Annex 3

NHS England Risk Management Framework

Version 30 June 2025

Version	Date	Summary of changes
V1.0	September 2019	Drafted by Senior Risk Manager, signed off by 17 May 2019 ARAC 'pending Executive and Board level discussions on risk appetite'
V2.0	November 2019	Risk appetite added, signed off by NHS England (NHSE) ARAC in July 2019 and by the NHS Improvement (NHSI) Board, on behalf of NHSI, in October 2019
V3.0	September 2022	Risk appetite updated (with version agreed in June 2021) Reference to NHSI removed Executive Risk Management Group replaced by Executive Risk Group Introduces Risk Coordination and Escalation Group Clarifies risk escalation process. Signed off by the Chief Risk Officer in September 2022 and by NHSE ARAC, by correspondence, in October 2022
V4.0	2025	Full review to restructure and simplify the document

Beware when using a printed version of this document. It may have been subsequently amended. Please check online for the latest version

Contents

Supporting documents associated with the Risk Management Framework

NHSE Risk Appetite
NHS England risk management process and procedures manual

1. Introduction

Good risk management is a critical success factor for an organisation such as NHSE. Risk is inherent in everything we do. NHSE will ensure that decisions made on behalf of the organisation are taken with consideration to the effective management of risks. The aim of this framework is to:

- define NHSE's approach to risk management and its governance, and set out the processes and tools used to manage risk
- set out roles and responsibilities of staff for managing risks, to ensure consistency and accountability
- provide consistency across the organisation by articulating a single methodology for managing risk and establishing a common risk language.

As a result of implementing this Risk Management Framework:

- the Board will have a means of receiving assurance that strategic and operational risks are being identified and managed
- risk management will become an integral part of NHSE's culture
- risk management will be integrated into activities across the organisation, including policy making, planning and decision making
- adverse incidents, risks and complaints are minimised through effective risk identification, prioritisation, treatment and management.

The underlying risk principles applied throughout this framework are consistent with the overarching principles of

- UK Government's Orange Book: Management of Risk – Principles and Concepts
- ISO 31000:2018 Risk Management – Guidelines
- The UK Corporate Governance Code 2024 and the Financial Reporting Council's Guidance on Risk Management, Internal Control and Related Financial and Business Reporting.

An overview of helpful terms used in relation to risk management is included at *Annex 1: Risk management terms and*

2. Scope

This framework is intended for use by all NHSE employees, Non Executive Directors, contractors, secondees and consultants who carry out duties on behalf of NHSE. The broad principles of the framework also apply to Commissioning Support Units (CSUs), although they will have their own local arrangements for recording and governance.

It is applicable to all risks, both strategic and operational, that NHSE could be exposed to.

To avoid duplication of the same area of concern as both an issue and a risk, **issues are out of scope for this framework**. Management of issues will either be through programme / project management reporting, or through existing local management reporting. This ensures that the risk management process is focused and is not overwhelmed by the demands of issue management. Materialised risks (i.e. pre-identified risks that later become issues) will continue to be tracked via the risk reporting process to ensure adequate visibility and provide assurance that they are being controlled, however they may be managed separately. Issues that may impact existing risks should be considered when undertaking risk review exercises.

2.1 Roles & responsibilities

Each area of the organisation must undertake an ongoing robust assessment of risks and escalate risks through NHSE's governance and escalation route, as set out in the NHSE Risk management process and procedures manual. **It is the responsibility of all staff to maintain risk awareness, identifying and reporting risks as appropriate to their line manager and / or director.** Annex 2: Roles & Responsibilities summarises risk roles and responsibilities for:

- All staff
- Risk Owners
- Risk Register Owners, e.g. including Heads of function, Programme Directors
- Directorate / Region embedded risk colleagues, Directorate / Regional SLTs
- SLT Risk Leads
- Executive Risk Group
- Executive Corporate Group
- Audit & Risk Assurance Committee
- Other Board Committees
- Board
- Executive Directors
- Chief Risk Officer
- Risk Management team

3. Risk Appetite

The Board is responsible for risk appetite and has developed a Risk Appetite Statement which forms part of NHSE's overall risk management strategy and will guide staff in their actions and ability to accept and manage risks.

