Policy and Sustainability Committee

10:00am, Tuesday, 24 October 2023

Council Risk Appetite

Executive/routine
Wards

1. Recommendations

1.1 Committee is asked to set the Council's risk appetite and to approve the methodology to manage Risk Appetite to support the management of risk within the City of Edinburgh Council as part of the Council's Risk Management Framework.

1.2 To refer this report to the Governance, Risk and Best Value Committee.

Deborah Smart

Executive Director – Corporate Services

Contact: Chris Lawson, Head of Health, Safety and Risk

E-mail: chris.lawson@edinburgh.gov.uk | Tel: 0131 529 7476

Report

Council Risk Appetite

2. Executive Summary

2.1 This report defines the Risk Appetite of the City of Edinburgh Council. The purpose of this paper is to set out the Council's risk appetite statement for approval by the Policy and Sustainability Committee. This document should be read together with the Council's Risk Management Policy which is also being submitted for approval to the Policy and Sustainability Committee.

3. Background

3.1 The concept of having and setting a Risk appetite is not new to the City of Edinburgh Council as it has done so for a number of years now. Most recently in November 2021 the Council revised its risk appetite in response to the changing context brought about as a result of the COVID-19 pandemic.

3.2 Now that the operating context has changed, since the threat from the pandemic has largely subsided, with the broad-ranging controls and restrictions put in place by the Government with the aim of protecting people having been removed.

3.3 The risk appetite within the Council is framed around the 13 Enterprise risks used to group and escalate risks from Services through to Directorates and the Corporate Leadership Team as appropriate.

4. Main report

4.1 Risk appetite is defined as the amount and type of planned risk that an organisation, or a part of it, is willing to take to deliver their strategic priorities and services. Risk appetite is underpinned by the policy approach of the organisation.

4.1.1 The Scottish Government notes in the risk management section of its Scottish Public Finance Manual that 'the concept of a "risk appetite" is key to achieving effective risk management and it is essential to consider it before moving on to consideration of how risks can be addressed. The concept may be looked at in different ways depending on whether the risk being considered is a threat or an opportunity:

- when considering threats the concept of risk appetite embraces the level of exposure which is considered tolerable and justifiable should it be realised. In this sense it is about comparing the cost (financial or otherwise) of constraining the risk with the cost of the exposure should the exposure become a reality and finding an acceptable balance;

- when considering opportunities the concept embraces consideration of how much one is prepared to actively put at risk in order to obtain the benefits of the opportunity. In this sense it is about comparing the value (financial or otherwise) of potential benefits with the losses which might be incurred (some losses may be incurred with or without realising the benefits).

4.2 The Risk management policy includes a requirement for all parts of the Council to consider risk appetite in their strategic and operational decision making.

4.3 Once approved, risk appetite statements should be communicated throughout the organisation to ensure that risk appetite is consistently and effectively considered in decision making and ongoing management of operational risks.

4.4 The Council is responsible for designing and maintaining an appropriate risk management policy; setting its risk appetite; and implementing and maintaining an operational risk management framework.

4.5 Both the Council's risk appetite statement and risk management policy are reviewed by the Corporate Leadership Team (CLT) and approved by the Policy and Sustainability Committee.

4.6 The Council also has an established governance framework that is designed to support achievement of risk appetite through application of, and compliance with, schemes of delegation; governance structures (for example, Council executive and operational management committees); completion of annual governance statements by directorates and divisions; an extensive range of policies and operational frameworks (for example, health and safety; human resources; digital services; and fraud prevention) and supporting processes that are designed to manage and mitigate risk at levels that are appropriate and acceptable for the Council.

4.7 The focus of this report is on Risk Appetite and risk tolerance which are considered to be inextricably linked to performance over time. Risk appetite is concerned with the pursuit of risk whereas risk tolerance is about what level of risk the organisation is prepared to accept.

4.8 The Council, like all organisations, must be prepared to take some risk, otherwise the finite resources available will be utilised over-manging risk and in-turn reduce the capacity of the organisation to perform to the best of its ability.

