national target, the risk of missing the target will be based on the time left during which the target is measured. The SMT (or equivalent risk review group) might have assessed the probability of missing a key target as being quite high at the beginning of the year, but six months later, if all the control measures have been effective, there is a much-reduced probability of the target not being met. If it is not possible to determine a numerical probability, the probability **Definitions** can be used to determine the most appropriate likelihood

The Three Risk Scores (Inherent, Residual & Target)

In NHSBT, three risk scores must be considered: **Inherent, Residual and Target** scores.

For any one risk, all three risk scores must be assessed at the same time to ensure the risk is assessed as a whole and all aspects looked at together, especially when there is a change in situation and the risk is being re-assessed.

The **Inherent Risk** is a measure of the current risk without the controls which have been put in place by NHSBT. It is derived by multiplying the scores of Impact x Likelihood.

After the initial, Inherent Risk scoring exercise (see section above on '*Guidance on Impact and Likelihood Scoring*'), attention must be given to any existing **controls** in place which manage or mitigate the risk, considering:

- whether the control(s) reduce the likelihood, or the impact of the risk being realised;
- whether the identified control(s) are effective, thus the **residual** risk score reduced accordingly;
- should those controls not be fully effective, to record this gap in Pentana.

The **Residual Risk** is the current risk after the identified controls are in place. It is the measure of the risk with controls that NHSBT has put in place, meaning NHSBT has reduced the risk, removed the source of the risk, modified the impacts/consequences, changed the likelihood, transferred the risk or retained the risk.

If there are no controls in place at this time, the Residual risk score will be the same as the Inherent risk score. Both scores should have been agreed at the SMT level (or equivalent risk review group). It remains the responsibility of the Risk Lead to consider any additional considerations which may impact on the course of action to be implemented.

The **Target Risk** is the acceptable level of risk, as defined by an organisation's risk appetite, which is achievable with the implementation of agreed actions. A target risk score is specific to an individual risk and should be a realistic and achievable goal with the current available resources. It should not be thought of as a 'short-term' risk reduction target. The target risk should be the best residual score that could be achieved once all actions are completed.

The target risk score should be set within the organisation's risk appetite (*i.e.* within a tolerated level) and agreed at SMT level (or equivalent risk review group). See **Green** section on '*Risk Appetite*', page 6.

Relationship between the three Risk scores, Controls and Actions

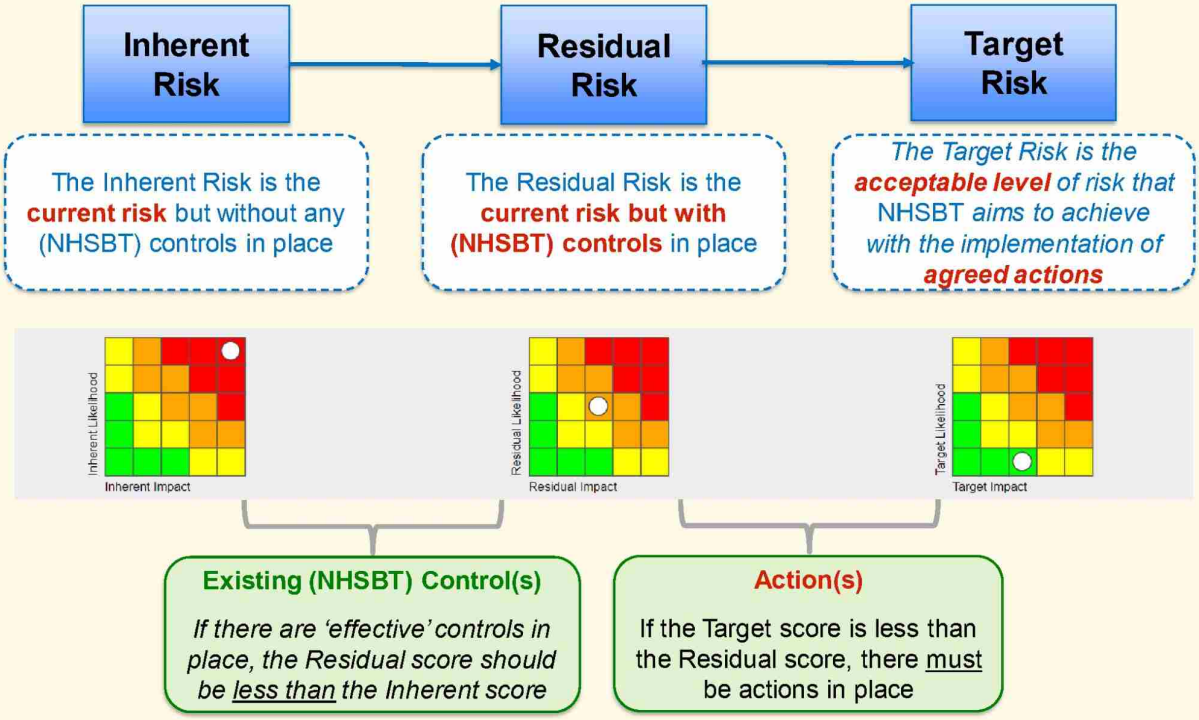


Diagram 8: *Relationship between the three Risk scores, Controls and Actions.*

Diagram 8 describes the difference between the three risks and the relationship between the scoring of those risks and the presence of controls and actions. In Pentana, if there are 'effective' controls in place, the Residual score should be less than the Inherent score. If the Target score is less than the Residual score, there must be actions in place.

If the above cannot be achieved for any reason, this must be escalated and discussed at the appropriate forum (SMT or equivalent risk review group), and the reasons recorded in Pentana.

Reviewing Risks

For further guidance on reviewing risks, refer to the next section '*Using Pentana: Recording, Reporting & Assurances'*, page 29.

Note, the Inherent Risk must also be reviewed/changed if the internal or external situation has changed (*e.g.* following an event/incident, increase in complaints/incidents, *etc.*).

Note: Detailed guidance for updating risks within **Pentana** are available *via* the intranet page under *Support Functions, 'Risk Management', 'Bite size Guidance'*

Risk Evaluation & Treatment (Actions & Controls)

Risk Evaluation

The purpose of risk evaluation is to make and support informed decisions. Risk evaluation involves comparing the results of the risk analysis with the established **Risk Appetite** (see **Green** section, page 6) to determine where additional action is required. This can lead to a decision to:

- do nothing further (tolerate);
- consider risk treatment options (treat/transfer/terminate);
- consider an action plan and sub-actions;
- undertake further analysis to better understand the risk;
- maintain existing controls;
- reconsider the objectives/strategy.

Decisions should be made at the senior management team (SMT) level or equivalent risk review group, and not made in isolation.

Decisions should take account of the wider context and the actual perceived consequences to internal and external stakeholders. The outcome of risk evaluation should be clearly communicated and then validated at the SMT level (or equivalent risk review group).

The risk must then be recorded within Pentana following the detailed '*Bite-size Guidance*' available *via* the intranet page under *Support Functions*, '*Risk Management*'.

