Policy and Sustainability Committee

10.00am, Tuesday 6 October 2020

Council's Risk Appetite Statement

Item number	
Executive/routine	**Executive**
Wards	
Council Commitments	

1. Recommendations

It is recommended that the Committee:

1.1 notes that the Council's attitude to taking risk should be set at the top level and cascaded down, and that this 'risk appetite' may be different across different services and types of risks;

1.2 notes that risk appetite is already set and established in many areas through governance arrangements; frameworks; policies, existing controls and schemes of delegation;

1.3 approves the Council's risk appetite presented within this report;

1.4 refers the report to the Governance, Risk and Best Value (GRBV) Committee for consideration; and,

1.5 notes that training on the Risk Appetite Statement together with the Council's Enterprise Risk Management Policy and the refreshed operational risk management framework will be provided for elected members after the GRBV committee meeting on 3rd November 2020.

Stephen S. Moir

Executive Director of Resources

Contact: Lesley Newdall, Senior Audit and Risk Manager

Legal and Risk Division, Resources Directorate

E-mail: lesley.newdall@edinburgh.gov.uk | Tel: 0131 529 4377

Report

Council's Risk Appetite Statement

2. Executive Summary

2.1 The purpose of this paper is to set out the Council's risk appetite statement for approval by the Corporate Policy and Sustainability Committee:

2.2 This document should be read together with the Council's Enterprise Risk Management Policy (the Policy) which is also being submitted for approval to the Corporate Policy and Sustainability Committee on 6 October 2020.

2.3 The risk appetite statement included in this report supersedes the Council's existing risk appetite statement dated 7 August 2018.

3. Background

Definitions

3.1 Risk is defined as the positive or negative impact of an uncertain event or issue on achievement of organisational objectives and delivery of services.

3.2 Not all risk is undesirable, and if risk is avoided completely then organisations limit their chances of fully achieving their objectives.

3.3 Some risks can be identified, and actions implemented to ensure that their negative impacts are effectively controlled, and their positive impacts realised, whilst other unexpected risks associated with unplanned events (for example some risks associated with the Covid-19 pandemic) cannot easily be identified in advance and fully mitigated.

3.4 When unplanned events occur, organisations depend on their resilience and contingency plans to respond to the impacts of these events, and should establish appropriate processes to identify; assess; record; and manage the new risks that they present.

3.5 Risk appetite is defined as the amount and type of planned risk that an organisation is willing to take to meet their strategic objectives and deliver services. Risk appetite can and will vary across levels of seniority, and between individuals and groups, based on a number of factors including conscious and unconscious bias;

knowledge and understanding; and past experience. Risk appetite will change over time and can also vary between different types of risks and events.

3.6 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’, and highlights that:

3.6.1 when considering opportunities, risk appetite involves assessing how much risk the organisation is prepared to take to realise the benefits of the opportunity, essentially comparing the value (financial or otherwise) of potential benefits with the losses that might be incurred.

3.6.2 when considering threats, risk appetite involves assessing the level of exposure that can be justified and tolerated by comparing the cost (financial or otherwise) of mitigating the risk with the cost of the exposure if the risk crystallises into an issue, and finding an acceptable balance.

3.7 Target risk is defined as the maximum level of risk that an organisation is prepared to accept in pursuit of a specific objective, and is used to determine whether additional controls or mitigating actions are required to reduce the potential impact of a specific risk.

3.8 A risk management policy establishes a structured organisational approach to risk management with the objective of ensuring that risk based decisions are explicit; consistent; and transparent, and that all known current and future risks are identified; recorded; assessed; and their negative impacts appropriately mitigated and managed in line with the organisation’s risk appetite.

3.9 Risk management policies typically include a requirement for all parts of an organisation to consider risk appetite in their strategic and operational decision making. They also specify management’s responsibilities for establishing appropriate target parameters for the risks that they manage, and implementing appropriate mitigations to ensure that these are achieved, enabling effective ongoing management of risk across the organisation in line with risk appetite.

3.10 A risk management policy is usually supported by an operational risk management framework that provides detailed guidance to ensure that policy requirements are consistently and effectively applied throughout the organisation.

3.11 Risk appetite should be agreed at a strategic level and recorded in a risk appetite statement that is then approved and reviewed on an ongoing basis.

