Commissioner for Ethical Standards in Public Life in Scotland

Risk Management Policy

Date policy adopted: 24/10/2012
Review frequency: Three years
Date of last review: 12/06/2013
Date policy must be reviewed by: 30/06/2016

Introduction

The Commission for Ethical Standards in Public Life in Scotland (the Commission) has a wide range of strategic and business objectives as well as statutory duties. The fulfilment of these duties and achievement of these objectives is surrounded by uncertainty. Risk is defined as this uncertainty of outcome and arises equally from positive opportunity or negative threat. The impact of risk may be positive as well as negative.

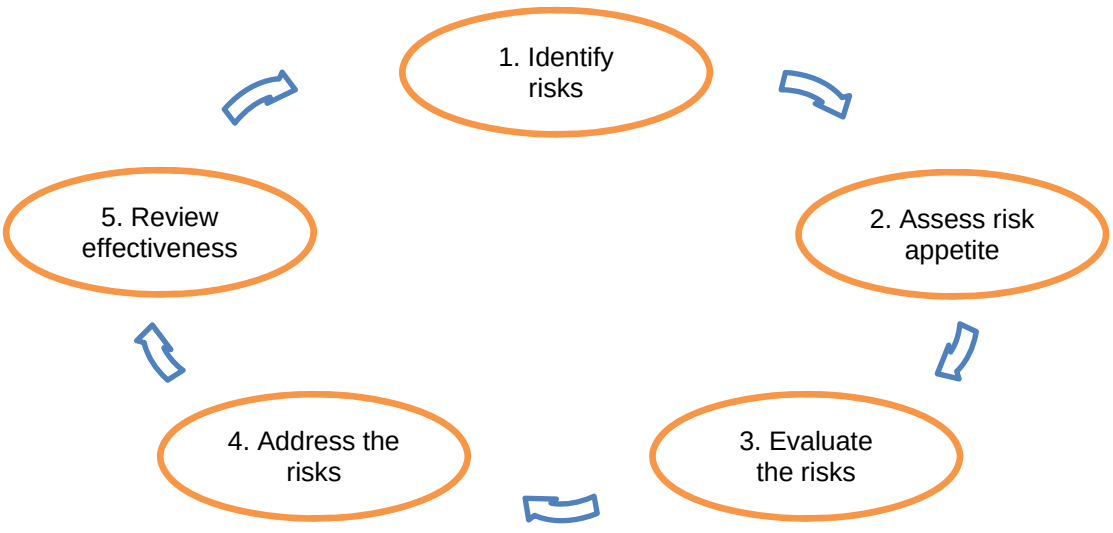
Risk management is a structured approach to identifying, assessing and controlling risks that emerge. Its purpose is to support better decision making through understanding the risks inherent in the Commission's activities and their likely impact.

This document sets out the Commission's risk management policy and approach.

Policy and Principles

Policy

The Commission will take a pragmatic approach to risk management. It will manage its risk through an appropriate and proportionate framework. Key stages in the framework are set out below.



The aim of the framework is to:

- provide the Commission and others with assurance that threats are effectively managed and that opportunities are appropriately exploited to the benefit of the organisation
- give confidence to those that scrutinise the organisation in the robustness of corporate governance arrangements
- enable the organisation to take informed decisions across all its functions.

Principles

- The Commission will foster a culture that embeds risk management into all aspects of its business.

- Risk management should be a key feature of corporate decision-making processes to ensure that the impact of policy decisions on risk is considered each time a strategic decision is taken or a policy is approved.

- Risk management should be embedded in strategic, financial and business planning.

- Risk management policies will be clearly communicated to all staff.

- All processes and procedures should be designed to minimise risk and the impact of risk, in a manner that is proportionate and affordable.

- The Commission will maintain, review and update its risk register regularly.

- The Commission's risk management policy and procedures will operate without prejudice to the statutory functions of each Commissioner.

1. Identifying risks

In order to manage risk, an organisation needs to know what risks it faces.

Identification will focus on:

- risks to the achievement of the Commission's strategic objectives and
- risks arising from annual operational business plans.

Ongoing risk identification will form part of the strategic and business planning process.

Risks will be recorded in a Risk Register. The Risk Register will be developed and maintained by the Business Manager. The Business Manager will consult all staff to identify key risks to the business.