NHSE define risk appetite as 'the amount of risk that we are willing to take, retain or tolerate in the pursuit of our objectives'. It is key to achieving effective risk management and should be considered before risks are addressed. Risk appetite within NHSE is:

- set by the Board
- aligned with NHSE's strategic objectives and principal risks
- integrated with our control culture, balancing our propensity to take risk with the propensity to exercise control
- not a single, fixed concept. There will be a range of appetites for different risks and these appetites may vary over time; in particular the Board will consider varying the amount of risk which it is prepared to take as circumstances change i.e., during periods of increased uncertainty or adverse changes in the operating environment.

The purpose of risk appetite within the organisation is to:

- provide awareness and an overall view of our risk profile, giving context to our risk position and exposure
- help guide and steer decision making across the organisation by providing a position against which potential decisions can be tested and challenged
    - when considering threats, risk appetite sets the level of exposure which is considered acceptable should the risk be realised. It balances the cost (financial or otherwise) of constraining the risk with the cost of the exposure should it become a reality.
    - when considering opportunities, risk appetite considers how much we are prepared to actively put at risk to obtain the benefits of the opportunity. It is about comparing the value (financial or otherwise) of potential benefits with the losses which might be incurred.

Due to the nature of the organisation and its duties, a one-dimensional and heavily quantitative approach to risk appetite would not drive the right results. To support consistency and enable staff to take well calculated risks to improve delivery when opportunities arise, and also to identify when a more cautious approach should be taken to mitigate a threat, the NHSE Board has adopted a qualitative approach to risk appetite and has structured risk appetite around several principal risk types. Each Risk Owner should determine which risk appetite category their risks best align to.

All risks should be analysed with risk appetite in mind. Where target scores remain outside the agreed appetite level, additional mitigations will need to be proposed, or a decision taken by the appropriate governance forum to tolerate a position of operating outside of appetite.

4. Managing risks

Effective risk management enables NHSE to monitor and address the risks that would prevent the organisation achieving its aims and objectives. It ensures there are controls in place to mitigate the risks and sets out treatment plans for those risks that are not yet within risk appetite.

4.1 Risk register structure

Risks are linked to objectives and strategic aims, which exist at different levels. These levels are reflected in the risk register structure.

Table 1: Risk register structure

Risk Register	Risk Register Owner	Risks that would feature here
Strategic Risk Register	The Board & Executive	Key organisational risks related to strategic decisions or objectives, usually longer term in nature and mitigated through actions such as political negotiation, scenario planning and strategic decision-making.
Operational Risk Register	The Board & Executive	Key organisational risks related to systems, processes and 'on the ground' delivery. These types of risk are often shorter term, with the potential to affect day to day activity, and are largely mitigated through process improvement, risk-based audits, employee training, and the implementation of systems.
Level 1	National Executive, or Regional Director	Risks that are related to the delivery of Directorate or Regional objectives and have the potential to become key organisational risks. They require oversight from the national/regional director and their senior leadership team.
Level 2	Sub-directorates / teams immediately below directorates and regions, including portfolios	Risks that are related to the delivery of team objectives and have the potential to threaten delivery of a directorate or regional objective should they not be adequately mitigated.
Level 3	Sub teams, including programmes	Risks that are related to the delivery of sub-team operations and objectives and have the potential to threaten delivery of a broader objective should they not be adequately mitigated.
Level 4	Individual teams, pieces of work and projects	Risks that are related to the delivery of individual team operations and objectives and have the potential to threaten delivery of a sub-team objective should they not be adequately mitigated.

4.2 Risk management process

NHSE's Risk management process and procedures manual is a document that sets out key activities to be undertaken during a risk's lifecycle. The risk management process is summarised below and can be accessed in full here.

4.2.1 Identification and scoring

The risks we manage across NHSE are complex and often multi-factorial, with impacts straddling several of our business areas. Our risks are nuanced and rarely able to be assessed using quantitative methods. Therefore, the risk scoring guidance set out within the NHSE Risk management process and procedures manual should be applied by the subject matter experts articulating and managing each risk, with risk score calibration then taking place within the risk management governance framework to ensure consistency.