4.9 Appendix 1 sets out the risk appetite scale for the Council across the 13 Enterprise Risks used to group and escalate risks within the Council. Given the complexity and diversity of the Council's operations and activities, the risk appetite for some categories has been set by way of range rather than a specific risk appetite level

across the entire category.   Committee is asked to approve Appendix 1 as the Council's Risk Appetite.

4.10   Risk Appetite should be seen primarily as a decision-making tool owned by the Council Leadership Team. The organisation should only change risk appetite if required to in terms of a changing risk context and environment. Risk Appetite must be reviewed and agreed annually or if the operational risk context requires a change (for example the response to Covid-19).

4.11   By way of an example of applying Risk Appetite   Having less available budget could impact compliance decision making in relation to eg property related requirements. A decision may be taken to delay or not carry out works. As this risk would fall into the regulatory compliance and health and safety category where the maximum risk appetite is "low" then this would mean that the decision not to carry out the work would not be possible as it would be outwith agreed risk appetite. Alternatively approval to sit outside risk appetite would need to be sought.

4.12   However it should be noted that it is the overall risk appetite which is of relevance, through risk aggregation. Again by way of example, a particular service may be able to justify sitting outside risk appetite for one or more risk categories where the Council's overall risk appetite remains within the relevant range, subject to approval as noted in the example above.

5.   Next Steps

5.1   The Corporate Risk Management team and colleagues responsible for ensuring the Council's Risk Framework is operating and applied effectively will promote the risk appetite through the Senior Leadership Team and those Officers with key responsibility for the Management of Risk within their respective Council Services.

5.2   The Council's Risk Management Team will also ensure that as part of the wider leadership development programme, that risk management is built into the way the Council manages all aspect of its business.

5.3   The Council's Risk Framework will continue to be promote, educate and encourage the use of Risk Appetite and Risk Tolerance in decision making and the management of objectives.

6.   Financial impact

6.1   There are no direct financial implications associated with the Policy, although there may be costs associated with implementing controls to mitigate risks and/or failing to mitigate risks.

7.   Equality and Poverty Impact

7.1   This report does not directly impact equality and poverty, however, in setting a low risk appetite for regulatory compliance further underpins the need to ensure regulatory requirements and duties placed on the Council are adhered to.

8.   Climate and Nature Emergency Implications

8.1   This paper does not directly impact the climate or nature emergency.

9.   Risk, policy, compliance, governance and community impact

9.1   This report should help reduce risk for the City of Edinburgh Council, as it seeks to set out the risk management framework for the Council, to support effective risk management and risk aware decision making.

