

Risk Management Policy

Responsible Officer – Director, Finance

Author – Corporate office

Date effective from May 2017

Date last amended October 2023

Review date September 2026

# Contents

Introduction3

Risk management3

Risk identification and assessment 3

Categorising risk4

Risk appetite 5

Oversight6

Annual report governance statement and the role of audit 7

Review8

Appendix A – Quantifying and monitoring risks9

Appendix B – Risk register12

Appendix C – Version control sheet13

# Introduction

1. Risk is the uncertainty surrounding events and their outcomes that may have an impact on NICE. All our activities carry some risk, arising either from potential threats or the non-realisation of opportunities which may harm, prevent, hinder or interfere with the achievement of our objectives.
2. Risk is inherent in every activity and this policy sets out how NICE will manage risks to ensure a balanced approach to opportunity and risk. It explains the approach to risk management; defines risk and how it is assessed, evaluated and escalated in the context of NICE’s risk appetite; and documents roles and responsibilities for the management of risks.

# Risk management

1. Risk management enables organisations to evaluate and respond to risks and opportunities and seeks to manage the impact of uncertainty by increasing the probability of success and reducing the likelihood of failure.
2. Effective risk management involves evaluating the uncertainties and implications within options and managing impacts once choices are made. It provides a process for identifying risks around new, proposed and current business activities, and involves the categorisation and evaluation of each risk and the application of management controls to mitigate the risk. The evaluation is based on a judgement of the likely impact if no further action is taken, combined with an assessment of the likelihood of the risk re-occurring.
3. Risk management should be both an integral part of all organisational activities to support decision-making in achieving objectives and embedded within the culture of the organisation.

# Risk identification

1. Like all organisations, NICE faces risks, actual and theoretical, that range from the trivial to the existential. This policy is intended to address both the **strategic** risks which arise from our strategic ambitions and from the potential external threats to NICE from the developments in our operating environment, and the **operational** risks to our objectives and plans to manage and deliver our operational activities.
2. Risk assessment is a qualitative or quantitative evaluation of the nature and magnitude of risk to our objectives and planned activities. The evaluation is based upon known vulnerabilities and threats and considers the **likelihood** of the threats being realised and their **impact** on our work.
3. The Executive Team (ET) will ensure the strategic risks that may affect delivery of NICE’s strategy are identified, assessed and included in the strategic risk register which is reviewed by the Audit and Risk Committee and Board. ET will continually review the strategic risks to ensure they remain relevant as the operating environment changes and recommend changes to the Audit and Risk Committee and Board. In identifying the strategic risks ET will also consider risk interdependencies with Department of Health and Social Care (DHSC) Arms-Length Bodies (ALBs), and other key partners. This will include the other ALBs NICE is dependent on to deliver its priorities. Directors will also ensure that risks in their directorate, which are not strategic in nature, are identified, assessed and incorporated in the operational risk register when they have a potential cross-organisational impact.
4. Directors are required to include a risk assessment in ET and Board reports where there is a substantive new development proposed or substantive change to existing activities.
5. Risk registers are also produced for significant projects, and these will be used to provide mitigations and assurances to ET, for example a large digital transformation project, which is internally facing but is organisation-wide.

# Risk assessment

1. Each risk will be assigned an overall **assessment** depending on its impact and the likelihood of it occurring by applying the approach set out in appendix A. This initial assessment takes account of the mitigating controls in place to manage the risk (for example policies and procedures) and the sources of assurance to assess whether the controls are operating as intended (for example internal audit reviews) and provides a **current risk** rating. Any further planned actions to reduce the risk score are recorded, with the aim of reaching a **target risk** rating, using the format in appendix B. The target rating should be informed by NICE’s risk appetite (that is set out later in this policy).
2. Risks are scored using a 5x5 matrix giving each risk a score of 1 to 5 for the **likelihood** of it arising and a score of 1 to 5 for its potential **impact** on the organisation. In assessing the likelihood of risks arising, a judgement will be made as to whether the possibility of a risk realising is deemed to be rare, unlikely, possible, likely or almost certain. In assessing the impact on the organisation of a risk realising, a judgement will be made as to whether the result is deemed to be very low, low, moderate, high or severe.
3. An overall assessment of each risk is made according to its impact and likelihood of occurrence based on the current controls in place, using the scoring matrix set out in in Appendix A, leading to an overall rating of very low (light green), low (green), medium (yellow), high (amber), very high (red).

