QAA's Approach to Risk Management

Policy statement (summary of main points): Sets out QAA's approach to the identification, evaluation and management of risk. It covers: • Definition and categories of risk • Risk Assessment • Risk Management: Roles and responsibilities • Guidance on completing the risk register	
Strategic aim of the policy: Identifies and mitigates against major threats to the achievement of QAA's strategic aims, as outlined in QAA's Strategy.	
Link to other policies, procedures and guidelines: • Strategy • Annual Plan and KPIs • Budget • Finance report • Treasury Management Policy	
Created/owned by: Governance Team	November 2014
Approved by: QAA Board	June 2017
Last reviewed/updated:	June 2023
Next review due:	June 2025
For further information, contact:	QAA Governance team governance@qaa.ac.uk

Introduction

This document sets out the Quality Assurance Agency's (QAA) approach to risk management.

Definitions

The following definitions apply to QAA's approach to risk management:

Risk	An event or situation, the likelihood and/or impact of which is currently unknown, which, if realised, will adversely affect QAA's ability to achieve its current or future aims and objectives.
Risk Appetite	The expected amount of risk that should reasonably be taken in the course of the organisation's business whilst ensuring the acceptable tolerance limit is not exceeded.
Risk Assessment	The process by which risks are identified, measured and rated.
Risk Management	Actions taken to reduce the likelihood that an identified potential risk will crystallise, or to minimise or contain the impact of an identified risk once that risk has crystallised within the risk appetite set by the Board.
Risk Tolerance	The maximum amount of risk that QAA is willing to bear. Distinct from risk appetite in that it defines absolute limits of acceptability, rather than degree of risk that can be reasonably taken by the organisation.

Risk Assessment

QAA undertakes risk assessment in three stages:

1 Risk identification
2 Risk measurement
3 Risk rating

Each stage is explained as follows:

Risk identification

QAA considers that a risk comprises two elements:

- One or more causes - which could include triggers that could make the potential risk crystallise
- One or more impacts - the consequences of the crystallisation of the risk.

QAA makes a distinction between **strategic** risks and **operational** risks.

Strategic risks are threats to the achievement of QAA's strategic aims, as outlined in QAA's Strategy. Strategic risks might relate to funding, products, services and markets and to government policy and requirements. While QAA distinguishes between strategic and operational risks, strategic risks will include risks relating to serious operational service failures, which compromise the ability of QAA to deliver against its strategic aims. Strategic risks are recorded in the QAA Strategic Risk Register.

Operational risks are threats relating primarily to the day-to-day conduct and delivery of QAA's business through people, processes, systems and resources. Operational risks are recorded as an integral part of QAA's Annual Plan (there is no separate register of operational risks) and relate to the achievement of the objectives under each of the aims of the QAA Strategy. These may also be supplemented by specific registers for individual business areas or significant projects.

When setting the Annual Plan for each operational year, potential risks associated with particular activities will be identified. This includes forward-looking risk identification (what could happen) and historic risk identification (what has happened, as a guide to what could happen in the future).

Both categories of risk cover a broad spectrum of possible risk scenarios and impacts, including commercial, financial, fraud, legal, reputational impacts, damage to assets, systems failure.

Risk measurement

QAA measures risk by considering the degree of impact that a trigger, the likelihood of which is currently unknown, would have on QAA's ability to achieve its objectives. Each identified risk is evaluated in terms of likelihood and impact and these measurements are used to determine the rating of that risk.

The following metrics apply to QAA's measurement of risk, and are reviewed and approved annually by the Board to ensure their ongoing appropriateness:

Risk rating

Risks can be plotted on the QAA Risk Tolerance Grid (see page 4), showing the current rating and target rating. The placement of each risk on the grid reflects its rating.

QAA rates identified risks according to the following categories:

- Significant risk (red)
- Priority risk (yellow)
- Acceptable risk (green).

Each of these categories is explained in further detail on the next page. The ranges of each risk category are represented by coloured sections in the Grid on page 5.

QAA Risk Tolerance Grid

Probability

	Low risk	Medium risk	High risk
Probable risk More than a 50% chance of occurrence		Risk appetite limit	
Possible risk 10% - 50% chance of occurrence			Risk appetite limit
Remote risk Less than a 10% chance of occurrence			
	Low risk Financial impact likely to be less than £1 million total or £250k pa Low impact on delivery of strategic or operational activities Low stakeholder concern	**Medium risk** Financial impact likely to exceed £1 million total or £250k pa Moderate impact on delivery of strategic or operational activities Moderate stakeholder concern	**High risk** Financial impact likely to exceed £2.5 million total or £750k pa Significant impact on delivery of the organisation's strategic or operational activities Significant stakeholder concern

Impact

QAA Risk Rating Scale

Risk rating	Description
Significant risk	**Significant risks** are risks identified as falling above QAA's risk tolerance limit **Significant risks** necessitate urgent action by management **Significant risks MUST** be reported to the Board The Board will either: • supervise the management of the **significant risk** by the executive team, or • manage the **significant risk** directly
Priority risk	**Priority risks** fall within the risk tolerance limit, but have the potential to fall outside the tolerance limit if they are not effectively managed **Priority risks MUST** be actively managed and prioritised within an acceptable timeframe **Priority risks** that score 'High Impact' or 'Probably Likelihood' **MUST** be reported to the Board
Acceptable risk	**Acceptable risks** fall well within the organisation's risk tolerance limit **Acceptable risks MUST** be effectively managed

Normal practice is that the Chief Executive has responsibility for ensuring that all risks in the Strategic Risk Register are managed, can delegate as appropriate within the Senior Leadership Team, and is ultimately accountable to the Board. The Board approves the Strategic Risk Register, informed both by the executive team and by any advice (on the management of risk in general and on specific risks and mitigations) provided by the Audit and Risk Committee, which scrutinises the Strategic Risk Register at each of its meetings.