NHSBT manages risk in four ways: **Terminate, Tolerate, Transfer or Treat**:

Terminate the risk – Avoid the risk by deciding not to start or continue with the activity that gave rise to the unacceptable risk. Alternatives are to choose a different or less risky activity/approach. If removed, the risk can be archived in the risk register. Decision to be discussed and agreed by the relevant SMT (or risk review group). This also applies to 'archiving' risks in Pentana.

Tolerate the risk – Accept and retain the risk through an informed decision that the risk is at an acceptable level (within pre-agreed appetite/tolerance level). This may apply to situations where a residual risk remains after other treatment options have been put into place. No further action is needed to treat the risk, but ongoing monitoring is still expected.

Transfer the risk – Implement an action plan that moves or shares the risk with another party such as outsourcing through third party contracts or insurance. No extra action is needed to treat the risk, but ongoing monitoring is still expected. Decision to be discussed and agreed by the relevant SMT (or risk review group). This also applies to 'archiving' risks in Pentana.

Treat the risk – Implement an action plan that reduces the impact and/or likelihood to an acceptable level, where elimination of the risk is considered to be excessive in terms of time or expense. Ongoing monitoring is expected.

Risk Treatment

Risk Treatment is a risk modification process, it is the day-to-day management of a risk. It involves selecting and implementing one or more treatment options (*e.g.* Terminate, Tolerate, Transfer or Treat).

Risk treatment involves an iterative process of:

- formulating and selecting risk treatment options (at SMT or equivalent risk review group);
- planning and implementing risk treatment ;
- assessing the effectiveness of that treatment;
- deciding whether the remaining risk is acceptable;
- if not acceptable, taking further treatment.

Selecting the most appropriate treatment option(s) involves balancing the potential benefits derived in relation to the achievement of the objectives.

Note 1: Risk treatment can also introduce new risks that need to be managed.

Note 2: If there are no treatment options available or if treatment options do not sufficiently modify the risk, the risk should be updated (in the *Notes* section within Pentana) and kept under ongoing review. Should the Target Risk Score not be reached, or not be able to be set within the risk appetite level, the Risk Lead must escalate this for discussion and agreement at the SMT (or equivalent risk review group). Should the SMT or risk review group be unable to reduce or influence the scoring, this risk must be escalated to the Risk Management Committee (RMC).

Actions and Workplans (also known as 'action planning' or 'treating the risk')

In situations where a decision is made to **treat** a risk, the next stage of the process involves identifying the options available for mitigating the risk, assessing those options, preparing risk management action plans and implementing them.

An **Action** (or Risk Action) is an agreed task that has to be performed or implemented to help address potential risks, by either reducing the likelihood of these risks occurring and/or reducing the impact of these risks should they occur. Sometimes an action can maintain the risk. Some actions, once implemented, may become controls.

Once the actions are agreed at SMT level (or equivalent risk review group), the **Risk Owner** will enter them into Pentana, following the detailed '*Bite-size Guidance'* available *via* the intranet page under *Support Functions*, '*Risk Management*'.

The Risk Owner has the option to identify and delegate an **Action Owner** particularly when the action is more appropriately managed by a supporting function such as Estates or DDTS, for example. Agreement between the two parties should take place before assigning ownership within Pentana.

Relationship between Actions, Residual & Target Risk Scores

For any risk, should its Residual risk score be unacceptable (*i.e.* a lower Target risk score needs to be achieved) there *must* Action(s) in place to reach that lower Target score, along with the **Target Date which should be approximately one month after the completion date of the last Action,** to allow time to assess the effectiveness of the action and the level of risk.

Diagram 9 shows the relationship between Risks, Parent Workplans and Sub-Actions.

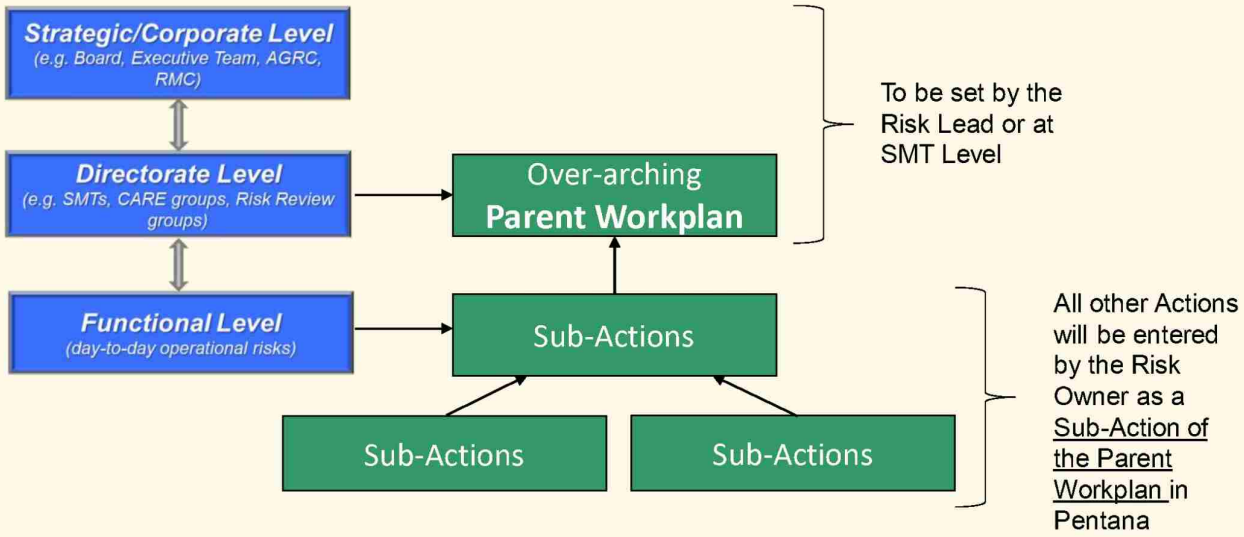


Diagram 9: *Relationship between Risks, the Parent Workplan and Sub-Actions.*

Reviewing Actions

Actions should be reviewed regularly until they are completed, or every time the related Risk is reviewed, *i.e.* **within 6 months for High Red risks (scored 15 or more) as a minimum, and within 12 months as a minimum for all other risks.**

Once an action is completed, the Action Owner should liaise with the Risk Owner to discuss how it has mitigated the risk in reality and whether it has changed the effectiveness of current controls, or if it can become a new control. The risk scores can then be reviewed.

Ideally an action should not increase the risk, however, if there is another benefit then this should be discussed at the appropriate forum (SMT or equivalent risk review group) and the rationale recorded in Pentana in the *Notes* section.

Note: Detailed guidance for adding or updating actions within **Pentana** is available *via* the intranet page under *Support Functions*, *'Risk Management'*, *'Bite-size Guidance'*

Controls

A **control** is a measure that maintains and/or modifies *risk*. It can be preventive, detective and/or corrective in nature. It can be a physical barrier, a process or an activity that maintains/reduces the impact or likelihood of a risk occurring.

Controls include, but are not limited to, policy, procedure, practice, process, technology, technique, method, systems, devices or training. *Risk treatments* can become controls (or modify existing controls) once they are implemented.