# Risk treatment

1. Identified risks will be reviewed to determine the action to be taken. This is called the **treatment** of risks and will be informed by the risk appetite. Options open to treat risks include:

* avoiding the risk, if feasible, by deciding not to start or continue with the activity that gives rise to the risk
* taking or increasing the risk in order to pursue an opportunity or a strategic priority
* retaining the risk by informed decision
* changing the likelihood, where possible
* changing the impact, including planning contingency activities
* sharing the risk with another organisation (eg through a contract or partnership agreement)
* escalating the risk to the DHSC, where appropriate

Alternatively, it may be decided to tolerate the current level of risk, accept the current controls are sufficient and not invest further resources in reducing the risk.

# Risk appetite

1. Decisions on risk treatment must be informed by an understanding of the extent to which we are prepared to accept the risks associated with the actions we plan to take. This concept is known as ‘**risk appetite**’: the extent to which we will tolerate known risks, in return for the benefits expected from a particular action or set of actions.
2. The Board will determine and annually review NICE’s risk appetite (set out below) and ensure that planning and decision-making reflects this approach.
3. The concept of risk appetite should be used to inform discussions about how much risk we are willing to bear in the pursuit of our objectives. If properly applied, it results in improved outcomes and use of resources, allowing resources to be prioritised to support the management of risks to achieving outcomes/objectives, whilst maintaining performance and demonstrating value for money.
4. It is often not possible to manage all risks at any point in time to the optimal level, but the ‘risk appetite’ discipline provides a means to guide decisions on when risks should be tolerated.
5. The following section sets out our current risk appetite across the different risk areas using the following definitions:

|  |  |
| --- | --- |
| * Minimalist | Preference for safe options that have a low degree of residual risk |
| * Cautious | Willing to tolerate a degree of risk where we have identified scope to achieve significant benefit and/or realise an opportunity and the risks can be managed. |
| * Open | Willing to consider all options and choose one that is most likely to result in successful delivery |
| * Eager | Keen to be innovative and to choose options that suspend previous held assumptions and accept greater uncertainty |

1. It is important to note that risks will not necessarily fit neatly into one of these categories and may intersect across these areas. Therefore, it will be important to use this appetite statement as a guide to inform the approach to managing and accepting risks.

## Risk appetite statement

1. NICE’s core purpose is to help practitioners and commissioners get the best possible care to patients fast while ensuring value for the taxpayer. We do this by producing guidance for health and care practitioners and providing rigorous and independent assessment of new health technologies.
2. Historically NICE has had a cautious risk appetite and sought to operate with a low level of risk wherever possible given the impact of our recommendations and need to ensure confidence in our work. However, with the pace of change in the health and care system NICE must adopt a more nuanced risk appetite in which we accept, and seek, a wider degree of risk while remaining committed to robust methods, processes, and internal governance.
3. NICE has an ambitious transformation strategy to ensure we continue to meet the needs of our key users. This includes developing new ways of working to ensure our guidance is more relevant, timely and useable. To achieve these transformation goals, we will maximise opportunities to be more agile, efficient and make the best use of data and new technologies to improve our products and our users’ experience. We are therefore seeking to accept a greater degree of risk and move towards an **open** risk appetite across product, process and technology innovation while ensuring the implications of the transformation are managed as set out below. Our risk appetite is premised on the need to ensure compliance with statutory requirements and our obligations under Managing Public Money as set out in our standing financial orders.

