Risk Management Policy

The Scottish Information Commissioner's risk management policy and approach

Scottish Information
Commissioner

Contents

Risk Policy

Introduction

1. This document sets out the Scottish Information Commissioner's (the Commissioner) risk management policy and approach, including the organisation's risk appetite.

2. Risk is defined as an uncertain event or set of events which, should it occur, will have an effect upon the achievement of objectives. Risk arises equally from the possibility that opportunities will not be realised as it does from the possibility that threats will materialise. The impact of risk may be positive as well as negative.

Policy and principles

Policy

3. The Commissioner actively manages 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.

4. The aim of the framework is to:

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

Principles

5. The Commissioner fosters a culture that embeds risk management into all aspects of the business.

6. Risk management is embedded in corporate decision-making processes to ensure that the impact of policy decisions on risk is considered each time a strategic or operationally significant decision is taken or policy and procedures are approved.

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

8. Risk management is embedded in strategic, operational, financial and business planning.

9. The Commissioner maintains, reviews and updates the strategic and operational risk registers regularly.

Approach

Overview

10. The Senior Management Team (SMT) acting in its strategic capacity will define the organisation's risk appetite and will articulate the organisation's risk tolerance.

Strategic Risk

11. The Commissioner defines strategic risks as those which relate to the organisation’s ability to deliver long-term and strategic aims and which derive from the relationship with the external environment and legislative context.

12. The SMT acting in its strategic capacity will identify strategic risk and articulate it through a strategic risk register. The strategic risk register will be considered and reviewed by the SMT at the Quarterly Senior Management Team Meeting (QSMTM) or as needed in relation to a particular event or development. It will be presented annually to the Advisory Audit Board (AAB) for comment and advice.

Operational Risk

13. Operational risks relate to issues which impact directly on day-to-day activity or which are created through failures in day-to-day activity, and which impact on the operational delivery of the annual operational plan.

14. The SMT acting in its operational capacity will articulate operational risk through an operational risk register. Individual risks are owned by Heads of Department. The operational risk register is a living document and should be updated when new risks arise. It will be reviewed every two months to ensure appropriate recording and responses to operational developments.

Risk appetite

15. The risk appetite is set at two levels, reflecting the differing natures of our duties and powers. Statutory duties impose on us functions which must be carried out, or carried out in a particular way, or to achieve a particular outcome. Statutory powers give us the ability to carry out functions but they are not prescriptive about approach or outcomes.

16. **Statutory functions:** our appetite is cautious to open. We will use appropriate caution to ensure we meet statutory requirements, but aim to push the boundaries to achieve an acceptable level of reward, particularly in relation to our interpretation of FOI legislation and operational effectiveness.

17. **Statutory powers**: our appetite is open, willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward (and value for money). This relates to those functions where we are given powers to act but legislation does not specify what we must do or how we should discharge our functions.

18. In setting our risk appetite in this way, we recognise that the appetite for some categories of risk will be more cautious or hungry depending on what they are and what type of impact they have.

Ownership of risk

19. Ultimate ownership of risk lies with the Commissioner through their roles of being the person responsible for governance of the organisation and Accountable Officer.

20. Strategic risk is collectively owned by the SMT acting in its strategic and governance capacity.

21. The Commissioner delegates ownership of specific operational risks to Heads of Department which are recorded on the operational risk register.

Control of risk

22. Controls are the measures or procedures put in place to manage or mitigate the likelihood or impact of risk. Every risk identified must have a control measure and some may have more than one. Planned Action if implemented will become controls.

Reporting and Assurance

Assurance

23. Risk is ultimately owned by the Commissioner who receives assurance that risk is being monitored and managed appropriately from reports, comments, advice and feedback from:

- The Senior Management Team
- Internal Audit
- External Audit
- The Advisory Audit Board (AAB)

24. Sources of assurance include:

- Risk Registers
- Management reporting
- Audit reports
- Quality and Performance Indicators
- Feedback from staff and other stakeholders

Monitoring and review

25. Risk is actively managed through monitoring and review of activity associated with or impacting on risk, and the delivery of strategic and operational objectives. The key tools in the management of risk are:

- The strategic and operational risk registers
- Committee reports and minutes
- Audit reports and action plans

26. The strategic risk register will be updated on an on-going basis and formally reviewed at each Quarterly Senior Management Team meeting (QSMTM).