Note that controls may not always exert the intended or assumed modifying effect thus it is important to monitoring and review the effectiveness of controls.

Diagram 10 gives examples of the three types of controls used within NHSBT; preventative, detective and/or corrective.

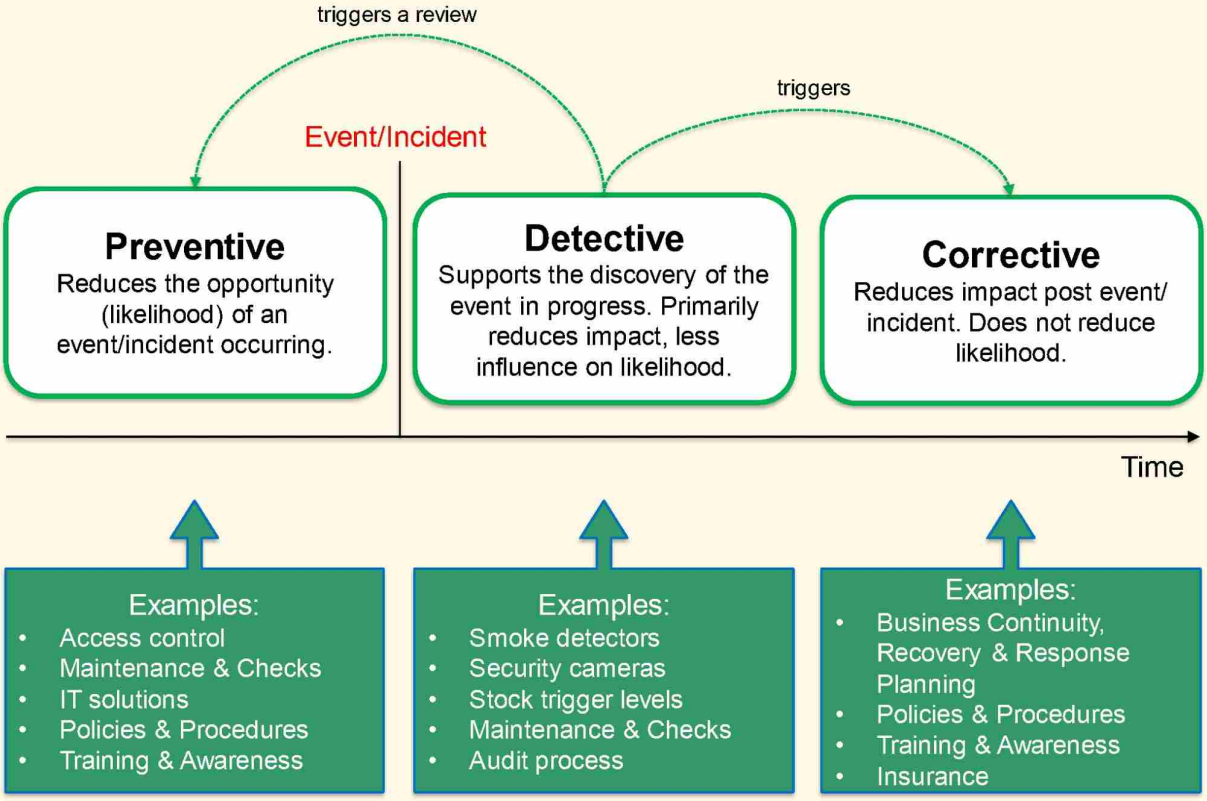


Diagram 10: *Examples of controls used within NHSBT.*

Note: Detailed guidance for adding or updating controls within **Pentana** is available *via* the intranet page under *Support Functions*, '*Risk Management*', '*Bite-size Guidance*'.

Controls in Pentana

The **Risk Owner** must enter controls following the detailed '*Bite-size Guidance'* available *via* the intranet page under *Support Functions*, '*Risk Management*'.

Once the Risk Owner has selected one or more of the pre-set controls within Pentana, they can enter the details of the key controls, assign effectiveness and assurance ratings, and describe any gaps in the controls according to their perception of how the control is mitigating the specific risk.

The Risk Owner and the Control Owner can liaise with each other, as appropriate, to discuss the gaps in controls with the aim to understand those gaps and any improvement actions that may be needed.

Relationship between Controls, Inherent & Residual Risk Scores

The Inherent risk score is the current risk level without (NHSBT's) controls in place, thus once controls are considered and added to Pentana, the Residual risk score must be reduced accordingly to reflect the presence and effectiveness of those controls.

In rare circumstances where the controls are completely ineffective, the Residual score may remain the same as the Inherent score, however, the Risk Owner must enter the rationale in the *Notes* section in Pentana and address or escalate the gap(s) (to their SMT or equivalent risk review group) as soon as practicably possible.

Note: Actions must be put in place to rectify any gaps in the controls.

Reviewing Controls

Controls should be reviewed whenever an Action is completed, or every time the related Risk is reviewed, *i.e.* **within 6 months for High Red risks (scored 15 or more) as a minimum and no longer than 12 months as a minimum for all other risks.**

Control Management and the Effectiveness of Controls

'Control management' is implicit to supporting good risk management. Entering a control into Pentana is not the endpoint of this area of the process. It is about knowing how effective the controls are, and if they are not as effective as they should be, the gaps should be identified and acted upon as soon as practicably possible. **Table 1** below shows the guidance for measuring control effectiveness.

Effectiveness Level	Guidance
Control Not Effective	The control is not appropriately designed or implemented effectively (or there are significant gaps) relative to what is required. Much more could be done.
Control Partially Effective	Even though the control is appropriate, some aspects are not implemented effectively.
Control Fully Effective	The control is as good as practicably possible, both completely appropriate for what it is required to mitigate and implemented as well as it can be.

Table 1: *Guidance for measuring control effectiveness.*

Control effectiveness is a relative measure, not an absolute one. It is relative to how it influences the level of risk in reality. Control effectiveness is really an indicator of risk management effectiveness. Control effectiveness provides a means of prioritising risks for attention. If a risk has low control effectiveness, there is more that could be done, and managers should be investigating and implementing improvement actions. When a high risk has controls that are missing or weak, there must be actions in place to improve the controls.

Assuring Controls – Pentana allows assurance levels to be assigned to controls, and gaps recorded. These are separate to assuring the over-arching management of the risk. The **Risk Owner** can score the effectiveness of controls, and assign assurance levels, by following the detailed '*Bite-size Guidance'* available *via* the intranet page under *Support Functions*, '*Risk Management*'.

Gaps in Controls

Once the controls have been given an effectiveness level, this information can be considered when reviewing the level of the risk. *i.e.* the higher the risk, the more important the effectiveness of the control becomes.

Any gaps should be identified and explained within Pentana. The gaps should focus the Risk Owner's attention to any actions that may be needed to improve those controls. These actions can be entered as 'normal' actions, and there must be at least one remedial action recorded within Pentana to improve controls which are partially or not effective.