NHSE's risks should be scored at the point they are identified. For each risk on our risk registers, we should determine:

- its inherent score: the level of risk before any action has been taken to manage it or if existing controls failed entirely
- its current score: the level of risk that remains after all existing controls have been applied
- where risks are outside acceptable levels of tolerance, a target risk score: the level of risk that is expected to remain once future mitigations are in place.

All scores must be recorded in the relevant risk register in CoreStream.

4.2.2 Treatment

Once a risk has been identified, the risk owner needs to consider how it will be treated. There are many treatment options: you can avoid the risk, you can remove the source of the risk, you can modify the consequences, you can change the likelihood, you can share the risk with others[1], you can simply retain or accept the risk, or you can even increase the risk to pursue an opportunity. The level and type of treatment will vary depending on the level of residual risk that has been determined and the tolerance for managing risk to within its risk appetite.

To change the risk's likelihood and/or consequences, existing controls will need to be enhanced, or new controls implemented. A risk action plan (also referred to as a risk mitigation plan) should be put in place to address any gap in controls.

If a risk is being accepted it still needs to be regularly monitored, as circumstances may change which could result in different treatment in the future.

4.2.3 Review

Risk should be considered regularly as part of the normal flow of management information about the organisation's activities and in significant decisions on strategy, business planning,

[1] Risk sharing is the practice of distributing risks amongst several organisations, departments or teams to provide alternative approaches to mitigating the risk. It is largely used in financial organisations, often relating to insurance.

major new projects and programmes, and other prioritisation and resource allocation decisions.

It is NHSE's **minimum expectation that risks will be reviewed quarterly by risk owners and considered collectively by the appropriate management forum on the same timescale.** Evidence of such reviews may be required to assess compliance with the framework across the organisation.

4.3 Recording risks

CoreStream is the system that we use to manage all risks at NHSE, therefore all risks must be recorded on the platform and cannot be kept locally; this includes programme risks. Using a single platform allows:

- adopting a shared risk management language
- effective risk escalation
- oversight and assurance
- risk aggregation.

NHSE's risk registers allow regions and directorates to capture all the information needed to manage risk appropriately and determine whether any risks should be escalated through our governance structure. Risk registers should be kept up to date and reviewed no less than quarterly. New risks should be added as they are discovered.

4.4 Risk governance

Risk governance is a fundamental part of corporate governance and the broader internal control system. Risk governance refers to the architecture within which risk management operates in NHSE.

Good risk governance:

- gives a clear structure of risk responsibility throughout the organisation so that everybody is aware of their own risk responsibilities and accountabilities and those of others with whom they work
- establishes clear and effective lines of communication up and down the organisation and a culture in which good and bad news travel freely
- results in risk being accepted and managed within known and agreed risk appetites.

4.4.1 Three Lines Model

NHSE utilises The Three Lines[2] (of defence) model to govern our risks and demonstrate that we are managing the organisation well.

The three lines model provides a structure for describing the assurance activity related to risk management across the organisation. It gives regions and corporate teams autonomy for identifying, managing and reporting risk; with our specialist functions such as the corporate risk management and legal teams providing oversight; and internal/external audit providing independent assurance.

[2] The Orange Book now refers to what was previously known as the Three Lines of Defence Model as the Three Lines Model. This model was developed by The Institute of Internal Auditors and is a long standing industry standard. three-lines-model-updated.pdf (theiia.org)

4.4.1a The first line of defence

The first line of defence relates to functions that own and manage risk. Staff and managers working in regions and corporate teams have direct ownership, responsibility, and accountability for identifying, managing and controlling risks to their objectives. Assurance is provided through the monitoring and reporting of risk and control activities through senior leadership/management team meetings. This can include the review of performance metrics, deep dive reviews of concern areas, etc. and it is ongoing.