27. The operational risk register is a living document and management tool that should be updated as new risks appear/disappear. Records will be formally reviewed at least every two months at a Monthly Senior Management Team Meeting (MSMTM).

28. Mandatory features of the risk registers are:

(i) A description of each risk, its category, inherent risk likelihood and impact, control measure, residual likelihood and impact, owner and actions needed.

(ii) An update table summarising changes made over the year.

29. Committee reports (CR) are set in a format that includes specific reference to risk. The minutes of the QSMTM or the MSMTM at which the CR is considered should record any changes that need to be taken account of in the risk register(s).

30. The SMT will consider an annual risk management report from the HOCS which gives a statement of assurance about risk management.

Risk scoring system

31. Risk will be scored by assessing the likelihood and impact on a scale of 1-5, multiplying them to give an overall ranking which also sets the tolerance level.

Roles and responsibilities

Title	Responsibility	Role	Frequency of reporting
Commissioner	• Ownership of risk and risk policy	• Approve risk management policy (with SMT) • Assurance that policy is applied and risk is managed effectively	• As required to external and internal stakeholders
Senior Management Team (SMT)	• Shared ownership of risk • Management of risk • Providing assurance to SIC • Ownership of specific operational risks	• On-going updating of the operational risk register for owned risks • Quarterly reporting and review of the risk register • Complete Committee Report in support of decisions/ policy approval as required	• Quarterly to Commissioner/ SMT • As required to Commissioner/ SMT
Head of Corporate Services (HOCS)	• Operational owner of the risk registers • Annual assessment and assurance statement to the SMT	• Co-ordinate content and updating of risk registers • Drafting of annual risk report	• Reports to SMT – QSMTM and MSMTM • Ad hoc as required to SMT • Annually to SMT and the Commissioner
All staff	• Operational management of risk through application of policies and procedures	• Contribute to the management of risk through applying policies and procedures appropriately and consistently • Raise concerns or identified risk with line management, SMT or SIC as appropriate.	• As required by line management
Advisory Audit Board (AAB)	• Annual review of strategic risk register • Providing advice and assurance to the Commissioner	• Monitor the risk policy • Advise the Commissioner and the SMT as appropriate • Provide support and advice to the Commissioner (in their role as accountable officer) and Senior Management Team as appropriate • Liaise with auditors over areas of concern	• Annually to the Commissioner
Internal and External Audit	• Report and advise on risk to the Commissioner and AAB • Provide assurance to the Commissioner	• Carry out and report on audits to the programme agreed with the Commissioner • Give appropriate advice to the Commissioner at all levels in relation to risk management • Bring concerns about risk to the attention of the Commissioner	• As agreed through audit programme

Document Control Sheet

Document Information	
Full name of current version: Class, Title, Version No and Status. *E.g. C5 Key Documents Handbook v01 CURRENT ISSUE*	C1 Risk Management Policy 2024-25 CURRENT ISSUE
VC File Id	215054
Type	Policy
Approver	SMT
Responsible Manager	HOCS
Date of next planned review	May 2025
Approval & Publication	
Approval Date (major version)	06/09/2024
For publication *(Y/N)*	Y
Date published	23/09/2024
Name of document in website file library	RiskManagementPolicy202425
Corrections / Unplanned or Ad hoc reviews (see Summary of changes below for details)	
Date of last update	

Summary of changes to document				
Date	**Action by** *(initials)*	**Version updated** *(e.g. v01.25-36)*	**New version number** *(e.g. v01.27, or 02.03)*	**Brief description** (*e.g. updated paras 1-8, updated HOPI to HOCS, reviewed whole section on PI test, whole document updated, corrected typos, reformatted to new branding*)
23/09/2024	SL	01.00	01.01	New document created and DCS updated

Scottish Information Commissioner
Kinburn Castle
Doubledykes Road
St Andrews, Fife
KY16 9DS

t   01334 464610
enquiries@foi.scot

www.foi.scot