RISK MANAGEMENT POLICY

Introduction

1. This document provides details of the Standards Commission for Scotland ("Standards Commission") policy and approach to the management of risk.

2. A risk is a circumstance, event or factor which may impact on the Standards Commission's ability to achieve its Strategic Objectives. Risks arise equally 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 should be considered in terms of both opportunities and threats.

Policy and Principles

Policy

1. The Standards Commission for Scotland will manage its risk through an appropriate and proportionate framework which identifies, assesses, addresses, reviews and reports on risk, in the context of its risk appetite and environment.

2. The aim of the framework is to:

- Provide the Standards Commission and others with assurance that threats are constrained and managed 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 across its functions.

Principles

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

4. Risk management will be 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 will be designed to identify and manage risk in a manner that is proportionate and helps to achieve best value.

6. Risk management will be embedded in strategic, financial and business planning, including business continuity planning.

7. Risk will only be included in the risk register if it threatens the achievement of the Standards Commission's business plan.

RISK MANAGEMENT POLICY

Approach

Roles and Responsibilities

8. The Standards Commission will agree 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 will monitor and updated the risk register as necessary and no less than once during each quarter year in order to:
   - discuss, evaluate and recommend the key business risks which might affect the ability to deliver the business plan;
   - 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 will discuss and rate 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 will make a recommendation to the Audit & Risk Committee about the rating value attached to each risk.

11. The Standards Commission's Audit & Risk Committee will review the Risk Register, including the rating value for each risk and the risk tolerance level at its meetings. Thereafter the Risk Register will be reviewed by the Standards Commission's Audit & Risk Committee at each meeting to ensure it is relevant in the evolving business and political landscape and that it reflects changing priorities. Thereafter a report of the review will be provided for consideration by Members at the next available meeting of the Standards Commission.

Strategic Risk Categories

12. In identifying risks, the Standards Commission will consider 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. 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 will determine the tolerance level assigned to each risk to inform further action. The tolerance level is reflected in the target risk score and takes into account the nature and impact of the risk and the cost of controlling the risk. The Risk Register contains a risk heat map, which demonstrates the tolerance threshold for each risk.

    i. **Tolerate -** Monitor the risk but take no action because both the likelihood and impact are acceptable or because there is no cost-effective control.

    ii. **Transfer -** The risk will be transferred to another party outside the organisation. For example, contracting out a business function.

    iii. **Terminate -** Close down the business function or activity

    iv. **Treat -** Take appropriate action to manage the risk though the introduction of control measures.

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 -** A specific action or series of actions to ensure that a particular outcome is achieved. This could include, for example, actions to terminate the risk, put in place a detective control or reduce the likelihood of risk.

    ii. **Corrective -** Action to correct the impact of the risk realised.

    iii. **Preventative -** Action designed to identify when a risk is realised and is impacting or likely to impact on the Standards Commission.

    iv. **Detective -** Action designed to identify occasions of undesirable outcomes having been realised. The effect is, by definition, "after the event" so they are only appropriate when it is possible to accept the loss or damage occurred.

15. Controls should be proportionate to the risk and should be designed to give a reasonable assurance of confirming likely loss to the tolerated level agreed by the Standards Commission. Control actions have associated costs so the Standards Commission will always consider whether they provide value for money in respect of the risks being controlled. They 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:
    - The Audit and Risk Committee
    - The Executive Team
    - Internal and External Auditors via regular audits and *ad hoc* audits.

17. The sources of assurance include:
    - Audit & Risk Committee's Annual Report
    - Risk Register
    - Management Reporting
    - Key Performance Indicators
    - Feedback from staff and other stakeholders

Review

18. Risk is proactively managed through monitoring and review of activity associated with or impacting on risk and its management. The Standards Commission will determine matter for inclusion in the Risk Register at the commencement of each operational year. The Risk owners will review and update the risk register on an ongoing basis. Review is managed through the Audit & Risk Committee at each of its meetings.

Audit & Risk Committee

19. The Audit & Risk Committee will review 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 or refer issues to the Standards Commission for discussion and decision.

21. The Audit & Risk Committee will report to the Standards Commission three times per year to give assurance that risk is appropriately managed.

Executive Team

22. The Executive Team will report to the Audit & Risk Committee through review of the strategic 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 strategic risk register is reviewed and updated regularly as part of the assurance to the Audit & Risk Committee and Standards Commission. The Executive Team will report 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 MANAGEMENT POLICY

Risk Register

25. The Risk Register consists of a strategic risk heat map and a summary of the individual risks identified.

Strategic Risk Heat Map

27. This is a reporting tool that will enable the Audit and Risk Committee to take an overview of strategic risk. It is a visual representation of the risk position and informs the Audit and Risk Committee and the Standards Commission whether its risk map 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.

Document Control & Version information

29 The Risk Management Policy will be reviewed biennially.

Summary of changes made to the document				
Date	Action by (initials)	Version Updated	New Version number	Brief Description *(for example – corrected typos – whole document; updated para. 1 – revised, reformatted, Corporate Branding)*
12/12/16	SCS	2013	V1/2016	Review, update & reformat policy