4.4.1b The second line of defence

The second line of defence relates to functions that oversee or specialise in risk management and compliance. They guide, support, and challenge the first line by bringing expertise and subject matter knowledge to help ensure risks and controls are effectively managed and assured. The corporate risk management team and other internal oversight teams such as governance, legal, IT, performance/business planning, finance and HR (among others) form the second line of defence and are responsible for co-ordinating, facilitating and overseeing the organisation's effectiveness and integrity.

Each directorate and region should consider and document how the second line will be enacted within their area of the organisation.

4.4.1c The third line of defence

The third line of defence relates to functions that provide independent assurance, namely audit. It provides assurance to senior management and the Board over both the first- and second-lines' efforts.

Internal audit and external scrutiny through the National Audit Office provide independent, objective assurance and challenge concerning the integrity and effectiveness of risk management and internal control. Assurance is provided through monitoring and reporting of strategic/corporate risk and control activities through the Audit and Risk Committee (ARC).

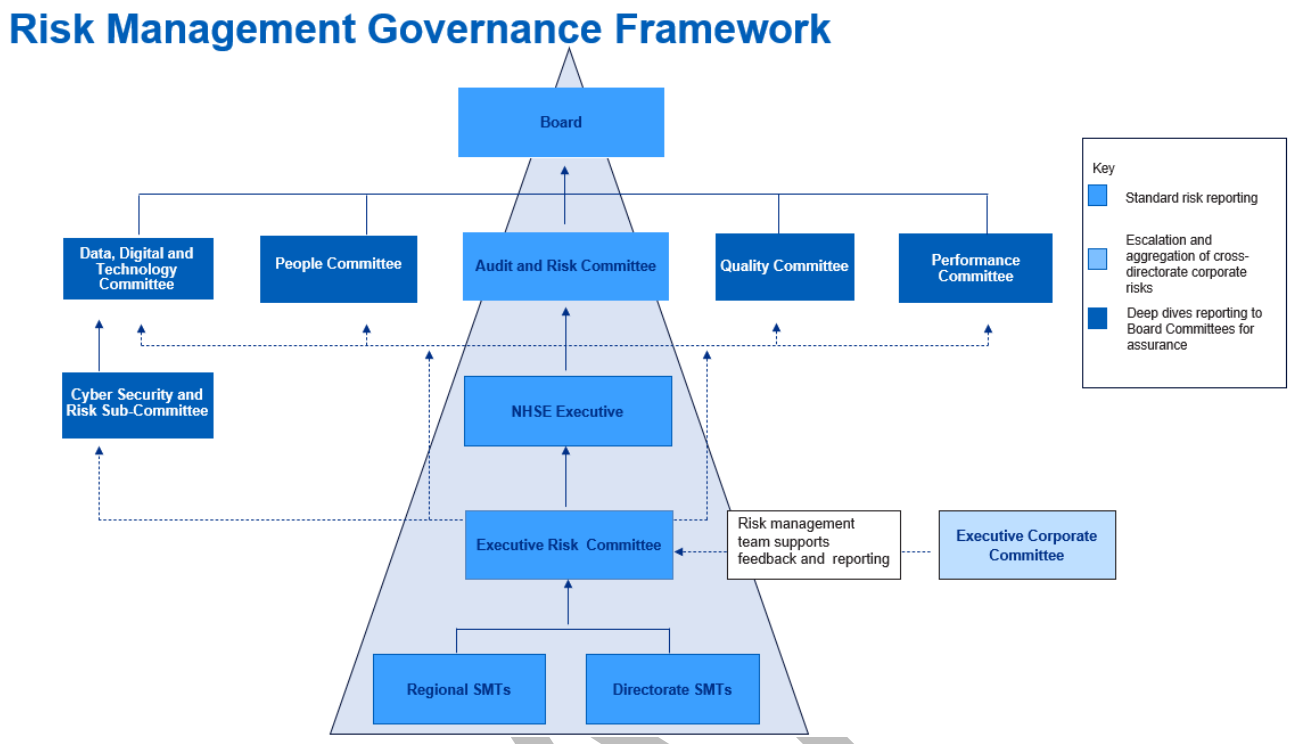
4.4.2 Risk governance for the Strategic Risk Register (SRR) & Operational Risk Register (ORR)

The Executive Risk Group will be responsible for overall risk oversight and approval, while Board committees will receive assurance on the effective management of those strategic risks, and top operational risks, that fall under their remit.