Risk Management: Roles and responsibilities

Risk Management is a cross-organisational responsibility.

QAA Board

Role

The Board has ultimate responsibility for the risks faced by QAA and for the management of risk.

Responsibilities

The Board is responsible for:

1 setting QAA's Risk Tolerance limits, which it reviews annually for appropriateness
2 setting QAA's Risk Appetite, which it reviews annually for appropriateness and to ensure that it aligns with the Risk Tolerance
3 challenging and holding to account the Chief Executive on the effectiveness and appropriateness of the controls in place in respect of risk management.

The Board requires assurance that risks are being managed effectively. At each of its meetings, the Board shall receive and review the current QAA Strategic Risk Register, with particular attention to any risks that fall outside of the Board's Risk Appetite ('significant risks') and their plans for mitigation.

Reporting

In order to comply with Charity Commission requirements, the Board, as charity trustees, must make a risk management statement in the Annual Directors' Report, confirming that they have 'given consideration to the major risks to which the charity is exposed and satisfied themselves that systems or procedures are established in order to manage those risks'.

Audit & Risk Committee

Role

The Audit & Risk Committee monitors the overall effectiveness of QAA's internal control arrangements for Risk Management.

Responsibilities

The Audit & Risk Committee advises the Board on:

1 the ongoing appropriateness of the Risk Tolerance and Risk Appetite thresholds
2 the appropriateness of QAA's approach to Risk Appetite and Risk Management
3 the appropriateness of the controls in place to manage identified risks
4 the implications of recommendations made by the internal auditors
5 the implications of recommendations made by the external auditors
6 the current risk exposure of the organisation, and future risk strategy
7 the content of the Board's annual statement in relation to risk management.

At each of its meetings, the Audit & Risk Committee shall:

1 review the Strategic Risk Register
2 consider any operational or project-level risks which appear to approach or to fall outside of the Risk Appetite limit, as identified and escalated to the Committee by the Executive
3 consider the Executive's observation of QAA's Risk Appetite, and the Executive's agreed response to identified risks (particularly Priority and Significant Risks), exercising appropriate challenge.

The Audit & Risk Committee may also, at its discretion, review other registers associated with objectives and projects, to assure itself that risks are being managed effectively at operational level.

Reporting

The Audit & Risk Committee will report at each succeeding Board meeting on the effectiveness of risk management and will highlight risks that the Committee believes should be brought to the Board's attention.

Chief Executive

Role and responsibilities

The Chief Executive (or his delegate) is accountable to the Board for QAA's risk management, and specifically for overseeing the effective management of all identified risks falling within the risk appetite.

The Chief Executive is advised by the Executive on the effectiveness of the controls in place in respect of each identified risk.

Reporting

The Chief Executive reports to the Audit & Risk Committee, and where appropriate, to the Board, on the effectiveness of the management of identified risks.

Executive team

Role

The Executive is responsible for ensuring that risk management is effectively carried out within QAA, both at strategic and operational levels.

Responsibility

The Executive shall:

1 oversee SLT's review of the strategic risk register and approve proposed changes
2 be responsible for oversight of operational risk assessment and management as part of the annual planning process, and escalation of risks to the Strategic Risk Register if appropriate
3 receive reports on exceptions or deviations from the Annual Plan, which include notification of impact on, or status changes to, identified

operational risks
4 consider and decide upon appropriate corrective or mitigating action required in relation to identified exceptions
5 challenge the effectiveness of the observation and implementation of risk management across the organisation.

Reporting

Each member of Executive is individually accountable to the Chief Executive for the management of:

1 any Strategic Risk allocated by the Chief Executive for their supervision
2 any Operational Risk identified within their areas of responsibility in the Annual Plan.

Senior Leadership Team

Role

SLT supports the Executive in the management of operational risks, and the maintenance of effective controls.

Responsibilities

SLT shall:

1 review the strategic risk register on a monthly basis, and ensure that appropriate mitigations are in place
2 escalate operational risks for Executive attention as needed.

Reporting

SLT highlights to the Executive any risks which may require escalation to the Strategic Risk Register. SLT members will also ensure that staff within their area are familiar with QAA's approach to risk and those identified risks relating to their area of activity.

Staff

Role

All QAA staff are expected to actively engage in risk management.

Responsibilities

Staff shall make every effort to ensure that they:

1 are familiar with QAA's Approach to Risk Management, and those identified risks relating to their areas of activity
2 take responsibility for the risks they own.

Reporting

Staff will ensure that they escalate, where appropriate, information or intelligence which indicates a change to either the likelihood or impact of an identified risk or a new risk.

Published – 30 November 2023