* **Reputation:** NICE is a globally recognised organisation with a reputation for excellence. Our guidance is scrutinised by a range of stakeholders who look to NICE to provide the highest quality advice. We remain committed to retaining this reputation and minimising adverse feedback, but we seek to move towards a **cautious** appetite for reputational risk in which we recognise the risk of not taking action or changing the way we work.
* **Finance:** NICE is mandated to deliver a balanced budget each year and achieve the best value for money for taxpayers. We are required to demonstrate transparency and probity but also ensure the effective use of public funds and therefore our appetite for financial risk is **cautious**, but **minimalist** to any risk to financial propriety and regularity.
* **Governance:** NICE is a public body, accountable to government, and we aim to operate with the highest standards of probity and in compliance with all relevant legislation. Our appetite for governance risk is therefore **cautious**. However, this is premised on the recognition that the approach to governance must be proportionate as an over-complex or risk averse approach could undermine the effective use of public resources.
* **Legal challenge:** NICE’s guidance programmes operate in line with robust methods and processes to provide rigorous, independent assessments of health technologies and interventions. However, NICE, can and does, face challenge to its recommendations. Our risk appetite in terms of legal challenge in the guidance programmes is **cautious.** This does not prevent new ways of working but recognises the importance of considering the risks of challenge when developing and formulating these new ways of working, in a way that is proportionate to the level of risk of challenge in each particular guidance programme.
* **Workforce:** Our workforce account for the majority of NICE’s expenditure and our staff are central to delivering NICE’s objectives. The recruitment market is challenging and there is competition for many of NICE’s technical roles. Therefore, our wider risk appetite for workforce risks is **open** – reflecting the need to offer working arrangements that enhance recruitment and retention, while supporting delivery of the transformation However as a public sector employer, it is vital that NICE acts in accordance with the law and good practice and therefore our risk appetite is **minimalist** to risks to compliance with the statutory employment legislation.
* **Partnerships:** NICE works with a range of partners in both the public and commercial sectors. Our appetite for risk in partnerships is **open,** but we will remain mindful of the need to consider our reputation, adhere to public procurement regulations and competition law, and protect public funds.
* **IT Security:** A cyber security incident could have significant implications for NICE’s activities and reputation. Our appetite for IT security risks is therefore **minimalist,** and NICE will seek to comply with recognised national standards to mitigate as far as possible any cyber security risks within the available resources. We recognise that it may be necessary to accept a higher level of risk where a particular system/software remains the best available approach to achieving business outcomes.

# Assurance

24 The strategic and operational risk registers will outline the assurance on the effectiveness of the controls in place to manage each risk, drawing on the ‘3 lines of defence’ model. An assurance mapping tool is available to help identify any gaps in assurance where action is required to improve the controls.

# Oversight

1. The **Board** has ultimate responsibility for risk management within NICE including major decisions affecting NICE’s risk profile, appetite or exposure. It will review the strategic risk register six-monthly and periodically dedicate time specifically for horizon scanning in order to identify and consider the nature of emerging risks, sources of uncertainty, threats and trends, and also to reflect on any learning from NICE’s response to unforeseen events. The Board will review the risk appetite annually.
2. The **Audit and Risk Committee** provides an independent and objective view of the arrangements for the management of risk. It will advise the Board on the co-ordination and prioritisation of risk management issues throughout NICE and advises the Board on the effectiveness of the internal control system. It satisfies itself that risks have been identified and there is assurance that risks are being effectively managed.
3. The Audit and Risk Committee reviews the strategic risk register at each of its quarterly meetings, along with a ‘deep dive’ on a specific risk area. The relevant risk owner, or their deputy, will be invited to attend the meeting.
4. The Audit and Risk Committee will report to the Board on internal controls and alert the Board to any emerging issues. The Board will receive minutes of the Audit and Risk Committee, plus an annual report from the committee to provide assurance that the approach to risk management is effective, comprehensive and robust particularly in regard to the significant risks facing NICE.
5. The **Executive Team** reviews the strategic risk register monthly and prior to the Audit and Risk Committee’s quarterly review. ET will take account of the on-going identification and evaluation of risks and in particular the quality and timeliness of information provided on key risks and the identification of ineffective controls and new risks, to ensure that corrective action can be taken. It will also consider whether new strategic risks have arisen that need to be added to the register.
6. The strategic risks are also shared with the DHSC Sponsor Team for review at the quarterly accountability meetings.
7. The **Operational Management Committee (OMC)** comprises senior managers from each directorate and reviews the operational risk register bi-monthly as part of its responsibility for operational issues with a cross organisation impact. The operational risk register has both a risk owner and a risk lead, with the risk owner being an ET member and the risk lead being a senior manager. This ensures that the overall accountability remains with ET members whilst the responsibility for oversight and management of the risks sits with senior managers.
8. The OMC ensures that any new emerging risks or existing risks that are increasing in threat level and are turning into strategic in nature, are **escalated** to ET to consider whether they are appropriate for inclusion on the strategic risk register.
9. Alternately, as part of ET’s review of the strategic risk register, where a risk has been mitigated significantly resulting in the risk level decreasing to low or very low, ET may decide that the risk is no longer of a strategic nature and can be **de-escalated** to the operational risk register.
10. Risks may also be removed from the operational risk register if the OMC considers a threat level has decreased significantly or been mitigated sufficiently. A register of risks that have been **removed** is maintained by the corporate governance and risk manager.
11. The Chief Executive, as Accounting Officer, is responsible for ensuring NICE has a robust approach to risk management in place and risk is integral to NICE’s governance and decision making. They are supported by the Finance Director, who as the executive lead for risk management, is responsible for leading NICE’s overall approach to risk management and ensures that ET evaluate the risks identified by directors and apply handling strategies and implement policies to support the process of internal control.
12. The corporate governance and risk manager has responsibility for coordinating the strategic and operational risk registers, and for supporting the ET, OMC, Board and Audit and Risk Committee in their responsibilities for risk assessment and management. They will proactively support directorates in the risk management process, promoting consistency in the risk ratings and entries in the risk register, applying challenge as appropriate.

