Corporate Policy and Strategy Committee

10.00am, Tuesday 7 August 2018

Enterprise Risk Management Policy

Item number	7.7
Report number	
Executive/routine	
Wards	
Council Commitments	

Executive Summary

Risk management helps all areas of the Council make better decisions and successfully achieve the Council's objectives. Risk management is fundamentally about better business management and it should be considered in this context rather than as a separate standalone activity.

The Enterprise Risk Management Policy ('the policy') is the Council's over-arching risk management document, and describes the Council's risk management framework which aims to protect the Council's people, assets, finances, reputation, and service delivery from the impacts of unplanned events, while also identifying opportunities to make improvements across all areas.

The policy supersedes the existing policy dated December 2016.

•EDINBVRGH•
THE CITY OF EDINBURGH COUNCIL

Report

Enterprise Risk Management Policy

1. Recommendations

1.1 The Committee is requested to approve the Enterprise Risk Management Policy set out in Appendix 1 to this report.

2. Background

2.1 Risk management is fundamentally about better business management and helping an organisation best manage its resources to support the achievement of its objectives. Having an effective risk management framework in place is part of good corporate governance.

2.2 Enterprise Risk Management describes risk management as it applies across the whole spectrum of an organisation's activities. It aims to ensure that the principles of risk management are applied appropriately at all levels of activity through a robust risk management framework.

2.3 The Council's risk management framework aims to protect the Council's people, assets, finances, reputation, and service delivery from the impacts of unplanned events, while identifying opportunities to make improvements across all areas.

2.4 The risk management framework consists of the policy, procedure, software, structures, meetings, training, education and communication.

2.5 There is no legislation relating to enterprise risk management and it is for the Council to design and put in place its own risk management framework. Good practice has been incorporated from a number of sources, including ISO31000 Risk Management – Guidelines, the Institute of Risk Management, Management of Risk®, NASA's Risk Management Handbook, and other local authorities.

2.6 The Corporate Risk Team works with service areas and Directorates to help them identify and assess threats and opportunities, then plan and implement appropriate controls and actions.

2.7 Risks are escalated through the risk management structures as appropriate, and the Council's top risks are reported regularly to the Governance, Risk and Best Value Committee.

3. Main report

3.1 The current Enterprise Risk Management Policy is dated December 2016. The new policy set out in Appendix 1 and recommended for approval seeks to provide greater clarity and definition, as well as incorporating good practice from across the risk management community.

3.2 This policy sets out how the Council will undertake risk management at all levels, and is the over-arching policy for all risk management activities across the Council. Arrangements to manage risks described in other policies should seek to align with this policy where possible.

3.3 This policy is applicable to all Council staff in all areas and at all levels. This Policy is applicable to all Council staff. The policy set out that when working collaboratively in partnership or under contract with third parties, appropriate risk management arrangements must be agreed and understood.

3.4 The policy describes key roles and responsibilities in relation to risk management.

3.5 The policy will be implemented to accord with the Council's agreed risk appetite which sets out the amount of risk that the Council is prepared to accept.

4. Measures of success

4.1 Efficient achievement of the Council's requirements, aims, objectives and commitments.

4.2 Reducing the negative impact of unplanned events which could damage the Council's people, assets, finances, reputation, or service delivery.

5. Financial impact

5.1 There are no direct financial implications associated with the policy.

5.2 There may be financial implications associated with the cost of implementing controls to mitigate risks and/or failing to mitigate risks.

6. Risk, policy, compliance and governance impact

6.1 This policy sets the framework risk management across the Council.

6.2 This policy aims to ensure that effective risk management is embedded throughout the Council. Risks of not implementing this policy include:

6.2.1 Inability to achieve Council outcomes and objectives;

6.2.2 Ineffective and inefficient service delivery;

6.2.3 Financial inefficiency and loss; and

6.2.4 Reputational damage to the Council.

7. Equalities impact

7.1 An effective risk management framework will help ensure compliance with all relevant equalities considerations.

8. Sustainability impact

8.1 An effective risk management framework will help ensure compliance with all relevant sustainability considerations.

8.2 Opportunities to improve the Council's position on sustainability issues may be identified through the risk management framework.