10.   Background reading/external references

10.1   Risk Appetite & Tolerance, Executive Summary (2011)

10.2   Scottish Public Finance Manual, Scottish Government, (2023)

10.3   Current risk appetite approved November 2021

11.   Appendices

11.1   **Appendix 1 Council Risk Appetite Categories**

11.2   **Appendix 2 Risk appetite ready reckoner**

Council Risk Appetite Categories   **Appendix 1**

Risk ID	Risk category	Risk Impact	Operational Risk Appetite Range		Commentary
			From	To	
R1	Strategic Delivery	Inability to design and / or implement a strategic plan for the Council.	Low	Moderate	1.The Council has a low to moderate operational risk appetite in relation to strategic delivery risk, and aims to ensure effective delivery of the Council's strategy and commitments in line with agreed timeframes. 2. Strategic delivery is monitored through the ongoing performance reporting process and established Council governance processes. 3. Executive Directors and Service Directors are expected to establish appropriate monitoring and oversight controls to ensure that their strategic and service delivery objectives are achieved in line with the overarching Council strategy.
R2	Financial and Budget Management	Inability to perform financial planning; deliver an annual balanced budget; manage cash flows; and confirm ongoing adequacy of reserves	Low	Moderate	1. The Council has a low to moderate operational risk appetite in relation to financial risk, and may be prepared to accept some risk subject to: • setting and achieving an annual balanced revenue budget in line with legislative requirements • maintaining a General Fund unallocated reserves balance in line with legislative requirements. 2. The Council's target financial risk is set out in various documents including the Scheme of Delegation to Officers; Contract Standing Orders; Committee Terms of Reference and Delegated Functions; and the Financial Regulations, and is also supported by the controls embedded in established financial technology systems. 3. Executive Directors and Service Directors are expected to implement appropriate system based and manual controls to prevent financial errors and detect and resolve them when they occur.
R3	Programme and Project Delivery	Inability to deliver major projects and programmes effectively, on time and within budget	Low	High	1. The Council is prepared to initiate a range of low to high risk major change initiatives where these support strategic delivery; improved organisational capability and service delivery; or improvements to across the Council's operational property and technology estates and infrastructures. 2. The Corporate Leadership Team; Executive Directors; Service Directors; and Project Managers are expected to design; implement; and maintain appropriate programme and project management and governance controls to manage these risks.
R4	Health and Safety (including public safety)	Employees and / or citizens (including those in the Council's care)	Minimum possible	Low	1. Recognising that accidents can occur as a result of unknown and / or unplanned events, the Council has an appetite to fully comply with all relevant health and safety requirements to minimise any health and safety risks that could potentially result in loss of life or injury to citizens or employees.

Risk ID	Risk category	Risk Impact	Operational Risk Appetite Range		Commentary
			From	To	
		suffer unnecessary injury and / or harm			2. Executive Directors and Service Directors are expected to ensure that Health and Safety policies; frameworks; and guidance are consistently and effectively applied, with incidents identified, reported, and immediately addressed.
R5	Resilience	Inability to respond to a sudden high impact event or major incident	Low	Moderate	1. Recognising that it is not always possible to effectively mitigate the risks associated with unplanned events, the Council has a low to moderate operational risk appetite in relation to resilience. 2. The Council has an established resilience management framework that includes resilience and contingency plans for certain scenarios, and provides guidance to first line directorates and divisions in relation to identifying critical systems and services and establishing appropriate resilience plans. 3. Executive Directors and Service Directors are responsible for ensuring that this framework is consistently maintained and routinely tested and can be effectively applied in the event of a resilience situation.
R6	Supplier, Contractor, and Partnership Management	Inability to effectively manage the Council's most significant supplier and partnership relationships	Low	High	1. The Council has a low to high operational risk appetite range in relation to ongoing supplier, contractor and partnership management. It should be noted that this appetite will vary depending on the criticality of the service provided or supported by third parties. 2. The Council has an established procurement process that is aligned with Audit Scotland Best Value requirements and is supported by the Contract Standing Orders, and an established contract management framework. 3. Executive Directors and Service Directors are expected to ensure that the procurement and contract management frameworks are consistently and effectively applied, with issues identified, reported, and immediately addressed. This will typically involve ongoing focus on high risk contracts supporting delivery of critical services or projects.
R7	Technology and Information	Potential failure of cyber defences; network security; application security; and physical security and operational arrangements	Low	Moderate	1. The Council has a low to moderate operational risk appetite in relation to technology and information risk and aims to ensure that this is achieved working together with CGI, the Council's technology partner and through direct contract management by service areas with any 'shadow IT' suppliers. 2. This risk appetite applies to both the Council's technology networks; cloud based applications used to support delivery of services; and processes where manual documents are used and retained. 3. This risk appetite will vary depending on the nature; significance; and criticality of systems used, and the services that they support. 4. Technology risk is managed through ongoing use of inbuilt technology security controls such as user access; encryption; data loss prevention; firewalls; and ongoing vulnerability scanning and a range of technology security protocols and procedures.