The **Executive Risk Group** will be responsible for assessing and challenging the effectiveness of risk mitigation plans, ensuring relevant actions are implemented and escalating as appropriate to the NHS Executive. In addition to reviewing the Strategic and Operational risk registers at each meeting, they will get risk based deep dives of those risks where:

- the current score has increased or is expected to increase steeply
- it is consider that the risk cannot reduce to the agreed appetite level after the mitigation plan is implemented.

The **Board Committees** will get assurance through periodic deep dives, supported by papers, that risks are being effectively mitigated or have adequate plans in place where the current risk score is not within appetite.



4.5 Risk reporting & monitoring

Regions and directorates will regularly monitor and report risks affecting their activities – and the effectiveness of control measures for managing them – to senior managers or executive directors during routine management meetings, committees, groups or panels. Each team is responsible for defining their internal risk review and reporting arrangements, which should be proportionate to its local needs. Individual risks and risk registers should be reviewed no less than quarterly.

4.5.1 Cross Directorate Risks

Risks may be identified in directorates or regions where the responsibility to mitigate them sits elsewhere. In the first instance, colleagues should seek to work collaboratively across the organisation to clarify the risk, agree ownership, identify mitigating actions and their owners, and agree how, if required, the team initially identifying the risk will be kept informed of progress with mitigating it.

Where a way forward acceptable to both/all parties with a stake in the risk cannot be reached, the risk management team will support in the brokering of a solution. This may, particularly for risks at Level 1, or proposed for inclusion on the Operational Risk Register, include escalation to the Executive Corporate Group who have a responsibility to assist in the successful delivery of NHS England's corporate and business plans by highlighting specific areas of risk for further consideration with a particular focus on corporate performance, operations, and internal control. Where cross-organisation risks do not fit within the remit of the ECG, they will be raised to the relevant governance forum at the time.

4.5.2 Escalation of risks

It is recommended that the following are considered for escalation at each level:

- risks scored 16 to 25 at the point of identification
- risks scored 16 to 25 if there has been no movement in their risk score over the previous two quarters
- risks where the score has increased despite a mitigation plan being in place.

The above is only a guide, and in general risks should be considered for escalation where:

- sufficient capability is not held at the current risk reporting level to manage the risk successfully
- the risk rating has significantly worsened
- the mitigation plan is not expected to bring the risk within appetite
- the risk is related to cross-cutting issues and/or has a wider impact than just one region or corporate team, or
- the risk cannot be effectively controlled at current level (outside of team's control).

Where a team believes a risk may require escalation, the process for doing this will be as follows:

- As a **general rule**: escalation of a risk to the next level (e.g. from level 4 to level 3) must be endorsed by the risk register owner where the risk currently sits, as well as the receiving risk register owner and / or the forum at that level. Once this agreement is received, the risk can be moved on CoreStream.
- Escalation **from level 1 risk register onto the SRR or ORR**: escalation must be endorsed by the national director leading on the area that the risk is being escalated from. The risk is submitted to the Assistant Director of Risk Management with evidence of endorsement, for inclusion onto the Executive Risk Group (ERG) agenda. Escalation of the risk must be approved by ERG.
- Escalation of a cross-organisation risk **either newly identified or from a level 1 risk register onto the ORR**: escalation must be endorsed by the national director leading on the area that the risk is being escalated from. The risk is submitted to the Assistant Director of Risk Management with evidence of endorsement, for inclusion onto the agenda of the Executive Corporate Group (ECG) or other relevant governance forum. Escalation of the risk must be approved by group, with a subsequent risk owner identified and action plan developed. Continued monitoring and reporting of the risk will sit with the ERG, other than where deep dives may be required.