9. Consultation and engagement

9.1 The policy has been agreed by the Council's Corporate Leadership Team

10. Background reading/external references

10.1 ISO31000 Risk Management - Guidelines

10.2 Institute of Risk Management

10.3 Management of Risk

Stephen S. Moir

Executive Director of Resources

Contact: Duncan Harwood, Chief Risk Officer

E-mail: duncan.harwood@edinburgh.gov.uk | Tel: 0131 469 3193

11. Appendices

Appendix 1 – Enterprise Risk Management Policy

Enterprise Risk Management Policy

Implementation date: 7 August 2018

Control schedule

Approved by	Corporate Policy and Strategy Committee
Approval date	7 August 2018
Senior Responsible Officer	Duncan Harwood
Author	Duncan Harwood
Scheduled for review	August 2019

Version control

Version	Date	Author	Comment
1.0	August 2018	Duncan Harwood	This document supersedes the Enterprise Risk Management Policy v0.3 dated December 2016

Committee decisions affecting this policy

Date	Committee	Link to report	Link to minute
7 Aug 2018	Corporate Policy and Strategy Committee		

·EDINBVRGH·
THE CITY OF EDINBURGH COUNCIL

Enterprise Risk Management Policy

Policy statement

General

1.1 The Council delivers a range of services, under a variety of legislation, for the benefit of the people of Edinburgh. The operating environment is complex and changeable, and the Council’s performance is regularly and closely scrutinised. Risk management aims to help all areas of the Council make better decisions, and in doing so effectively support the achievement of objectives by the Council.

1.2 Risk management is fundamentally about better business management, and it should be seen in this context rather than as a separate standalone activity.

1.3 The Council’s Risk Management Framework seeks to protect the Council’s people, assets, finances, service delivery and reputation from the impacts of unplanned events, while identifying opportunities for improvement across all areas. This Risk Management Framework includes this Policy and the procedures, software, structures, meetings, templates, training, education and communications relating to risk management within the Council.

Scope

2.1 ‘Enterprise Risk Management’ describes the management of risk across the whole spectrum of the Council’s activities. As such, this document is the over-arching policy for risk management across the Council. Arrangements to manage risks described in other policies should seek to align with this Policy to where possible.

2.2 This Policy does not replace any statutory risk management or reporting requirements.

2.3 This Policy is applicable to all Council staff. When working collaboratively in partnership or under contract with third parties, appropriate risk management arrangements must be agreed and understood.

2.4 The Council’s arms-length external organisations (ALEOs) are responsible for the management of risk within their organisations, and are expected to have their own appropriate risk management arrangements in place.

Definitions

In this document the following terms and definitions are used:

3.1 **Action** - A planned measure which is intended to reduce the **Likelihood** and/or **Impact** of a **Risk**. Once an action has been appropriately implemented it becomes a **Control**. An action aims to reduce the **Current Risk** towards the **Target Risk**.

3.2 **Action Owner** - A single role or individual responsible for the implementation of an **Action**. This may be a different person to the **Risk Owner**.

3.3 **Assurance** - The process by which the design and effectiveness of **Controls** are confirmed to be functioning as intended. Assurance can be provided by all **Lines of Defence**.

3.4 **Control** - A measure that is designed to reduce **Risk**. A control could include any policy, procedure, practice, process, technology, technique, method, or device that reduces **Risk**. A control will be either *preventative* or *detective*. Controls may not always be operating as they were intended. The design and operating effectiveness of **Controls** is assessed through **Assurance**.

3.5 **Current Risk** - The level of **Risk** at the current time, taking into account the **Controls** in place and their effectiveness. If the **Controls** are effective then the **Current Risk** will be less than the **Original Risk**.

3.6 **Enterprise Risk Management (ERM)** - ERM describes risk management as it applies across the whole spectrum of the Council’s activities. It aims to ensure that the principles of **Risk Management** are applied appropriately at all levels of activity.

3.7 **Impact** - The result of a particular event occurring. Impacts could affect one or more categories (service delivery, infrastructure, compliance and/or financial).

3.8 **Inherent Risk** – See **Original Risk**.

3.9 **Issue** - A relevant event that has happened or is happening now, was not planned, and requires management action. A **Risk** may turn into an **Issue**, or an **Issue** may identify a **Risk**.

3.10 **Lines of Defence** - The **three Lines of Defence** model broadly defines first line as ‘within services’ (the “doers”), second line as ‘within corporate support functions’ (the “helpers”), and third line as ‘Internal Audit, External Audit, and external assurance providers’ (the “checkers”).

3.11 **Likelihood** - The chance of something happening. It can be measured qualitatively (“rarely”, “often” etc) or quantitatively (“50% probability”, “once every five years” etc).

3.12 **Objective** - A specific goal to be achieved. At the highest level these are defined in our Aims, Outcomes, Council Commitments and statutory requirements.