Risk ID	Risk category	Risk Impact	Operational Risk Appetite Range		Commentary
			From	To	
					5. Executive Directors and Service Directors are responsible for ensuring ongoing compliance with technology security protocols and procedures, including the Council's protocol for externally hosted 'cloud' services. 6. The Council is also progressing towards full alignment with the Scottish Government's Public Sector Cyber Action Plan and the UK Government National Cyber Security Centre guidance.
R8	Governance and Decision Making	Inability of management and elected members to effectively manage and scrutinise performance, and take appropriate strategic and operational decisions	Minimum possible	Low	1. The Council has a minimum possible to low risk operational appetite in relation to governance and decision making. 2. The Council's target governance and decision making risk is detailed in its established Committee and corporate structures; schemes of delegation; levels of authority; and the member-officer protocol. 3. No officer or elected member may knowingly take or recommend decisions or actions which breach legislation.
R9	Service Delivery	Inability to deliver quality services that meet citizen needs effectively and in line with statutory requirements	Low	High	1. The Council has a low to high operational risk appetite range in relation to the risks associated with ongoing service delivery that will vary depending on the nature and criticality of individual services. 2. It is acknowledged that, despite best efforts, there may be occasional gaps in service delivery. 3. Recognising the potential impact on service users the Council will always strive to return to optimal service delivery as soon as possible, and ensure effective ongoing engagement with service users where issues occur. 4. Executive Directors and Service Directors are expected to implement appropriate controls to prevent service delivery gaps, and detect and resolve them when they occur.
R10	Workforce	Insufficient resources to support delivery of quality services that meet citizen needs effectively and in line with statutory requirements	Low	Moderate	1. The Council has a low to moderate operational risk appetite range in relation to the risks associated with workforce capacity and capability. 2. It is acknowledged that, despite best efforts, there may be occasional gaps in workforce capacity and capability. 3. Recognising the potential impact on service delivery, the Council will always strive to return to optimal service workforce capacity and capability as soon as possible, and ensure effective ongoing engagement with employees and trade unions when issues occur. 4. Executive Directors and Service Directors are expected to maintain appropriate workforce plans that are aligned with the Council's People Strategy and Strategic Workforce Plan, and ensure sufficient capacity and capability to support service delivery. It is acknowledged that there is also a key dependency on both employment market and agency worker availability.

Risk ID	Risk category	Risk Impact	Operational Risk Appetite Range		Commentary
			From	To	
R11	Regulatory and Legislative Compliance	Delivery of Council services and decisions are not aligned with applicable legal and regulatory requirements	Low	Low	1. The Council aims to comply with applicable regulatory and legislative requirements to the fullest extent possible. 2. No officer or elected member may knowingly take or recommend decisions or actions which breach legislation. 3. Executive Directors and Service Directors are expected to implement appropriate controls to ensure ongoing compliance, and identify; report; and resolve breaches when they occur.
R12	Reputational Risk	Adverse publicity as a result of decisions taken and / or inappropriate provision of sensitive strategic, commercial and / or operational information to external parties	Low	Moderate	1. The Council is prepared to tolerate a low to moderate level of occasional isolated reputational damage. 2. The Council recognises that, as a large organisation delivering a wide range of complex services to the public and directed by elected politicians, it is likely to suffer occasional reputational damage. 3. Executive Directors and Service Directors are expected to implement appropriate controls to prevent significant or systemic reputational damage, and identify and address issues when they occur.
R13	Fraud and Serious Organised Crime	Isolated or systemic instances of internal and / or external fraud and / or serious organised crime	Low	Moderate	1. The Council is prepared to tolerate a low to moderate level of occasional isolated fraud and serious organised crime. 2. The Council recognises that, as a large organisation delivering a wide range of complex services to the public and directed by elected politicians, it is likely to suffer occasional fraud, and potentially be subject to targeted serious organised crime. 3. Executive Directors and Service Directors are expected to implement appropriate controls to prevent significant or systemic damage from fraud and / or serious organised crime, and identify and address issues when they occur.

Risk appetite ready reckoner

Risk category	Risk Appetite
Regulatory and Legislative Compliance	Low
Health and Safety (including public safety)	Low
Governance and Decision Making	Low
Workforce	Moderate
Financial and Budget Management	Moderate
Strategic Delivery	Moderate
Technology and Information	Moderate
Fraud and Serious Organised Crime	Moderate
Resilience	Moderate
Reputational Risk	Moderate
Service Delivery	High
Programme and Project Delivery	High
Supplier, Contractor, and Partnership Management	High