

NISQ D22 Managing Risk Policy

supported by

NISQ F41 the Risk and Adverse Risk Register

NISQ GL 1 Audit, Risk and Compliance Department

1. Purpose of this document

1.1 The policy supports NISQ 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 Governing Board, Division Directors and the Chief Compliance Officer (CCO). It outlines the risk management process and identifies the reporting procedures.

1.3 In addition, it describes the relationship between the Governing Body, Division Directors and Audit, Risk and Compliance Department – Chief Compliance Officer and the process used to evaluate the effectiveness of NISQ 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 NISQ activities. All NISQ 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 NISQ Objectives

2.2 Risk assessment is a qualitative or quantitative evaluation of the nature and magnitude of risk to NISQ 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.

2.3 NISQ has addressed this area by creating the Risk Register F41, where it has already considered a number of Risk that will, may, potentially happen.

2.4 Risk management is the process of evaluating and responding to risks to NISQ 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. – The NISQ Risk Matrix.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Has Occurred |  |  |  |
| **Likelihood** | Will Occur |  |  |  |
|  | May  Occur |  |  |  |
| NISQ  Governing Body | Immediate Action and Review every Three Days | Minor  CCEA Regulations Notified Promptly | Moderate  CCEA Regulations Notified Promptly | Significant  CCEA Regulations Notified Promptly |
| Director Qualifications Division | Urgent Action and Review every  Seven Days | **Adverse Effect Impact** | | |
| CCO | Timely Action and Review every 14 days | **NISQ**  **Risk and Adverse Effect Matrix** | | |
|  | |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Reviewed By | Minor | Moderate | Significant |
| Chief Compliance Officer | Reviewed By | Reviewed by | Reviewed by |
| Director Qualification Division | Reviewed by | Reviewed by | Reviewed by |
| CCEA REGULATIONS | **Promptly Notified** | **Promptly notified** | **Promptly notified** |
| NISQ Approval Panel | Reviewed by | Reviewed by | Reviewed by |
| Governing Body | Informed | Reviewed by | Reviewed by |

3. Risk appetite

3.1 The level of risk associated with the attainment of NISQ objectives is reviewed by, and referenced to, the risk appetite accepted by the Governing Body “the Governors” and challenged by the Challenge, Review and Advisory Committee members. This provides oversight and consistency in the level of risk taken by NISQ 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:

**Risk management**

3.2 **Contextual risk**

NISQ recognises it works in a changing educational and security 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 specialised security and security fields. NISQ will accept moderate risks in pursuit of these goals providing any change does not impact the General Conditions of Recognition and other Regulatory requirements.

3.3 **Developmental risk**

NISQ 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 Learner and the wider public. These risks will be closely monitored, and project managed by the Audit, Risk and Compliance Department so that NISQ objectives are achieved and to ensure CCEA Regulations, Learners and stakeholders have confidence in our products.

3.4 **Reputational risk**

NIQS 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 Qualifications, Meeting the General Conditions of Recognition, by making use of the independent Challenge, Review and Advisory Committee experts, listening and reacting to regular feedback from CCEA Regulations, Approved Centres, Learners and other users of Qualifications, utilising formal external consultation when required, and providing great transparency of everything we do.

4. Approach to risk management

4.1 Risk management is central to the strategic management of NISQ. It provides a systematic process for identifying risks attaching to new and current 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 reoccurring.

4.2 NISQ 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 NISQ, as in the Audit, Risk and Compliance Department.

4.3 The internal controls for risk management will be scrutinised by the NISQ Governing Body, internal development report and forms part of the Annual Statement of Compliance for CCEA Regulations.

4.4 Risk management is a continuous process involving risk identification, Risk management v2.3

risk assessment, allocation of leads to manage risk, consideration of the residual risks after controls implemented.

4.5 The Chief Compliance Officer will ensure that fundamental risks are identified, assessed and monitored and incorporated in the Risk Register. Although adhering to a continuous ability to monitor risk, a monthly review to consider Risk and Adverse Effect will be undertaken by the Chief Compliance Officer. Emerging risks will be added as required to the Risk Register and actions and controls put in place to mitigate them and provide assurance to the Governing Body. Any new Risk and possible Adverse Effect will be reported to CCEA Regulations promptly and to the NISQ Governing body as per the Risk Matrix, (monthly report NISQ 75 being used).