Directorates, Services, teams and individuals will have their own objectives, and others may arise from external codes, targets, frameworks and recommendations.

3.13 **Opportunity -** An uncertain event that would have a favourable impact upon objectives if it occurred.

3.14 **Original Risk** - The exposure arising from an identified **Risk** before any measures have been taken to manage it. Also called **Inherent** Risk.

3.15 **Risk -** The effect of uncertainty upon **Objectives**. Risk includes potential upside (**Opportunity**) as well as downside (**Threat**). A **Risk** is scored as its **Likelihood** multiplied by **Impact**. The description of a **Risk** should include potential cause(s), event, and effect(s).

3.16 **Risk Appetite** - The amount of **Risk** the Council, or a part of it, is willing to accept.

3.17 **Risk Management -** The systematic application of principles, tools and processes to the tasks of identifying and assessing risks, planning and implementing **Controls**, and monitoring progress.

3.18 **Risk Management Framework -** The sum of all components which contribute to risk management. It includes the policy, procedure, software, structures, meetings, templates, training, education and communications.

3.19 **Risk Owner -** A single role or individual responsible for the management and control of all aspects of a **Risk**.

3.20 **Target Risk** - The **Risk** remaining after all **Controls** and **Actions** have been successfully implemented and are functioning as intended. The level of **Risk** that a **Risk Owner** intends to achieve, in line with the **Risk Appetite**, and which is endorsed by the relevant management structure.

3.21 **Threat** - An uncertain event that could have a negative impact on objectives.

Policy content

4.1 At all levels of the Council, everyone should consider risk in everything they do, as part of good business management.

4.2 We should recognise that risk is not all ‘bad’, and that if we seek to avoid risk completely then we reduce our chances of achieving our objectives.

4.3 The Council sets an overarching risk appetite and seeks to ensure that risks at all levels and within all service areas are managed within this overall risk appetite. The overall risk appetite is reviewed annually.

4.4 Risk appetite can and will vary between individuals, groups, and levels of seniority based upon conscious and unconscious biases, levels of understanding, past experiences and other factors. Risk appetite may change over time and can vary between similar events.

4.5 We all identify and assess threats and opportunities, then plan and implement appropriate controls and actions, so that potential negative consequences resulting from unplanned events are at a level which is appropriate for the Council.

4.6 We identify, own, and manage risks at the most appropriate level and escalate risks through the appropriate risk management structures to a level where they can be managed appropriately.

4.7 Risk Committees are held at Corporate Leadership Team and Directorate levels, and Risk Management Groups within each Directorate. These aim to ensure the sharing of relevant information, challenge and scrutiny of risks, controls and actions, early warning of emerging threats, and escalation of risks to appropriate risk owners.

4.8 All decisions are made with full consideration of risks, utilising appropriate qualitative and quantitative tools and techniques where appropriate, and following appropriate engagement and input from all relevant stakeholders.

4.9 Requests for additional resources to manage risks are considered appropriately.

4.10 Proactive reporting and early identification of risks is encouraged at all levels.

4.11 Robust recording and reporting mechanisms are used that allow for information to be reported efficiently.

4.12 Roles and responsibilities for risk management are established and communicated.

4.13 The Council promotes a culture where people are able to discuss and challenge risks and controls at all levels in a constructive manner.

4.14 The Corporate Risk Team seeks to continually improve our risk management framework based upon good practice, feedback, and developments within the risk management community.

4.15 When working with partners risk is managed and escalated appropriately.

4.16 When working with suppliers, contractors and other third parties risk is owned and managed appropriately.

4.17 Assurance about the design and effective of controls is sought through the three lines of defence, recognising that responsibility for managing risks, controls and actions sits usually with the first line.

4.18 The Council uses risk-based internal audit planning to prioritise and concentrate resources and ensure appropriate focus upon areas of greatest risk.

4.19 The Council’s top risks, as agreed by the Corporate Leadership Team, are reported to the Governance, Risk and Best Value Committee, who provide challenge and scrutiny on a regular basis.

4.20 We manage risk within projects at the project level and escalate as appropriate. Where appropriate we carry out cost and schedule risk analyses to provide meaningful management information and inform decision-making and resource allocation.

4.21 We describe the risk management structures, escalation processes, scoring, ranking, training, communications, software user guides and all other documentation within a Risk Management Procedure document.

Implementation

5.1 Implementation of this Policy will be effective from 7 August 2018. This Policy supersedes any previously approved Enterprise Risk Management Policy document.