3.12 Once approved, risk appetite statements should be communicated throughout the organisation to ensure that all strategic and operational decisions made are aligned with organisational risk appetite, with appropriate target risks considered and established to manage negative risk impacts in line with the organisation’s risk appetite.

The Council's approach to risk management and appetite

3.13 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.

3.14 Both the Council's risk appetite statement and risk management policy are reviewed by the Corporate Leadership Team (CLT) and approved annually by the Policy and Sustainability Committee. Definitions supporting the Council's risk appetite are included at Appendix 2.

3.15 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.

3.16 In August 2018, the Corporate Policy and Strategy Committee approved the Council's new risk appetite statement that detailed the Council's risk appetite in relation to ongoing service delivery; infrastructure; compliance; and financial risks. The risk appetite statement was reviewed by the Policy and Sustainability Committee in October 2019 and confirmed as remaining fit for purpose.

The Three Lines Model

3.17 The Council has adopted the Institute of Internal Auditors Three Lines model to support the application of the Council's Enterprise Risk Management Policy and operation of its risk management framework:

3.17.1 first line divisions and directorates are responsible for identifying; assessing; recording; addressing; and escalating risks (where required) associated with decision making and ongoing service delivery.

3.17.2 the second line Corporate Risk Management team is responsible for maintaining the Policy; developing the supporting operational risk management framework; providing ongoing oversight, challenge and assurance in a 'constructive critical friend' capacity; and driving a positive risk culture through delivery of ongoing training and engagement across first line teams.

3.17.3 independent assurance on the design and effective application of risk management policies and frameworks is provided by Internal Audit.

4. Main report

The Council's Risk Appetite Statement

4.1 The Council's risk appetite statement is set out at Appendix 1 and outlines the Council's risk appetite range (based on definitions included at Appendix 2) in relation to eleven key strategic and operational risks, with the outcomes as follows:

4.1.1 **Minimum possible to low** - three risk categories were identified (Health and Safety; Regulatory and Legislative Compliance and Governance and Decision Making) where the Council has a minimum possible to low risk appetite range, confirming that these risks are unacceptable; cannot be tolerated; and must be urgently and immediately addressed to prevent them from becoming issues where possible.

4.1.2 **Low to moderate** – five risk categories were identified (Strategic Delivery; Financial and Budget Management; Resilience; Technology and Information; and Reputational) where the Council has a low to moderate risk appetite range, confirming that in some instances (low) mitigating actions should be implemented immediately, or as soon as possible (moderate) to treat the risk and prevent it from becoming an issue, or detect the issue and ensure that it is subsequently addressed.

4.1.3 **Low to high** – the remaining three risk categories (Programme and Project Delivery; Supplier, Contractor and Partnership Management; and Service Delivery) have a low to high risk appetite range, reflecting the significant volume and levels of criticality or programmes and projects; contractual and partnership arrangements and services delivered by the Council.

4.1.4 Whilst some of risks these will be considered acceptable and can be tolerated (high), it is important to ensure that the most significant risks that fall within the low to moderate risk appetite range are identified by directorates and divisions, with appropriate mitigating actions implemented either immediately or as soon as possible to treat these risks and prevent them from becoming issues, or to detect issues retrospectively and ensure that they are addressed.

Covid-19

4.2 As noted at 3.3 above, the unexpected risks associated with unplanned events cannot always be identified in advance, and appropriate mitigating actions implemented, and this was the Council's experience with the March 2020 Covid-19 pandemic.

4.3 As the Council's Covid-19 resilience response was mainly dependent on implementing Scottish Government and Public Health Scotland guidance, it was unable to set an appropriate risk appetite and target risks for the new Covid-19 risks that it faced.

4.4 Instead, the Council established the following three key Covid-19 objectives:

i) to protect the most vulnerable in our City;

ii) to minimise the risks to our colleagues; and,

iii) to continue to provide services in challenging circumstances

4.5 The Council did establish a risk management process to ensure that ongoing Covid-19 risks are identified; assessed; recorded; and managed through the Covid-19 risk management plan, and support achievement of these objectives. Details of this process were shared with this Committee on 23 July 2020.

4.6 Whilst it is acknowledged that Covid-19 risks will continue to impact the Council for the foreseeable future, it is not considered appropriate to set a Covid-19 risk appetite and supporting target risks given the unpredictable nature of the situation.

