

# Glasgow City Council Internal Audit Section

## Committee Summary

### Corporate Review – Risk Management Compliance

Item 4(g)  
21st May 2025

1

## 1 Introduction

- 1.1 As part of the agreed Internal Audit Plan, we have carried out a review of compliance with the Council's Risk Management and Policy Framework.
  - Accountability for risks by risk owners, and.
  - Review of a sample of risks and mitigating actions.
- 1.2 In order to manage risk within the Council, a Risk Management and Policy Framework is in place to provide guidance to staff with risk management responsibilities on the completion and review of Risk Registers.
- 1.3 A robust risk management framework is a fundamental component of effective corporate governance within an organisation. This includes the processes in place for identifying, assessing, managing, reporting and controlling risks.
- 1.4 The purpose of the audit was to gain assurance that the risk management arrangements in place are fit for purpose and are operating effectively. The scope of the audit included:
  - Ownership of risks;
  - Risk acceptance arrangements;
  - Identification and evaluation of risk;
  - Procedures for the recording and reporting of risk;
  - Ongoing monitoring and assessment of risk and the associated controls;

## 2 Audit Opinion

- 2.1 Based on the audit work carried out, a **reasonable** level of assurance was obtained on compliance with the current framework however a limited level of assurance can be placed upon the Risk Management and Policy Framework due to the updates required. The audit has identified scope for improvement in the existing arrangements with **two** recommendations which management should address.

## 3 Main Findings

- 3.1 Some of the key controls are in place and generally operating effectively. The Council's approach to Risk Management is documented within the Risk Management and Policy Framework (RMPF) which was developed in line with best practice principles. The Policy is currently being reviewed and is expected to be updated to include the Council's revised approach to risk tolerance, risk appetite and risk acceptance. It is expected that the revised Policy will be finalised by December 2025 and rolled out to staff thereafter.
- 3.2 Each Service has a dedicated Risk Management Champion and suitable arrangements for identifying new and developing risk are in place. All risks listed within the Services' Risk Registers have been assessed for likelihood / impact as well as inherent and residual risk.
- 3.3 We reviewed a sample of 20 risks from across the Services. The likelihood / impact scoring allocated for each risk was in line with the guidance available, and the overall risk scores were accurately calculated. The risk approach taken for each risk is clearly stated within the Risk Register and each risk sampled was treated in line with the Risk Management and Policy Framework. Within each Service, Risk Registers are adequately monitored and suitable reporting takes place. The Corporate Risk Register is appropriately maintained and reported on a bi-annual basis to the Corporate Management Team and Finance and Audit Scrutiny Committee.
- 3.4 As part of the sample of 20 risks from across the Services, we were able to verify that risk mitigating actions have been recorded within the Risk Register against each risk and these actions are reasonable and appropriate. For each risk in the sample, appropriate Risk Owners / Responsible Officers have been allocated.
- 3.5 We also selected a sample of three risks from the Risk Register for each service (15 risks in total) in order to verify that the stated mitigating actions were performed as expected. From the sample of 15 risks, we were able to verify that the stated mitigating actions were in place for all of the risks sampled.
- 3.6 However, we noted that there are some areas where controls could be strengthened. We reviewed the full Risk Registers

for each Service and found 22 instances where minor details such as the risk and its alignment to the Strategic Plan were not recorded on the Risk Register.

- 3.7 Each risk has a risk treatment approach recorded in the Risk Register. The treatment approach indicates how the Service intends to manage the risk and there are four options – (1) tolerate, (2) treat, (3) transfer or (4) terminate. In order to effectively treat a risk, there should be future mitigating action(s) to be taken and these should be recorded in an action plan. If no further mitigating action is to be taken the risk treatment approach should be changed to tolerate. From the sample of risks reviewed, 13 risks were listed with the “treat” risk approach and there was no active action plan in place for 11 of these risks
- 3.8 An action plan is provided at section four outlining our observations, risk and recommendation. We have made two recommendations for improvement. The priority of the recommendations are:

Priority	Definition	Total
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	1
Medium	Less critically important controls absent, not being operated as designed or could be improved.	0
Low	Lower level controls absent, not being operated as designed or could be improved.	1
Service Improvement	Opportunities for business improvement and/or efficiencies have been identified.	0

- 3.9 The audit has been undertaken in accordance with the Public Sector Internal Audit Standards.
- 3.10 We would like to thank officers involved in this audit for their cooperation and assistance.
- 3.11 It is recommended that the Head of Audit and Inspection submits a further report to Committee on the implementation of the actions contained in the attached Action Plan.