# Annual report governance statement and role of audit

1. The annual governance statement in the annual report and accounts assesses the effectiveness and operation of NICE’s risk management arrangements.The statement is informed by the work of internal and external audit.
2. Internal audit is responsible for aspects of the annual review of the effectiveness of the internal control system within the organisation. They will periodically review the arrangements for risk management and levels of assurance around the controls reported to the Audit and Risk Committee.
3. External audit provides advice and feedback to the Audit and Risk Committee on the operation of the internal financial controls reviewed as part of the annual audit and also gives a view on the completeness of the annual governance statement.
4. The Audit and Risk Committee will review the auditors’ findings and management’s response.

# Review

1. This policy will be reviewed every three years or sooner if required (such as publication of new guidance). The risk appetite statement will be reviewed annually.

# Appendix A: Quantifying and monitoring risks

Each risk is allocated an **impact** score using the descriptions below ranging from very low with a score of 1 to severe with a score of 5.

Table 1

|  |  |  |
| --- | --- | --- |
| **Category** | **Score** | **Examples** |
| Very low | 1 | * **Financial** - minimal impact on budgets * **People** - minor changes required to working practices * **Objectives / outputs** - no impact on the quality, timeliness or utility of any outputs * **Reputation** - no external challenge or criticism expected * **System impact** – minimal anticipated impact on the health and social care system |
| Low | 2 | * **Financial** - some impact on one or more budgets, manageable within the budget(s) concerned * **People** -some changes to working practices or minor changes to staff roles * **Objectives / outputs** - minimal impact on the quality, timeliness or utility of any outputs * **Reputation** - some external criticism which is not likely to be material enough to result in reputational damage * **System impact** – potential for some impact on the health and social care system |
| Moderate | 3 | * **Financial** - material financial consequences for the budget or budgets directly concerned, which can be managed within the affected budget(s) or by the use of underspending in unaffected budgets * **People** - material impact on the employment position of staff, which may need to be managed through formal change processes * **Objectives / outputs** - some impact on the quality, timeliness or utility of any outputs, which can be resolved before publication * **Reputation** - external criticism of the Institute’s judgement, which can be met successfully, and which is unlikely to result in reputational damage * **System impact** – likely to have an impact on the health and social care system which will require senior management and/or board discussion |
| High | 4 | * **Financial** - material financial consequences, which can only be managed by the use of reserves and/or in year transfers from unaffected budgets, or exceptionally, transitional funding from the Department of Health and Social Care * **People** - impact on the employment position of staff, which can only be managed by formal change processes, with risk of redeployment and, exceptionally redundancy * **Objectives / outputs** - significant impact on the quality, timeliness or utility of any outputs, which may require amendment, withdrawal and/or replacement post-publication * **Reputation** - external criticism of the Institute’s judgement, which may result in substantial reputational damage * **System impact** – highly likely to have a negative impact on the health and social care system which will likely require sustained senior management/board focus and possible discussion with DHSC sponsor team |
| Severe | 5 | * **Financial** - significant financial consequences which can only be managed by transitional funding from the Department of Health and Social Care * **People** - protracted unavailability of critical skills/people or high risk of requirement to reduce the headcount through redundancy * **Objectives / outputs** - severe impact on the quality, timeliness or utility of any outputs, which require withdrawal and/or replacement post-publication * **Reputation** - national and international criticism of the Institute leading to sustained adverse media and potential Government intervention * **System impact** – significant negative impact on health and social care system which likely to require DHSC and/or wider government action |

Similarly, the **likelihood** of each risk materialising will be assessed on a scale of 1 to 5 as outlined in the table below.

