
RISK MANAGEMENT POLICY

Introduction

1. This document provides details of the Standards Commission for Scotland's policy and approach to the management of risk.
2. A risk is any internal or external circumstance, event or factor which may impact on the Standards Commission's ability to achieve its strategic objectives. Risks arise both from the possibility that opportunities may not be realised as well as the possibility of threats materialising. The impact of risks to the Standards Commission are considered in terms of both opportunities and threats.

Policy and Principles

Policy

1. The Standards Commission manages risk through a framework that seeks to identify, assess, address, review and report on risk, in an appropriate and proportionate manner, with consideration given to both the organisation's appetite for risk and the environment in which it operates.
2. The aim of the framework is to:
 - Provide the Standards Commission and others with assurance that threats are constrained and managed properly, and that opportunities are appropriately exploited to the benefit of the organisation.
 - Give confidence to those who scrutinise the Standards Commission about the robustness of its corporate governance arrangements.
 - Enable the Standards Commission to make informed decisions about its work, priorities, use of resources, and internal and external engagement.

Principles

3. The Standards Commission fosters a culture that embeds risk management into all aspects of its business.
4. Risk management is embedded into the corporate decision-making processes to ensure that the impact of any potential risk is considered each time a strategic decision is taken and as policies and processes are introduced or amended.
5. All processes and procedures are designed to identify and manage risk in a manner that is proportionate and helps to achieve best value.
6. Risk management is embedded in strategic, financial and business planning, including business continuity planning.
7. A risk will only be included in the risk register if it threatens the achievement of the Standards Commission's business plan.

Roles and Responsibilities

8. The Standards Commission agrees its risk register annually, at the start of each of each operational year, to ensure that risks to the implementation of the strategic and operational objectives are identified going forward.
9. The Standards Commission's Executive Team monitors and updates the risk register at least three times a year, in order to:
 - discuss, evaluate and recommend the key business risks that might affect the ability to deliver the business plan and / or adversely affect confidence in the ethical standards framework;
 - assess existing controls (the measures in place to reduce or limit risk);
 - determine the appropriate response to each risk;
 - allocate responsibility for managing each risk; and
 - identify and record activities undertaken since the previous review, to reduce or limit risks on the register.
10. The Executive Team considers and rates the likelihood of each risk occurring and its impact should it occur, in light of the controls in place and actions taken. The Executive Team then makes a recommendation to the Audit & Risk Committee about the rating value attached to each risk.
11. The Audit & Risk Committee reviews the risk register, including the rating value for each risk and the risk tolerance level at each of its meetings to ensure it is relevant in the evolving business and political landscape and that it reflects changing priorities. A report of the review is thereafter provided for consideration by Members at the next available meeting of the Standards Commission.

Identification of Strategic Risks

12. In identifying risks, the Standards Commission considers the following categories:
 - i. **Reputational** – risks to the Standards Commission's name, influence and standing and how it is perceived by its stakeholders.
 - ii. **Strategic and Operational** – risks to the achievement of the Standards Commission's strategic aims and business plan. These are risks that threaten how the Standards Commission delivers its key functions and statutory obligations.
 - iii. **Financial, Resources and Government** – risks arising from the robustness and effectiveness of the systems by which the Standards Commission governs and manages resources. This includes risks relating to financial controls and systems, which could prevent the Standards Commission from achieving best value.
 - iv. **Organisational development and change management** – risks arising from the development of the organisation and how well it implements change.

Risk Tolerance

13. The Standards Commission's tolerance to each business risk is identified as one of the following:
 - i. Avoid
 - ii. Highly Cautious
 - iii. Cautious
 - iv. Open

The tolerance to each risk is identified in the risk register through a system of colour coding when each risk is plotted on the Risk Map. When considering the controls and actions in place to mitigate each risk, the Standards Commission will bear in mind that there can be more tolerance of certain risks than others.

Control of Risk

14. Controls are the measures or procedures put in place by the Standards Commission and its Executive Team to manage mitigation or the impact of the risk. There are four categories of risk control. Each risk

identified should have a control measure and some may have more than one. Controls fall into the following four categories:

- i. **Directive** - Action designed to ensure that a particular outcome is achieved. For example, this could include actions to terminate the risk, put in place a detective control or reduce the likelihood of risk.
- ii. **Corrective** - Action taken to correct the undesirable outcome should the risk be realised.
- iii. **Preventative** - Action designed to prevent or limit the likelihood of the risk occurring..
- iv. **Detective** - Action designed to identify occasions of undesirable outcomes having been realised. The effect is, by definition, 'after the event' so such actions are only appropriate when it is possible to accept the loss or damage occurred.