5. Next Steps

5.1 Once approved by the Committee, the risk appetite statement will be shared and communicated across the Council.

5.2 Directors will (where appropriate) set target risks within their respective divisions and across the services that they deliver. As noted at 3.15 above, target risk is already specified for a number of matters through the Council's established governance frameworks.

6. Financial impact

6.1 There is no direct financial impact arising from this report, however, effective risk management in line with the Council's agreed risk appetite should have a positive impact on Council finances.

7. Stakeholder/Community Impact

7.1 Provision of assurance that the Council considers and specifies appropriate thresholds for the amount and type of planned risk that it is willing to take to support achievement of strategic objectives; ongoing service delivery; and protect its people; citizens; assets; and reputation.

8. Background reading/external references

8.1 Scottish Public Finance Manual

8.2 Institute of Internal Auditors Three Lines Model

9. Appendices

9.1 Appendix 1 – City of Edinburgh Council Risk Appetite Statement

9.2 Appendix 2 – Risk Appetite Definitions

Appendix 1 - City of Edinburgh Council - Risk Appetite Statement

	Risk Appetite Range		
Risk Description	**From**	**To**	**Commentary**
Strategic Delivery	**Low**	**Moderate**	1. The Council has a low to moderate 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 Heads of Service 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.
Financial and Budget Management	**Low**	**Moderate**	1. The Council has a low to moderate 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.

	Risk Appetite Range		
Risk Description	**From**	**To**	**Commentary**
	🟩	🟧	3. Executive Directors and Heads of Service are expected to implement appropriate system based and manual controls to prevent financial errors and detect and resolve them when they occur.
Programme and Project Delivery	**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 and Heads of Service; and Project Managers are expected to design; implement; and maintain appropriate programme and project management and governance controls to manage these risks.
Health and Safety (including public safety)	**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. 2. Executive Directors and Heads of Services are expected to ensure that Health and Safety policies; frameworks; and guidance are consistently and effectively applied, with incidents identified, reported, and immediately addressed.

	Risk Appetite Range		
Risk Description	**From**	**To**	**Commentary**
Resilience	**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 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 Heads of Service 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.
Supplier, Contractor, and Partnership Management	**Low**	**High**	1. The Council has a low to high 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 Heads of Services are expected to ensure that the procurement and contract management frameworks are

	Risk Appetite Range		
Risk Description	**From**	**To**	**Commentary**
	🟩	🟥	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.
Technology and Information	**Low**	**Moderate**	1. The Council has a low to moderate 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. 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. Target 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. 5. The Council is also progressing towards full alignment with the Scottish Government's cyber resilience framework and the UK Government National Cyber Security Centre guidance. 6. Executive Directors and Heads of Service are responsible for ensuring ongoing compliance with technology security protocols and

	Risk Appetite Range		
Risk Description	**From**	**To**	**Commentary**
	🟩	🟧	procedures, including the Council’s protocol for externally hosted ‘cloud’ services.
Governance and Decision Making	**Minimum Possible**	**Low**	1. The Council has a minimum possible to low risk 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.
Service Delivery	**Low**	**High**	1. The Council has a low to high 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 Heads of Service are expected to implement appropriate controls to prevent service delivery gaps, and detect and resolve them when they occur.

	Risk Appetite Range		
Risk Description	**From**	**To**	**Commentary**
Regulatory and Legislative Compliance	**Minimum Possible**	**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 Heads of Service are expected to implement appropriate controls to ensure ongoing compliance, and identify; report; and resolve breaches when they occur.
Reputational	**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 Heads of Service are expected to implement appropriate controls to prevent significant or systemic reputational damage, and identify and address issues when they occur.

Appendix 2 – Risk Appetite Definitions

Risk Appetite Description	Definition
Minimum Possible	The level of risk is completely unacceptable and will not be tolerated. Appropriate mitigating actions should be implemented urgently to ensure that the risk is treated to the fullest extent possible, with the objective of preventing the risk from becoming an issue.
Low	The level of risk is unacceptable and will not be tolerated. Appropriate mitigating actions should be implemented immediately to treat the risk and prevent it from becoming an issue where possible.
Moderate	A moderate level of risk can be accepted. Appropriate mitigating actions should be implemented as soon as possible to either prevent the risk from becoming an issue, or detect the issue and ensure that it is addressed.
High	A high level of risk can be accepted. Appropriate actions should be implemented to identify issues resulting from these risks and address them where feasible and practical.