Risk Management Policy

The Scottish Information Commissioner's risk management policy and approach

Scottish Information Commissioner

Contents

Introduction **1**
Policy and principles **1**
Policy 1
Principles 1
Approach **1**
Overview 1
Strategic Risk 1
Operational Risk 2
Risk appetite 2
Tolerance 3
Ownership of risk 3
Control of risk 3
Reporting and Assurance **4**
Assurance 4
Monitoring and review 4
Risk scoring system 5
Roles and responsibilities **6**
Document Control Sheet **7**

Cross-referenced VC documents

VC No	VC name
VC117046	2019 - 20 Strategic Risk Register
VC117047	2019 - 20 Operational Risk Register

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:

   (i) 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.

   (ii) Enable the organisation to take informed decisions across all its functions.

   (iii) 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 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.

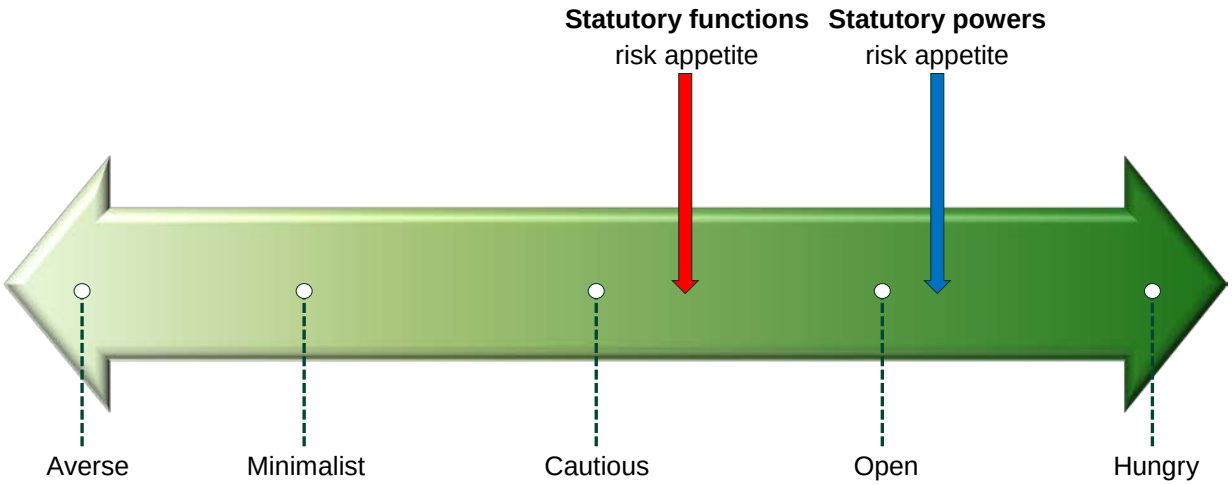
14. The SMT acting in its operational capacity will articulate operational risk through an operational risk register. Individual risks are owned by Heads of Department. The operational risk register is reviewed every two months and at the QSMTM, or as needed in relation to operational developments or in relation to changes in the strategic environment. The QSMTM will consider the quarterly operational risk management report, based on a quarterly heat map.

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.

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.

Tolerance

19. At each risk review, or when a new risk is added to the Risk Register, for each risk identified we will assess the risk and decide what tolerance level will be assigned to it to inform further action. The tolerance level will take into account the likelihood and impact of the risk, the risk appetite and cost of controlling the risk. The tolerance level will be derived from how the risk is scored (see below).

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.

Ownership of risk

20. Ultimate ownership of risk lies with the Commissioner through their roles of being the person responsible for governance of the organisation and accountable officer.

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

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

Control of risk

23. Controls are the measures or procedures put in place to manage or mitigate the likelihood or impact of risk. There are four categories of risk control. Every risk identified must have a control measure and some may have more than one.

