Glasgow City Council Internal Audit Section
Committee Summary
Corporate Review – Strategic Risk Mitigation

Item 3(c)

20th March 2024

1 Introduction

1.1 As part of the agreed Internal Audit plan we have carried out a review of mitigating actions that Council Services have outlined in their risk register, for the management of strategic risks. The purpose of the audit was to verify that the actions documented have been adequately implemented and to assess the effectiveness of these in reducing the levels of risk faced by the Council.

1.2 Internal Audit are in the process of hosting and facilitating risk workshops with Services during 2023/24, focusing on operational risk management. In order to minimise the likelihood of any duplication with this exercise, this audit concentrated solely on the strategic risks that apply to Services and those contained in the Corporate Risk Register.

1.3 Strategic risks differ from operational risks in that they are high level risks which may impact the Council's ability to deliver its key strategic objectives. Strategic risks may arise for a number of reasons e.g. environmental, regulatory or political change etc.

1.4 The Council's approach to risk management is governed by the Risk Management Policy and Framework (RMPF) and each Service is required to maintain a risk register detailing the main risks facing the Service and the control actions to mitigate these risks.

1.5 The RMPF was updated in November 2019 following the introduction of the Pentana Risk system. All Services are required to comply with the framework and all Service risk registers are now stored and maintained via Pentana Risk.

1.6 The scope of the audit included a review of:

- The strategic risks noted on Service and Corporate Risk Registers, ensuring they are recorded, assessed and assigned to risk owners and responsible officers.
- The mitigating actions recorded against a sample of risks ensuring that the implementation of these could be verified.
- The monitoring and reporting arrangements in place, ensuring that Service and Corporate Management are routinely made aware of the risks affecting the Council.

1.7 As part of the audit we reviewed a sample of strategic risks from the Corporate Risk Register and each of the five Service risk registers, i.e.:

- Chief Executive's Department (CEX)
- Education Services (EDU)
- Financial Services (FS)
- Neighbourhoods, Regenerations and Sustainability Services (NRS)

- Social Work Services (SWS)

2 Audit Opinion

2.1 Based on the audit work carried out a reasonable level of assurance can be placed upon the control environment. The audit has identified some scope for improvement in the existing arrangements and five recommendations which management should address.

3 Main Findings

3.1 We are pleased to report that the key controls are in place and generally operating effectively.

3.2 All Services were able to provide a risk register for the quarter requested, with a complete record of all material risks. We confirmed that the registers adopted the format specified in the RMPF.

3.3 We found that all Services had performed assessments to determine the inherent and residual risk score, based on the impact and probability of each risk. We also verified that the total risk scores assigned to each risk had been calculated accurately and had been allocated the appropriate RAG status, per the risk score. The Risk Management System automatically calculates the total risk scores, following user input, therefore enhancing accuracy.

3.4 We found that all Services had applied one of the 4Ts of risk management (tolerate, treat, transfer and terminate) to each of the risks recorded on the risk register and were generally managing the risk in line with the risk treatments applied.

3.5 We verified that mitigating actions for each risk were considered and assessed to determine their appropriateness in managing the likelihood and impact.

3.6 Risk reporting requirements were clearly defined, documented and complied with by all Services. Consistency in reporting to the relevant Leadership teams was enhanced by the application of the Pentana system to generate standardised reports across all Services.

3.7 However, our audit testing found that there are some areas of non-compliance. The Corporate Risk Register was incomplete and not sufficiently updated with risk owners and responsible officers.

3.8 Although inherent and residual scores were recorded in all Service risk registers, we noted some issues in SWS and FS where, in some instances, the residual scores were higher than the inherent scores.

3.9 Although the RMPF provides guidance on risk management, we observed that it had not adequately covered the process

for formally requesting and approving the acceptance of risks that fall outside the Council's normal risk tolerance level or that are outwith management control.

3.10 We identified that one mitigating action, recorded against one of the SWS risks sampled, was not being implemented as described. We were also not provided with the necessary evidence in support of the mitigating actions for one risk listed on the Corporate Risk Register. We were therefore unable to verify that the risk was being managed as specified in the register.

3.11 Through review of the Service risk registers we identified elements of non-compliance that were not identified by Service management or the corporate risk function as part of their monitoring processes.