Using Pentana:
Recording & Reporting, Monitoring & Review, & Assurances

Recording and Reporting (using Pentana)

Accurate and timely recording and reporting of risks provided transparency and visibility in order to:

- communicate risk management activities and outcomes across NHSBT;
- support NHSBT in the continuous provision of safe, high quality and cost-effective products and services;
- provide information for decision-making;
- improve risk management activities;
- assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

Note: **There must not be any 'draft' risks recorded within Pentana**: Only risks which have been reviewed, challenged and agreed at an SMT (or equivalent risk review group) can be added to Pentana by the Risk Lead, or persons with delegated authority.

Pentana

NHSBT uses the Pentana risk management system to record and report risks. It is a cloud-based performance and risk management software, replacing all previous risk registers.

It is a live system thus provides real-time data when accessed on-line and when senior management reports are automatically generated, hence, it is important that there must not be any 'draft' risks within Pentana.

All Risk Descriptions within Pentana must be articulated as per agreed format:

"There is a risk that…….. caused by…… resulting in……."

Note: Detailed guidance for using **Pentana** is available *via* the intranet page under *Support Functions*, '*Risk Management*', '*Bite-size Guidance*'.

Monitoring and Review

The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes.

Monitoring and review should take place within and throughout all the steps of the risk management process. Monitoring and review include planning, gathering and analysing information, recoding results and providing feedback.

Once a risk assessment has been completed, the Risk Lead is responsible for ensuring the risk is presented to members at the next available SMT (or equivalent risk review group) for the relevant area or directorate.

The detail of each risk presented must be discussed during the meeting and the initial risk description, scores, controls and recommendations/actions to mitigate examined and challenged.

The SMT (or equivalent risk review group) have responsibility to ensure each risk presented to them is discussed and challenged and agreement reached regarding the:

- articulation and accuracy of the risk identified;
- the risk score allocated;
- the controls in place, seeking assurance the controls are in place and their effectiveness;
- establishing any necessary target risk score for the risk.

The purpose of this challenge is to ensure the content and detail of each risk is clear, understood and accepted by the SMT (or equivalent risk review group). Discussions regarding the risks must be recorded in the minutes of that meeting.

Risks at the Corporate or Governance Oversight levels which require adding to Pentana must be communicated to the Risk Management Team who retain responsibility for adding these risks to Pentana.

The following rules apply to the review periods for risks:

P1 Risks (score 15-25):	*Must* be reviewed within 6 months as a minimum from when the risk was added or the previous review date. P1 (High) risks can be reviewed sooner than 6 months as appropriate.
All other Risks:	*Must* be reviewed within 12 months as a minimum from when the risk was added or the previous review date.
Target Date:	This should be set to approximately one month from the

Assurances

An **assurance** is a piece of evidence, usually a document, that describes the effectiveness of a control, for example, audit report, quality and finance reports, key performance indicators, compliance certificates, training records, minutes of a meeting.

The assurance process that provides confidence that business objectives will be achieved with a tolerable level of residual risk. Checking the design and implementation of critical controls is an important component of assurance. Measuring the level of assurance is a way to highlight 'gaps' in assurances so those gaps can be prioritised and minimised.

In NHSBT, assurances are recorded and reported *via* Pentana, enabling the appropriate stakeholders to make decisions and develop policies. The quality and integrity of information or of underlying operational processes must be granular and descriptive enough to provide confidence to stakeholders, whether internal or external to NHSBT.

The importance of assurance

- In the context of risk management, the treatment or mitigation of the risk can be led by the gaps found in assurances (*i.e.* gaps in the controls).
- For most aspects of NHSBT's services, assurances are required to comply with regulatory bodies and to maintain accreditation.
- The Executive Team, the Board and other external bodies require assurances and gaps in assurances as part of their oversight of risks they are responsible for.
- When something goes wrong, analysing assurances allows greater scrutiny of controls.

Assurances in Pentana

Assurances must be documented within Pentana and are a mandatory part of the risk management process. The information will be seen in automatically generated senior management reports, providing a level of 'self-assurance'.

It is important to remember that should this assurance be challenged by an external audit process, any outputs and recommendations from that audit will generally carry a higher weighting and supersede any 'self-assurances' that were previously documented.

Note that assuring the over-arching risk is a separate task (in Pentana), using the 'three lines of assurance' as per 'Bite-size' guidance packages *via* the intranet page under *Support Functions*, '*Risk Management*'.

Archiving Risks and Actions

Note: Risks and Actions must not be deleted in Pentana. They will not be retrievable if deleted.

Should an **action** need to be archived, the *Risk Owner* must ensure:

- the action has been completed and closed within Pentana, with explanation in the *Notes* field of how the action has mitigated the risk;
- if appropriate, that a new control is added to the risk, or the existing control(s) are updated to reflect the completion of the action;
- the over-arching risk is updated to reflect the above steps;
- to notify the Risk Management Team that the action can be archived (by emailing the mailbox pentanariskmanagement@nhsbt.nhs.uk).

Should a **risk** need to be archived, the *Risk Owner* must ensure:

- all actions within that risk have been completed;
- the target score has been reached (and if not, an explanation in the *Notes* field in Pentana, for example, in the cases where the risk has been transferred, terminated or no longer exists);
- the closure of the risk is discussed and agreed by the relevant Risk Lead and SMT (or equivalent risk review group);
- the *Notes* field in Pentana has been completed with an explanation of why the risk can be closed, at which group or committee this was agreed, and the date of agreement.

- The *Risk Lead* must then notify the Risk Management Team, providing the details below (by emailing the mailbox pentanariskmanagement@nhsbt.nhs.uk):
  - risk identification details (*i.e.* Title and Code);
  - confirmation that the risk has been reviewed and is ready for archiving;
  - confirmation that the *Notes* field in Pentana has been completed with an explanation of why the risk can be closed.

Definitions

- A glossary of terms and definitions routinely used are detailed within **Appendix A**.

Related Documents / References

- **FRM6604** Risk Assessment Template

Appendices

- **Appendix A** – Terms & Definitions
- **Appendix B** – Roles and Responsibilities
- **Appendix C** – Guidance for Impact and Likelihood Scoring

Appendix A: Terms and Definitions

An **Accident** is an unplanned *event* that results in personal injury or property damage.

An **Action** (or **Risk Action**) is an agreed task that has to be performed or implemented to help address potential risks, by either reducing the likelihood of these risks occurring and/or reducing the impact of these risks should they occur. Sometimes an action can maintain the risk. Some actions, once implemented, may become *controls*.

Accountability generally means being responsible for one's own actions and being answerable to those actions. Accountability cannot be shared, unlike *responsibility*. In *risk management*, the accountable person is the individual who is ultimately answerable for the risk/decision/activity, and this is the only person assigned to it.

An **Assurance** is a piece of evidence, usually a document, that describes the effectiveness of a control, for example, audit report, quality and finance reports, key performance indicators, compliance certificates, training records, minutes of a meeting.

Authority, in the context of a business organisation, is the power and right of a person to use and allocate the resources efficiently, to take decisions and to give orders so as to achieve the organisational *objectives*.

Board Assurance Framework (BAF) is a document that sets out strategic objectives, identifies risks in relation to each strategic objective along with controls in place and assurances available on their operation. The most effective boards use this as a dynamic tool to drive the board agenda. Formats vary but the framework generally includes: Objective, Principal risk, Key controls, Sources of assurance, Gaps in control/assurance and Action plans for addressing gaps.

