Ethical Standards Commissioner

Commissioner for Ethical Standards in Public Life in Scotland
Thistle House
91 Haymarket Terrace
Edinburgh
EH12 5HE

Risk Management Policy

Date policy adopted: 24/10/2012
Date of last review: 14/12/2021

1. Purpose and Scope

The Ethical Standards Commissioner (the Commissioner) and their office (ESC) has a wide range of strategic and business objectives as well as statutory functions.

This policy outlines how ESC will identify and manage the key risks to achieving these objectives and fulfilling its statutory functions.

Risks arise from possible threats to ESC's ability to achieve its objectives, and failure to take advantage of opportunities.

Risk management is a structured approach to identifying, assessing, monitoring and, where possible and appropriate, controlling and/or mitigating risks that emerge. Its purpose is to support better decision making through understanding the risks inherent in ESC's activities and their likely impact on the office's ability to fulfil its statutory functions.

This policy forms part of the contract of employment. Employees should bear in mind that refusal to co-operate in the application of any of our policies or procedures may be treated as misconduct and dealt with under the disciplinary procedures.

This policy applies to all employees regardless of working pattern or nature of employment contract. It will not apply to others carrying out work on behalf of ESC (agency staff, contractors etc) who will be governed by the contract under which they have been employed or contracted.

2. Policy Statement

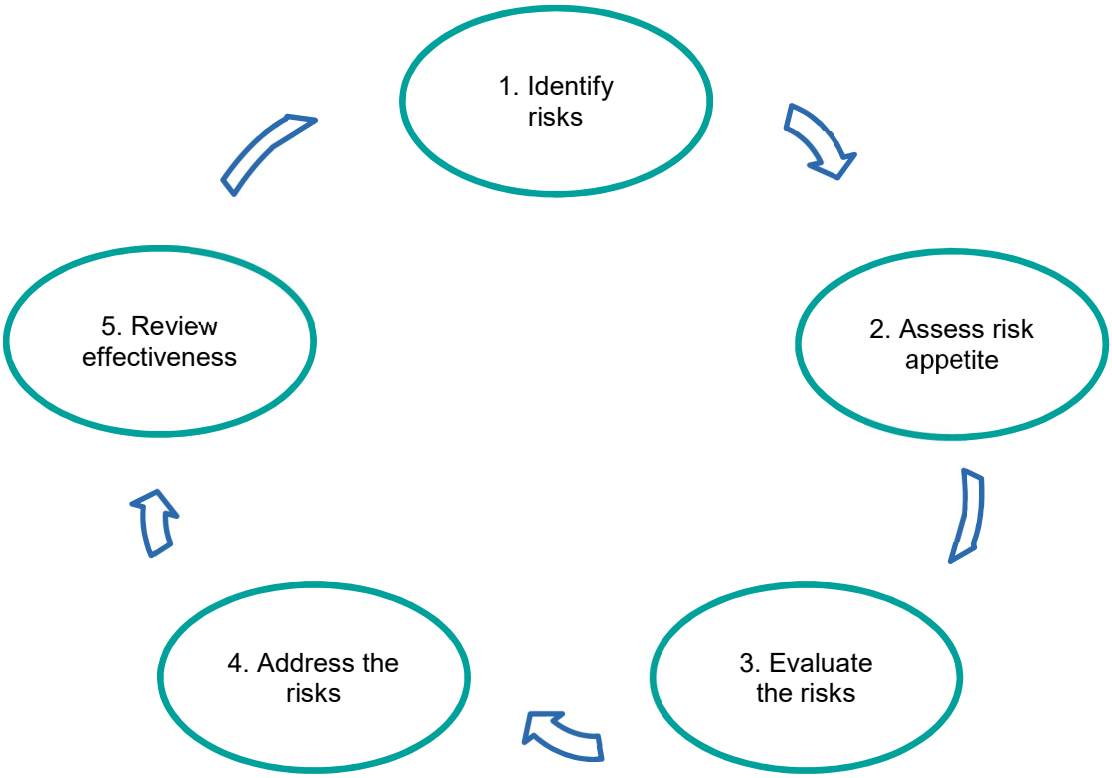
Policy

ESC will take a pragmatic and honest approach to risk management. In this context, honesty means acknowledging risks to the organisation that may be unpalatable to discuss and/or to put into the public domain. The office 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 Commissioner, Accountable Officer, Advisory Audit Board (AAB), the Auditor General for Scotland (AGS) 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

- ESC 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 take account of, manage, treat or tolerate risk and the impact of risk, in a manner that is proportionate and affordable.
- ESC will maintain, review and update the risk register regularly.
- ESC's risk management policy and procedures will operate without prejudice to the statutory functions of the Commissioner.

