Item 4(d)

21st May 2025

Glasgow City Council Internal Audit Section
Committee Summary
Financial Services – SAP ERP Roles and Permissions

1 Introduction

1.1 As part of the agreed Internal Audit Plan, we have carried out a review of the roles and permissions of those staff with access to the Council's Enterprise Resource Planning (ERP) system, SAP.

1.2 The SAP system is used by the Council to manage its main business processes including the financial ledger, payroll and human resources.

1.3 SAP Governance, Risk and Compliance (GRC) is a suite of tools that enables the monitoring of SAP user accounts, risks, and usage. SAP GRC has been introduced by the Council in three phases and the project is now complete.

1.4 The final phase comprised reviewing the roles and permissions currently within SAP to rationalise these, ensuring that access is based on need, is justified and allocated to staff based on the corporate matrix which should now be used by any new user to obtain appropriate SAP access permissions.

1.5 The purpose of the audit was to gain assurance that the Council has arrangements in place to ensure staff have access to the ERP system based on need and commensurate with their role. The scope of the audit included a review of the key controls in the following areas:

- Roles and responsibilities;
- Monitoring and control of segregation of duties conflicts (where staff members may have access to two or more system features that conflict, offering an opportunity for fraud);
- Movers and leavers, and
- Monitoring and control of privileged user accounts.

1.6 This audit examined the arrangements in place within the current ERP system. A new ERP system has recently been procured, with detailed project work ongoing to plan for its implementation by December 2027. Lessons learned from this review will help to inform the implementation of roles and permissions within the new system.

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 two recommendations which management should address.

3 Main Findings

3.1 The GRC Project Board was established to support the introduction of SAP GRC and consisted of senior officers across Financial Services. The Board compiled guidance and procedures for granting SAP access including devising a role matrix to ensure system access is based on the role in question (however as noted below the Board no longer actively meets).

3.2 Each Service has a dedicated representative responsible for authorising SAP access. A sample of eight new user applications was selected and we confirmed that access was based on need appropriate to the role in question. A suite of information is extracted from the GRC module and sent to business process owners in order for the requested SAP roles and subsequent risks identified, to be reviewed.

3.3 Certain users are sometimes granted "super user" status for a period in order that they can cover any system emergencies. This is known as fire fighter status. This access was found to be appropriately monitored, controlled and authorised.

3.4 However, we noted that there are some areas where controls could be strengthened.

3.5 We found that the guidance documentation for amending SAP access was out of date and referred to the previous IT supplier ACCESS LLP. Additionally, the appointed authoriser for one ALEO was found to be incorrect, with the senior officer involved having changed roles however the SAP user access form had not been updated to reflect this.

3.6 Regular user reviews are not currently being undertaken. We identified that there were 3 duplicate user IDs on the list for current employees and 10 staff who had left GCC still had a SAP user ID listed against their name. We noted that permissions are automatically removed after 30 days without activity and this had been applied to the 13 staff referred to above, however the last full user access review took place in 2021.

3.7 Although the number of segregation of duties conflicts has decreased following the implementation of GRC, there were still a high number of conflicts identified by the GRC module across the Council as of February 2025 (with almost half of these conflicts classified as high). The conflicts are built into

the SAP GRC system which classifies them as high, medium or low risk. Segregation of duties conflicts arise when one user has access to two corresponding transactions. We have been advised that the high number of conflicts is due to the levels of staff cover required across the Council for business continuity purposes and that there are currently no plans to bring this level down further. While the reasons for this approach are understandable, we noted that there has been no formal risk acceptance of the remaining level of risk.

3.8 Additionally, a list of the top 25 high risk users is identified as part of each GRC executive report but there is no guidance regarding what action should be taken in relation to this. The GRC Project Board no longer regularly meet to discuss the report and there is potential for key segregation of duties issues to be missed.

3.9 An action plan is provided at section four outlining our observations, risks, and recommendations. We have made two recommendations for improvement. Whilst these recommendations relate to the existing SAP system they should be considered as part of the transition to Oracle. 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.	2
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.	0
Service Improvement	Opportunities for business improvement and/or efficiencies have been identified.	0

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

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

3.12 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: SAP usage is appropriately monitored and GRC outputs are used effectively.				
1.	Although the total number of segregation of duties conflicts has significantly reduced since SAP GRC was introduced, a high number of segregation of duties conflicts still exist. If there is a change of more than 5% in the number of conflicts, this is highlighted in the GRC Executive Report along with the top 25 high risk users. The GRC Project Board no longer meet, and board members are kept informed of issues and changes by distribution of the GRC executive report. However, we identified that no reports were shared between September 2024 and February 2025. Whilst it is likely that due to the finite staff/resources available the number of conflicts will never reduce to zero, there is no formal approach in place to review and potentially tolerate/mitigate the residual risks. There is therefore an increased risk that the GRC information produced is not being used effectively to manage the risk	Management should review the arrangements for addressing the reported segregation of duties conflicts. This should include implementing a formal risk management approach which considers how risks should be mitigated/tolerated.	**High**	**Response:** Accepted The GRC paperwork will be sent to the appropriate officers every two months with any increase in conflicts over 5% required to be investigated. A risk report will be added to the paperwork and a formal risk acceptance progressed regarding the remaining baseline level of segregation of duties issues identified. **Officer Responsible for Implementation:** Business Manger **Timescales for Implementation:** 30th July 2025

No.	Observation and Risk	Recommendation	Priority	Management Response
	of fraud or error by staff having inappropriate access to certain transactions in the Council's ERP system.			

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: SAP administration processes are up to date and help to ensure that access is managed effectively.				
2.	Although no inappropriate SAP access or use was identified, the audit found three areas for improvement in the administration of SAP access. The guidance for making changes to SAP accounts on the Council's intranet requires to be updated as this refers to a previous IT supplier. The SAP authorisations list requires to be reviewed and updated, as we identified one staff member listed who has changed Service area. Additionally, the SAP user list should be reviewed as our sampling work determined four users who had duplicate IDs registered against their names and a further seven users who had left GCC within the last year but still had a SAP ID. The last documented full user access review took place in 2021. Without effective user access management there is an increased risk of staff retaining inappropriate access, access not being obtained or approved correctly, or licences not being used efficiently.	Management should introduce regular user access reviews for the SAP ERP system. Additionally, management should ensure that the guidance for making changes to SAP accounts and the approved authorisers are up to date.	**High**	**Response:** Accepted User reviews (location and manager changes) will be issued to managers every 8 weeks for review. User with position changes will have SAP roles removed by CGI. Users (leavers) will be picked up in the existing exit monitoring process. The guidance and documentation will be reviewed and updated. **Officer Responsible for Implementation:** Business Manger **Timescales for Implementation:** 30th June 2025