Directive (DIR)	A specific action or series of actions to ensure that a particular outcome is achieved. This could include, for example, actions to terminate risk, put in place a detective control or reduce the likelihood of risk.
Preventative (P)	Action designed to prevent or reduce the likelihood of the situation giving rise to the risk occurring in the first place.
Detective (Det)	Action designed to detect when a risk is realised (or is going to be realised) and is impacting or likely to impact on the SIC.
Corrective (C)	Action to correct the impact of risk realised.

Reporting and Assurance

Assurance

24. 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:

    (i) The Senior Management Team

    (ii) The HOCS

    (iii) Internal Audit

    (iv) External Audit

    (v) The Advisory Audit Board (AAB)

25. Sources of assurance include:

    (i) Risk Registers

    (ii) Management reporting

    (iii) Audit reports

    (iv) Quality and Performance Indicators

    (v) Feedback from staff and other stakeholders

Monitoring and review

26. 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:

    (i) The Strategic and Operational Risk Registers

    (ii) Committee reports and minutes

    (iii) Audit reports and action plans

    (iv) An Annual Risk Report which reports on both the Strategic and Operational Risk Registers

27. The strategic risk register will be updated on an on-going basis and formally reviewed at the QSMTM.

28. The operational risk register will be updated on an on-going basis and formally reviewed monthly. A quarterly heat map will form the basis of a report to the QSMTM.

29. 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.

30. Additionally, the operational risk register will contain a risk “heat map” which gives a graphical representation of the Commissioner’s risk profile by quarter.

31. In line with governance arrangements, a committee report should accompany every paper/ policy requiring sign-off or a decision by the Commissioner and/ or SMT. This paper is in a set format that includes specific reference to risk. Minutes should record any changes required to the Risk Register(s)

32. Audit reports will inform the content of the risk registers and the approach to risk managemen and, in particular, the actions or control measures required to address newly identified risks or weaknesses.

33. The SMT will receive and consider an annual risk management report which gives a statement about the risk profile, comments and makes recommendations about the risk management system – policy, reporting and register – and a statement of assurance about risk management.

Risk scoring system

				Impact						
				Insignificant	Minor	Moderate	Major	Catastrophic	Tolerance	risk ranking
				1	2	3	4	5		
likelihood	Almost certain	>80%	5	5	10	15	20	25	Treat, Transfer or Terminate	Very high
	Likely	50-80%	4	4	8	12	16	20	Treat	High
	Possible	20-50%	3	3	6	9	12	15	Treat or tolerate	Medium
	Unlikely	5-20%	2	2	4	6	8	10	Tolerate or treat	Low
	Rare	<5%	1	1	2	3	4	5	Tolerate	Very Low
								Tolerance line		

34. 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.

35. This is summarised in the diagram above.

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 through the HOCS • Quarterly reporting and review of the risk register to SMT though the HOCS • Ensure staff are aware of risk, that it is embedded in processes and performance management and that staff are appropriately trained to deal with risk • Complete Committee Report in support of decisions/ policy approval required	• Quarterly to Commissioner/ SMT • As required to Commissioner/ SMT
Head of Corporate Services (HOCS)	• Operational owner of the risk registers • Quarterly review and update of Strategic Risk Register • Monthly review and update of the Operational Risk Register • Annual assessment and review of risk to the SMT	• Co-ordinate content and update risk registers • Drafting of annual risk report	• Quarterly to SMT • 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 SIC	• Monitor the risk policy • Advise the SIC and 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 SIC and AAB • Provide assurance to SIC	• 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 v06 CURRENT ISSUE
VC FileId	119981
Type	Policy
Approver	SMT
Responsible Manager	HOCS
Date of next planned review	April 2020
Approval & Publication	
Approval Date (major version)	09/05/19
For publication *(Y/N)*	Y
Date published	20/06/2019
Name of document in website file library	RiskManagementPolicy
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*)
20/06/19	BOW	6.00	6.01	New document created upon approval of draft
20/06/19	BOW	6.01	6.02	DCS updated, published on website

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

t 01334 464610
f 01334 464611
enquiries@itspublicknowledge.info

www.itspublicknowledge.info