3.12 We observed two risks in SWS, one risk in FS and two risks in CEX where the recorded risk treatment did not accurately reflect the current management of the risk.

3.13 In EDU, we found that risks were not reported to the Senior Management Team (SMT) for review in line with the documented frequency.

3.14 An action plan is provided at section four outlining our observations, risks and recommendations. We have made five recommendations for improvement. The priority of each recommendation is:

Priority	Definition	Total
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	0
Medium	Less critically important controls absent, not being operated as designed or could be improved.	5
Low	Lower level controls absent, not being operated as designed or could be improved.	0
Service Improvement	Opportunities for business improvement and/or efficiencies have been identified.	0

3.15 The audit has been undertaken in accordance with the Public Sector Internal Audit Standards.

3.16 We would like to thank officers involved in this audit for their cooperation and assistance.

3.17 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
Key Control: Risk Registers are up to date and sufficiently detailed.				
1	The RMPF underpins the Council's risk management approach and outlines the format that Service risk registers should adopt. This includes completing all of the relevant fields as specified in the RMPF. However we observed that the recorded risk owner for one risk and both the risk owner and responsible officer for three risks were not up to date on the Corporate Risk Register within Pentana (the Council's Risk Management System). From our sample of 3 risks in each Service we found one instance in both FS and SWS where the residual score was higher than the inherent score. Although we identified these discrepancies, they were not detected as part of the ongoing monitoring arrangements in place. There is increased risk that risks are not adequately managed.	The Corporate Risk Manager should ensure that responsible officers and risk owners are assigned for each of the documented risks on the Corporate Risk Register. SWS and FS Management should conduct a review of the Service Risk Register and ensure that any discrepancies in the inherent and residual risk scores are addressed. Both the Senior Management Teams in each Service, along with Service Risk Champions should ensure that adequate checks are performed each period and that instances of non-compliance are brought to the attention of the relevant risk owners and remediated.	**Medium**	**Response:** Corporate Risk Register – The information for each risk was correct at the time of reporting to CMT and FASC in line with RMPF reporting cycle. The findings noted have now all been corrected. SWS: Inherent and Residual risk scores for all risks will be reviewed with risk owners at next quarterly review and any discrepancies resolved. Confirmation of inherent scores will be in included in all future quarterly reviews. FS – Service Risk Register to be reviewed. **Officer Responsible for Implementation:** Corporate Risk Register – Corporate Governance and Planning Manager

No.	Observation and Risk	Recommendation	Priority	Management Response
				SWS – HSCP Resilience Manager (Service Risk Management Champion) FS – Head of FS Governance and Change **Timescales for Implementation:** Corporate Risk Register – 29 February 2024 (Complete) SWS – 31 May 2024 FS – 30 April 2024

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: The authority to accept risk has been clearly defined and documented.				
2	We found that, whilst there is an understanding that risks can be tolerated where they have been assessed as falling below the Council's risk tolerance score of 10, there is currently no mechanism in place for formally accepting risks that are being tolerated and are scored 10 or above. For example, we identified one instance in EDU and another in SWS where risks of 10 or more were being tolerated although there was no formal risk acceptance from the SMT. There is therefore an increase likelihood that significant risks are not being appropriately managed.	The Corporate Risk Manager should, as part of its scheduled review in 2024/25, update the RMPF so that a more active approach is taken in relation to risk tolerance and appetite and that, where appropriate, risks can be accepted with proper authority. The Corporate Risk Manager should thereafter notify Services of any revised approaches within the updated RMPF and support their compliance.	**Medium**	**Response:** Accepted. The regular review of the Corporate Risk Management Policy and Framework provides an opportunity for refinement processes and amendments to be made reflecting the organisation's approach to risk management. **Officer Responsible for Implementation:** Corporate Governance and Planning Manager **Timescales for Implementation:** 31 December 2024