Business Partner: An individual in a *Business Partner* role or capacity is an experienced subject matter expert who works cross-functionally with a variety of stakeholders to support the execution of risk and compliance activities to support and drive change across the business, thus enabling and supporting the achievement of organisational *objectives*.

A **Cause (or risk cause)** is the reason why something could go wrong. The existence of the *cause* does not mean the event will happen.

To establish the **Context** means to define the external and internal parameters that organisations must consider when they manage risk. An organisation's external context includes external stakeholders, international environment, as well as any external factors that influence its *objectives*. An organisation's internal context includes internal stakeholders, its approach to *governance*, its contractual relationships, and its capabilities, culture, and standards.

A **Control** is a measure that maintains and/or modifies *risk*. It can be preventive, detective

and/or corrective in nature. It can be a physical barrier, a process or an activity that maintains/reduces the impact or likelihood of a risk occurring. Controls include, but are not limited to, policy, procedure, practice, process, technology, technique, method, systems, devices or training. *Risk treatments* can become controls (or modify existing controls) once they are implemented. Note that controls may not always exert the intended or assumed modifying effect thus it is importance of monitoring review the effectiveness of controls.

An **Event (or risk event)** is an occurrence or change of a particular set of circumstances. In NHSBT we may refer to this as an *incident*. It can be a *risk source*. Events always have causes and usually have *impacts* or *consequences*. Events without consequences are referred to as near misses. A risk event is something that could go wrong; however, the existence of the *cause* does not mean the event will happen.

Governance, in the context of a business organisation, is the system of rules, practices and processes by which an organisation is directed and controlled. At a corporate level, it includes the processes through which the organisations objectives are set and pursued in the context of the social, regulatory and market environment.

A **Hazard** is something that has the potential to cause harm.

The **Impact (or consequence)** is the outcome of an *event* affecting *objectives*. A single *event* can generate a range of impacts which can have both positive and negative effects on *objectives*. Impacts can be certain or uncertain and can be expressed qualitatively or quantitatively. Impacts can escalate through cascading and cumulative effects.

An **Incident** is something that has happened which was not expected or planned. In NHSBT, it is usually unwanted, with the potential to *impact* adversely on NHSBT's *objectives*.

The **Inherent Risk** is a measure of the current risk without the controls which have been put in place by NHSBT. It is derived by multiplying the scores of Impact x Likelihood.

The **Likelihood** is the chance of something happening. It can be thought of as the possibility, probability or frequency of something happening. It can be described objectively or subjectively, qualitatively or quantitatively.

To **Monitor** means to supervise and to continually check and critically observe. It means to determine the current status and to assess whether or not required or expected performance levels are being achieved.

An **Objective** refers to an organisation's stated or unstated aims or responses to address major change, competitiveness, social issues and business advantages. This includes an organisation's response to statutory and regulatory demands, moral expectations, stakeholder requirements and professional guidelines.

A **PESTLE analysis** is a framework to analyse the key factors (Political, Economic, Sociological, Technological, Legal and Environmental) influencing an organisation from the outside.

The **Residual Risk** is the current risk after the identified controls are in place. It is the measure of the risk with controls that NHSBT has put in place, meaning NHSBT has reduced the risk, removed the source of the risk, modified the impacts/consequences, changed the likelihood, transferred the risk or retained the risk.

Responsibility generally means being in charge of something within one's power, control or management. Responsibility can be shared. In *risk management*, the responsible person is the individual who actually completes the assigned tasks or oversees the management/coordination of the completion of the tasks (*i.e.* sharing the responsibility with other individuals who are assigned to complete the tasks).

To **Review** is an activity carried out in order to determine if something is a suitable, adequate, and an effective way of achieving established objectives. This includes, but not limited to, the risk management policy, action plans, risks, risk criteria, risk treatments, risk management controls, residual risks, and risk assessment process.

Risk is the effect of uncertainty on objectives. Risks are things/*events* that might happen, which could result in harm/loss/damage or an opportunity. In NHSBT, this harm, loss or damage could potentially impact adversely on NHSBT's *objectives* including harm to staff/donors/patients/visitors and the delivery of safe, high quality products or services.

A **Risk Action Plan** (or **Workplan**) is the course of *action* which an organisation agrees upon to help them to address potential risks by reducing the likelihood of these risks occurring and/or reducing the impact of these risks should they occur.

Risk Appetite (or risk criteria) is the level of risk that an organisation can (or will) accept. It is used to evaluate the significance or importance of the organisation's risks. They are used to determine whether a specific level of risk is acceptable or tolerable. In practice, risk appetite guides NHSBT to determine the commitment to undertake or continue an activity and informs decisions regarding treatment of the risk(s).

Risk Analysis is the process of understanding the nature of the risk, its characteristics (events, sources, impact, likelihood, *etc.*) and the level of risk, providing an input into risk evaluation and treatment decisions.

Risk Assessment is a process used to evaluate the risk and establish if the current controls are adequate or further action is required to manage the risk. It is the overall process of risk identification, risk analysis and risk evaluation. It is not an end-point process, rather it can be thought of as a tool to enable the generation of action plans if needed.

Risk Evaluation is a process that is used to compare the *risk analysis* results with the *risk appetite* in order to determine whether or not a specific level of risk is acceptable or tolerable.

Risk Identification is a process that involves finding, recognising, and describing the risks that could influence the achievement of *objectives*. It is the process of determining what, where, when, why, and how something could happen. This includes possible sources of risk,

events and circumstances, possible causes and potential impacts. A variety of resources can be used such as historical data, theoretical analysis, informed opinions, expert advice and stakeholder input.

Risk Management refers to a coordinated set of activities and methods that is used to direct an organisation and to control the many risks that can affect its ability to achieve *objectives*. The term also refers an organisation's risk management programme which includes risk management principles, a risk management framework, and a risk management process.

An organisation's **Risk Management Plan** describes how it intends to manage risk. It describes the management components (*e.g.* procedures, practices, responsibilities, activities), the approach, and the resources that are used to manage risk. The plans can be applied to products, processes, projects or to an entire organisation or part of it.

A **Risk Register** is a tool for documenting risks and documenting the management of those risks such as controls, actions and assurances. In NHSBT, this is an online resource, known as Pentana, where all organisational risks that have been agreed at Senior Management level are recorded, monitored and reviewed.

Risk Scoring is the process of measuring the **level of risk**, i.e. its magnitude. It is estimated by considering 'how bad' (*impact or consequence*) a risk may be and 'how likely' (*likelihood*) the impact is to occur. Risk scores can be assigned to a single risk or a combination of risks.

Risk Treatment is a risk modification process. It involves selecting and implementing one or more treatment options (*e.g.* Terminate, Tolerate, Transfer, Treat). Risk treatments become *controls* (or modify existing controls) once they are implemented.

A **Single Point of Failure (SPF)** is a person, facility, piece of equipment, application, or another resource for which there is no redundancy in place. If such a resource goes down, any system or process of which it is an essential part will come to a halt.

