Risk Management Policy

Responsible Officer
Ben Bennett, Business Planning & Resources Director

Author
Julian Lewis, Governance Manager

Date effective from
December 2008

Date last amended
December 2012

Review date
December 2015
1 Purpose of this document

1.1 The policy supports the Institute’s arrangements for risk management, internal control, information governance and corporate governance.

1.2 The policy explains the approach to risk management (including information risk management), the definition of risk and how it is assessed, documents the roles and responsibilities of the Board, Audit Committee, the senior management team, Senior Information Risk Officer and other key officers. It outlines the risk management process, and identifies the reporting procedures.

1.3 In addition, it describes the relationship between the Board, Senior Management Team and Audit Committee and the process used to evaluate the effectiveness of the Institute’s risk and internal control procedures.

2 Definition of risk

2.1 Risk is the uncertainty surrounding events and their outcomes that may have a significant effect on Institute activities. All Institute 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 business objectives.

2.2 Risk assessment is a qualitative or quantitative evaluation of the nature and magnitude of risk to the Institute’s objectives. The evaluation is based upon known or theoretical vulnerabilities and threats, as well as the likelihood of the threats being realized and the potential impact on the Institute.

2.3 Risk management is the process of evaluating and responding to risks to the Institute’s business for the purpose of reducing those risks to acceptable levels. Risk management is inclusive of the risk assessment process, and uses the results of risk assessments to make decisions on the acceptance of risks or on taking action to reduce those risks.

3 Risk appetite

3.1 The level of risk associated with the attainment of NICE objectives is reviewed by, and referenced to, the risk appetite accepted by SMT and the Board. This provides oversight and consistency in the level of risk taken by NICE as a whole and ensures that the balance of risk against benefits across directorates is appropriately managed and aligned at all times. The key descriptors to be considered when evaluating risk are as follows:
3.2 **Contextual risk**

NICE recognises it works in a changing political environment where its judgements have a considerable public profile and sensitivity which may necessitate a refinement to its existing processes. It will accept some risks in these circumstances to ensure it is positioned to optimum advantage within the health and social care fields. NICE will accept moderate risks in pursuit of these goals providing any change does not unduely impact on its core work.

3.3 **Developmental risk**

NICE accepts a degree of risk that is part and parcel of its willingness to take on new functions, facilitate change and evolve to meet government priorities and develop its core business to the benefit of the NHS and the wider public. These risks will be closely monitored and project managed by senior managers so that business objectives are achieved and to ensure our stakeholders and customers have confidence in our products.

3.4 **Reputational risk**

NICE has a low risk appetite for actions and decisions which may damage the quality of our work and thus our reputation. So we put a strong emphasis on rigorous processes to be followed in developing the work, with major use of external experts and representative interests, engagement of those affected, extensive and formal consultation, and great transparency of everything we do.

4 **Approach to risk management**

4.1 Risk management is central to the strategic management of the Institute. It provides a systematic process for identifying risks attaching to new and current business activities. This process involves the categorisation and evaluation of each risk and the application of management controls to mitigate the risk based on a judgement of the likely impact if no action is taken combined with an assessment of the likelihood of the risk re-occurring.

4.2 The Institute will ensure there is sufficient flexibility to respond to risks and adequate resources to mitigate risks. It is recognised that risks can be most effectively managed if the management is embedded within the culture of the Institute.

4.3 The internal controls for risk management will be scrutinised by internal and external audit but these can only be minimised the consequences of occurrence based on impact and likelihood but the risk itself will not be eliminated.

4.4 Risk management is a continuous process involving risk identification,
risk assessment, allocation of leads to manage risk, consideration of the residual risks after controls implemented.

4.5 Programmes will ensure that fundamental risks in their department are identified, assessed and monitored and incorporated in the Risk Register. Emerging risks will be added as required, and actions and controls put in place to mitigate them and provide assurance to the Board.

5 Risk Register

5.1 The principle document to facilitate the identification, recording and assessment of risks is the Risk Register and this will detail all significant risks that threaten the Institute.

5.2 Risks are initially identified through discussion between the Governance Manager and Institute Programmes. These are then critically analysed by the Senior Management Team and reviewed by the Audit Committee.

5.3 The identification of risks is set against the Institute’s Directions from the Department of Health, its business objectives, significant matters arising during the year and incident reports.

5.4 Risks are assessed according to their potential impact if left unmitigated and likelihood of occurrence using the scoring matrix in Appendix A.

6 Responsibilities

6.1 The Board will determine the risk appetite for the Institute and set the culture of risk management within the Institute with particular regard to new initiatives and emerging risks.

6.2 The Board will have ultimate responsibility for risk management within the Institute including major decisions affecting the Institute’s risk profile or exposure. The Chief Executive will approve the annual Statement of Internal Control.

6.3 The Board will receive minutes of the Audit Committee and an annual risk management report to provide assurance that the Institute’s approach to risk management is effective, comprehensive and robust particularly in regard to major risks facing the Institute.

6.4 The Audit Committee will act under delegated authority of the Board to provide 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 the Institute.

6.5 The Audit Committee will report to the Board on internal controls and alert the Board to any emerging issues.

6.6 It will oversee internal and external audit and review their
recommendations and advise the Board on the effectiveness of the internal control system including the Institute’s system for the management of risk.