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Actions have been identified and implemented to mitigate the identified risks.				
3	Although a mitigating action in SWS was recorded against one of the risks, we found that this was not currently implemented and therefore was not actively controlling the risk. The action related to contacting services users affected by the removal of analogue telephone services, however we found that this was not taking place. During our review of the Corporate Risk Register we could not obtain assurance that one risk was being treated as sufficient evidence was not provided. This risk related to the protection and governance of information assets and is owned by the Head of Information and Data Protection Officer. If the mitigating actions are not implemented as described there is an increased likelihood that the risk is not being adequately addressed.	a) SWS management should review the mitigating actions listed against each risk and verify that they are being implemented as described or removed as necessary. b) The Head of Information and Data Protection Officer should verify that the mitigating actions outlined for the risk noted are being implemented as described. c) The Corporate Risk Manager should also consider implementing periodic spot checks of the mitigating actions on the Corporate Risk Register, to routinely verify that the recorded actions are being fulfilled.	**Medium**	**Response:** A – All SWS risks are reviewed quarterly by risk owners, which includes confirmation that risk controls are up to date. This will continue at next and future reviews. The missing mitigating action identified by the audit will be removed and the risk owner requested to comprehensively update control actions as part of next quarterly review. B – Accepted C – Corporate Risk Register. Accepted. At present spot checks are routinely made within the corporate risk register, for content and fields being completed. A process similar to, if not included within the Risk of the Quarter process will be produced to allow mitigations to be evidenced and monitored by the Risk Management Forum

No.	Observation and Risk	Recommendation	Priority	Management Response
				Officer Responsible for Implementation: A – HSCP Resilience Manager (Service Risk Management Champion) B – Head of Information and Data Protection Officer C – Corporate Governance and Planning Manager **Timescales for Implementation:** A – 31 May 2024 B – 30 April 2024 C – 30 November 2024

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: The risk treatment approach is appropriate to the risk.				
4	We found instances where the recorded risk treatment in the Service Risk Register did not align with the actual treatment of the risk. From the sample of 3 risks per Service we found: • Two instances in CEX, one in FS and one in SWS where all mitigations had been implemented as outlined (and no further actions were planned), however the risk was recorded as being treated rather than tolerated. It should be noted that for the SWS instance, the residual risk score after treatment is higher than the Council's risk tolerance level and it may not be possible, therefore, to tolerate the risk. • One instance in SWS where the risk was recorded as being tolerated but actions were still ongoing to mitigate the risk, which suggests that the action is actually being treated. There is therefore an increased likelihood that risks are not being managed in a manner that reflects their recorded risk treatment, which could result in appropriate management decisions not being made.	The Service Risks Managers in CEX, FS and SWS should review the risk treatment recorded against each risk and assess whether this is an accurate reflection of the current management of the risk. For example, if all documented mitigations have been implemented and the Service are content that no further mitigation or escalation is required, then the risk treatment should be updated to reflect this (i.e. changed from treat to tolerate). Where the risk treatment is recorded as tolerate and the residual score remains high or very high, Risk Owners should ensure that risks are monitored by SMT and/or CMT for consideration and recording, in line with section 5.2.3 of the RMPF.	**Medium**	**Response:** FS – Service risk register to be reviewed in line with recommendation. CEX – Accepted. Risks treatment will be reviewed for all risks within SRR – for next review period. SWS – Risk Treatments on all SWS risks will be reviewed and, where appropriate, in agreement with risk owner and in line with current Risk Management Framework, amended accordingly. **Officer Responsible for Implementation:** FS – Head of FS Governance and Change CEX – Corporate Governance and Planning Manager SWS – HSCP Resilience Manager (Service Risk Management Champion)

No.	Observation and Risk	Recommendation	Priority	Management Response
				Timescales for Implementation: FS – 30 April 2024 CEX – 31 May 2024 SWS – 31 May 2024

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Risk Registers are reported to the relevant governance forums at the required frequency.				
5	The RMPF documents the requirement for Services to submit their Risk Registers for formal review on a quarterly basis to the SMT. We noted that in EDU, risks were not reported to the SMT for review in line with the documented frequency. If service risk registers are not regularly report to the SMT, there is an increased risk that the risks and corresponding mitigating actions are not subject to appropriate scrutiny.	EDU Management should ensure that the Service Risk Register is formally reviewed by the SMT at the required frequency as outlined in the RMPF.	**Medium**	**Response: Accepted** This arose as some quarterly reviews were scheduled during school holiday periods when Directorate meetings are less frequent. The Education quarterly risk register review schedule has been amended to ensure formal review dates are scheduled to meet quarterly reporting requirements. **Officer Responsible for Implementation:** Support Services Manager **Timescales for Implementation:** 31 March 2024