A **Source (or risk source)** is an element which alone or in combination has the potential to give rise to *risk*. It is where the risk originates and has the intrinsic potential to give rise to risk. Potential risk sources include at least the following: commercial relationships and obligations, legal expectations and liabilities, economic shifts and circumstances, technological innovations and upheavals, political changes and trends, natural events and forces, human frailties and tendencies, and management of shortcomings and excesses.

A **Stakeholder (or interested party)** is a person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

The **Target Risk** is the acceptable level of risk, as defined by an organisation's *risk appetite*, which is achievable with the implementation of agreed actions. A target risk score is specific to an individual risk and should be a realistic and achievable goal with the current available resources. It should not be thought of as a 'short-term' risk reduction target. The target risk should be the best residual score that could be achieved once all actions are completed.

Terminate the risk – Avoid the risk by deciding not to start or continue with the activity that gave rise to the unacceptable risk. Alternatives are to choose a different or less risky activity/approach. If removed, the risk can be archived in the risk register. Decision to be discussed and agreed by the relevant SMT (or risk review group). This also applies to 'archiving' risks in Pentana.

Tolerate the risk – Accept and retain the risk through an informed decision that the risk is at an acceptable level (within pre-agreed appetite/tolerance level). This may apply to situations where a residual risk remains after other treatment options have been put into place. No further action is needed to treat the risk, but ongoing monitoring is still expected.

Transfer the risk – Implement an action plan that moves or shares the risk with another party such as outsourcing through third party contracts or insurance. No extra action is needed to treat the risk, but ongoing monitoring is still expected. Decision to be discussed and agreed by the relevant SMT (or risk review group). This also applies to 'archiving' risks in Pentana.

Treat the risk – Implement an action plan that reduces the impact and/or likelihood to an acceptable level, where elimination of the risk is considered to be excessive in terms of time or expense. Ongoing monitoring is expected.

Appendix B: Roles and Responsibilities

General
All Staff All members of staff (including those acting on behalf of NHSBT *e.g.* temporary staff, agency, and contractors) are responsible for maintaining risk awareness, identifying and escalating risks as appropriate to their Supervisor or Line Manager. In addition, they will ensure that they familiarise themselves and comply with NHSBT's policies and procedures and attend mandatory and other relevant training courses.
Supervisors and Line Managers • Following notification (from any source) of a risk, Supervisors and Line Managers (including Risk Leads) are responsible for deciding on the necessary course of action and whether it is appropriate to arrange for a formal risk assessment to be undertaken. • The Supervisor or Line Manager must provide timely feedback to the reporting member of staff with a simple explanation how the risk/concern will be managed (*e.g.* whether 'no further action required' or 'a formal risk assessment will be undertaken'). • Any and all risks that are deemed genuine must be discussed and approved at senior management team (SMT) level (or risk review group), thus it is the responsibility of the Supervisor or Line Manager to escalate the risk up their management chain to the appropriate Risk Lead and/or SMT group.
Individuals
Chief Executive Officer (CEO) As Accountable Officer, the Chief Executive has responsibility for maintaining a sound system of internal control that supports the achievement of the organisation's objectives. To support this responsibility the Chief Executive Officer will: • ensure that management processes fulfil the responsibilities for risk management as set out in the Risk Management Manual (MPD1336); • ensure that full support and commitment is provided and maintained in every activity relating to risk management; • ensure planning for adequate staffing, finances and other resources is undertaken; • ensure an appropriate Board Assurance Framework (BAF) is prepared and regularly updated and receives appropriate consideration; • ensure that an Annual Governance Statement, adequately reflecting the risk management issues within NHSBT, is prepared and signed off each year; and • define and endorse the risk management policy (statement of intent) on behalf of the Board and Executive Team.
All Executive Directors (Portfolio Owners) • Executive Directors will ensure that risk is a regular item on their Senior Management Team (SMT) agendas, and that risk registers incorporate risk arising from both normal business and change programmes. • They will also ensure that risk registers are used as one of the principal inputs in development of directorate strategy and that all activities undertaken within their directorates are consistent with the safe operation of NHSBT. • Lead implementation of strategy across NHSBT. Manage performance within their area and deal effectively with suboptimal outcomes; • Actively support and promote a positive culture for the organisation and reflect this in their own behaviour. Nurture good leadership at all levels, actively addressing problems impacting staff's ability to do a good job; • Take principal responsibility for providing accurate, timely and clear information to the Board.
Director of Strategy The Director of Strategy is the lead director for risk management and is delegated by the CEO to: • chair the Risk Management Committee; • determine risk management performance indicators that align with NHSBT's other corporate performance indicators; • align risk management objectives with NHSBT's corporate objectives and strategies; • assign accountabilities and responsibilities at appropriate levels within the organisation; • 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 appropriate.

All Non-Executive Directors (NEDs)

- Bring independence, external perspectives, skills, and challenge to strategy development;
- Actively support and promote a healthy risk culture for NHSBT and reflect this in their own behaviour;
- Provide visible leadership in developing a healthy culture so that staff believe NEDs provide a safe point of access to the Board for raising concerns;
- Satisfy themselves of the integrity of information and intelligence.

Risk Leads

The Risk Lead will:

- be a 'champion' for risk management within their directorate, function or department, helping to develop a positive culture within their area and at their SMT meetings, encouraging open, expert and honest discussions around risk;
- coordinate the risk management process at their appropriate Governance Oversight meetings in accordance with NHSBT's Risk Management Manual (MPD1336);
- co-operate with their Director to ensure that risk is discussed as an item on the directorate SMT agenda according to the meeting's terms-of-reference (within 12 months as a minimum). High-level risks (residual score of 15 or more) must be discussed within 6 months as a minimum or sooner if appropriate;
- provide regular briefings to the responsible Director regarding the status of risks and associated actions within their area of responsibility;
- ensure that risks are escalated/communicated to the appropriate division or area of business;
- provide timely feedback (describing the next actions and/or outcome) to staff who have raised a risk to them;
- provide guidance and support to Risk Owners;
- ensure resilience within their directorate, function or department with regards to appointing deputies to manage risks, actions or controls in the absence of currently appointed persons;
- Risk Leads have the authority to delegate responsibilities and/or actions from the risk management process, however, the SMT retains overall responsibility for the risk management process for their directorate.

The Risk Lead must:

- raise risks to the stakeholders of their SMT (or equivalent risk review group) in these circumstances:
  1. Any High (Red) risks that cannot wait for discussion at the next scheduled SMT (or equivalent) must be raised immediately to the stakeholders of the group;
  2. Should the option of transferring or terminating a risk be chosen, this must be discussed and agreed by the relevant SMT (or equivalent). This also applies to 'archiving' risks in Pentana;
  3. Should the Target Risk Score of a risk not be reached, or not be able to be set within the risk appetite level, this must be escalated for discussion and agreement at the SMT (or equivalent). Should the SMT (or equivalent) be unable to reduce or influence the scoring, this risk must be escalated to the Risk Management Committee (RMC).