Roles and responsibilities

6.1 **Council (exercised through the Governance, Risk and Best Value Committee)**

6.1.1 Consider the Council Risk Report provided on a quarterly basis.

6.1.2 Scrutinise and challenge specific risks, requesting updates or information from risk owners where appropriate.

6.1.3 Satisfy themselves that the risk management framework is operating effectively.

6.1.4 Consider requests for additional resources for improving controls.

6.2 **Council (exercised through the Corporate Policy and Strategy Committee)**

6.2.1 Set the Council’s Risk Appetite.

6.3 **Chief Executive**

6.3.1 Responsible for ensuring that all risks to the Council are managed appropriately.

6.3.2 Sets and promotes an appropriate culture for all Council staff, where risk is considered in all decision-making, and where risk management is an integral part of business management.

6.4 Executive Directors and Chief Officer of the Health and Social Care Partnership

6.4.1 Responsible for the identification, recording, management and monitoring of all risks within their areas of responsibility, including establishing risk owners for all appropriate risks within their areas of responsibility.

6.4.2 Ensure that the Council’s Risk Appetite is considered when managing and monitoring risks within areas of responsibility.

6.4.3 Responsible for escalating risks to the Corporate Leadership Team for consideration where appropriate.

6.4.4 Responsible for cascading risk management processes within areas of responsibility.

6.4.5 Be prepared to discuss (and justify where appropriate) risks, controls and actions at Risk Committees and the Governance, Risk and Best Value Committee as required.

6.4.6 Accountable for all information in the risk management system within areas of responsibility.

6.4.7 As the first line of defence, be able to provide assurance that the risk management framework is operating effectively within their respective areas of responsibility.

6.5 Heads of Service (including those with statutory responsibilities)

6.5.1 Responsible for the identification, recording, management and monitoring of all risks within their areas of responsibility, including establishing risk owners for all appropriate risks within their areas of responsibility.

6.5.2 Ensure that the Council’s Risk Appetite is considered when managing and monitoring risks within areas of responsibility.

6.5.3 Responsible for escalating risks to Directorate level for consideration where appropriate.

6.5.4 Responsible for cascading risk management processes within areas of responsibility.

6.5.5 Be prepared to discuss (and justify where appropriate) risks, controls and actions at Risk Committees and Governance, Risk and Best Value Committee as required.

6.5.6 Accountable for all information in the risk management system within areas of responsibility.

6.5.7 As part of the first line of defence, be able to provide assurance that the risk management framework is operating effectively within their respective areas of responsibility.

6.5.8 Ensure that all staff within their areas of responsibility understand risk management as it applies to their position and responsibilities.

6.6 Section 95 Chief Financial Officer / Head of Finance

6.6.1 Duties as defined in the Local Government (Scotland) Act 1973.

6.6.2 Responsible for the proper administration of the Council’s financial affairs.

6.6.3 Determine the system of accounting and control, the form of the accounts and supporting records, and ensure the accounts and supporting records are kept up to date.

6.6.4 Establish a programme of review for all relevant documents, including the Council’s financial rules and regulations.

6.6.5 Determine the proper action to be taken in the event of a breach or non-compliance of the Council’s rules, regulations, procedures or policies issued under their authority.

6.7 Chief Social Work Officer / Head of Safer and Stronger Communities

6.7.1 Role as defined under the Social Work (Scotland) Act 1968 and subsequent and related legislation and guidance.

6.7.2 Reports to the Chief Executive, Elected Members and the Integration Joint board as appropriate, providing information on issues which may identify risk to safety of vulnerable people or impact on the social work service and also on the findings of relevant service quality and performance reports.

6.8 Monitoring Officer / Head of Legal and Risk

6.8.1 Main liaison with Elected Members on corporate risk matters.

6.8.2 As a member of the Corporate Leadership Team, champion risk management within the Corporate Leadership Team.

6.8.3 Duties of the Monitoring Officer as defined in Section 5 of the Local Government and Housing Act 1989.

6.9 Chief Risk Officer and Corporate Risk Team

6.9.1 Subject-matter expert for risk management within the Council.

6.9.2 Provide effective challenge to risk owners across all levels of the Council to ensure risks, controls and actions are being managed appropriately.

6.9.3 Engage with Elected Members and Officers as appropriate to ensure that risk management remains visible, accessible, proportionate and relevant to all those involved in decision-making.

6.9.4 Engage with stakeholders to identify and implement improvements to corporate processes.

6.9.5 Accountable for the delivery, effectiveness, and continuous improvement of the Council's Risk Management Framework.