4.5.3 Urgent risk escalation

Risks can be raised at any meeting and at any level in our organisation. Staff must immediately escalate to their executive director and business lead for risk:

- newly emerging, high impact, highly likelihood risks
- risks breaching risk appetite
- risks with a significant or rapid change in severity resulting in a RAG rating of red

In these cases, staff should not wait for the quarterly reporting cycle. The corporate risk management team should be informed at the same time if the risk needs escalation onto the SRR or ORR.

The executive director leading on the area affected by the risk must decide whether the risk needs to be escalated to the wider executive team immediately or at its next available meeting, for consideration and action. Otherwise the risk will form part of established quarterly reporting.

5. Managing compliance with the Risk Management Framework

As set out in Annex 2, there are a range of roles and responsibilities across the organisation that support our compliance with this Framework. The Risk Management Team are directly accountable to the Chief Risk Officer and will support the implementation of and compliance with this framework by:

- supporting teams in implementing the framework; and overseeing and challenging the organisation on risk management
- monitoring compliance with the risk management framework and supporting the adoption of good practices
- co-ordinating central reporting of material and principal risks, opportunities and emerging risks through the risk governance structure (quarterly).

Compliance reporting will be informed by the above activities and reported to ERG at least twice a year, and annually to ARAC. Additional assurance activities may also be undertaken by NHSE's internal audit function.

5.1 Training and support

The Risk Management Team supports the delivery of NHSE's risk training plan, which aims to embed an excellent risk management culture across NHSE, improve compliance with the risk management framework, strengthen governance and improve the quality of corporate reporting and risk data. This is achieved through the provision of simple, accessible and effective training for everyone, including:

- supporting colleagues to understand why they need to manage risk, what is expected of them and what their responsibilities are
- tailoring the core offer, as appropriate, to different stakeholder groups
- improving how we communicate about the training opportunities that are available.

Risk reference materials are published on The Hub to support colleagues to:

- manage their risks more effectively and understand their roles and responsibilities
- improve data quality to enable more informed reporting for all levels of risk
- improve the way risk governance is assured at all levels.

The Hub details all aspects of training and support available from the Risk Management team, including CoreStream Risk Manager training.

Annex 1: Risk management terms and definitions

Term	Definition
Assurance	An evaluated opinion, based on evidence gained from review, on governance, risk management and internal control framework.
Control (may also be referred to as Internal Control)	Measure that are already in place and mitigate the risk. Note: Controls include, but are not limited to, any process, policy, device, standard contract, practice, or other conditions and/or actions which modify risk. Controls may not always exert the intended or assumed modifying effect or may be achieving this partially. When there are gaps in controls, a mitigation plan should be agreed.
Consequence	Outcome of event affecting objectives. Note: an event can lead to a range of consequences.
Deep dive (may also be referred to/interpreted as a thematic risk review)	A technique used to rapidly assess a current or emerging risk/issue specific to a single entity or across a number of corporate teams/regions. It can focus on finding out what is happening and suggesting ways of tackling the problem, or it can focus on the effectiveness of exiting controls and mitigation plans.
Directorate/regional level risk	Risks to achieving objectives within individual directorate/regional business plans, impacting business as usual processes, activities and/or programmes/projects. Note: These risks will be specific to the corporate team/region in question and by their nature will include operational or project delivery risks over which the corporate team/region has full or partial control.
Event	Occurrence or change of a particular set of circumstances. Note: An event can have one or more occurrences and can have several causes and several impacts/consequences. An event can also be something that is expected which does not happen, or something that is not expected which does happen. An event can be a risk source. An event can also be a change in circumstances. Events are sometimes referred to as incidents or accidents. Events without consequences are sometimes referred to a near-misses, near-hits or close-calls.
Impact (may also be referred to/interpreted as 'consequence')	Outcome of an event affecting objectives. Note: An impact/consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives. Impacts/consequences can be expressed qualitatively or quantitatively. Any impact/consequence can escalate through cascading and cumulative effects.
Inherent risk (also known as the gross risk)	The exposure arising from a specific risk before any action has been taken to manage it (or the risk that would crystallise if controls failed in their entirety).
Issue	Threats which have already manifested themselves, were not planned and require management action. Note: The approach to managing issues may well be different from management of risks, which only have the potential to happen in the future. Once a risk occurs it becomes an issue.
Likelihood (may also be referred to/interpreted as 'probability')	Chance of something happening. Note: In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and