3. Implementation, monitoring and review of the policy

Overall responsibility for policy implementation, monitoring and review lies with ESC. Everyone covered by the scope of the policy is obliged to adhere to, and facilitate implementation of the policy. Appropriate action will be taken to inform all new and existing employees and others covered by the scope of the existence of the policy and their role in adhering to it. The policy will be reviewed at such times as legislation or a change to ESC policy position requires it. The policy will be made available to the general public

4. 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 ESC's strategic objectives and
- risks arising from biennial 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 Head of Corporate Services. The Head of Corporate Services will consult all staff to identify key risks to the business.

Strategic Risk Categories

ESC groups risks into five categories:

- Reputation and credibility – risk arising from how ESC is perceived by its stakeholders.
- Operational delivery – risk arising from or threatening the efficiency and effectiveness with which ESC delivers the office's key functions. Key functions include investigating complaints about lobbying, MSPs, board members 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 ESC manages resources, including finance, human and physical resources.
- Governance– risk arising from the robustness and effectiveness of the systems by which ESC 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).

5. Evaluating the risks

Having identified the key risks, ESC will assess the likelihood of their occurrence and the potential impact on the office's objectives.

The likelihood of a risk occurring will be assessed as follows:

Likelihood	Rare	Unlikely	Possible	Likely	Almost Certain
Score	1	2	3	4	5

The impact if the risk occurs will be assessed as insignificant, minor, moderate, major or catastrophe.

Impact	Definition	Score
Insignificant	• Little disruption to operations • Some financial loss • Little effect on delivering objectives/statutory functions • Possible damage to reputation • No or insignificant environmental damage • No or insignificant impact on information governance (cyber-security, data protection, records management) • No or insignificant equality issues • No or insignificant H&S issues • No or insignificant regulatory consequences	1
Minor	• Some disruption to operations • A greater degree of financial loss • Some effect on delivering objectives/statutory functions • Probable but not significant damage to reputation • Minor environmental damage • Minor impact on information governance (cyber-security, data protection, records management) • Minor equality issues • Minor H&S issues • Minor regulatory consequences	2
Moderate	• Disruption to operations for limited time • More significant financial loss • Partial failure to deliver objectives/statutory functions • Damage to reputation • Moderate damage to local environment • Moderate impact on information governance (cyber-security, data protection, records management) • Moderate equality issues • Moderate H&S issues, short-term illness or injury, serious threat to injury • Moderate regulatory consequences	3
Major	• Loss of operations for more than 48hrs but less than 7 days • Severe financial loss that puts objectives at risk • Significant impact on delivering objectives/statutory functions • Damage to reputation and extended media coverage • Major damage to local environment • Major impact on information governance (cyber-security, data protection, records management) • Major equality issues • Major H&S issues, extensive injuries, possible loss of life • Major regulatory consequences	4
Extreme/ catastrophic	• Loss of operations for more than 7 days • Major financial loss that threatens ESC's ability to continue • Failure to deliver objectives/statutory functions • Loss of trust or reputation and extended local media coverage • Extreme damage to local environment • Catastrophic impact on information governance (cyber-security, data protection, records management) • Extreme equality issues • Extreme H&S issues, loss of life • Extreme regulatory consequences	5

The combination of these elements will lead to an overall risk assessment of:

Score	1 - 3	4 - 6	7 - 9	10 - 15	16 - 25
Risk assessment	Very low	Low	Medium	High	Very high

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

6. Addressing the risk

Having evaluated the risks, the Commissioner and the Senior Management Team (SMT) 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 Commissioner and the Accountable Officer.

ESC, via the SMT will delegate ownership of specific risks to the appropriate staff members. Ownership of specific risks will be recorded on the Risk Register.

7. 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 Head of Corporate Services
- The Senior Management Team
- External Audit
- Internal Audit
- The Audit Advisory Board (AAB)

Sources of assurance include:

- Risk Register
- Management reporting
- Audit reports, including internal and external auditor's 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 ESC's Annual Business Plan reviews as well as twice yearly as a minimum by the SMT. Unanticipated risks arising will require ad hoc updates also. 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 ESC's external auditor, internal 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.

Ethical Standards Commissioner

Equality Impact Assessment

Does this policy comply with the general Public Sector Equality Duty (s149 Equality Act 2010)?

This policy applies to all employees. The impact of its implementation was considered when drafting. We consulted with all employees prior to publication to identify and address any issues. We have concluded that the implementation of this policy is unlikely to have any direct equality implications.

Data Protection Impact Assessment

Have we considered any effect the policy may have on the collecting, processing and storing of personal data?

The records generated by this policy are unlikely to contain personal data. Suitable retention and destruction policies are in place to manage this material.

Information Security Impact Assessment

Have we considered the impact any policy may have on our cyber-resilience?

The implementation of this policy should have no impact on our cyber-resilience.

Records Management Impact

Have we considered the impact any policy may have on our ability to manage our records?

The implementation of this policy should have no impact on our ability to manage our records.

Version	Description	Date	Author
1.0	First draft	12/11/2021	Head of Corporate Services
1.1	Second draft	15/12/2021	Head of Corporate Services
1.2	Final (following staff consultation)	07/02/2022	Head of Corporate Services