All Heads of Centres (HoC)

- The HoC, along with the site Estates & Facilities Manager, is responsible for reviewing and escalating the site-level risks associated with their centre (as required, but at least once a year).
- Subject matter experts may be included in discussions as appropriate (*e.g.* Quality, Health, Safety & Wellbeing, Business Continuity, *etc.*).
- Risks must be updated on Pentana by the assigned Risk and/or Action Owner.
- The HoC must ensure that site-level risks are escalated to the appropriate function (*e.g.* via Centre Partnership Committee (CPC) meetings) and/or area of business in a timely manner.

Oversight Bodies

NHSBT Board

- The Board is responsible for ensuring that NHSBT has appropriate risk management processes in place to deliver the strategic plan, comply with the registration requirements of regulators and satisfy the requirements of the 2005 Statutory Instrument. This includes systematically assessing and managing its risks;
- Risk management by the board is underpinned by four interlocking systems of control: (i) The Board Assurance Framework (BAF), (ii) Organisational Risk Management, (iii) Audit and (iv) The statement on internal control;
- The approach to risk management needs to be systematic and rigorous. However, it is crucial that boards do not allow too much effort to be expended on processes. What matters substantively is recognition of, and reaction to, real risks – not unthinking pursuance of bureaucratic processes.

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.

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.

Other Roles

Risk Owners

- A Risk Owner is an individual who has been given the autonomy and responsibility for the addition and overall management of NHSBT's response to a particular risk recorded within Pentana.
- In Pentana, when adding a new risk, the Risk Owner is responsible for adding Controls and Actions as appropriate. Should the tasks need to be delegated, the Risk Owner is responsible for nominating the Action Owners where appropriate.
- The Risk Owner is responsible for providing information regarding the effectiveness of key controls for each risk, according to their perception of how the controls are mitigating those risks in reality.
- The Risk Owner is responsible for the overall management of the risk but will not be held accountable should the risk eventuate, or the event comes to pass.
- The Risk Owner is required to provide assurance, to Risk Leads, that the risk is being managed and actions are on target or to raise concerns or barriers to completing the actions.
- There must only be one risk owner per risk at any level.
- Guidance and support are provided by the Risk Lead.
- For each risk, should the appetite and/or treatment(s) be different to the guidance stated in this manual (MPD1336), the Risk Owner must provide sufficient justification within Pentana.

Control Owners

- A Control Owner, in conjunction with the Risk Owner, is responsible for reviewing, updating and maintaining the effectiveness of current controls in place.
- The Control Owner is responsible for providing assurance regarding control effectiveness to the Executive Team and Board at an agreed frequency.

Action Owners

- An Action Owner is responsible for completing the assigned actions/tasks or overseas the

management/coordination of the completion of the tasks, which when implemented will either remove or mitigate the given risk.

- The Action Owner is responsible for providing regular updates, at a frequency agreed with the Risk Owner.
- Once the action is completed and implemented, it is the responsibility of the Action Owner to communicate this with the Risk Owner.

Business Partner Risk Leads

- Business Partner Risk Leads are subject matter experts from NHSBT's Support Services such as: Health & Safety, Quality, Business Continuity, People, Clinical, DDTS, Estates & Facilities, Finance, Communications and Risk.
- They have a key role in supporting their associated areas of business with regards to (i) understanding the related risks, (ii) challenging the details of the risk and the controls/actions to ensure they are appropriately recorded and managed, (iii) escalating the risk to their own SMT (or equivalent risk review group) for consideration, and (iv) communicating any risks their own SMT has identified across to the relevant Risk Leads.
- They may take on the responsibilities (or appropriately delegate) the actions that their team performs to mitigate a given risk, however, the Directorate or Functional area retains the ownership (and thus oversight) of the risk because it impacts on their area of business.
- The Risk Management Team have a Business Partnering role and are also responsible for coordinating NHSBT's Risk Management Programme, including relevant Training and Awareness programmes. All High risks (residual score of 15 or more) will be highlighted to the Executive Team through assurance reports from the Risk Management Team.

Authors and Owners of risk documents

Authors and Owners of any risk-related documentation produced for use within NHSBT have a responsibility to liaise with the Risk Management Team during risk-related documentation development. This is to ensure risk management processes (and associated training) across the organisation (*e.g.* Health, Safety& Wellbeing, Quality, *etc.*) remain consistent.

Appendix C: Guidance for Impact and Likelihood Scoring

Note: This guidance gives *examples* of some risk scenarios and is not an exhaustive list.

Primary Risk Impact Area (Area which is the most significantly impacted)	Impact Score Guidance and ***examples*** of descriptors				
	1	2	3	4	5
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
General	No impact on NHSBT's objectives	Only minor impact to NHSBT's objectives	Moderate impact on NHSBT's objectives	Could significantly impact on NHSBT's objectives	Would have significant impact on NHSBT's objectives and requires a radical review
Business Continuity Impacts arising from hazards to assets; buildings and other physical assets, people, services and resources, *e.g.* interruptions to business, power failure, fire, death, injury, theft, loss of supplier, weak business continuity plans.	Minor or no loss/interruption. No delay to the delivery of key products / services. No reputational or financial implications.	Loss/interruption of less than 1 working day. Minor delay to the delivery of key products / services. Minor reputational or financial implications.	Loss/interruption between 1 working day – 1 week. Moderate delay to the delivery of key products / services. Moderate reputational or financial implications.	Loss/interruption of more than 1 week. Major delay to the delivery of key products / services. Major reputational or financial implications.	Permanent loss of service or facility. Complete inability to deliver key products / services. Catastrophic reputational or financial implications.
Clinical Harm (or potential harm) to patients or donors during the course of NHSBT activities or treatments.	Minimal injury requiring no/minimal intervention or treatment. No time off / < 3 days off work.	Minor injury or illness, requiring minor intervention. Requiring time off work for >3 days. Increase in length of hospital stay by 1-6 days.	Major injury leading to long-term incapacity / disability. Requiring time off work for 7-15 days. Increase in length of hospital stay by 7-15 days. RIDDOR / agency reportable incident.	Increase in length of hospital stay by >15 days. Mismanagement of patient care with long-term effects. Death of a single patient / donor. Multiple permanent injuries or irreversible health effects.	Systematic failures. Incident leading to death. An event which impacts on a large number of patients. Catastrophic reputational or financial implications.
Compliance, Regulatory or Quality Impacts arising from failure to comply with laws and regulations, from commercial liabilities included in contractual arrangements and loss of intellectual property. Failure to maintain quality standards set by NHSBT.	No or minimal impact or breech of guidance or statutory duty. Recommendation for improvement to internal standards. Small number of minor issues requiring improvement.	Single failure to meet internal standards or follow protocol. Multiple minor recommendations which can be easily addressed by local management. Reduced performance rating if unresolved. Product / service effectiveness or performance rating will be reduced if the recommendations are unresolved.	Repeated failure to meet internal standards or follow protocols. Major audit finding by statutory regulator or single breech in statutory duty. Improvement notice. Product / service has moderately reduced effectiveness or performance rating.	Repeated or significant failure to meet external standards, national guidance, standards, regulations or legislation. Multiple major audit findings or single critical findings by statutory regulator. Multiple material breeches in statutory duty. Improvement notices. Critical report. Prohibition notice. Enforcement action. Major reputational or financial implications. Product / service has low effectiveness or performance rating.	Multiple critical or gross failure to meet external standards, national guidance, standards, regulations or legislation. Multiple breeches in statutory duty with high likelihood of enforcement action. Severely critical report with catastrophic reputational or financial implications. Product / service has unacceptably low effectiveness or performance rating. Ombudsman inquiry/ inquest/ prosecution.