6.9.6 Responsible for reporting risk to the Governance, Risk and Best Value Committee.

6.9.7 Responsible for identifying emerging risks to the Head of Legal and Risk and others as appropriate.

6.9.8 Accountable for the provision of training, information and education about risk management, tools and techniques to Elected Members and to senior management within the Council.

6.9.9 Promote awareness of risk management across all areas of the Council and third parties as appropriate.

6.9.10 Organise and facilitate Corporate Leadership Team Risk Committees, providing appropriate scrutiny and challenge and ensuring timely sharing of information.

6.9.11 Organise and facilitate Directorate Risk Committees, providing appropriate scrutiny and challenge and ensuring timely sharing of information.

6.9.12 Prepare the Council's Risk Appetite Statement for the Corporate Policy and Strategy Committee.

6.9.13 Assist the first line of defence with the qualitative and/or quantitative assessment of risks.

6.10 Quality Assurance and Safety Manager, NHS Lothian

6.10.1 Working alongside the Council's Chief Risk Officer and Corporate Risk Team, share responsibility for risk management arrangements within the Health and Social Care Partnership, including appropriate escalation mechanisms and reporting processes.

6.11 Risk Coordinators

6.11.1 Be the visible champion of risk management within each Directorate.

6.11.2 Chair Risk Management Groups within each Directorate.

6.11.3 Organise administrative support for Risk Management Groups (logistics, minute-taking and producing a Note of Meeting within one week).

6.12 All staff

6.12.1 Understand risk management as it applies to their role. At the most basic level this could mean an understanding of:

- What health and safety considerations are relevant to my job?
- What training and knowledge do I need to be able to do my job?
- What do I do if I see something going wrong, or if I think something could go wrong?
- How could we do things better?

6.12.2 Consider how unplanned events could affect the achievement of objectives, and those of others, and escalate this information to line management where appropriate.

6.12.3 Carry out actions as directed in support of risk management.

6.12.4 Ensure that controls are operating as intended.

6.12.5 Ensure that the Council's Risk Appetite is considered when managing and monitoring risks within areas of responsibility.

6.12.6 Feedback any suggestions or improvements to the risk management framework.

Related documents

7.1 All Council policies are designed to reduce risk in some form, and as such they are all related to this document.

7.2 In addition to the policies accessible via the Council's online Policy Register, key related documents are listed below. This is not a complete list and further guidance may be sought from a member of the Corporate Risk Team.

7.2.1 Council Business Plan 2017-22

7.2.2 Procedural Standing Orders for Council and Committee Meetings

7.2.3 Committee Terms of Reference and Delegated Functions

7.2.4 Contract Standing Orders

7.2.5 Scheme of Delegation to Officers

7.2.6 Employee Code of Conduct

7.2.7 Financial Regulations of the City of Edinburgh Council

7.2.8 Corporate Debt Policy

7.2.9 The Role of Chief Social Work Officer – Guidance Issued by Scottish Ministers pursuant to Section 5(1) of the Social Work (Scotland) Act 1968

7.2.10 Local Government and Housing Act 1989

7.2.11 Local Government etc. (Scotland) Act 1994

7.2.12 Local Government (Scotland) Act 1973

7.2.13 Social Work (Scotland) Act 1968

Equalities impact

8.1 An effective risk management framework seeks to ensure compliance with all relevant equalities considerations.

Sustainability impact

9.1 An effective risk management framework seeks to ensure compliance with all relevant sustainability considerations.

9.2 Opportunities to improve the Council's position on sustainability issues may be identified through the risk management framework.

Risk assessment

10.1 This policy aims to ensure that effective risk management is embedded throughout the Council. The risks of not implementing this policy include:

10.1.1 Inability to achieve Council outcomes and objectives;

10.1.2 Ineffective and inefficient service delivery;

10.1.3 Financial inefficiency and loss; and

10.1.4 Reputational damage to the Council.

10.2 Given the uncertainties involved in attempting to quantify future events, even a perfectly functioning risk management framework cannot guarantee to foresee every potential negative outcome to the Council. There will always be a chance that very-low-probability/very-high-impact events occur.

10.3 Given the scale and nature of the Council’s operations it is likely that the Council’s reputation will frequently suffer a degree of damage. However, this damage will not usually have significant lasting effects. The Council’s Risk Management Framework will therefore prioritise compliance, service delivery and financial impacts above reputational damage.

Review

11.1 This policy will be reviewed annually.