Term	Definition
	described using general terms or mathematically (such as a probability or a frequency over a given time period).
Residual risk (also known as the mitigated risk)	The exposure arising from a specific risk after action has been taken to manage it and making the assumption that the action is effective.
Risk	Effect of uncertainty on objectives. Note: This definition relates to uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. It is the combination of likelihood and impact, including perceived importance. It recognises that we operate in an uncertain world and that potential threats, actions or events may occur (internally or externally) which could adversely or beneficially affect our ability to deliver our commitments/objectives. An effect is a deviation from the expected; it can be positive, negative or both, and can address, create or result in opportunities and threats. Objectives can have different aspects and categories and can be applied at different levels (i.e. strategic, regional/corporate team or programme/project objectives). Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.
Risk appetite (may also be referred to/interpreted as a risk tolerance or risk criteria)	The amount of risk that we are willing to seek or accept in the pursuit of long-term objectives. Note: Risk appetite represents a balance between the potential benefits of innovation and the threats that change inevitably brings. It is used to determine whether a specified level of risk is acceptable or tolerable; and should reflect organisational values, policies, and objectives, be based on external and internal context, should consider the views of stakeholders, and should be derived from standards, laws, policies, and other requirements such as delegations of authority and operating limits/thresholds.

Annex 2: Roles & responsibilities

Role	Responsibility
All staff	Responsible for: • participating (as appropriate) in the identification, assessment, planning and management of threats and opportunities; • undertaking relevant training to support their participation in risk management.
Risk Owner	A risk owner is the responsible point of contact for an identified risk, who coordinates efforts to mitigate and manage the risk with various individuals who may also own parts of the risk. The responsibilities of the risk owner are to ensure that: • risks are identified, assessed, managed and monitored • risks are clearly articulated in risk registers • controls and treatment plans are in place to mitigate the risk to within risk appetite • risk information is kept up to date on a minimum quarterly basis, and is of a sufficiently high quality to support risk reviews and assurance.
Risk Register Owners, e.g. including Heads of function, Programme Directors	Responsible for: • participating (as appropriate) in the identification, assessment, planning and management of threats and opportunities; • keeping a record of the identified risks in a risk register; • undertaking a regular review (minimum quarterly) of the risks on the risk register; and • escalating risks as appropriate and in accordance with this framework.
Directorate / Region embedded risk colleagues	Across each Region and Directorate there will be embedded colleagues who act as the liaison point for risk management in their region or corporate team. They support executive directors in implementing this framework. This includes developing and maintaining a local risk register on CoreStream, and ensuring there is a robust governance structure for reporting and escalating risks within the directorate. They will also escalate risks as appropriate, on behalf of their executive directors. The roles in each Region and Directorate may vary, however there is an expectation that there will be: • an SLT Risk Lead: A director or other senior officer nominated to act as the senior point of contact for risk management, promoting the importance of risk management across the directorate/region, and supporting robust discussion of risk at SLTs or other forums • a Risk Lead: appointed by their director and it is recommended that as a minimum they operate in a business manager or equivalent role to ensure consistency of application and adequate internal focus. They should also be regular attendees at their local management/leadership meetings, have the authority to challenge their colleagues on risk, and have enough capacity to dedicate to developing and maintaining robust risk governance and managing the risk process on behalf of their areas. Risk leads may be supported by local risk co-ordinators