Competitive Impacts arising externally from actions of customers, suppliers, competitors, new entrants or substitute services, especially in respect to pricing and development of new channels to market.	Minimal or no impact to NHSBT's current market position. Income / profitability is minimally or not affected. Minimal or no loss in customer confidence or public profile.	Minor impact to NHSBT's current market position. Loss in income / profitability <15%. Minor loss in customer confidence or public/stakeholder profile.	Moderate impact to NHSBT's current market position. Loss in income / profitability 15-29%. Moderate loss in customer confidence or public/stakeholder profile.	Major impact to NHSBT's current market position. Loss in income / profitability 30-50%. Major loss in customer confidence or public/stakeholder profile. NHSBT unable to gain market position for one product / service.	Catastrophic impact to NHSBT's current market position. Loss in income / profitability >50%. Total loss in customer confidence and/or public /stakeholder profile. NHSBT completely unable to gain any market position for multiple products / services.
DDTS Systems and Technology Impacts arising from the use of technology (software and hardware), telephony, operational and information systems, infrastructure, reliance on legacy systems, unsupported technology, weak disaster recovery plans.	No impact on NHSBT's objectives.	Only minor impact to NHSBT's objectives.	Moderate impact on NHSBT's objectives.	Could significantly impact on NHSBT's objectives.	Would have significant impact on NHSBT's objectives and requires a radical review.
Environmental Actual or potential threat of adverse effects on living organisms and the environment arising from NHSBT's activities including effluent, emissions, waste.	Minimal or no impact on the environment. No legislation applies. No interested party concerns.	Minor impact on environment. Direct or potential legislation. Minimal or no management needed. Of low concern to interested parties.	Moderate impact on environment. Direct legislation. Infrequent management needed. Would negatively affect reputation in local area.	Major impact on environment. Direct legislation. High level of management needed. Failure would require significant remedial action by NHSBT management. Would negatively affect reputation nationally. Potential to adversely affect achievement of NHSBT's sustainability strategy aims.	Catastrophic impact on environment. Direct legislation. High level of management needed. Failure would require notification to enforcement agency. Total loss in public / customer / stakeholder confidence. Potential to prevent achievement of NHSBT's sustainability strategy aims.
Financial Impacts arising from financial transactions and accounting and reporting requirements, *e.g.* fraud, interest exposures and treasury management, misstated management and financial accounts, misleading or omitted disclosures.	Small loss. Risk of claim remote.	Claim less than £10,000.	Claim(s) between £10,000 and £100,000.	Claim(s) between £100,000 and £1 million. Purchasers failing to pay on time. Uncertain delivery of key objective.	Claim(s) >£1 million. Loss of contract / payment by results. Failure to meet specification / slippage. Non-delivery of key objective.
Health, Safety and Wellbeing Physical or psychological harm to people (staff, public, contractors, visitors) associated with NHSBT's processes and/or those within the care of NHSBT's sites/management.	Minimal injury requiring no/minimal intervention or treatment. No time off or <3 days off work.	Minor injury or illness, requiring minor intervention. Requiring time off work for >3 days.	Moderate injury requiring professional intervention. Requiring time off work for 4 - 14 days. RIDDOR / agency reportable incident.	Major injury leading to long-term incapacity / disability. Requiring time off work for >14 days.	Incident leading to death. Multiple permanent injuries or irreversible health effects.

Information Governance and/or Information Security Impacts arising from the possible compromise to the security, confidentiality, integrity and availability of NHSBT's information assets; *e.g.* unauthorised access or use, disclosure, disruption, storage, modification or destruction of key personal and organisation information.	Minor breach of confidentiality. Single individual affected.	Breach with potential for theft, loss or communicating / sharing inappropriate information with between 20 – 50 people affected. Theft, loss or clinical information of up to 20 people affected (unencrypted media).	Breach with potential for theft, loss or communicating / sharing inappropriate information with between 50 – 100 people affected. Loss or misuse of very sensitive / confidential information relating to 2-5 persons. Potential for local media coverage due to IG breach. Potential reduction in public / customer / stakeholder confidence.	Serious breach with potential for theft, loss or communicating / sharing completely inappropriate information with between 100 - 500 people affected. Loss or misuse of very sensitive / confidential information relating to 5-20 persons. Local media coverage due to IG breach, potential for national media coverage. Reduction in public / customer / stakeholder confidence.	Major breach with potential for theft, loss or communicating / sharing completely inappropriate information with over 500 people affected. Loss or misuse of extremely sensitive / confidential information relating to over 20 people (*e.g.* sexual health information, along with names and addresses). National media coverage due to IG breach. Total loss in public / customer / stakeholder confidence.
Reputational Negative publicity, negative public perception or uncontrolled events that could have an adverse impact on public, customer or stakeholder confidence in NHSBT's service provision or quality of products.	Rumours. Potential for public / customer / stakeholder concern.	Local media (or social media) coverage – short-term reduction in public / customer / stakeholder confidence. Elements of public / customer / stakeholder expectation not being met.	Local media (or social media) coverage – long-term reduction in public / customer / stakeholder confidence.	National media (or social media) coverage with <3 days service well below reasonable public / customer / stakeholder expectation.	National media (or social media) coverage with >3 days service well below reasonable public / customer / stakeholder expectation. MP concerned (questions in the House). Total loss in public / customer / stakeholder confidence.
People Impacts arising from employees and their relationship with NHSBT; *e.g.* inability to recruit staff to key areas, shortage of skilled staff, loss of essential people, high turn-over, difficulty in retaining staff, low morale, poor development programmes, ineffective succession planning, industrial action.	Short-term low staffing level (or key-skills) that temporarily reduces quality of services (< 1 day).	Low staffing level (or key-skills) that reduces the quality of services.	Late delivery of key objective/service due to lack of staff (or key-skills). Unsafe staffing level or competence (>1 day). Poor staff attendance for mandatory / key training. Low staff morale.	Uncertain delivery of key objective/service due to lack of staff (or key-skills). Unsafe staffing level or competence (>5 days). No staff attending mandatory / key training. Very low staff morale.	Non-delivery of key objective/service due to lack of staff (or key-skills). Ongoing unsafe staffing levels or competence. No staff attending mandatory / key training on an ongoing basis. Extremely low staff morale.

	Likelihood Score Guidance				
Description	Rare	Unlikely	Possible	Likely	Almost Certain
Score	1	2	3	4	5
Definition	Probably never happen	Do not expect it to happen, but it is possible	It is possible it may happen	Highly likely to happen	Likely to occur in the majority of cases
Timeframe	5-yearly	Annually	Monthly	Weekly	Daily
Probability	<10%	10-20%	20-60%	60-90%	>90%