5 Risk Register and Adverse Effect NISQ F41

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 NISQ.

5.2 Risks are initially identified through discussion between the Chief, Compliance Officer, The NISQ Divisions, CCEA Regulations, learners and the Approved Centres. These are then critically analysed by and reviewed by the Audit, Risk and Compliance Department, Chief Compliance Officer and the Director Qualification Division.

5.3 The identification of risks is set against NISQ functioning as a Awarding Organisation, its 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 (2.4).

6 Responsibilities

6.1 The Governing Body will determine the risk appetite for NISQ and set the culture of risk management within NISQ with particular regard to the General Conditions of Recognition, new Qualifications, new initiatives and emerging risks.

6.2 The Governing Body will have ultimate responsibility for risk management within NISQ including major decisions affecting the NISQ risk profile or exposure.

6.3 The Governing Body will create minutes of any risk management report to provide assurance that NISQ approach to risk management is effective, comprehensive and robust particularly in regard to major risks facing NISQ, these will be available to see on [www.nisq.uk](http://www.nisq.uk).

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

6.4 The Audit, Risk and Compliance Department will monitor and critically review the management of fundamental risks and the maintenance of the risk register to ensure there are fit for purpose.

6.5 It will approve a monthly risk report for submission to the NISQ Governing Body.

6.6 The Chief Compliance Officer has responsibility for the recording and assessment of risks, including those relating to information risk, maintaining the Risk Register and reporting these to the NISQ Governing Body, CCEA Regulations

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 (including Learners), threaten the NISQ meeting the General Conditions of Recognition or damage public reputation.

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

7.3 The Chief Compliance Officer will carry out a monthly information risk assessment to report to the NISQ Governing Body.

7.4 The CCO will report all serious breaches of information security to CCEA Regulations Promptly and the NISQ Governing Body. Any significant breaches will be included in the Annual Statement of Compliance for CCEA Regulations.

7.5 All sensitive personal data will be handled at the highest level as appropriate. Portable media will be encrypted on a risk assessed basis.

7.6 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. NISQ D17 Collecting and Protecting Information. As per Data Protection Legislation.

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

7.8 IT systems will have robust security to and contracts with third parties will include a standard clause on information security.

8 Statement of Internal Control

8.1 The Governing Body will assess the effectiveness and operation of NISQ’s risk management arrangements.

8.2 The Challenge, Review and Advisory Committee will be responsible for aspects of the review of the effectiveness of the Risk Management within NISQ.

8.3 NISQ will provide feedback annually to CCEA Regulations through an Annual Statement of Compliance, detailing if NISQ has met or not met the General Conditions of Recognition.

9. Procedure for dealing with Risk – Extract from NISQ D13

Any near misses or actual risk/adverse events should be reported to the Chief Compliance Officer in the first instance and in absence to the Director Qualifications Division. Details of the adverse event should be emailed or in writing using the guidance below to ensure a complete picture of the risk/adverse event is identified:

What – what happened?

• the qualifications, subjects, assessments, certificates affected

• the nature and cause of the incident (lost assessments/evidence, IT systems/software failure, lack of or errors in resources)

• how the incident came to light

Who – who is involved?

• number of learners and/or staff affected

• whether students and other stakeholders are aware of the incident

• the possible or actual impact on students

When – when did it happen?

• Dates/times

• When may the effects be felt?

Where – where did it happen?

• location(s) including NISQ and the NISQ Approved Centre premises

Why – why did it happen?

• actions already taken or planned by NISQ to identify causes and effects and to mitigate adverse impact. It will also be useful to state the likelihood and impact of the adverse event identifying whether the event is minor or could significantly impact NISQ, NISQ Approved Centre, Learners or third parties

10. Risk Rating Structure

* 1 Minor - could cause some embarrassment to NISQ if information came to light. Could result in non-compliance and may escalate if no action taken.
* CCEA Regulations Informed
* 2 Moderate - the risk has already been identified and actions put in place however there has been one occurrence.
* CCEA Regulations Informed
* 3 Significant - may impact a number of NISQ Approved Centres, Learners and/or third parties and has the potential for reputational damage, regulatory non-compliance, loss in Public Confidence
* CCEA Regulations Informed

WMMCDowell

NISQ Director Qualification Division