## 4 Action Plan

No.	Observation and Risk	Recommendation	Priority	Management Response
<b>Key Control:</b> Service Risk Register are fully complete.				
1	<p>We reviewed the full Risk Registers for each Service and found 22 instances where minor details such as the risks' alignment to the Strategic Plan or where the Related Objective field were not completed on the Risk Register.</p> <p>Chief Executive's - two risks on the register where minor expected fields were not complete.</p> <p>Education - one risk on the register where a minor expected field was not complete.</p> <p>Financial Services - four risks on the register where minor expected fields were not complete.</p> <p>Health and Social Care Partnership - 15 risks on the register where minor expected fields had not been completed.</p> <p>Without consistent completion of all fields within the Risk Register there is an increased risk that risk management actions in place do not align with the Council's strategic objectives.</p>	Each Service should review the Service Risk Register and ensure that all fields are fully completed.	Low	<p><b>Response:</b></p> <p>Chief Executive's - Accepted. CED reviews its risk register quarterly and will ensure any specific issues with fields not being complete are resolved through the March 2025 review.</p> <p>Education – Accepted. This omission was corrected within the next quarterly update of the risk register.</p> <p>Financial Services – Accepted. FS Governance will review FS risk register to ensure fields are fully complete by the appropriate FS managers.</p> <p>Health and Social Care Partnership – Accepted. All risks with missing minor expected fields will be reviewed and updated during the current quarterly review (Q4, 2024/25)</p>

No.	Observation and Risk	Recommendation	Priority	Management Response
				<p>The HSCP carries out a quarterly review of all risks on Pentana, and checking all fields are completed will be added to this quarterly review process going forward.</p> <p><b>Officer Responsible for Implementation:</b></p> <p>Chief Executive's - Corporate Governance and Planning Manager</p> <p>Education - Head of Resources</p> <p>Financial Services - Head of FS Governance &amp; Change</p> <p>Health and Social Care Partnership - Business Development Manager</p> <p><b>Timescales for Implementation:</b></p> <p>Chief Executive's - 30 April 2025</p> <p>Education – 07 March 2025 - Implemented</p> <p>Financial Services - 30 April 2025</p> <p>Health and Social Care Partnership - 31 March 2025</p>

No.	Observation and Risk	Recommendation	Priority	Management Response
<b>Key Control:</b> Risks which are to be treated are subject to ongoing action.				
2	<p>Each risk has a risk treatment approach. The treatment approach indicates what the intention is for the management of that risk - tolerate, treat, transfer or terminate. Where a risk is marked as treat, then there should be future mitigating action(s) to be taken and these should be recorded in an action plan. Where there are no further mitigating actions to be taken the risk treatment approach should be changed to tolerate. From the sample of risks reviewed, 13 risks were listed with the "treat" risk approach and, although there were mitigations listed, there was no active action plan in place for 11 of these.</p> <p>The current arrangements do not clearly outline how risk treatments are managed for the treat option, or agreed and recorded for tolerate, transfer or terminate. As such it is not clear whether all risks have been correctly categorised and where appropriate risk accepted is authorised at the appropriate level.</p>	<p>The Corporate Risk Manager should, as part of the ongoing review to the RMPF, ensure it is updated to reflect the requirement for Risk Owners to actively manage risks which are to be treated and an appropriate process is in place for accepting risks which are to be tolerated, transferred or terminated.</p> <p>Thereafter all Services should be briefed on the requirements of the updated Policy, either through the Risk Management Forum and / or briefings at Service Leadership team meetings. Any training for risk owners should also be provided following any required updates.</p> <p>The Corporate Risk Manager should continue to monitor compliance with the framework once the revisions have been published.</p>	High	<p><b>Response:</b></p> <p>Accepted. Corporate Risk Manager accepts both the observation and recommendation and reflects the direction of the travel for the management of risk within the organisation. This recommendations links with the ongoing review of the RMPF as noted within the report.</p> <p><b>Officer Responsible for Implementation:</b></p> <p>Corporate Risk Manager (Corporate Governance and Planning Manager)</p> <p><b>Timescales for Implementation:</b></p> <p>31 December 2025</p>