Strategic Risk Categories

The Commission groups its risks into five categories:

- **Reputation and credibility** – risk arising from how the Commission is perceived by its stakeholders.
- **Operational delivery** – risk arising from or threatening the efficiency and effectiveness with which the Commission delivers its key functions. These include investigating complaints about MSPs and local authority councillors, monitoring the public appointments process and reporting breaches of the relevant Codes.
- **Resources** – risk arising from the robustness and effectiveness of the systems by which the Commission manages resources, including finance, human and physical resources.
- **Governance**– risk arising from the robustness and effectiveness of the systems by which the Commission governs its resources and performs its functions.
- **External impact** – risk arising from events, issues and impacts from and relating to the external environment (PESTLE analysis).

2. Assessing risk appetite

The concept of a "risk appetite" is key to achieving effective risk management and should be considered before moving on to evaluating and addressing risks.

- When considering a negative risk (a threat to achieving the Commission's objectives) it is necessary to find a balance between the cost (financial or otherwise) of controlling the risk and the negative impact of the risk occurring.

- When considering a positive risk (an opportunity which will assist the Commission in achieving its objectives) it necessary to find a balance between the value (financial or otherwise) of the potential benefits and the losses that might be incurred.

The level of risk that is acceptable will be determined by the staff member responsible for managing that risk in conjunction with the Accountable Officer and members of the Management Team. Risk appetite may vary on a case by case basis depending on the perceived threat or benefit being considered.

In general, for the Commission to deliver its objectives it needs to balance opportunities to innovate and improve with its responsibilities in terms of accountability, propriety, regularity and value for money.

3. Evaluating the risks

Having identified the key risks, the Commission will assess the likelihood of their occurrence and the potential impact on its objectives.

The likelihood of a risk occurring will be assessed as almost certain, likely, possible, unlikely and rare. The impact if the risk occurs will be assessed as insignificant, minor, moderate, major or catastrophe. The combination of these elements will lead to an overall risk assessment of very low, low, medium, high or very high.

This methodology helps the Commission to prioritise its response to risk, to determine which risks need to be managed and which are less critical.

4. Addressing the risk

Having evaluated the risks, the Commission must decide how each risk should be addressed. Response to the risks will fall into four tolerance levels.

Tolerate	Monitor the risk but take no action because either; the likelihood and impact are acceptable or because there is no cost-effective control. Risks that are tolerated are usually supported by a contingency plan to mitigate the effects should the situation arise.
Transfer	The risk will be transferred to another party outside the organisation. For example, contracting out a business function or taking out insurance.
Terminate	Close down the business function or activity.
Treat	Take action to manage the risk through control measures.

The tolerance level will take into account the likelihood and impact of the risk, the risk appetite and the cost of controlling the risk. The tolerance level will be derived from the risk ranking.

Risk ranking	Very low	Low	Medium	High	Very high
Tolerance	Tolerate	Tolerate or treat	Treat or tolerate	Treat	Treat, transfer or terminate

The tolerance level for each risk will inform the specific actions, timescales and responsibilities necessary to manage the risk down to an acceptable level.

The risk, its score, appetite and tolerance level as well as associated actions and timescales to address the risk will be recorded in the risk register.

Ownership of risk

Ultimate ownership of risk lies with the Accountable Officer.

The Commission will delegate ownership of specific risks to the appropriate staff members. Ownership of specific risks will be recorded on the Risk Register.

5. Reviewing the risks

Risk is ultimately owned by the Accountable Officer. The Accountable Officer receives assurance that risk is being monitored and managed appropriately from reports, comments, advice and feedback from:

- The Business Manager
- The Management Team
- External Audit
- The Audit Advisory Board (AAB)

Sources of assurance include:

- Risk Register
- Management reporting
- Audit reports
- Key Performance Indicators
- Feedback from staff and other stakeholders

The Risk Register will be updated on an on-going basis and formally reviewed at the Commission's Annual Business Plan reviews. Mandatory features of the Risk Register are:

- a description of each risk
- its strategic risk category
- risk appetite level
- inherent risk likelihood and impact
- risk tolerance level
- control measure
- owner and
- actions needed.

The Risk Register and Risk Management Policy will be reviewed by the Commission's external auditor and Advisory Audit Board on an annual basis.

Audit reports will inform the content of the Risk Register and the approach to risk management; in particular, actions or control measures required to address newly identified risks or weaknesses.