6.7 It will satisfy itself that risks are being actively managed with the appropriate controls in place and that they are working effectively.

6.8 It will monitor and critically review the management of fundamental risks and the maintenance of the risk register to ensure there are fit for purpose.

6.9 It will approve an annual risk report for submission to the Board.

6.10 **The Senior Management Team** will have day-to-day responsibility for the identification and management of risks that threaten the achievement of business objectives and will implement policies to support the process of internal control.

6.11 It will consider the Institute’s objectives and its financial and non-financial targets, organisational structure and calibre of the senior management, culture, approach, and resources with respect to the management of risk, delegation of authority and public reporting.

6.12 It 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 time it takes for ineffective controls to be recognised or new risks identified to ensure that corrective action can be taken.

6.13 The senior management team will identify and evaluate the fundamental risks faced by the Institute for incorporation in the Risk Register and for consideration by the Audit Committee.

6.14 The Business Planning & Resources Director acts as the Senior Information Risk Officer with special responsibility for information risk management.

6.15 The Governance Manager has responsibility for the recording and assessment of risks, including those relating to information risk, maintaining the Risk Register and reporting these to the Senior Management Team and Audit Committee for critical review and evaluation.

7 **Information risk management**

7.1 Information risk relates to the loss, misuse or unauthorised disclosure, of sensitive personal data or confidential information that may cause damage or distress to any individual, threaten the Institute’s business or damage its reputation.

7.2 Information risks relating to sensitive personal data and confidential information in hard and soft format will be systematically evaluated
throughout the Institute and action taken on a risk assessed basis.

7.3 The Business Planning & Resources Director will act as Senior Information Risk Officer (SIRO) with Board level responsibility for information risk. He will be supported by the Governance Manager and, where necessary, Information Asset Owners who will monitor and report on information governance issues on an annual basis.

7.4 The SIRO will carry out an annual information risk assessment to report to the Audit Committee and Board and to inform the Statement of Internal Control.

7.5 The SIRO will report all serious breaches of information security to the Audit Committee and Department of Health as appropriate in line with DH reporting guidelines. Any significant breaches will be included in the Institute’s annual report.

7.6 All sensitive personal data will be handled at PROTECT level and training and advice provided to staff as appropriate. Portable media will be encrypted on a risk assessed basis.

7.7 Policies will be put in place to support information risk management including information security, data protection, confidentiality and an information charter on the management of information.

7.8 Reports will be submitted to the senior management team and Audit Committee on any variation from best practice for the management of sensitive data as set down by the DH with a rationale and justification for proposed actions.

7.9 Appropriate resources will be made available to support information governance as part of the business planning process. This will include effective records management and secure destruction of data when there is no longer a business need for retention.

7.10 IT systems will have robust security to DH standards and contracts with third parties will include a standard OGC clause on information security.

7.11 Privacy Impact Assessments will be carried out as necessary.

7.12 Training will be provided as necessary for key personnel in line with DH standards.

8 Statement of Internal Control

8.1 The Statement of Internal Control will assess the effectiveness and operation of the Institute’s risk management arrangements.

8.2 Internal audit will be responsible for aspects of the annual review of the effectiveness of the internal control system within the organisation.
8.3 External audit will provide feedback to the Audit Committee on the operation of the internal financial controls reviewed as part of the annual audit.

Issue date: February 2009

Review date: January 2012
## Appendix A

### KEY

<table>
<thead>
<tr>
<th>Risk</th>
<th>CE intervention required to mitigate threat to organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>High 20-25</td>
<td>Director action required and/or specific responsibility delegated and overseen</td>
</tr>
<tr>
<td>Medium 8-15</td>
<td>Activity manageable by established procedures</td>
</tr>
<tr>
<td>Low 1-6</td>
<td></td>
</tr>
</tbody>
</table>

### Scoring

<table>
<thead>
<tr>
<th>Impact</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Insignificant; No financial loss; disruption to day to day work manageable within existing systems</td>
</tr>
<tr>
<td>2</td>
<td>Minor; Minor financial loss / disruption to systems; procedures require review but manageable; limited slippage in work activity</td>
</tr>
<tr>
<td>3</td>
<td>Moderate; Disruption to financial systems; significant slippage in work activity; delay in recruiting staff; procedures and protocols require significant review</td>
</tr>
<tr>
<td>4</td>
<td>Major; Major financial loss; large scale disruption to guidance production; business activity severely undermined; poor quality guidance leading to loss of confidence in NICE</td>
</tr>
<tr>
<td>5</td>
<td>Catastrophic; Huge financial loss; significant threat to viability of the organisation in total or in part; huge disruption to business activity; almost total lack of confidence in Guidance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Very unlikely; May only occur in exceptional circumstances</td>
</tr>
<tr>
<td>2</td>
<td>Unlikely; Could occur at some time but unlikely</td>
</tr>
<tr>
<td>3</td>
<td>Possible; May occur at some time</td>
</tr>
<tr>
<td>4</td>
<td>Likely; Will probably occur / re-occur at some point</td>
</tr>
<tr>
<td>5</td>
<td>Very likely; Almost certain to occur / re-occur</td>
</tr>
</tbody>
</table>
## Appendix B - Version Control Sheet

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Replaces</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td>Julian Lewis</td>
<td>Risk Management Policy 2003</td>
<td>Incorporates information risk management</td>
</tr>
</tbody>
</table>