Role	Responsibility
	• local Risk Co-ordinators: supporting the application of the risk management framework within a team, managing and co-ordinating risk reporting and administering team activity on CoreStream.
Directorate / Regional SLTs	Responsible for: • approval and review of the Level 1 risk register, at least quarterly • consideration and approval of candidate risks for inclusion in the Level 1 risk register as they arise • oversight and approval of updates to directorate/ regional risks that sit on the operational or strategic risk register, before submission • oversight of directorate/ regional compliance with the Risk Management Framework, at least quarterly.
Executive Risk Group	Responsible for: • oversight of NHSE's risk exposure in the context of the risk appetite that has been agreed by the Board • consideration and approval (where appropriate) of candidate risks for escalation onto the SRR, and approval of de-escalation • review and approval of the SRR and ORR, including calibration of risk scores • risk horizon scanning • advising on the development of the Risk Management Framework and monitoring its operation with periodic reviews, including oversight of the risk governance arrangements in place across the wider governance framework • raising issues for discussion, decision, or action by other committees • evaluating the effectiveness of plans designed to mitigate risks and assessing their adequacy, particularly during at risk escalation stage and during the deep dive process. Ensuring that relevant actions are carried out as planned and escalating significant issues to the NHS Executive when necessary.
Executive Corporate Group	Responsible for • assisting in the successful delivery of NHS England's corporate and business plans by highlighting specific areas of risk for further consideration with a particular focus on corporate performance, operations, and internal control. • considering the escalation of cross-organisation risks which require collaborative working of corporate functions to be resolved.
Audit & Risk Assurance Committee	The full duties of ARAC in relation to risk management are set out in The Orange Book[3] Oversees and challenges the appropriateness and effectiveness of NHSE's risk management framework, including risk management processes and activities planned to mitigate NHSE's principal risks.
Other Board Committees	• oversight of risks relevant to the Committee's remit

[3] Page 45, Duties of ARAC: The Orange Book – Management of Risk – Principles and Concepts (publishing.service.gov.uk)

Role	Responsibility
	• to receive assurance, through periodic deep dives (supported by a paper in a standard template), that risks are being effectively mitigated or have adequate plans in place where the current risk score is not within the Board's appetite.
Board	• the full duties of the Board in relation to risk management are set out in The Orange Book[4] • approves risk management policy, including setting NHSE's Risk Appetite • seeks assurance on the effective management of NHSE's principal risks (recorded in the SRR & ORR).
Executive Directors	National and regional executive directors are responsible for the governance arrangements in their areas and will support and promote risk management. They must ensure that risk management is integrated into all activities, and should demonstrate leadership and commitment by ensuring: • their region or directorate implements the framework • risk is considered when setting their objectives/drafting their business plan and discussed alongside their performance and in relevant local management meetings • all risks, controls and risk management issues under their remit are adequately co-ordinated, managed, monitored, reviewed and reported/escalated at their relevant governance meeting in accordance with the requirements of this framework • necessary resources are allocated to managing risk/that they identify individuals who have the accountability and authority to manage risk under their remit (i.e. risk owners) • they raise relevant risks at the ERG meeting, NHS Executive meeting or other decision-making forum, where appropriate. Where principal risks (recorded on the SRR or ORR) have increased, or risks are outside agreed appetite or tolerance, owning executive directors may be called on to attend ARAC to discuss mitigations.
Chief Executive	The full duties of the Chief Executive, as Accounting Officer are set out in The Orange Book[5]
Chief Risk Officer	The Deputy Chief Executive acts as Chief Risk Officer (CRO) for the organisation. The CRO owns this risk management framework and any associated procedures and will ensure that the overall risk to the organisation is presented to, and challenged at, the appropriate governance structures in NHSE.
Risk Management Team	The Risk Management team is the corporate team directly accountable to the Chief Risk Officer. The team is responsible for: • maintaining a suitable risk management framework and any associated procedures and updating them every two years or following significant change • supporting teams in implementing the framework; and overseeing and challenging the organisation on risk management

[4] Page 43: Duties of the Board: The Orange Book – Management of Risk – Principles and Concepts (publishing.service.gov.uk)

[5] Page 44, Duties of the Accounting Officer: The Orange Book – Management of Risk – Principles and Concepts (publishing.service.gov.uk)

Role	Responsibility
	• monitoring compliance with the risk management framework and supporting the adoption of good practices • co-ordinating central reporting of material and principal risks, opportunities and emerging risks through the risk governance structure (quarterly) • Providing expert advice and support to directorates/teams • Providing materials and training to support the implementation of this framework.