Table 2

|  |  |  |
| --- | --- | --- |
| **Category** | **Score** | **Definition** |
| Rare | 1 | Highly unlikely to occur in the following 12 months (less than 20% probability) |
| Unlikely | 2 | Unlikely to occur in the following 12 months (between 20% but less than 40% probability) |
| Possible | 3 | May occur in the following 12 months (between 40% but less than 60% probability) |
| Likely | 4 | Likely to occur in the following 12 months (between 60% but less than 80% probability) |
| Almost certain | 5 | Highly likely to occur in the following 12 months (greater than 80% probability) |

**Note**: In the case of strategic risks, a timescale of 24 months should be taken into account given the longer term nature of these risks.

A **summative** score will be calculated, in each case, by multiplying the impact and likelihood scores, to give a total score. This will lead to an overall rating of the risk. Risks can then be mapped into a risk matrix that has five zones (red, amber, yellow, green and light green).

Table 3

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Impact** | **Severe**  **5** | **5**  *Low* | **10**  *Medium* | **15**  *High* | **20**  *Very high* | **25**  *Very high* |
| **High**  **4** | **4**  *Low* | **8**  *Medium* | **12**  *High* | **16**  *High* | **20**  *Very high* |
| **Moderate**  **3** | **3**  *Very Low* | **6**  *Low* | **9**  *Medium* | **12**  *High* | **15**  *High* |
| **Low**  **2** | **2**  *Very Low* | **4**  *Low* | **6**  *Low* | **8**  *Medium* | **10**  *Medium* |
| **Very low**  **1** | **1**  *Very Low* | **2**  *Very Low* | **3**  *Very Low* | **4**  *Low* | **5**  *Low* |
|  | **Rare**  **1** | **Unlikely**  **2** | **Possible**  **3** | **Likely**  **4** | **Almost certain**  **5** |
| **Likelihood** | | | | | |

When assessing the likelihood and impact of risk, the most credible worst-case scenario should be considered, not the worst-case.

# Appendix B: Risk register template (example)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk ref** | **Risk** | **Lead** | **Key controls to manage the risk (by lowering the likelihood and/or impact of the risk)** | **Sources of assurance that the risk is being managed (using ‘Three Lines’ model)** | **Current rating** | | | **Target rating** | | |
| **I** | **L** | **S** | **I** | **L** | **S** |
| 4 | **Organisational transformation**  We are unable to … | SR | **Controls currently in place**  Leadership development programmes for ET, PD/AD and change leaders  **Further actions planned or in progress to lower risk**  Develop 5-year transformation plan leading to integrated behaviours and processes | Key Performance indicators  Data from staff suvey surveys  Reputation survey results  Internal audit of business planning and performance |  |  |  |  |  |  |

**Risk:** the risk itself, expressedin terms of a cause and an event, and their impact.

**Key controls:** the actions in place to mitigate the risk, together with any timings (also known as controls). This includes reporting arrangements (e.g. to Board, ARC, ET).

**Actions to strengthen mitigation and assurance:** the further planned actions to strengthen the controls (to move the current rating to the target rating) and to strengthen the assurance on the controls. This should include dates for completing the actions. The risk owner should ensure that actions are **SMART** (specific, measurable, achievable, relevant, time bound) and that a realistic completion date is assigned to each action.

**Sources of assurance:** any assurance on the effectiveness of the controls/mitigations, based on the ‘three lines’ model, with particular emphasis on any sources of external, independent assurance.

**Current rating:** the score allocated to the impact and likelihood of the risk, and the RAG (Red, Amber, Yellow, Green, Light green) rating allocated to it *after the application of current controls/mitigations.*

**Target score:** the target score allocated, after the additional proposed mitigating actions, to the impact and likelihood of the risk, and the RAG rating allocated to it.

# Appendix C - Version Control Sheet

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Replaces** | **Comment** |
| 2 |  | Julian Lewis | Risk Management Policy 2003 | Incorporates information risk management |
| 2.1 | July 2016 | Julian Lewis | All previous versions |  |
| 3 | 2 May 2017 | Andrew Dillon | All previous versions | Responds to the January 2017 internal audit report and subsequent Audit and Risk Committee, and ET discussions. Changes include the risk appetite, risk identification, evaluation and management process, and risk register template |
| 4 | May 2020 | Elaine Repton | V3 | Periodic review and aligned to HM Treasury’s Orange Book. |
| 4.1 | March 2022 | Elaine Repton | V4 | Updated terminology to reflect strategic and operational risk registers and to implement a 5x5 risk scoring matrix. |
| 4.2 | May 2023 | Elaine Repton | V4.1 | Updated the risk impact and likelihood descriptors. |
| 5 | October 2023 | Elaine Repton | V4.2 | Revised risk appetite section and revised risk register template |