15. Controls should be proportionate to the risk and the tolerated risk level agreed by the Standards Commission. If any control actions have associated costs the Standards Commission will always consider whether the actions provide value for money in respect of the risks being controlled. The actions are mainly designed to contain the risk, rather than obviate it.

Reporting and Assurance

Assurance

16. Risk is ultimately owned by the Standards Commission. The Standards Commission receives assurance that risk is being monitored and managed appropriately from its:
 - Audit and Risk Committee;
 - Review of management reports (including reports on expenditure against budget and performance against agreed key performance indicators);
 - Executive Team; and
 - Internal and External Auditors, via regular and *ad hoc* audits.
17. The sources of assurance include:
 - the Audit & Risk Committee's Annual Report;
 - the Risk Register;
 - Management Reporting;
 - Key Performance Indicators; and
 - Feedback from staff and other stakeholders.

Review

18. Risk is proactively managed through the monitoring and review of risks and controls throughout the year. The Standards Commission determines matters to be included in the risk register at the start of each operational year. The Executive Team reviews and updates the risk register on an ongoing basis. The formal review is managed through the Audit & Risk Committee at each of its meetings.

Audit & Risk Committee

19. The Audit & Risk Committee reviews risks through the monitoring of the risk register and outputs of internal and external auditors.
20. Where necessary the Audit & Risk Committee will direct the Executive Team to take appropriate action and / or refer issues to the Standards Commission for discussion and decision.
21. The Audit & Risk Committee reports to the Standards Commission three times per year to give assurance that risk is appropriately managed.

Executive Team

22. The Executive Team reports to the Audit & Risk Committee through review of the risk register and will bring *ad hoc* risk issues to the attention of the Audit & Risk Committee outwith the regular reporting cycle.

23. The Executive Team is responsible for ensuring the risk register is reviewed and updated regularly as part of the assurance to the Audit & Risk Committee and Standards Commission. The Executive Team reports to the Audit & Risk Committee at all of its meetings.

Internal and External Audit

24. Auditors will bring to the attention of the Executive Team and the Audit & Risk Committee any areas of risk and will also report on the effectiveness of the Standards Commission’s risk management. The Auditors will also provide advice and guidance in relation to risk management and specific areas of risk.

Risk Register

25. The risk register consists of:

- a strategic risk heat map;
- a summary of each of the identified risks;
- the associated controls and planned actions for each risk; and
- details of the specific actions taken against each risk

Strategic Risk Heat Map

27. This is a reporting tool that will enable the Audit & Risk Committee to take an overview of strategic risk. It is a visual representation of the risk position and informs the Audit & Risk Committee and the Standards Commission whether the rating value for each risk is consistent with its tolerance for that risk.

Individual Risks

28. The summary of risks is linked to the Standards Commission’s strategic objectives. A description of the impact and root cause of each risk is outlined, along with their likelihood of occurrence, their impact and which operational risks contribute to these factors. The aim is to keep this at a high level, linked to the corporate strategic objectives. Each individual risk will be allocated a short name to ensure they are easily identifiable.

Document Control & Version information

29. The Risk Management Policy will be reviewed annually.



Summary of changes made to the document				
Date	Action by (initials)	Version Updated	New Version number	Brief Description <i>(for example – corrected typos – whole document; updated para. 1 – revised, reformatted, Corporate Branding)</i>
12/12/16	SCS	2013	2016 v1	Review, update & reformat policy
18/12/17	SCS	2016	2017 v1	Review, minor alterations
17/12/18	ET	2017	2018 v1	Review, reformat & correct minor typographical errors
16/12/19	SCS	2018	2019 v1	Review, strengthen provisions to emphasise that risks can arise from both internal and external circumstances, events and factors and that appropriate risk management is required to assist Standards Commission to not only make informed decisions about its own work but also about its external engagement.
14/12/20	SCS	2019	2020 v1	Minor alterations following annual review
25/11/21	SCS	2020 v1	2021 V1	Minor updates following annual review

12/12/22	SCS	2021 v1	2022 v1	Minor updates following annual review including amendments to wording in respect of categorisation of risk tolerance to reflect wording in risk register.
12/12/23	SCS	2022 v1	2023 v1	Minor updates following annual review